



# KRIPTOGRAFI *LIGHTWEIGHT* VERSI 1.0

Deputi Bidang Strategi dan Kebijakan Keamanan Siber dan Sandi  
Badan Siber dan Sandi Negara

2025

# **KRIPTOGRAFI *LIGHTWEIGHT***

## **VERSI 1.0**



Direktorat Kebijakan Teknologi Keamanan Siber dan Sandi  
Badan Siber dan Sandi Negara (BSSN)  
Jl. Cijayanti No. 70, Kec. Babakan Madang, Kabupaten Bogor  
Website : <https://www.bssn.go.id>  
Email : [humas@bssn.go.id](mailto:humas@bssn.go.id)

## **TIM PERUMUS**

Pengarah : Tjahjo Khurniawan

Penanggung Jawab : Soetedjo Joewono

Pereviu : Muhammad Arief, MSEE, M.Sc (BRIN)

Tim Penyusun :

1. Sari Agustini Hafman
2. Adang Rochiyat
3. Anjariah Dwi Astuti
4. Oky Jati Permana
5. Andreas Lugas

Penyunting :

1. Sari Agustini Hafman
2. Oky Jati Permana
3. Andreas Lugas



## PENGANTAR

Puji syukur kita panjatkan ke hadirat Tuhan Yang Maha Esa atas limpahan rahmat dan karunia-Nya sehingga dokumen *Kriptografi Lightweight Versi 1.0* ini dapat diselesaikan dengan baik. Penyusunan dokumen ini merupakan wujud komitmen Badan Siber dan Sandi Negara (BSSN) dalam memperkuat keamanan informasi nasional di tengah perkembangan ekosistem digital yang semakin kompleks.

Pada era digital saat ini, ruang siber semakin terintegrasi dengan berbagai perangkat berdaya rendah seperti *Internet of Things* (IoT), RFID, kartu pintar, dan sistem tertanam. Perluasan perangkat tersebut menghadirkan tantangan baru karena keterbatasan sumber daya komputasi menuntut mekanisme kriptografi yang lebih efisien tanpa mengurangi tingkat keamanan. Dalam konteks tersebut, kriptografi *lightweight* menjadi komponen penting untuk memastikan keamanan data dan komunikasi pada perangkat yang memiliki keterbatasan memori, daya, maupun performa.

Di sisi lain, dinamika ancaman siber nasional dan global menunjukkan bahwa keamanan informasi tidak hanya berkaitan dengan pelindungan data pribadi dan informasi strategis, tetapi juga menjadi elemen penting dalam menjaga stabilitas ekosistem digital dan kedaulatan ruang siber Indonesia. BSSN sebagai garda terdepan dalam menghadapi ancaman siber terus memperkuat strategi, regulasi, serta kebijakan keamanan informasi yang



adaptif dan responsif terhadap perkembangan teknologi dan pola ancaman yang semakin kompleks.

Dokumen *Kriptografi Lightweight Versi 1.0* ini disusun untuk memberikan landasan strategis dan teknis bagi para pembuat kebijakan, praktisi keamanan siber dan sandi, penyelenggara layanan keamanan informasi, serta pengembang perangkat yang beroperasi dengan keterbatasan sumber daya. Dokumen ini memuat penjelasan menyeluruh mengenai prinsip-prinsip kriptografi *lightweight* yang merujuk pada standar internasional, termasuk ISO/IEC 29192 dan rekomendasi NIST, serta kajian terhadap berbagai algoritma yang relevan seperti ChaCha20, PRESENT, LEA, dan SPONGENT. Dengan demikian, dokumen ini diharapkan menjadi pedoman yang kredibel dan aplikatif dalam memastikan penerapan mekanisme kriptografi yang efisien tetapi tetap aman pada perangkat berdaya rendah.

Kami berharap dokumen ini dapat menjadi referensi nasional dalam memperkuat keamanan perangkat berdaya rendah, meningkatkan ketahanan infrastruktur digital, dan menjaga integritas ruang siber Indonesia. Selain itu, dokumen ini diharapkan dapat membantu seluruh pemangku kepentingan dalam membangun ekosistem keamanan informasi yang tangguh, efisien, dan berkelanjutan, sehingga mendukung terwujudnya transformasi digital Indonesia yang berdaulat, tepercaya, dan berorientasi pada masa depan.

Drs. Nugroho Sulistyo Budi, M.M., M.Han.  
Kepala Badan Siber dan Sandi Negara  
Desember 2025

## PENGANTAR DEPUTI I



Puji syukur kita panjatkan ke hadirat Tuhan Yang Maha Esa atas tersusunnya Dokumen *Kriptografi Lightweight Versi 1.0* ini sebagai wujud komitmen BSSN dalam memperkuat keamanan informasi nasional.

Perkembangan ekosistem digital yang semakin luas dan melibatkan berbagai perangkat dengan sumber daya terbatas, seperti *Internet of Things* (IoT), RFID, kartu pintar, dan sistem tertanam, menuntut penerapan mekanisme kriptografi yang efisien tanpa mengurangi tingkat keamanan. Dokumen ini disusun sebagai rujukan terkait kriptografi *lightweight* dengan mengacu pada standar nasional dan internasional, serta memuat kajian terhadap berbagai algoritma kriptografi *lightweight* seperti ChaCha20, PRESENT, LEA, dan SPONGENT.

Dokumen ini diharapkan menjadi rujukan bagi pembuat kebijakan, praktisi keamanan siber dan sandi, serta penyedia layanan keamanan informasi dalam memahami kriptografi *lightweight* secara tepat, efektif dan sesuai standar. Dengan dokumen ini, BSSN berkomitmen mendukung pengembangan infrastruktur digital nasional yang aman, efisien, dan berkelanjutan.

Akhir kata, saya menyampaikan apresiasi kepada seluruh tim penyusun dan pihak yang telah berkontribusi dalam penyusunan dokumen ini. Semoga dokumen *Kriptografi Lightweight Versi 1.0* ini dapat menjadi salah satu referensi dalam mendukung terwujudnya transformasi digital Indonesia yang berdaulat dan berkeamanan tinggi.

Tjahjo Khurniawan

Deputi Bidang Strategi dan Kebijakan Keamanan Siber dan Sandi

Desember 2025

## RINGKASAN EKSEKUTIF

Kriptografi merupakan fondasi utama dalam menjaga kerahasiaan, integritas, dan autentikasi informasi sejak ribuan tahun lalu. Dari hieroglif Mesir Kuno hingga pengembangan standar modern seperti DES, RSA, dan AES, teknologi kriptografi terus berevolusi untuk menjawab tantangan keamanan informasi di setiap era. Namun, munculnya perangkat *Internet of Things* (IoT), *Radio Frequency Identification* (RFID), kartu pintar, dan sistem tertanam menghadirkan tantangan baru diantaranya keterbatasan daya, memori, kapasitas pemrosesan, dan *bandwidth* komunikasi. Algoritma kriptografi modern yang kuat sering kali tidak dapat diimplementasikan secara efisien pada perangkat-perangkat tersebut.

Untuk menjawab kebutuhan ini, kriptografi *lightweight* hadir sebagai solusi yang menawarkan perlindungan keamanan dengan efisiensi tinggi. Dirancang khusus untuk lingkungan dengan sumber daya terbatas, kriptografi *lightweight* menyeimbangkan kebutuhan keamanan, kinerja, dan konsumsi energi. Teknologi ini sangat penting untuk memastikan keamanan data pada infrastruktur digital masa depan.

Dokumen Kriptografi *Lightweight* yang disusun Badan Siber dan Sandi Negara (BSSN) ini bertujuan untuk memberikan pemahaman komprehensif tentang konsep, kebutuhan, implementasi, dan daftar algoritma kriptografi *lightweight* yang sesuai dengan standar nasional dan internasional, termasuk ISO/IEC 29192, SNI ISO/IEC 18033, serta rekomendasi dari CRYPTREC dan eSTREAM. Selain memberikan landasan teoretis, dokumen ini juga memuat contoh algoritma, analisis keamanan, karakteristik performa perangkat keras dan perangkat lunak, serta lampiran implementasi dalam beberapa bahasa pemrograman.

Dokumen ini ditujukan bagi pemangku kepentingan di bidang keamanan siber dan sandi mulai dari pembuat kebijakan teknis, praktisi keamanan siber dan sandi, hingga penyedia layanan keamanan yang membutuhkan

acuan untuk memilih dan menerapkan algoritma kriptografi *lightweight* dalam sistem elektronik. Dokumen ini juga memperkuat pentingnya penerapan mekanisme yang memenuhi tingkat keamanan minimal 80–112 bit serta mematuhi berbagai persyaratan implementasi seperti luas area chip, konsumsi energi, ukuran kode program, penggunaan RAM, dan ketahanan terhadap serangan *side-channel*.

Dengan disusunnya dokumen ini, diharapkan seluruh pihak memiliki acuan yang konsisten, interoperabel, dan sesuai praktik internasional dalam menerapkan kriptografi *lightweight*. Penerapan teknologi ini tidak hanya meningkatkan keamanan perangkat dengan sumber daya terbatas, tetapi juga mendukung upaya nasional dalam membangun ekosistem keamanan siber yang kuat, adaptif, dan berkelanjutan di era digital yang semakin terhubung.

Apabila pembaca menemukan keraguan dalam dokumen ini, maka disarankan untuk melihat referensi asli yang terdapat pada daftar referensi.



## DAFTAR ISI

|                                                                                          |      |
|------------------------------------------------------------------------------------------|------|
| <b>PENGANTAR</b> .....                                                                   | iii  |
| <b>PENGANTAR DEPUTI I</b> .....                                                          | v    |
| <b>RINGKASAN EKSEKUTIF</b> .....                                                         | vi   |
| <b>DAFTAR ISI</b> .....                                                                  | viii |
| <b>DAFTAR GAMBAR</b> .....                                                               | ix   |
| <b>DAFTAR ISTILAH</b> .....                                                              | x    |
| <b>BAB I PENDAHULUAN</b> .....                                                           | 1    |
| A. Ruang Lingkup.....                                                                    | 2    |
| B. Target Audiens.....                                                                   | 4    |
| C. Rujukan.....                                                                          | 4    |
| D. Sistematika Penyusunan Dokumen.....                                                   | 5    |
| <b>BAB II PENGANTAR DAN KONSEP DASAR</b> .....                                           | 7    |
| A. <i>Lightweight Stream Cipher</i> .....                                                | 13   |
| B. <i>Lightweight Block Cipher</i> .....                                                 | 17   |
| C. <i>Lightweight Fungsi hash</i> .....                                                  | 24   |
| <b>BAB III CONTOH ALGORITMA KRIPTOGRAFI <i>LIGHTWEIGHT</i></b> .....                     | 32   |
| A. <i>Lightweight Stream Cipher</i> .....                                                | 33   |
| B. <i>Lightweight Block Cipher</i> .....                                                 | 43   |
| C. <i>Lightweight Fungsi Hash</i> .....                                                  | 67   |
| <b>BAB IV PENUTUP</b> .....                                                              | 90   |
| <b>LAMPIRAN</b> .....                                                                    | 93   |
| <b>CONTOH IMPLEMENTASI KRIPTOGRAFI <i>LIGHTWEIGHT</i> DALAM BAHASA PEMROGRAMAN</b> ..... | 93   |
| A. Implementasi SPECK 64 dan SPECK 128.....                                              | 93   |
| B. Implementasi PRESENT.....                                                             | 97   |
| C. Implementasi SIMON 64 dan SIMON 128.....                                              | 112  |
| D. Implementasi ChaCha 20.....                                                           | 116  |
| E. Implementasi SPONGENT.....                                                            | 120  |
| <b>REFERENSI</b> .....                                                                   | 124  |

## DAFTAR GAMBAR

|                                                  |    |
|--------------------------------------------------|----|
| Gambar 2.1 Fungsi keluaran binary-additive. .... | 16 |
| Gambar 2.2 Algoritma PRESENT .....               | 20 |
| Gambar 2.3 F-function .....                      | 21 |
| Gambar 2.4 Algoritma CLEFIA.....                 | 23 |
| Gambar 2.5 Algoritma LEA .....                   | 24 |
| Gambar 2.6 Konstruksi Sponge.....                | 27 |
| Gambar 2.7 Konstruksi Merkle-Damgard .....       | 28 |
| Gambar 2.8 Fungsi kompresi Davies Meyer .....    | 29 |



## DAFTAR ISTILAH

|                                   |                                                                                                                                                            |
|-----------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <i>Area (#GE)</i>                 | : Ukuran luas permukaan silikon yang digunakan oleh gerbang logika dan interkoneksi dalam sebuah sirkuit digital.                                          |
| <i>Circuit Size</i>               | : Ukuran sirkuit dalam implementasi perangkat keras berhubungan langsung dengan biaya. Ukuran sirkuit ini juga dikenal sebagai metrik untuk konsumsi daya. |
| <i>Cycle / Byte</i>               | : Jumlah siklus prosesor yang dibutuhkan untuk mengenkripsi satu blok atau satu byte data.                                                                 |
| <i>Digest size</i>                | : String bit yang merupakan keluaran dari fungsi <i>hash</i> .                                                                                             |
| <i>Energy</i>                     | : Daya atau tenaga listrik yang digunakan untuk mengoperasikan perangkat elektronik.                                                                       |
| <i>High-End CPU</i>               | : CPU kelas atas digunakan untuk membedakan platform implementasi cipher ringan dan berat.                                                                 |
| <i>Initialization Vector (IV)</i> | : Nilai yang digunakan dalam mendefinisikan titik awal dari suatu fungsi <i>hash</i> .                                                                     |
| <i>Latency</i>                    | : Waktu yang dibutuhkan untuk satu proses enkripsi (atau dekripsi).                                                                                        |
| <i>Low-End CPU</i>                | : CPU kelas bawah digunakan untuk membedakan platform implementasi cipher ringan dan berat.                                                                |
| <i>Memori</i>                     | : Jumlah ruang penyimpanan yang dibutuhkan untuk menyimpan data sementara atau permanen.                                                                   |
| <i>Platform</i>                   | : Sistem target (CPU, microcontroller, FPGA, dll.).                                                                                                        |
| <i>Padding</i>                    | : Menambahkan bit ekstra ke suatu string data.                                                                                                             |
| <i>Power Consumption</i>          | : Jumlah energi listrik yang digunakan oleh perangkat selama beroperasi.                                                                                   |
| <i>RAM</i>                        | : Jenis memori komputer yang digunakan untuk menyimpan data sementara.                                                                                     |
| <i>Bit Rate</i>                   | : Jumlah bit keluaran per siklus waktu.                                                                                                                    |

- ROM : Jenis memori yang berisi data permanen dan tidak dapat diubah setelah diprogram.
- Round* : Satu iterasi dari serangkaian transformasi dalam *cipher* (seperti substitusi, permutasi, dan penambahan kunci) yang diulang berkali-kali untuk meningkatkan keamanan.
- Throughput* : Jumlah bit diproses per satuan waktu.



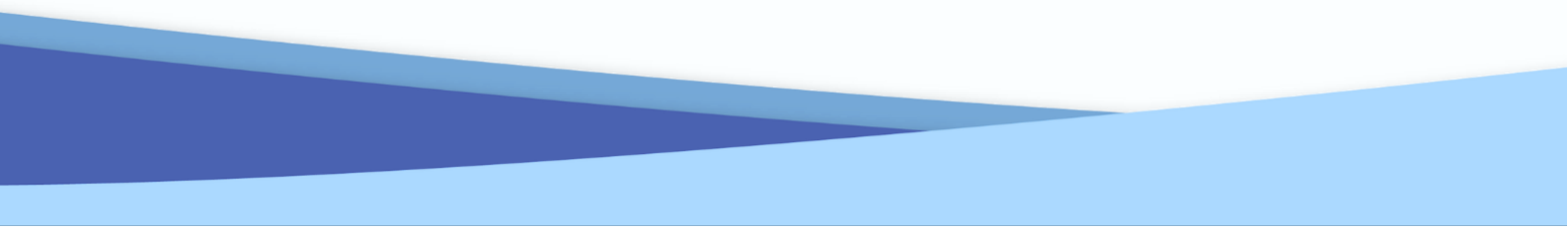


# BAB I

## PENDAHULUAN



GAMBARAN RUANG LINGKUP, TARGET AUDIENS,  
RUJUKAN, SERTA SISTEMATIKA PENYUSUNAN  
PANDUAN KRIPTOGRAFI *LIGHTWEIGHT*



## **BAB I**

### **PENDAHULUAN**

Bab ini memberikan gambaran umum untuk memahami dokumen Kriptografi *Lightweight*. Bab ini terdiri atas 4 (empat) subbab yang membahas tentang ruang lingkup, target audiens, rujukan dan sistematika penyusunan dokumen. Hal ini dimaksudkan sebagai kerangka awal sebelum memasuki pembahasan pada bab berikutnya.

#### **A. Ruang Lingkup**

Kriptografi telah menjadi bagian integral dari komunikasi rahasia selama ribuan tahun. Sejak zaman Mesir Kuno, penggunaan hieroglif yang menunjukkan upaya awal untuk menyembunyikan informasi dari pihak yang tidak berhak. Seiring dengan kemajuan teknologi komputer, penelitian di bidang kriptografi mengalami perkembangan yang pesat. Pada tahun 1972, IBM di bawah kepemimpinan W.L. Tuchman mulai mengembangkan algoritma enkripsi yang dikenal sebagai *Data Encryption Standard* (DES). Algoritma ini kemudian disetujui oleh pemerintah Amerika Serikat sebagai standar enkripsi nasional pada tahun 1977. Setelah itu, lahir berbagai algoritma kriptografi modern, seperti Rivest-Shamir-Adleman (RSA) dan *Advanced Encryption Standard* (AES), yang menjadi fondasi penting dalam sistem keamanan informasi saat ini.

Meskipun kriptografi modern telah terbukti kuat dan aman, penerapannya pada perangkat dengan keterbatasan daya dan memori, sering kali menjadi tantangan. Algoritma kriptografi seperti *Advanced Encryption Standard* (AES) dan *Rivest Shamir Adleman* (RSA) membutuhkan daya pemrosesan dan memori yang tidak selalu tersedia pada perangkat berdaya rendah. Seiring meningkatnya jumlah perangkat IoT dan *edge computing*, tantangan ini menjadi semakin relevan.

Kriptografi *lightweight* menawarkan alternatif yang lebih efisien dari segi energi, pemrosesan, dan memori, tanpa mengurangi standar keamanan. Dengan demikian, teknologi ini mampu menjaga integritas dan kerahasiaan informasi pada perangkat yang beroperasi dengan sumber daya minimal, menjadikannya solusi yang tepat untuk infrastruktur masa depan yang terhubung.

Kriptografi *lightweight* merupakan cabang kriptografi yang dirancang secara khusus untuk menyediakan solusi keamanan yang efisien pada perangkat dengan sumber daya terbatas, seperti perangkat *Internet of Things* (IoT), *Radio Frequency Identification* (RFID), kartu pintar, dan sistem tertanam (*embedded systems*). Pendekatan ini bertujuan untuk mencapai keseimbangan antara efisiensi komputasi dan tingkat keamanan, sehingga memungkinkan penerapan algoritma kriptografi pada perangkat dengan keterbatasan daya, memori, dan kapasitas pemrosesan. Dengan demikian, kriptografi *lightweight* menjadi solusi strategis dalam menghadapi tantangan keamanan di era digital yang semakin kompleks dan terhubung.

Dokumen ini disusun untuk memberikan pemahaman mengenai kriptografi *lightweight*, yang dirancang khusus untuk memenuhi kebutuhan sistem dengan keterbatasan daya, memori, dan kapasitas pemrosesan. Ruang lingkup dokumen ini mencakup beberapa bagian utama yang saling melengkapi, yaitu:

1. Pengantar dan Konsep Dasar

Berisi informasi tentang pengantar dan konsep dasar dari 3 (tiga) jenis kriptografi *lightweight* yaitu *lightweight stream cipher*, *lightweight block cipher* dan *lightweight fungsi hash*.

2. Contoh Algoritma Kriptografi *Lightweight*

Berisi informasi tentang daftar kriptografi *lightweight* yang terdiri atas *lightweight stream cipher*, *lightweight block cipher* dan *lightweight fungsi hash* berdasarkan standar atau jurnal internasional.

### 3. Lampiran

Berisi informasi tentang implementasi kriptografi *lightweight* menggunakan berbagai bahasa pemrograman.

## B. Target Audiens

Dokumen ini ditujukan bagi para penyelenggara sistem elektronik, baik publik maupun privat, yang meliputi:

1. Para pengambil kebijakan keamanan siber dan sandi yang memiliki pemahaman dasar tentang konsep kriptografi dan ingin memastikan keamanan informasi dalam organisasi berjalan sesuai standar keamanan nasional dan internasional;
2. Perumus kebijakan keamanan siber dan sandi dengan latar belakang teknis atau bekerja sama dengan pakar teknis dalam penyusunan kebijakan yang selaras dengan perkembangan kriptografi *lightweight*;
3. Profesional/praktisi keamanan siber dan sandi yang memiliki pemahaman tentang kriptografi, dasar matematika (aljabar boolean, teori bilangan, probabilitas dan analisis kompleksitas), dan arsitektur perangkat keras serta perangkat lunak untuk menimplementasikan kriptografi *lightweight* dalam sistem elektronik nya untuk memastikan sistem elektronik yang dikelola memenuhi standar internasional;
4. Penyedia layanan/produk keamanan teknologi informasi yang memiliki kapabilitas teknis dalam mengembangkan dan mengadaptasi kriptografi *lightweight* ke dalam layanan atau produk keamanan sesuai standar internasional.

## C. Rujukan

Penyusunan dokumen ini mengacu pada beberapa rujukan, diantaranya:

1. SNI ISO/IEC 18033-1:2021 Keamanan informasi — Algoritma enkripsi — Bagian 1: Umum;

2. SNI ISO/IEC 18033-4:2011 Teknologi informasi — Teknik keamanan — Algoritma enkripsi — Bagian 4: Penyandian alir;
3. ISO/IEC 29192-1:2012 — *Information Technology — Security techniques — Lightweight Cryptography —Part 1: General*;
4. ISO/IEC 29192-2:2012 — *Information Technology — Lightweight Cryptography —Part 2: Block Ciphers*;
5. ISO/IEC 29192-3:2012 — *Information technology — Security techniques — Lightweight cryptography Part 3: Stream ciphers*;
6. ISO/IEC 29192-5:2016 — *Information technology — Security techniques — Lightweight cryptography Part 5: Hash-functions*;
7. CRYPTREC *Cryptographic Technology Guideline (Lightweight Cryptography)*;
8. RFC 7748 - *Lightweight Cryptography for the Internet of Things*;
9. RFC 8439 - *ChaCha20 and Poly1305 for IETF Protocols*;
10. *eSTREAM Project - Lightweight Cryptography*.

#### **D. Sistematika Penyusunan Dokumen**

Dokumen ini terdiri dari beberapa bab yang menguraikan berbagai aspek kriptografi *lightweight*. Untuk selanjutnya, dokumen ini disusun sebagai berikut:

##### **Bab II Pengantar dan Konsep Dasar**

Membahas tentang pengertian, kendala, persyaratan yang harus dipenuhi kriptografi *lightweight* secara umum, penjelasan singkat tentang 3 (tiga) jenis kriptografi *lightweight* yaitu *lightweight stream cipher*, *lightweight block cipher* dan *lightweight fungsi hash* beserta contoh dari masing-masing algoritma tersebut

##### **Bab III Daftar Kriptografi *Lightweight***

Membahas tentang daftar rekomendasi kriptografi *lightweight* yang terdiri atas *lightweight stream cipher*, *block cipher* dan fungsi *hash* berdasarkan standar atau jurnal internasional.

##### **Bab IV Penutup**

Membahas tentang kesimpulan dari seluruh isi dokumen.

Lampiran

Membahas tentang implementasi kriptografi *lightweight* menggunakan berbagai bahasa pemrograman.



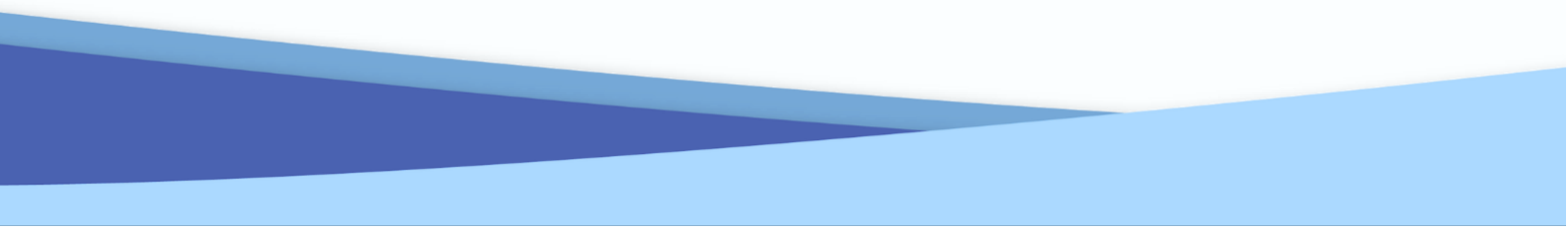


# BAB II

## PENGANTAR DAN KONSEP DASAR



PENJELASAN KONSEP, PERSYARATAN, DAN  
KARAKTERISTIK KRIPTOGRAFI *LIGHTWEIGHT*



## **BAB II**

### **PENGANTAR DAN KONSEP DASAR**

Penelitian dan pengembangan kriptografi *lightweight* mengalami peningkatan signifikan dalam beberapa tahun terakhir, seiring dengan meningkatnya kebutuhan akan solusi keamanan bagi perangkat yang memiliki keterbatasan sumber daya. Inisiatif-inisiatif akademik telah menghasilkan berbagai usulan sistem inovatif yang dipublikasikan dalam forum ilmiah internasional. Di Eropa, sejak tahun 2004 kriptografi *lightweight* telah menjadi salah satu fokus utama dalam Program Kerangka Kerja Komisi Eropa, yakni ECRYPT I dan ECRYPT II. Proses standardisasi juga terus berlangsung melalui pengembangan standar internasional seperti ISO/IEC 29192, yang mendefinisikan kriptografi *lightweight* untuk berbagai aplikasi teknis, dan ISO/IEC 29167, yang secara khusus menangani teknologi kriptografi untuk perangkat RFID. Di Amerika Serikat, sejak tahun 2015 *National Institute of Standards and Technology* (NIST) telah memulai inisiatif standardisasi kriptografi *lightweight*.

Kriptografi *lightweight* sangat cocok digunakan khususnya untuk lingkungan dengan keterbatasan sumber daya. Kategori keterbatasan sumber daya dalam kriptografi *lightweight* menurut ISO/IEC 29192-1:2012 [1] adalah sebagai berikut:

1. Luas area chip

Jika mekanisme kriptografi diimplementasikan dalam perangkat keras, luas area chip yang dibutuhkan mekanisme kriptografi tersebut dapat menjadi terbatas pada beberapa aplikasi (misalnya *tag* RFID). Dalam ISO/IEC 29192-1:2012 [1], luas area chip diukur dalam *gate equivalents*.

2. Konsumsi energi

Konsumsi energi dapat menjadi terbatas dalam penerapan kriptografi *lightweight*. Konsumsi energi dipengaruhi oleh beberapa faktor, diantaranya waktu pemrosesan, luas area chip (jika diimplementasikan dalam perangkat keras), frekuensi operasi, dan jumlah bit yang ditransmisikan antar entitas (terutama pada transmisi nirkabel). Untuk

meminimalkan konsumsi energi, seluruh faktor terkait tersebut harus dipertimbangkan.

### 3. Ukuran kode program dan ukuran RAM

Ukuran kode program (sering disebut ROM) dan ukuran RAM terbatas pada prosesor *low-end*. Jika dibandingkan dengan prosesor komputer umum, prosesor *low-end* memiliki himpunan instruksi yang sederhana, ruang terbatas untuk kode program, dan ruang terbatas di RAM untuk melakukan komputasi (misalnya pada prosesor tertanam).

### 4. *Bandwidth* komunikasi

Dalam beberapa kasus, *bandwidth* komunikasi dibatasi oleh jumlah maksimum bit yang dapat ditransmisikan selama satu sesi (misalnya tag RFID). Mekanisme dalam kategori ini dirancang agar lebih efisien dalam penggunaan jumlah bit yang dikirimkan melalui saluran komunikasi dibandingkan dengan mekanisme kriptografi yang digunakan secara umum.

### 5. Waktu eksekusi

Pada beberapa aplikasi seperti *contactless cards* dan RFID, waktu eksekusi untuk operasi yang benar dibatasi oleh implementasi (misalnya durasi kartu atau token berada dalam medan pembaca).

Dalam ISO/IEC 29192-1:2012 [1], kekuatan keamanan (*security strength*) suatu mekanisme kriptografi didefinisikan sebagai angka yang menunjukkan jumlah upaya (jumlah operasi) yang diperlukan untuk membobol suatu algoritma atau sistem kriptografi. Dua mekanisme dianggap memiliki kekuatan keamanan yang sebanding apabila jumlah upaya yang diperlukan untuk memecahkan mekanisme tersebut atau menemukan kuncinya dengan menggunakan sumber daya tertentu kira-kira sama.

Dalam ISO/IEC 29192-1:2012 [1], kekuatan keamanan 80-bit dianggap sebagai tingkat keamanan minimum untuk kriptografi *lightweight*. Ketahanan terhadap serangan *side-channel* dapat menjadi faktor penting dalam beberapa penerapan kriptografi *lightweight*. Tindakan pengamanan (*countermeasure*) terhadap analisis *side-channel* sering kali memerlukan tambahan luas area chip (untuk algoritma berbasis perangkat keras) atau

tambahan kode program (untuk algoritma berbasis perangkat lunak). Tindakan pengamanan ini bervariasi bergantung pada teknologi dan metode *side-channel* yang berlaku pada implementasi tertentu.

Banyak organisasi merekomendasikan penggunaan mekanisme kriptografi dengan kekuatan keamanan lebih dari 80-bit setelah tahun 2010. Namun, terdapat beberapa aplikasi kriptografi *lightweight* yang dapat menggunakan persyaratan keamanan lebih rendah, yaitu tidak perlu mengasumsikan adanya lawan dengan kemampuan sangat tinggi. Dalam kasus penggunaan kunci 80-bit, jumlah data yang dapat dienkripsi secara aman dengan satu kunci lebih terbatas sebelum dilakukan penggantian kunci (*rekeying*). Oleh karena itu, penting bagi perancang sistem keamanan kriptografi untuk memastikan bahwa batas aman penggunaan mekanisme kriptografi *lightweight* tidak terlampaui untuk satu kunci.

Agar suatu mekanisme kriptografi dapat diklasifikasikan sebagai *lightweight*, mekanisme tersebut harus dirancang khusus (*tailored*) untuk kombinasi kategori keterbatasan sumber daya seperti yang telah dijelaskan di atas. Untuk setiap kategori yang menjadi sasaran rancangan mekanisme kriptografi *lightweight*, harus disebutkan kategori tersebut dan disertakan bukti bahwa mekanisme kriptografi *lightweight* tersebut sesuai untuk kategori yang diklaim (misalnya luas area chip, konsumsi energi, dan sebagainya). Perlu dicatat bahwa mekanisme kriptografi yang hanya dioptimalkan untuk waktu eksekusi saja tidak selalu dianggap *lightweight*. Seluruh bukti kesesuaian untuk kategori tertentu harus berbasis bukti teoretis, yang dapat diperkuat dengan bukti implementasi nyata. Semua klaim terkait bukti implementasi nyata harus didokumentasikan secara lengkap agar dapat diverifikasi.

Contoh: Mekanisme A mengklaim dirancang agar sesuai untuk konsumsi energi rendah pada sistem komunikasi. Klaim ini dapat didukung secara teoretis dengan membandingkan jumlah bit yang ditransmisikan akibat penggunaan mekanisme A dengan mekanisme lain yang umum digunakan tetapi tidak dianggap sebagai mekanisme *lightweight*. Klaim ini dapat

diperkuat lebih lanjut dengan merujuk pada implementasi praktis yang mengukur konsumsi energi secara eksperimental, lalu membandingkannya dengan implementasi praktis lainnya yang menggunakan metode pengukuran serupa.

Berikut adalah beberapa persyaratan yang harus dipenuhi kriptografi *lightweight*:

#### 1. Persyaratan Implementasi

Persyaratan implementasi kriptografi *lightweight* dibagi menjadi dua kategori yaitu perangkat keras dan perangkat lunak, dengan penjelasan sebagai berikut:

##### a. Persyaratan Implementasi Perangkat Keras

Dua karakteristik fisik yang menjadi perhatian dalam implementasi perangkat keras kriptografi *lightweight* adalah:

- Luas area chip
- Konsumsi energi

Dalam ISO/IEC 29192-1:2012 [1], luas area chip diukur dalam *gate equivalents* (GE) untuk memungkinkan perbandingan terstandarisasi antar mekanisme kriptografi. Tidak ada ukuran target baku karena hal ini dipengaruhi oleh faktor ekonomi, jenis mekanisme, serta konteks penerapan.

Pada beberapa aplikasi, diperlukan perlindungan terhadap serangan *side-channel*, meskipun menambah *overhead*. Setiap algoritma perangkat keras yang dipublikasikan dalam ISO/IEC 29192 menyertakan estimasi ukuran yang diharapkan dalam GE.

Perbandingan konsumsi energi lebih kompleks karena sangat bergantung pada teknologi implementasi. Beberapa mekanisme hemat energi namun membutuhkan area chip besar. Dalam ISO/IEC 29192, konsumsi energi dievaluasi pada perangkat keras dengan luas area relatif kecil.

Pengukuran konsumsi energi secara eksperimental tetap penting bagi pengguna. Apabila tersedia, hasil pengukuran harus dilengkapi dengan metodologi yang terdokumentasi serta rincian teknologi yang digunakan.

Secara khusus, algoritma *block cipher* dan *stream cipher* dalam ISO/IEC 29192 untuk implementasi perangkat keras menyediakan ringkasan informasi berikut:

- Luas area chip
- Jumlah siklus (*cycles*)
- Jumlah bit per siklus
- Daya (*power*)
- Energi
- Energi per bit
- Teknologi: (pustaka spesifik dan nomor versinya)

b. Persyaratan Implementasi Perangkat Lunak

Dalam beberapa aplikasi kriptografi *lightweight*, implementasi perangkat lunak lebih disukai daripada perangkat keras. Faktor kritis yang dipertimbangkan antara lain:

- Ukuran kode program (*program code size*)
- Ukuran RAM

ISO/IEC 29192 tidak menetapkan batas absolut untuk persyaratan perangkat lunak. Hal ini bergantung pada faktor seperti arsitektur prosesor, *instruction set*, kapasitas memori, teknik optimisasi, serta kompromi antara kecepatan dan penggunaan memori. Mekanisme kriptografi *lightweight* dipertimbangkan masuk ke ISO/IEC 29192 jika kebutuhan kode dan RAM-nya jauh lebih kecil dibanding standar lain, misalnya ISO/IEC 18033 (AES), ISO/IEC 9798, dan ISO/IEC 11770.

Secara khusus, semua algoritma *block cipher* dan *stream cipher* untuk perangkat lunak dalam ISO/IEC 29192 menyediakan ringkasan informasi berikut:

- Ukuran kode program
- Ukuran RAM
- Kecepatan (*speed*)

#### **A. *Lightweight Stream Cipher***

*Lightweight stream cipher* umumnya dirancang hanya untuk menyediakan fungsi kerahasiaan (*confidentiality*), berbeda dengan *lightweight block cipher* yang memiliki kemampuan untuk mendukung berbagai fungsi kriptografi tambahan, seperti autentikasi dan integritas data [1]. Dalam lingkungan dengan keterbatasan sumber daya, baik dari sisi kapasitas memori maupun kompleksitas perangkat keras, *lightweight block cipher* sering kali menjadi pilihan yang lebih diutamakan karena fleksibilitasnya dalam memenuhi berbagai kebutuhan kriptografi serta efisiensinya dalam memproses data berukuran pendek. Namun demikian, apabila hanya diperlukan fungsi kerahasiaan dengan kebutuhan kecepatan tinggi dan penggunaan sumber daya yang sangat terbatas, maka *lightweight stream cipher* menjadi solusi yang lebih tepat dan efisien.

Berikut adalah penjelasan tentang *lightweight stream cipher* berdasarkan ISO/IEC 29192-3:2012 [2]:

##### **1. Model umum *stream cipher***

Dalam ISO/IEC 18033-4 [3], *stream cipher* didefinisikan berdasarkan spesifikasi dua proses utama yaitu pembangkit barisan kunci (*keystream generator*) dan fungsi keluaran. Penjelasan mengenai masing-masing proses adalah sebagai berikut:

a. *Keystream generator*

*Keystream generator* dalam *stream cipher* dapat diklasifikasikan menjadi dua jenis, yaitu *synchronous keystream generator* dan *self-synchronizing keystream generator*. Tetapi sesuai ISO/IEC 29192-3:2012 [2], *lightweight stream cipher* hanya menggunakan 1 (satu) jenis *key stream generator* yaitu *synchronous keystream generator*. Berikut adalah penjelasan dari *synchronous keystream generator*.

*Synchronous keystream generator* merupakan suatu *finite-state machine*. *Synchronous keystream generator* didefinisikan dengan:

- Fungsi inisialisasi (*Init*), yang menerima masukan berupa kunci  $K$  dan *Initialization Vector* (IV), serta menghasilkan *state* awal  $S_0$  untuk *keystream generator*. IV harus dipilih sedemikian rupa sehingga tidak ada dua pesan yang dienkripsi menggunakan kunci dan IV yang sama.
- Fungsi *next-state* (*Next*), yang menerima masukan berupa *state* saat ini dari *keystream generator*  $S_i$ , dan menghasilkan *state* berikutnya  $S_{i+1}$ .
- Fungsi *keystream* (*Strm*), yang menerima *state*  $S_i$  dari *keystream generator* sebagai masukan dan menghasilkan blok *keystream*  $Z_i$ .

Ketika *synchronous keystream generator* pertama kali diinisialisasi, maka *keystream generator* akan memasuki *state* awal  $S_0$  yang didefinisikan sebagai:

$$S_0 = \text{Init}(IV, K)$$

Setelah itu, untuk  $i = 0, 1, \dots$  *keystream generator* :

- Menghasilkan blok *keystream*  $Z_i = \text{Strm}(S_i, K)$
- Memperbarui *state* dari *finite state machine*  $S_{i+1} = \text{Next}(S_i, K)$ .

Dengan demikian, untuk mendefinisikan suatu *synchronous keystream generator* cukup dengan menentukan fungsi-fungsi

*Init*, *Next*, dan *Strm*, termasuk panjang kunci, kunci, *IV*, *state*, dan blok keluaran.

b. Fungsi Keluaran

Fungsi keluaran menurut ISO/IEC 29192-3:2012 [2] adalah teknik yang digunakan dalam *stream cipher* untuk menggabungkan *keystream* dengan *plaintext* untuk menghasilkan *ciphertext*.

Fungsi keluaran untuk *synchronous stream cipher* atau *self-synchronizing stream cipher* adalah sebuah fungsi *invertible Out* yang menggabungkan blok *plaintext*  $P_i$ , blok *keystream*  $Z_i$ , untuk menghasilkan blok *ciphertext*  $C_i (i \geq 0)$ . Model umum untuk fungsi output *stream cipher* didefinisikan sebagai berikut: Enkripsi blok *plaintext*  $P_i$  dengan blok *keystream*  $Z_i$  dinyatakan sebagai:

$$C_i = Out(P_i, Z_i)$$

dan dekripsi blok *ciphertext*  $C_i$  dengan blok *keystream*  $Z_i$  dinyatakan sebagai

$$P_i = Out^{-1}(C_i, Z_i).$$

Fungsi keluaran harus memenuhi ketentuan bahwa untuk sebarang blok *keystream*  $Z_i$ , blok *plaintext*  $P_i$ :

$$P_i = Out^{-1}(Out(P_i, Z_i), Z_i)$$

Terdapat 2 (dua) jenis fungsi keluaran, yaitu fungsi keluaran aditif-biner (*binary-additive*) dan fungsi keluaran MULTI-S01. Sesuai ISO/IEC 29192-3:2012 [3], *lightweight stream cipher* hanya menggunakan 1 (satu) jenis fungsi keluaran yaitu fungsi keluaran *binary-additive*, dengan penjelasan sebagai berikut:

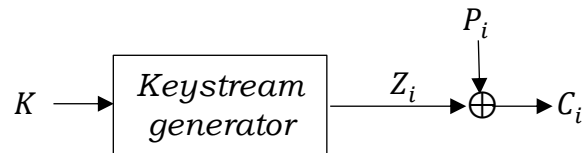
*binary-additive stream cipher* adalah *stream cipher* di mana blok *keystream*, *plaintext*, dan *ciphertext* berupa deretan digit biner, serta operasi untuk menggabungkan *plaintext* dengan *keystream* menggunakan XOR bit per bit (*bitwise XOR*). Misalkan  $n$  adalah panjang bit dari  $P_i$ . Fungsi keluaran *binary-additive* dinyatakan sebagai:

$$Out(P_i, Z_i) = P_i \oplus Z_i.$$

Operasi  $Out^{-1}$  dinyatakan sebagai:

$$Out^{-1}(C_i, Z_i) = C_i \oplus Z_i.$$

Fungsi keluaran *binary-additive* ditunjukkan pada Gambar 2.1.



Gambar 2.1 Fungsi keluaran *binary-additive*.

## 2. Tujuan perancangan

Seperti yang telah dijelaskan sebelumnya, *lightweight stream cipher* dirancang untuk melindungi kerahasiaan data yang disimpan (*data at rest*) atau data yang dikirimkan (*data in transit*). *Lightweight stream cipher* yang terdapat dalam ISO/IEC 29192-1:2012 [1] dievaluasi berdasarkan beberapa kriteria dengan mempertimbangkan kesesuaian untuk lingkungan yang terbatas.

Kriterianya adalah sebagai berikut:

### a. Keamanan mekanisme kriptografi

Keamanan 80-bit dianggap sebagai kekuatan keamanan minimum untuk kriptografi *lightweight*. Namun, direkomendasikan agar keamanan minimal 112-bit diterapkan untuk sistem yang akan memerlukan keamanan untuk jangka waktu yang lebih lama karena periode perlindungan yang diberikan suatu algoritma ditentukan oleh kekuatan keamanan serta daya komputasi musuh yang ingin memecahkan algoritma tersebut.

### b. Karakteristik implementasi perangkat keras (untuk mekanisme yang ditargetkan pada perangkat keras) berdasarkan area chip yang ditempati oleh mekanisme kriptografi dan konsumsi energi.

- c. Karakteristik implementasi perangkat lunak (untuk mekanisme yang ditargetkan pada perangkat lunak) berdasarkan ukuran kode dan ukuran RAM yang dibutuhkan saat implementasi di perangkat lunak.
- d. Permasalahan royalti (lisensi) yang memengaruhi mekanisme kriptografi.
- e. Kematangan mekanisme kriptografi
- f. Generalitas karakteristik *lightweight* yang diklaim untuk mekanisme kriptografi

Semakin independen karakteristik *lightweight* yang diklaim dari implementasi dalam teknologi tertentu, semakin baik, karena karakteristik tersebut akan dapat digunakan oleh khalayak yang lebih luas.

### 3. Contoh *lightweight* stream cipher

Berikut adalah beberapa contoh *lightweight* stream cipher.

- a. Enocoro-128v2 *keystream* generator
- b. Enocoro-80 *keystream* generator
- c. Trivium *keystream* generator
- d. Grain
- e. *Mutual Irregular Clocking Keystream Generator* (MICKEY).

## B. *Lightweight Block Cipher*

Berdasarkan ISO/IEC 29192-1:2012 [1] tujuan utama *lightweight block cipher* dirancang untuk melindungi kerahasiaan *data at rest* atau *data in transit*.

### 1. Definisi *lightweight block cipher*

Definisi *lightweight block cipher* diambil berdasarkan definisi *block cipher* yang terdapat dalam SNI ISO/IEC 18033-3 [4], yaitu *block cipher* adalah sistem enkripsi simetris yang memiliki sifat bahwa algoritma enkripsinya beroperasi pada blok-blok *plaintext* untuk menghasilkan blok-blok *ciphertext*. Setiap kunci pada *block cipher*

mendefinisikan suatu pemetaan tertentu yang dapat dibalik dari blok-blok *plaintext* ke blok-blok *ciphertext* (dan pemetaan kebalikannya yang digunakan untuk dekripsi).

*Block cipher* dapat digunakan dalam berbagai cara, diantaranya melalui penerapan mode operasi yang dapat memberikan jaminan kerahasiaan dan mode operasi yang memberikan kendali integritas. Penggunaan lain dari *block cipher* adalah penerapan *block cipher* sebagai fungsi pembangun fungsi *hash* (dapat dilihat pada ISO/IEC 10118-2) dan penerapan *block cipher* sebagai fungsi pembangun *random number generator* (dapat dilihat pada ISO/IEC 18031).

*Block cipher* yang dimuat dalam ISO/IEC 29192-2 [5] dievaluasi berdasarkan kriteria evaluasi dengan mempertimbangkan kesesuaiannya untuk lingkungan dengan keterbatasan sumber daya (*constrained environments*). Kriterianya adalah sebagai berikut:

- a. Keamanan mekanisme kriptografi  
Keamanan 80-bit dianggap sebagai kekuatan keamanan minimum untuk kriptografi *lightweight*. Namun, direkomendasikan agar keamanan minimal 112-bit diterapkan untuk sistem yang akan memerlukan keamanan untuk jangka waktu yang lebih lama karena periode perlindungan yang diberikan suatu algoritma ditentukan oleh kekuatan keamanan serta daya komputasi musuh yang ingin memecahkan algoritma tersebut.
- b. Karakteristik implementasi perangkat keras (untuk mekanisme yang ditargetkan pada perangkat keras) berdasarkan area chip yang ditempati oleh mekanisme kriptografi dan konsumsi energi.
- c. Karakteristik implementasi perangkat lunak (untuk mekanisme yang ditargetkan pada perangkat lunak) berdasarkan ukuran kode dan ukuran RAM yang dibutuhkan saat implementasi di perangkat lunak.

- d. Permasalahan lisensi yang memengaruhi mekanisme kriptografi.
- e. Kematangan mekanisme kriptografi
- f. Generalitas karakteristik *lightweight* yang diklaim untuk mekanisme kriptografi

Semakin independen karakteristik *lightweight* yang diklaim dari implementasi dalam teknologi tertentu, semakin baik, karena karakteristik tersebut akan dapat digunakan oleh khalayak yang lebih luas.

*Block cipher* dapat digunakan untuk memastikan integritas dan asal data. Dimungkinkan untuk membangun *lightweight message authentication code* (MAC) dari *block cipher* yang dimuat dalam ISO/IEC 29192-2 menggunakan algoritma MAC yang ditentukan dalam ISO/IEC 9797-1. Demikian pula, dimungkinkan membangun *lightweight hash function* dari *block cipher* yang dimuat dalam ISO/IEC 29192-2 menggunakan konstruksi fungsi hash yang ditentukan dalam ISO/IEC 10118-2.

Keamanan sebagian besar mode operasi *block cipher* (termasuk konstruksi MAC dan fungsi *hash*) menurun sebesar  $q^2/2^n$ , dengan  $n$  adalah ukuran blok dalam bit dan  $q$  adalah jumlah blok yang dienkripsi. Sebagai contoh, ketika  $n = 64$  bit, enkripsi sebanyak  $2^{32}$  blok sudah cukup untuk membuat *block cipher* rentan terhadap serangan. Oleh karena itu, perlu diperhatikan bahwa semakin pendek ukuran blok, semakin sedikit data yang dapat dienkripsi dengan satu kunci.

## 2. Contoh *lightweight block cipher*

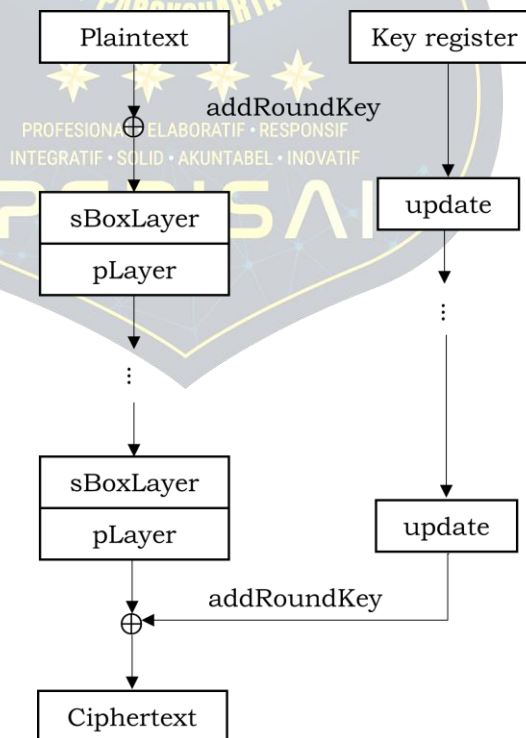
Berikut adalah beberapa contoh *lightweight block cipher* beserta deskripsi singkatnya.

a. PRESENT

Algoritma PRESENT adalah *lightweight block cipher* yang memproses blok data berukuran 64 bit, dengan menggunakan kunci sepanjang 80 bit (dikenal dengan PRESENT-80) atau 128 bit (dikenal dengan PRESENT-128). Algoritma PRESENT memiliki struktur *Substitution Permutation Network* (SPN) dengan *round* sebanyak 31 *round*. Komponen utama algoritma PRESENT adalah sebagai berikut:

- 1) sBoxlayer, menggunakan sebuah *Substitution box* (S-box) 4 bit ke 4 bit dinotasikan dengan  $S: \mathbb{F}_2^4 \rightarrow \mathbb{F}_2^4$  yang diaplikasikan sebanyak 16 kali secara paralel pada setiap *round* untuk memberikan sifat non-linearitas
- 2) pLayer, bit-bit keluaran dari S-box dipermutasikan sesuai pola tertentu untuk memastikan difusi yang optimal.
- 3) addroundkey, kunci *round* (*round key*) dioperasikan dengan XOR terhadap data pada setiap *round*.

Algoritma PRESENT ditunjukkan pada Gambar 2.2.



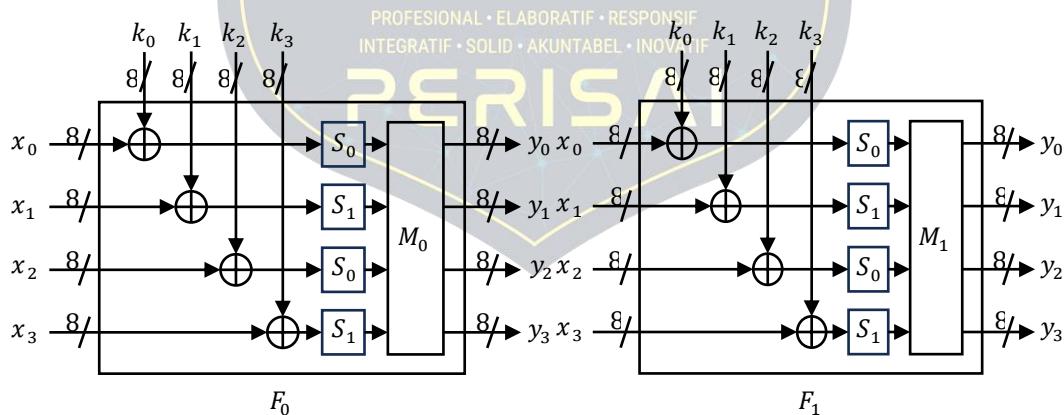
Gambar 2.2 Algoritma PRESENT

Digambar ulang dari [6].

b. CLEFIA

Algoritma CLEFIA adalah *lightweight block cipher* yang memproses blok data berukuran 128 bit dengan menggunakan kunci sepanjang 128, 192, atau 256 bit. Jumlah *round* secara berturut-turut adalah 18, 22, dan 26 untuk CLEFIA dengan kunci 128 bit, 192 bit, dan 256 bit. Fungsi enkripsi dan dekripsi CLEFIA memerlukan masing-masing 36 *round key* untuk kunci berukuran 128 bit, 44 *round key* untuk kunci berukuran 192 bit, dan 52 *round key* untuk kunci berukuran 256 bit. Jumlah total *round key* tersebut bergantung pada panjang kunci yang digunakan. Algoritma CLEFIA memiliki struktur *Generalized Fesistel Network* (GFN) tipe-2 dengan 4 cabang (4-branch type-2 GFN). Komponen utama algoritma CLEFIA adalah:

- 1) *F-function*, terdapat 2 (dua) buah *F-function* (ditunjukkan pada Gambar xx) yang masing-masing terdiri atas operasi XOR, dilanjutkan dengan substitusi menggunakan dua S-box berukuran 8-bit yang berbeda ( $S_0$  dan  $S_1$ ) diikuti operasi linier menggunakan dua buah matriks berukuran  $4 \times 4$  ( $M_0$  dan  $M_1$ ). *F-function* ditunjukkan pada Gambar 2.3.



Gambar 2.3 *F-function*

Digambar ulang dari [5].

- 2) *Key Whitening*, operasi XOR antara data dan kunci yang dilakukan di awal dan akhir proses enkripsi.

- 3) *Round Keys*, dibangkitkan melalui *key scheduling* yang memanfaatkan konstanta tetap (*fixed constants*) untuk menjamin variasi kunci pada setiap *round*.

Algoritma CLEFIA ditunjukkan pada Gambar 4.

c. *Low-power Encryption Algorithm (LEA)*

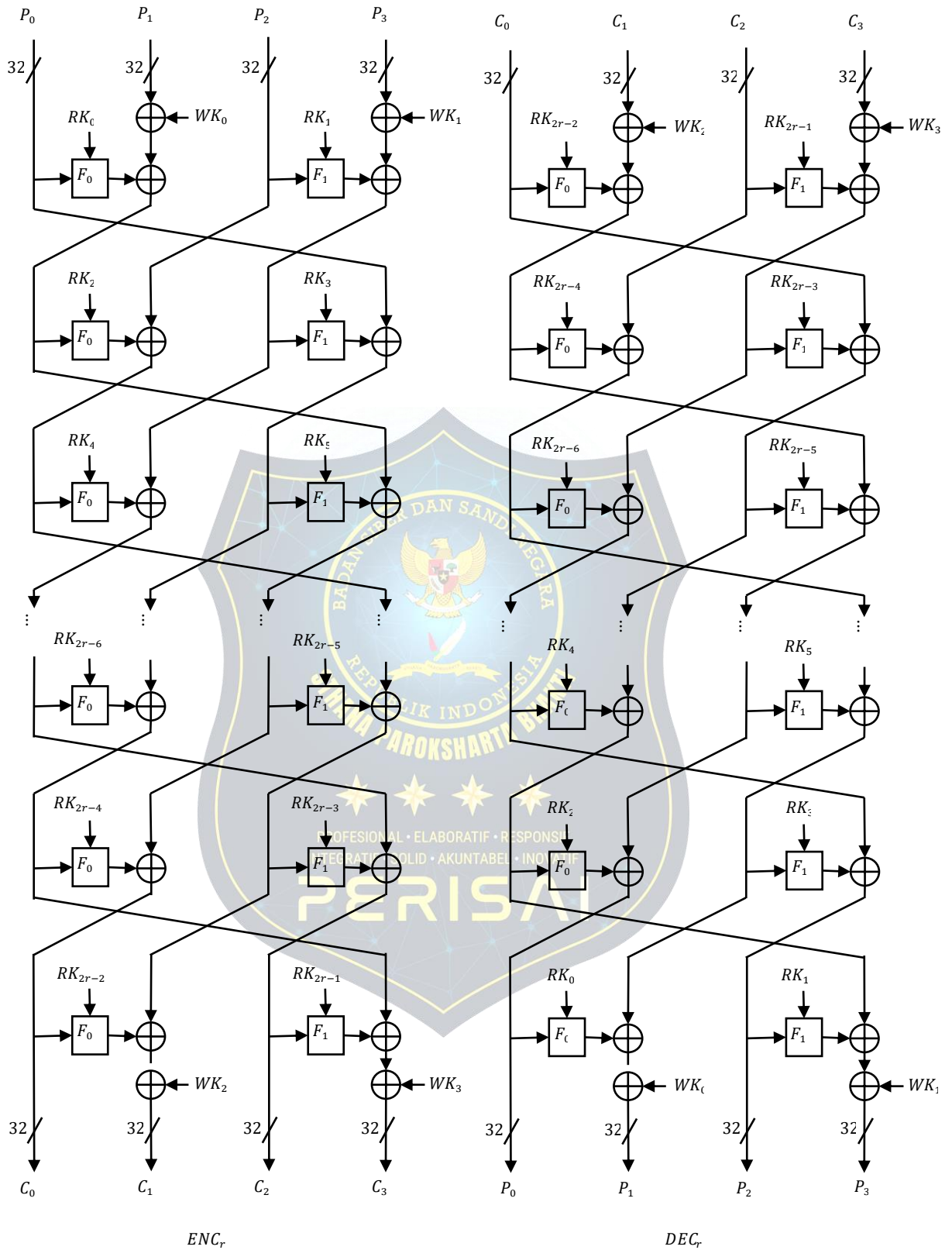
Algoritma LEA adalah *lightweight block cipher* berbasis *Addition–Rotation–XOR (ARX)* yang dikembangkan oleh KISA (*Korea Internet & Security Agency*) pada tahun 2013. LEA dirancang untuk memberikan keamanan tinggi dengan kinerja sangat cepat di perangkat keras maupun perangkat lunak, termasuk perangkat dengan sumber daya terbatas.

Algoritma LEA memproses blok data berukuran 128 bit dengan panjang kunci berukuran 128 bit (disebut LEA-128), 192 bit (LEA-192), dan 256 bit (LEA-256). Jumlah *round* adalah 24 untuk LEA-128, 28 untuk LEA-192, dan 32 untuk LEA-256. Fungsi enkripsi dan dekripsi LEA memerlukan 24 *round key* untuk LEA-128, 28 *round key* untuk LEA-192, atau 32 *round key* untuk LEA-256.

Algoritma LEA berstruktur ARX, dengan komponen utama sebagai berikut:

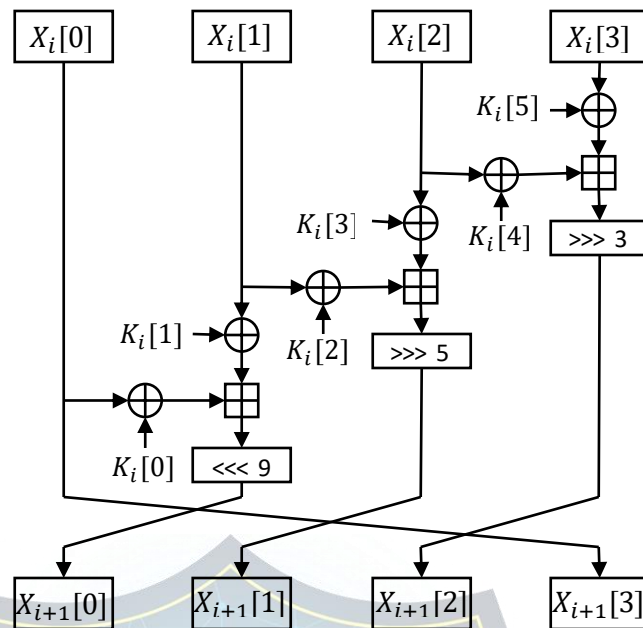
- 1) Operasi penjumlahan modulo  $2^{32}$  dinotasikan dengan  $\boxplus$ , untuk memberikan sifat non-linearitas.
- 2) Rotasi bit (*bitwise rotation*) dinotasikan dengan  $\lll, \ggg$  untuk memastikan difusi yang merata.
- 3) Operasi XOR dinotasikan dengan  $\oplus$  untuk memberikan kombinasi data dan kunci dengan biaya komputasi rendah.

Algoritma LEA ditunjukkan pada Gambar 2.4.



Gambar 2.4 Algoritma CLEFIA

Digambar ulang dari [5].



Gambar 2.5 Algoritma LEA  
Digambar ulang dari [5].

### C. **Lightweight Fungsi hash**

Fungsi *hash* merupakan komponen fundamental kriptografi yang digunakan secara luas pada berbagai protokol keamanan. Fungsi *hash* diterapkan dengan beragam tujuan, bahkan dalam cara-cara yang tidak biasa. Bagi kriptografer, penggunaan fungsi *hash* dianggap sebagai praktik standar dalam menjaga keamanan [7].

Secara umum, fungsi hash terbagi menjadi dua kelas [8]:

1. Fungsi *hash unkeyed*, yaitu fungsi *hash* dengan satu parameter input berupa pesan;
2. Fungsi *hash keyed*, yaitu fungsi *hash* dengan dua parameter input, yaitu pesan dan kunci rahasia.

Menurut SNI ISO/IEC 10118-1:2016 [9], fungsi *hash* adalah fungsi yang memetakan string bit dengan panjang variabel (tetapi biasanya diberi batas atas) ke string bit dengan panjang tetap, memenuhi dua karakteristik berikut:

1. Untuk keluaran tertentu, secara komputasi tidak mungkin menemukan input yang memetakan ke keluaran ini;
2. Untuk input tertentu, secara komputasi tidak mungkin menemukan input kedua yang dipetakan ke keluaran yang sama.

Berikut adalah jenis serangan terhadap fungsi hash [8] yang juga relevan pada *lightweight* fungsi hash, yaitu:

1. Pencarian kolisi (*collision search*): menemukan dua string data berbeda  $M_1$ ,  $M_2$  sedemikian rupa sehingga  $h(M_1) = h(M_2)$ .
2. Pencarian *preimage* (*preimage search*): diberikan string bit  $H$  dengan panjang yang sesuai, tujuan serangan adalah menemukan string data  $M$  sedemikian rupa sehingga  $h(M) = H$ .
3. Pencarian *preimage* kedua (*second preimage search*): diberikan string data  $M$ , tujuan serangan adalah menemukan string data lain  $M'$  sedemikian rupa sehingga  $h(M') = h(M)$  dan  $M' \neq M$ .
4. Serangan ekstensi panjang (*length-extension attack*): diberikan string bit  $h(M)$  untuk beberapa string data tidak kosong yang tidak diketahui  $M$ , tujuan serangan adalah menemukan string data  $M'$  dan nilai  $h(M || M')$ .

Pada dokumen ini dibahas 3 (tiga) konstruksi yang banyak digunakan saat mendesain *lightweight* fungsi hash.

1. Struktur Algoritma beserta Fungsi Primitifnya

- a. Konstruksi *Sponge*

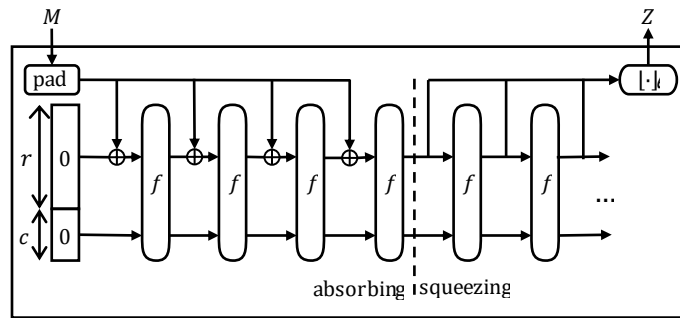
Fungsi *sponge* merupakan generalisasi dari fungsi hash yang mampu menangani input dan keluaran dengan panjang variabel, berbasis pada permutasi dengan panjang tetap. Dengan mekanisme ini, fungsi *sponge* tidak hanya berfungsi sebagai fungsi hash, tetapi juga dapat digunakan sebagai *stream cipher*. Secara teoretis, fungsi *sponge* memodelkan penggunaan memori terbatas pada setiap konstruksi konkret. Fungsi *sponge* acak (*random sponge*) memiliki kekuatan setara dengan *random oracle*, kecuali pada efek yang ditimbulkan oleh

keterbatasan memori, sehingga dapat dijadikan alternatif model *random oracle* dalam menyatakan klaim keamanan.

Konstruksi *sponge* adalah konstruksi iteratif sederhana untuk membangun sebuah fungsi  $F$  dengan input memiliki panjang variabel dan keluaran dengan panjang sebarang, yang berbasis pada transformasi atau permutasi  $f$  dengan panjang tetap, yang bekerja pada sejumlah  $b$  bit tetap dengan  $b$  disebut sebagai *width*. Konstruksi *sponge* beroperasi pada sebuah *state* berukuran  $b = r + c$  bit, dengan  $r$  disebut *bitrate* dan  $c$  disebut *capacity*. Tahapan kerja konstruksi *sponge* adalah sebagai berikut:

- 1) Semua bit dalam *state* diinisialisasi ke nol. Pesan input kemudian di-*padded* dan dipotong menjadi blok-blok sepanjang  $r$  bit.
- 2) Proses dilanjutkan dalam dua fase utama:
  - *Absorbing phase*: blok-blok pesan masukan sepanjang  $r$  bit dioperasikan dengan XOR ke dalam  $r$  bit pertama dari *state*, yang diselingi dengan penerapan fungsi  $f$ . Setelah semua blok pesan selesai diproses, konstruksi beralih ke fase berikutnya.
  - *Squeezing phase*:  $r$  bit pertama dari *state* dikeluarkan sebagai blok keluaran, diselingi dengan penerapan fungsi  $f$ . Jumlah blok keluaran ditentukan sesuai kebutuhan pengguna.
- 3) Sepanjang proses,  $c$  bit terakhir dari *state* tidak pernah langsung dipengaruhi oleh blok input dan tidak pernah dikeluarkan selama fase *squeezing*.

Konstruksi *sponge* ditunjukkan pada Gambar 2.5.



Gambar 2.6 Konstruksi Sponge

Digambar ulang dari [10].

b. Konstruksi *Merkle-Damgard* [11]

Konstruksi Merkle-Damgard merupakan pendekatan umum untuk memperluas fungsi kompresi menjadi fungsi hash penuh, dengan tetap mempertahankan sifat *collision-resistance* (tahan kolisi) dari fungsi kompresi tersebut. Transformasi ini banyak digunakan dalam praktik, misalnya pada fungsi hash MD5 dan keluarga SHA. Keberadaan transformasi ini memungkinkan perancangan fungsi *hash* tahan kolisi, sehingga proses perancangan menjadi lebih sederhana. Dari sisi teoretis, konstruksi Merkle-Damgard juga menarik karena menunjukkan bahwa kompresi satu bit sama sulitnya (atau sama mudahnya) dengan kompresi sejumlah bit sebarang.

Sebagai ilustrasi, misalkan fungsi kompresi  $(Gen, h)$  mengompresi input menjadi setengah panjangnya; misalnya, panjang input adalah  $2n$  dan panjang keluarannya adalah  $n$ . Konstruksi ini tetap berlaku untuk panjang input dan keluaran berapa pun, selama  $h$  melakukan kompresi. Dengan demikian, dapat dibangun fungsi *hash* tahan kolisi  $(Gen, h)$  yang memetakan input dengan panjang sebarang menjadi keluaran sepanjang  $n$  tanpa mengubah bagian  $Gen$ .

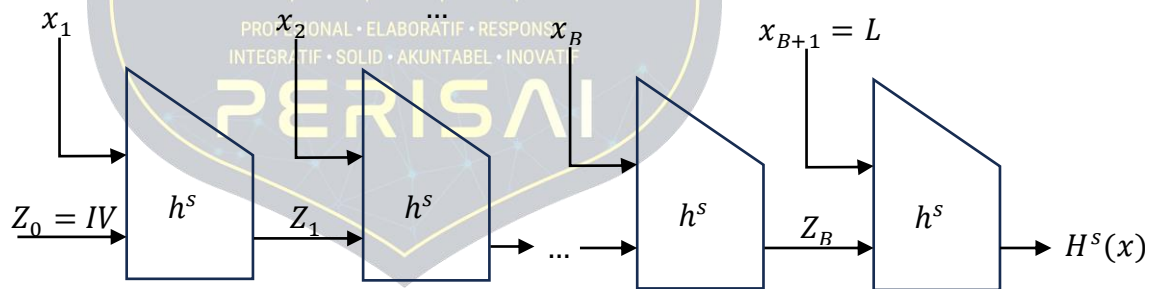
Konstruksi Merkle-Damgard digambarkan pada Gambar x dan didefinisikan sebagai berikut:

Misalkan terdapat fungsi *hash* dengan panjang tetap untuk masukan berukuran  $2n$  dan keluaran berukuran  $n$ . Fungsi hash  $(Gen, h)$  dikonstruksi sebagai berikut:

*Gen*: tetap, tidak berubah.

*H*: dengan input berupa kunci  $s$  dan string  $x \in \{0,1\}^*$  dengan panjang  $L > 2^n$ , lakukan langkah-langkah berikut:

- 1) Tetapkan  $B := \left\lceil \frac{L}{n} \right\rceil$  yaitu jumlah blok dalam  $x$ . Lakukan *padding* pada  $x$  dengan bit nol hingga panjangnya menjadi kelipatan  $n$ . Hasil *padding* di-parse menjadi deretan blok berukuran  $n$ -bit:  $x_1, \dots, x_B$ . Tetapkan  $x_{B+1} := L$ , dengan  $L$  direpresentasikan sebagai string  $n$ -bit.
- 2) Tetapkan  $z_0 := 0^n$ . Nilai  $z_0$  disebut *Initialization Vector* (IV), yang dapat berupa nilai sebarang dan dapat digantikan dengan konstanta apapun.
- 3) Untuk  $i = 1, \dots, B + 1$ , hitung
 
$$z_i = h^s(z_{i-1} \| x_i)$$
- 4) Hasil akhir adalah  $z_{B+1}$ .



Gambar 2.7 Konstruksi Merkle-Damgård

Digambar Ulang dari [11].

#### c. Konstruksi Davies-Meyer

Menurut Bart Preneel [12], fungsi *hash* Davies-Meyer merupakan konstruksi fungsi *hash* berbasis *block cipher*, dengan panjang hasil hash (dalam bit) sama dengan panjang blok dari *block cipher* tersebut. Fungsi *hash* Davies-Meyer

termasuk dalam kategori fungsi hash *unkeyed* yang memiliki sifat-sifat berikut:

- 1) ketahanan terhadap *preimage* (*preimage resistance*);
- 2) ketahanan terhadap *second preimage* (*second preimage resistance*); dan
- 3) ketahanan terhadap kolisi (*collision resistance*).

Sifat-sifat tersebut bergantung pada karakteristik dari *block cipher* yang digunakan dalam konstruksi fungsi *hash*.

Berikut adalah algoritma konstruksi fungsi *hash* Davies-Meyer [12]:

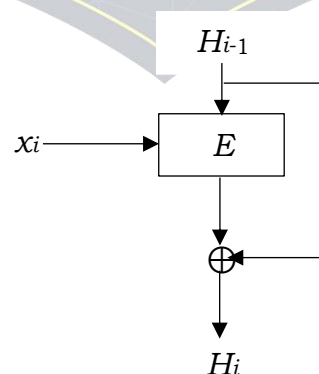
Input: string bit  $x$

Keluaran: kode *hash*  $n$ -bit dari  $x$

- 1) Bagi input  $x$  menjadi blok-blok berukuran  $k$ -bit dengan  $k$  adalah ukuran kunci. Lakukan *padding* jika diperlukan agar blok terakhir lengkap. Misalkan pesan yang sudah di-*padding* terdiri atas  $t$  blok  $k$ -bit:  $x_1, x_2, \dots, x_t$ .
- 2) Tentukan nilai IV berukuran  $n$ -bit.
- 3) Definisikan keluaran  $H_t$  sebagai berikut:

$$H_0 = IV; H_i = E_{x_i}(H_{i-1}) \oplus H_{i-1}, 1 \leq i \leq t.$$

Konstruksi fungsi *hash* Davies-Meyer ditunjukkan pada Gambar 2.8.



Gambar 2.8 Fungsi kompresi Davies Meyer

Digambar ulang dari [13].

## 2. Penggunaan

Fungsi hash konvensional mungkin kurang sesuai untuk lingkungan dengan keterbatasan sumber daya, terutama karena ukuran *internal state* yang besar serta kebutuhan konsumsi daya yang tinggi. Kondisi ini mendorong pengembangan *lightweight* fungsi hash [14].

Perbedaan utama antara fungsi hash konvensional dengan *lightweight* fungsi hash dapat dilihat pada aspek berikut [15]:

### a. Ukuran *internal state* dan keluaran lebih kecil

Ukuran keluaran yang besar penting bagi aplikasi yang membutuhkan ketahanan fungsi hash terhadap *collision*. Namun, untuk aplikasi yang tidak memerlukan ketahanan terhadap *collision*, ukuran *internal state* dan keluaran dapat dibuat lebih kecil. Jika dibutuhkan fungsi hash dengan sifat tahan kolisi, maka fungsi hash tersebut tetap dapat memberikan tingkat keamanan yang sama terhadap serangan *preimage*, *second-preimage*, dan kolisi, meskipun ukuran *internal state* diperkecil.

### b. Ukuran pesan yang lebih kecil

Fungsi hash konvensional dirancang untuk menangani input berukuran sangat besar (sekitar  $2^{64}$  bit). Sebaliknya, pada sebagian besar protokol yang menjadi target *lightweight* fungsi hash, ukuran input umumnya jauh lebih kecil (misalnya, maksimal 256 bit). Oleh karena itu, fungsi hash yang dioptimalkan untuk pesan pendek lebih sesuai digunakan dalam aplikasi *lightweight*.

## 3. Contoh *Lightweight* Fungsi Hash

Berikut beberapa contoh *lightweight* fungsi hash:

- a. PHOTON adalah *lightweight* fungsi hash dengan ukuran permutasi 100, 144, 196, 256, dan 288 bit, yang menghasilkan kode hash masing-masing sepanjang 80, 128, 160, 224, dan 256 bit.

- b. SPONGENT adalah *lightweight* fungsi *hash* dengan ukuran permutasi 88, 136, 176, 240, dan 272 bit, yang menghasilkan kode *hash* masing-masing sepanjang 88, 128, 160, 224, dan 256 bit.
- c. Lesamnta-LW adalah *lightweight* fungsi *hash* dengan ukuran permutasi 384 bit, yang menghasilkan kode *hash* sepanjang 256 bit.

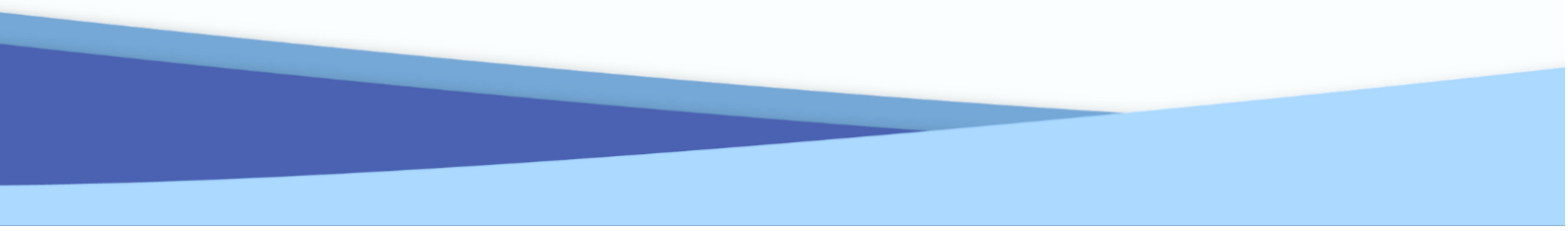




# BAB III

## CONTOH ALGORITMA KRIPTOGRAFI *LIGHTWEIGHT*

➤ DAFTAR ALGORITMA KRIPTOGRAFI *LIGHTWEIGHT*



### BAB III

## CONTOH ALGORITMA KRIPTOGRAFI *LIGHTWEIGHT*

### A. *Lightweight Stream Cipher*

Subbab ini berisi ringkasan *lightweight stream cipher* yang terdapat dalam dokumen CRYPTREC *Cryptographic Technology Guideline - Lightweight Cryptography* [16] dan CRYPTREC *Cryptographic Technology Guideline (Lightweight Cryptography) 2023 Edition* [17] yang diterbitkan oleh CRYPTREC *Lightweight Cryptography Working Group*. Ringkasan tersebut berisi informasi tentang profil algoritma, fitur, analisis keamanan, analisis performa pada perangkat keras dan/atau perangkat lunak, standarisasi dan informasi *open source* dari algoritma tersebut. Algoritma *lightweight block cipher* yang terdapat dalam subbab ini adalah ChaCha, Enocoro, Grain v1, MICKEY 2.0 dan Trivium.

#### 1. ChaCha20

|                           |              |                                                                                                                                                                                                                                                                                                                                                                                                                                                             |
|---------------------------|--------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Profil Algoritma          | Nama         | ChaCha20                                                                                                                                                                                                                                                                                                                                                                                                                                                    |
|                           | Perancang    | Daniel J. Bernstein (University of Illinois at Chicago, USA)                                                                                                                                                                                                                                                                                                                                                                                                |
|                           | Publikasi    | pada kegiatan SASC 2008 [18]                                                                                                                                                                                                                                                                                                                                                                                                                                |
|                           | Standarisasi | IETF RFC 7539 [19]                                                                                                                                                                                                                                                                                                                                                                                                                                          |
| Karakteristik kriptografi | Fitur        | ChaCha20 adalah <i>stream cipher</i> dengan kunci berukuran 256 bit dan IV berukuran 96 bit. Selain kunci rahasia dan IV, algoritma ini menggunakan konstanta 128 bit dan <i>block counter</i> 32 bit untuk menghasilkan keluaran berupa bilangan <i>pseudorandom</i> sepanjang 512 bit.<br><br>Algoritma ini memanfaatkan operasi penjumlahan aritmetika 32 bit, XOR, dan pergeseran siklik, sehingga cocok untuk diimplementasikan dalam perangkat lunak. |

|                   |                                                                                                                                                                                                                                                                    |                     |                    |                   |      |
|-------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------|--------------------|-------------------|------|
|                   | Dengan biaya inisialisasi yang rendah, ChaCha20 mampu memproses pesan pendek dengan cepat. Selain itu, karena tidak menggunakan <i>table lookups</i> , implementasi langsungnya ( <i>straightforward implementation</i> ) aman dari serangan <i>cache-timing</i> . |                     |                    |                   |      |
| Analisis Keamanan | Status analisis keamanan ChaCha20                                                                                                                                                                                                                                  |                     |                    |                   |      |
|                   | Round                                                                                                                                                                                                                                                              | Tipe serangan       | Waktu              | Data              | Ref  |
|                   | 6                                                                                                                                                                                                                                                                  | Differential        | 2 <sup>139</sup>   | 2 <sup>30</sup>   | [20] |
|                   |                                                                                                                                                                                                                                                                    | Differential        | 2 <sup>136</sup>   | 2 <sup>28</sup>   | [21] |
|                   |                                                                                                                                                                                                                                                                    | Differential-linear | 2 <sup>130</sup>   | 2 <sup>25</sup>   | [22] |
|                   |                                                                                                                                                                                                                                                                    | Differential-linear | 2 <sup>127,5</sup> | 2 <sup>27,5</sup> | [22] |
|                   |                                                                                                                                                                                                                                                                    | Differential-linear | 2 <sup>102,2</sup> | 2 <sup>30</sup>   | [23] |
|                   |                                                                                                                                                                                                                                                                    | Differential-linear | 2 <sup>77,4</sup>  | 2 <sup>30</sup>   | [24] |
|                   | 7                                                                                                                                                                                                                                                                  | Differential        | 2 <sup>248</sup>   | 2 <sup>27</sup>   | [20] |
|                   |                                                                                                                                                                                                                                                                    | Differential        | 2 <sup>465,5</sup> | 2 <sup>27</sup>   | [21] |
|                   |                                                                                                                                                                                                                                                                    | Differential-linear | 2 <sup>242,6</sup> | 2 <sup>27</sup>   | [25] |
|                   |                                                                                                                                                                                                                                                                    | Differential        | 2 <sup>238,9</sup> | 2 <sup>69,6</sup> | [26] |
|                   |                                                                                                                                                                                                                                                                    | Differential-linear | 2 <sup>237,7</sup> | 2 <sup>96</sup>   | [22] |
|                   |                                                                                                                                                                                                                                                                    | Differential-linear | 2 <sup>231,9</sup> | 2 <sup>50</sup>   | [23] |
|                   |                                                                                                                                                                                                                                                                    | Differential        | 2 <sup>231,6</sup> | 2 <sup>49,6</sup> | [27] |
|                   |                                                                                                                                                                                                                                                                    | Differential-linear | 2 <sup>230,9</sup> | 2 <sup>48,8</sup> | [24] |
|                   |                                                                                                                                                                                                                                                                    |                     |                    |                   |      |

|                   |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |      |                     |             |            |            |
|-------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------|---------------------|-------------|------------|------------|
|                   |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |      | Differential-linear | $2^{228,5}$ | $2^{80,5}$ | [28]       |
|                   |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |      | Differential-linear | $2^{224}$   | $2^{224}$  | [25], [28] |
|                   |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               | 7,25 | Differential        | $2^{255,6}$ | $2^{37,5}$ | [27]       |
|                   |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |      | Differential        | $2^{244,2}$ | $2^{69,1}$ | [27]       |
| Analisis Performa | <p>Evaluasi eBASC [29] pada bulan Juni 2016, algoritma tersebut mencapai 1,2 <i>cycles</i>/byte pada prosesor Intel Core i5. Selain itu, berdasarkan hasil evaluasi proyek <i>Fair Evaluation of Lightweight Cryptographic Systems</i> [30] pada bulan Juni 2016, algoritma tersebut memerlukan 144 <i>cycles</i> untuk inisialisasi pada prosesor ARM Cortex-M3 dan memiliki <i>throughput</i> 54,3 <i>cycles</i>/byte</p>                                                                                                                                                                                                                                                                                                                                                   |      |                     |             |            |            |
| Digunakan pada    | <p>ChaCha20 umumnya dipasangkan dengan <i>message authentication code</i> (MAC) Poly-1305 untuk menyediakan enkripsi terotentikasi (<i>authenticated encryption</i>)</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |      |                     |             |            |            |
| Contoh Aplikasi   | <p>Protokol :</p> <ul style="list-style-type: none"> <li>• SSH, via <a href="mailto:chacha20-poly1305@openssh.com">chacha20-poly1305@openssh.com</a></li> <li>• QUIC — <i>a secure transport protocol</i></li> <li>• WireGuard — <i>fast, modern, secure VPN tunnel</i></li> </ul> <p>Jaringan :</p> <ul style="list-style-type: none"> <li>• Lightning Network</li> </ul> <p>Sistem Operasi :</p> <ul style="list-style-type: none"> <li>• OpenBSD — digunakan dalam pembangkitan bilangan acak, serta dalam OpenSSH, OpenSMTPD, OpenIKED, LibreSSL, and WireGuard</li> <li>• Linux — digunakan baik dalam pembangkitan bilangan acak maupun WireGuard</li> <li>• Dragonfly BSD — digunakan dalam pembangkitan bilangan acak dan OpenSSH</li> </ul> <p>Perangkat Keras :</p> |      |                     |             |            |            |

|                                 |                                                                                                                                                                                           |
|---------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|                                 | <ul style="list-style-type: none"> <li>PAx5 — Sebuah platform otomasi rumah yang dirancang agar aman, stabil, dan dapat diperluas (<i>ChaCha Usage &amp; Deployment</i>, 2025)</li> </ul> |
| Informasi<br><i>Open Source</i> | OpenSSL, Google Chrome, Mozilla Firefox, OpenSSH.<br><a href="https://ianix.com/pub/chacha-deployment.html">https://ianix.com/pub/chacha-deployment.html</a>                              |

## 2. Enocoro

|                              |                      |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |
|------------------------------|----------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Profil<br>Algoritma          | Nama                 | Enocoro                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |
|                              | Perancang            | Hitachi, Ltd.                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |
|                              | Publikasi            | 2008 (WAIS 2008), 2010 (ISITA 2010)                                                                                                                                                                                                                                                                                                                                                                                                                                               |
|                              | Standarisasi         | <ul style="list-style-type: none"> <li>CRYPTREC <i>Candidate Recommended Cipher</i> (Enocoro-128v2),</li> <li>ISO 29192-0033(Enocoro-80, Enocoro-128v2)</li> </ul>                                                                                                                                                                                                                                                                                                                |
| Karakteristik<br>kriptografi | Fitur                | Enocoro terdiri atas dua algoritma, yaitu Enocoro-80 dengan kunci 80 bit dan Enocoro-128v2 dengan kunci 128 bit. Keduanya diklaim memiliki tingkat keamanan sesuai panjang kunci, namun keluaran masing-masing dibatasi hingga $2^{32}$ byte dan $2^{64}$ byte dengan kunci dan IV tetap. Berbeda dari <i>lightweight stream cipher</i> pada umumnya, Enocoro memproses data dalam satuan 8 bit dan mampu mencapai kecepatan setara AES bahkan pada implementasi perangkat lunak. |
|                              | Analisis<br>Keamanan | Sejak diterbitkannya makalah analisis oleh Ding dkk. [31]                                                                                                                                                                                                                                                                                                                                                                                                                         |

|                   |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |
|-------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|                   | <p>mengenai serangan dengan <i>weak stubs</i>, sejumlah penelitian lanjutan juga dipublikasikan. Funabiki dkk. [32] mengusulkan <i>cube attack</i> berbasis MILP terhadap Enocoro-128v2. Hasilnya menunjukkan bahwa <i>identification attack</i> dapat dilakukan secara efisien pada 21 dari 96 <i>round</i> serta <i>recovery attack</i> dapat dilaksanakan dengan 120 kalkulasi dan <math>2^8</math> data untuk 11 <i>round</i> Enocoro-128v2. Shibayama dkk. [33] menganalisis struktur Enocoro-128v2 secara mendalam untuk mengidentifikasi sifat diferensial orde tinggi, dan menemukan sifat diferensial orde ke-16 pada 22 <i>round</i>. Dengan memanfaatkan sifat tersebut, Shibayama dkk membuktikan bahwa <i>identification attack</i> yang efisien dapat dilakukan terhadap 22 dari 96 <i>round</i> Enocoro-128v2.</p> |
| Analisis Performa | <p>Enocoro-80 [34]:<br/> Pada implementasi di Pentium 4, inisiasi memerlukan 1.335 <i>cycles</i> dengan <i>throughput</i> 27 <i>cycles/byte</i>. Pada implementasi <i>Application-Specific Integrated Circuit</i> (ASIC), ukuran sirkuitnya adalah 2,7K GE dengan kecepatan pemrosesan 2.197,6 Mbps (teknologi 180 nanometer (nm) dan frekuensi maksimal 274,7 MHz).<br/> Enocoro-128v2 [35]:</p>                                                                                                                                                                                                                                                                                                                                                                                                                                 |

|  |                                                                                                                                                                                                                                                                                     |
|--|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|  | Pada implementasi Intel Core2 Duo diperlukan 1.530 siklus untuk inisialisasi dengan <i>throughput</i> 14,8 <i>cycles/byte</i> . Pada implementasi ASIC, ukuran sirkuitnya adalah 2,4K GE dengan kecepatan pemrosesan 6.250 Mbps (teknologi 90 nm dan frekuensi maksimum 781,3 MHz). |
|--|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|

### 3. Grain v1

|                           |                   |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |
|---------------------------|-------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Profil Algoritma          | Nama              | Grain v1                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |
|                           | Perancang         | Martin Hell, Thomas Johansson (Lund University) Willi Meier (FH Aargau)                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |
|                           | Publikasi         | 2005 (eSTREAM Project)                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |
|                           | Standarisasi      | Grain-128a, yang merupakan <i>authenticated encryption</i> berbasis Grain v1, telah distandardisasi dalam ISO/IEC 29167-13:2015                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |
| Karakteristik kriptografi | Fitur             | Grain v1 adalah <i>lightweight stream cipher</i> berorientasi perangkat keras yang termasuk dalam portofolio eSTREAM, dengan dua varian, yaitu: kunci 80 bit dan IV 64 bit, serta kunci 128 bit dan IV 80 bit. Grain v1 menggunakan satu <i>bitwise linear feedback shift register</i> dan satu <i>non-linear feedback shift register</i> . Dibandingkan <i>lightweight stream cipher</i> lain, Grain v1 lebih unggul untuk implementasi perangkat keras <i>lightweight</i> , mendukung tingkat paralelisme tertentu, dan memiliki kinerja perangkat lunak yang memadai untuk penggunaan praktis. |
|                           | Analisis Keamanan | Berbain dkk. mengevaluasi Grain, pendahulu Grain v1, dan melaporkan                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |

|                   | <p>bahwa kunci rahasia 80-bit dapat dipulihkan menggunakan <i>keystream</i> sepanjang <math>2^{38}</math> bit dengan kompleksitas <math>2^{43}</math> [36]. Karena Grain v1 telah diperbarui berdasarkan temuan tersebut, serangan yang dilakukan Berbain dkk. tidak lagi dapat diterapkan secara langsung. Dinur dkk. menunjukkan bahwa Grain v1 dengan kunci 128-bit memiliki inisialisasi yang kurang memadai serta <i>weak keys</i> sebesar 118 bit [37]. Meskipun <i>weak keys</i> tersebut besar, tetapi <i>key recovery attack</i> tetap membutuhkan kompleksitas sekitar <math>2^{103}</math>. Berikut adalah status analisis keamanan Grain v1 setelah September 2021:</p> <table><tr><th>Rounds</th><th>Tipe serangan</th><th>Waktu</th><th>Data</th><th>Ref</th></tr><tr><td>160 (full)</td><td><i>Fast Near Collision</i></td><td><math>2^{86,1}</math></td><td><math>2^{19}</math></td><td>[38]</td></tr><tr><td>160 (full)</td><td><i>Fast Correlation</i></td><td><math>2^{76,7}</math></td><td><math>2^{75,1}</math></td><td>[39]</td></tr></table> | Rounds     | Tipe serangan | Waktu | Data | Ref | 160 (full) | <i>Fast Near Collision</i> | $2^{86,1}$ | $2^{19}$ | [38] | 160 (full) | <i>Fast Correlation</i> | $2^{76,7}$ | $2^{75,1}$ | [39] |
|-------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------|---------------|-------|------|-----|------------|----------------------------|------------|----------|------|------------|-------------------------|------------|------------|------|
| Rounds            | Tipe serangan                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       | Waktu      | Data          | Ref   |      |     |            |                            |            |          |      |            |                         |            |            |      |
| 160 (full)        | <i>Fast Near Collision</i>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          | $2^{86,1}$ | $2^{19}$      | [38]  |      |     |            |                            |            |          |      |            |                         |            |            |      |
| 160 (full)        | <i>Fast Correlation</i>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             | $2^{76,7}$ | $2^{75,1}$    | [39]  |      |     |            |                            |            |          |      |            |                         |            |            |      |
| Analisis Performa | <p>Good, dkk. [40] mengevaluasi kinerja implementasi perangkat keras Grain v1 menggunakan <i>standar cell library</i> 0,13<math>\mu</math>m.</p> <ul style="list-style-type: none"><li>Grain v1 80-bit: Ukuran sirkuit 1.294 GE, frekuensi operasi maksimum 724,6 MHz dengan <i>throughput</i> 724,6 Mbps. Grain v1 80 bit dirancang untuk mendukung hingga 16 <i>round</i> secara paralel</li><li>Grain v1 128-bit: Ukuran sirkuit 1.857 GE, frekuensi operasi maksimum 925,9 MHz dengan <i>throughput</i> 925,9 Mbps. Grain v1 128-bit dirancang untuk mendukung hingga 32 <i>round</i> secara paralel.</li></ul>                                                                                                                                                                                                                                                                                                                                                                                                                                                 |            |               |       |      |     |            |                            |            |          |      |            |                         |            |            |      |

#### 4. MICKEY 2.0

| Profil<br>Algoritma             | Nama                                                                                                                                                                                                                                                                                                                            | MICKEY 2.0                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |           |              |                |      |  |       |               |                |        |      |                |     |            |        |          |           |              |           |      |            |                    |          |          |        |          |      |            |                    |            |          |        |          |
|---------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------|--------------|----------------|------|--|-------|---------------|----------------|--------|------|----------------|-----|------------|--------|----------|-----------|--------------|-----------|------|------------|--------------------|----------|----------|--------|----------|------|------------|--------------------|------------|----------|--------|----------|
|                                 | Perancang                                                                                                                                                                                                                                                                                                                       | Steve Babbage (Vodafone), Matthew Dodd                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |           |              |                |      |  |       |               |                |        |      |                |     |            |        |          |           |              |           |      |            |                    |          |          |        |          |      |            |                    |            |          |        |          |
|                                 | Publikasi                                                                                                                                                                                                                                                                                                                       | 2005 (eSTREAM Project)                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |           |              |                |      |  |       |               |                |        |      |                |     |            |        |          |           |              |           |      |            |                    |          |          |        |          |      |            |                    |            |          |        |          |
|                                 | Standarisasi                                                                                                                                                                                                                                                                                                                    | -                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |           |              |                |      |  |       |               |                |        |      |                |     |            |        |          |           |              |           |      |            |                    |          |          |        |          |      |            |                    |            |          |        |          |
| Karakteristik<br>kriptografi    | Fitur                                                                                                                                                                                                                                                                                                                           | MICKEY 2.0 adalah <i>stream cipher</i> berorientasi perangkat keras yang ttermasuk dalam portofolio eSTREAM. MICKEY 2.0 menggunakan kunci 80 bit dan IV 80 bit, dengan jumlah IV per kunci tetap dibatasi hingga $2^{40}$ serta panjang maksimum <i>keystream</i> $2^{40}$ bit untuk setiap pasangan kunci dan IV. MICKEY 2.0 terdiri atas satu <i>linear feedback shift register</i> dan satu <i>non-linear feedback shift register</i> dengan mekanisme <i>clock control</i> tidak beraturan sehingga pemrosesan paralel sulit dilakukan karena mekanisme tersebut.                                                                                                                                                                                                                                                                    |           |              |                |      |  |       |               |                |        |      |                |     |            |        |          |           |              |           |      |            |                    |          |          |        |          |      |            |                    |            |          |        |          |
|                                 | Analisis<br>Keamanan                                                                                                                                                                                                                                                                                                            | Berikut adalah status analisis keamanan MICKEY 2.0 setelah September 2021: <table><tr><th>Round</th><th>Tipe serangan</th><th>Waktu (daring)</th><th>Memori</th><th>Data</th><th>Waktu (luring)</th><th>Ref</th></tr><tr><td>200 (full)</td><td>TMDTO*</td><td><math>2^{47}</math></td><td><math>2^{120}</math></td><td><math>2^{80}</math> bit</td><td><math>2^{120}</math></td><td>[41]</td></tr><tr><td>200 (full)</td><td>TMDTO (<math>m = 64</math>)</td><td><math>2^{78}</math></td><td><math>2^{45}</math></td><td>80 bit</td><td><math>2^{79}</math></td><td>[42]</td></tr><tr><td>200 (full)</td><td>TMDTO (<math>m = 79</math>)</td><td><math>2^{79,6}</math></td><td><math>2^{45}</math></td><td>80 bit</td><td><math>2^{79}</math></td><td>[42]</td></tr></table> <p>*) <i>Time-memory-data-trade-off attack</i> (TMDTO)</p> |           |              |                |      |  | Round | Tipe serangan | Waktu (daring) | Memori | Data | Waktu (luring) | Ref | 200 (full) | TMDTO* | $2^{47}$ | $2^{120}$ | $2^{80}$ bit | $2^{120}$ | [41] | 200 (full) | TMDTO ( $m = 64$ ) | $2^{78}$ | $2^{45}$ | 80 bit | $2^{79}$ | [42] | 200 (full) | TMDTO ( $m = 79$ ) | $2^{79,6}$ | $2^{45}$ | 80 bit | $2^{79}$ |
| Round                           | Tipe serangan                                                                                                                                                                                                                                                                                                                   | Waktu (daring)                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           | Memori    | Data         | Waktu (luring) | Ref  |  |       |               |                |        |      |                |     |            |        |          |           |              |           |      |            |                    |          |          |        |          |      |            |                    |            |          |        |          |
| 200 (full)                      | TMDTO*                                                                                                                                                                                                                                                                                                                          | $2^{47}$                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 | $2^{120}$ | $2^{80}$ bit | $2^{120}$      | [41] |  |       |               |                |        |      |                |     |            |        |          |           |              |           |      |            |                    |          |          |        |          |      |            |                    |            |          |        |          |
| 200 (full)                      | TMDTO ( $m = 64$ )                                                                                                                                                                                                                                                                                                              | $2^{78}$                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 | $2^{45}$  | 80 bit       | $2^{79}$       | [42] |  |       |               |                |        |      |                |     |            |        |          |           |              |           |      |            |                    |          |          |        |          |      |            |                    |            |          |        |          |
| 200 (full)                      | TMDTO ( $m = 79$ )                                                                                                                                                                                                                                                                                                              | $2^{79,6}$                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               | $2^{45}$  | 80 bit       | $2^{79}$       | [42] |  |       |               |                |        |      |                |     |            |        |          |           |              |           |      |            |                    |          |          |        |          |      |            |                    |            |          |        |          |
| Analisis<br>Performa            | Good, dkk. [40] memberikan evaluasi terperinci tentang kinerja implementasi perangkat keras MICKEY 2.0. Evaluasi ini menggunakan perpustakaan sel standar 0,13 $\mu\text{m}$ . MICKEY 2.0 memiliki ukuran sirkuit 3.188 GE, frekuensi operasi maksimum 454,5 MHz, dan throughput 454,5 Mbps.                                    |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |           |              |                |      |  |       |               |                |        |      |                |     |            |        |          |           |              |           |      |            |                    |          |          |        |          |      |            |                    |            |          |        |          |
| Informasi<br><i>Open Source</i> | Kode yang dikembangkan perancang tersedia bebas di <a href="http://www.ecrypt.eu.org/stream/p3ciphers/mickey/mickey_p3source.zip">http://www.ecrypt.eu.org/stream/p3ciphers/mickey/mickey_p3source.zip</a> . Beberapa peneliti telah mengimplementasikan MICKEY 2.0, namun ketersediaan kode sumber terbuka belum terkonfirmasi |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |           |              |                |      |  |       |               |                |        |      |                |     |            |        |          |           |              |           |      |            |                    |          |          |        |          |      |            |                    |            |          |        |          |

## 5. Trivium

|                           |                   |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |
|---------------------------|-------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Profil<br>Algoritma       | Nama              | Trivium                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |
|                           | Perancang         | Christophe De Canni`ere, Bart Preneel<br>(Katholieke Universiteit Leuven)                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |
|                           | Publikasi         | 2005 (eSTREAM Project)                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |
|                           | Standarisasi      | ISO/IEC 29192-3                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |
| Karakteristik kriptografi | Fitur             | Trivium adalah <i>stream cipher</i> berorientasi perangkat keras yang termasuk dalam portofolio eSTREAM. Trivium menggunakan kunci 80 bit dan IV 80 bit, dengan panjang <i>keystream</i> untuk setiap pasangan kunci dan IV dibatasi hingga $2^{64}$ bit. Desainnya terdiri atas tiga <i>non-linear feedback shift register</i> berurutan dengan panjang berbeda. Berbasis operasi bit dan mendukung tingkat paralelisme tinggi, Trivium cocok untuk implementasi perangkat keras <i>lightweight</i> dan memiliki kecepatan tinggi pada implementasi perangkat lunak. Namun, Trivium kurang sesuai untuk pemrosesan data pendek karena membutuhkan waktu inisialisasi yang panjang. |
|                           | Analisis Keamanan | Hingga tahun 2016, belum ditemukan serangan yang mengancam keamanan Trivium. Maximov dkk. melaporkan bahwa internal <i>state</i> dapat dipulihkan dari <i>keystream</i> sepanjang $2^{61,5}$ bit dengan kompleksitas setara <i>exhaustive search</i> $2^{89,5}$ [43]. Sementara itu, Fouque dkk.                                                                                                                                                                                                                                                                                                                                                                                    |

|       |               | <p>melakukan <i>cube attacks</i> pada tahap inisialisasi Trivium melaporkan bahwa kunci dapat dipulihkan hingga 799 dari 1.152 langkah menggunakan <math>2^{40}</math> IV (beserta <i>keystream</i>-nya) dengan <i>exhaustive search</i> <math>2^{62}</math> [44].</p> <p>Berikut adalah status analisis keamanan Trivium setelah September 2021:</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |            |               |       |      |     |     |      |          |          |      |     |      |          |          |              |     |      |          |          |      |     |       |          |   |          |     |        |          |   |          |     |      |            |          |          |     |      |            |            |      |     |      |            |          |      |     |      |            |          |      |     |      |          |          |      |     |      |            |          |      |     |      |          |          |      |     |      |            |          |      |     |      |          |          |      |     |      |          |          |      |     |      |          |          |      |     |         |          |   |      |
|-------|---------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------|---------------|-------|------|-----|-----|------|----------|----------|------|-----|------|----------|----------|--------------|-----|------|----------|----------|------|-----|-------|----------|---|----------|-----|--------|----------|---|----------|-----|------|------------|----------|----------|-----|------|------------|------------|------|-----|------|------------|----------|------|-----|------|------------|----------|------|-----|------|----------|----------|------|-----|------|------------|----------|------|-----|------|----------|----------|------|-----|------|------------|----------|------|-----|------|----------|----------|------|-----|------|----------|----------|------|-----|------|----------|----------|------|-----|---------|----------|---|------|
|       |               | <table><tr><th>Round</th><th>Tipe serangan</th><th>Waktu</th><th>Data</th><th>Ref</th></tr><tr><td>799</td><td>Cube</td><td><math>2^{62}</math></td><td><math>2^{38}</math></td><td>[44]</td></tr><tr><td>832</td><td>Cube</td><td><math>2^{79}</math></td><td><math>2^{72}</math></td><td>[45, 46, 47]</td></tr><tr><td>835</td><td>Cube</td><td><math>2^{75}</math></td><td><math>2^{35}</math></td><td>[48]</td></tr><tr><td>836</td><td>Cube*</td><td><math>2^{79}</math></td><td>-</td><td>[49, 50]</td></tr><tr><td>839</td><td>Cube**</td><td><math>2^{79}</math></td><td>-</td><td>[49, 50]</td></tr><tr><td>840</td><td>Cube</td><td><math>2^{79,6}</math></td><td><math>2^{78}</math></td><td>[51, 52]</td></tr><tr><td>840</td><td>Cube</td><td><math>2^{77,8}</math></td><td><math>2^{76,6}</math></td><td>[53]</td></tr><tr><td>840</td><td>Cube</td><td><math>2^{76,3}</math></td><td><math>2^{62}</math></td><td>[54]</td></tr><tr><td>841</td><td>Cube</td><td><math>2^{78,6}</math></td><td><math>2^{77}</math></td><td>[53]</td></tr><tr><td>841</td><td>Cube</td><td><math>2^{78}</math></td><td><math>2^{56}</math></td><td>[54]</td></tr><tr><td>842</td><td>Cube</td><td><math>2^{78,6}</math></td><td><math>2^{77}</math></td><td>[53]</td></tr><tr><td>842</td><td>Cube</td><td><math>2^{78}</math></td><td><math>2^{56}</math></td><td>[54]</td></tr><tr><td>843</td><td>Cube</td><td><math>2^{79,6}</math></td><td><math>2^{78}</math></td><td>[55]</td></tr><tr><td>843</td><td>Cube</td><td><math>2^{77}</math></td><td><math>2^{56}</math></td><td>[54]</td></tr><tr><td>844</td><td>Cube</td><td><math>2^{79}</math></td><td><math>2^{56}</math></td><td>[54]</td></tr><tr><td>845</td><td>Cube</td><td><math>2^{79}</math></td><td><math>2^{56}</math></td><td>[54]</td></tr><tr><td>855</td><td>Cube **</td><td><math>2^{77}</math></td><td>-</td><td>[56]</td></tr></table> | Round      | Tipe serangan | Waktu | Data | Ref | 799 | Cube | $2^{62}$ | $2^{38}$ | [44] | 832 | Cube | $2^{79}$ | $2^{72}$ | [45, 46, 47] | 835 | Cube | $2^{75}$ | $2^{35}$ | [48] | 836 | Cube* | $2^{79}$ | - | [49, 50] | 839 | Cube** | $2^{79}$ | - | [49, 50] | 840 | Cube | $2^{79,6}$ | $2^{78}$ | [51, 52] | 840 | Cube | $2^{77,8}$ | $2^{76,6}$ | [53] | 840 | Cube | $2^{76,3}$ | $2^{62}$ | [54] | 841 | Cube | $2^{78,6}$ | $2^{77}$ | [53] | 841 | Cube | $2^{78}$ | $2^{56}$ | [54] | 842 | Cube | $2^{78,6}$ | $2^{77}$ | [53] | 842 | Cube | $2^{78}$ | $2^{56}$ | [54] | 843 | Cube | $2^{79,6}$ | $2^{78}$ | [55] | 843 | Cube | $2^{77}$ | $2^{56}$ | [54] | 844 | Cube | $2^{79}$ | $2^{56}$ | [54] | 845 | Cube | $2^{79}$ | $2^{56}$ | [54] | 855 | Cube ** | $2^{77}$ | - | [56] |
| Round | Tipe serangan | Waktu                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        | Data       | Ref           |       |      |     |     |      |          |          |      |     |      |          |          |              |     |      |          |          |      |     |       |          |   |          |     |        |          |   |          |     |      |            |          |          |     |      |            |            |      |     |      |            |          |      |     |      |            |          |      |     |      |          |          |      |     |      |            |          |      |     |      |          |          |      |     |      |            |          |      |     |      |          |          |      |     |      |          |          |      |     |      |          |          |      |     |         |          |   |      |
| 799   | Cube          | $2^{62}$                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     | $2^{38}$   | [44]          |       |      |     |     |      |          |          |      |     |      |          |          |              |     |      |          |          |      |     |       |          |   |          |     |        |          |   |          |     |      |            |          |          |     |      |            |            |      |     |      |            |          |      |     |      |            |          |      |     |      |          |          |      |     |      |            |          |      |     |      |          |          |      |     |      |            |          |      |     |      |          |          |      |     |      |          |          |      |     |      |          |          |      |     |         |          |   |      |
| 832   | Cube          | $2^{79}$                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     | $2^{72}$   | [45, 46, 47]  |       |      |     |     |      |          |          |      |     |      |          |          |              |     |      |          |          |      |     |       |          |   |          |     |        |          |   |          |     |      |            |          |          |     |      |            |            |      |     |      |            |          |      |     |      |            |          |      |     |      |          |          |      |     |      |            |          |      |     |      |          |          |      |     |      |            |          |      |     |      |          |          |      |     |      |          |          |      |     |      |          |          |      |     |         |          |   |      |
| 835   | Cube          | $2^{75}$                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     | $2^{35}$   | [48]          |       |      |     |     |      |          |          |      |     |      |          |          |              |     |      |          |          |      |     |       |          |   |          |     |        |          |   |          |     |      |            |          |          |     |      |            |            |      |     |      |            |          |      |     |      |            |          |      |     |      |          |          |      |     |      |            |          |      |     |      |          |          |      |     |      |            |          |      |     |      |          |          |      |     |      |          |          |      |     |      |          |          |      |     |         |          |   |      |
| 836   | Cube*         | $2^{79}$                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     | -          | [49, 50]      |       |      |     |     |      |          |          |      |     |      |          |          |              |     |      |          |          |      |     |       |          |   |          |     |        |          |   |          |     |      |            |          |          |     |      |            |            |      |     |      |            |          |      |     |      |            |          |      |     |      |          |          |      |     |      |            |          |      |     |      |          |          |      |     |      |            |          |      |     |      |          |          |      |     |      |          |          |      |     |      |          |          |      |     |         |          |   |      |
| 839   | Cube**        | $2^{79}$                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     | -          | [49, 50]      |       |      |     |     |      |          |          |      |     |      |          |          |              |     |      |          |          |      |     |       |          |   |          |     |        |          |   |          |     |      |            |          |          |     |      |            |            |      |     |      |            |          |      |     |      |            |          |      |     |      |          |          |      |     |      |            |          |      |     |      |          |          |      |     |      |            |          |      |     |      |          |          |      |     |      |          |          |      |     |      |          |          |      |     |         |          |   |      |
| 840   | Cube          | $2^{79,6}$                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   | $2^{78}$   | [51, 52]      |       |      |     |     |      |          |          |      |     |      |          |          |              |     |      |          |          |      |     |       |          |   |          |     |        |          |   |          |     |      |            |          |          |     |      |            |            |      |     |      |            |          |      |     |      |            |          |      |     |      |          |          |      |     |      |            |          |      |     |      |          |          |      |     |      |            |          |      |     |      |          |          |      |     |      |          |          |      |     |      |          |          |      |     |         |          |   |      |
| 840   | Cube          | $2^{77,8}$                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   | $2^{76,6}$ | [53]          |       |      |     |     |      |          |          |      |     |      |          |          |              |     |      |          |          |      |     |       |          |   |          |     |        |          |   |          |     |      |            |          |          |     |      |            |            |      |     |      |            |          |      |     |      |            |          |      |     |      |          |          |      |     |      |            |          |      |     |      |          |          |      |     |      |            |          |      |     |      |          |          |      |     |      |          |          |      |     |      |          |          |      |     |         |          |   |      |
| 840   | Cube          | $2^{76,3}$                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   | $2^{62}$   | [54]          |       |      |     |     |      |          |          |      |     |      |          |          |              |     |      |          |          |      |     |       |          |   |          |     |        |          |   |          |     |      |            |          |          |     |      |            |            |      |     |      |            |          |      |     |      |            |          |      |     |      |          |          |      |     |      |            |          |      |     |      |          |          |      |     |      |            |          |      |     |      |          |          |      |     |      |          |          |      |     |      |          |          |      |     |         |          |   |      |
| 841   | Cube          | $2^{78,6}$                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   | $2^{77}$   | [53]          |       |      |     |     |      |          |          |      |     |      |          |          |              |     |      |          |          |      |     |       |          |   |          |     |        |          |   |          |     |      |            |          |          |     |      |            |            |      |     |      |            |          |      |     |      |            |          |      |     |      |          |          |      |     |      |            |          |      |     |      |          |          |      |     |      |            |          |      |     |      |          |          |      |     |      |          |          |      |     |      |          |          |      |     |         |          |   |      |
| 841   | Cube          | $2^{78}$                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     | $2^{56}$   | [54]          |       |      |     |     |      |          |          |      |     |      |          |          |              |     |      |          |          |      |     |       |          |   |          |     |        |          |   |          |     |      |            |          |          |     |      |            |            |      |     |      |            |          |      |     |      |            |          |      |     |      |          |          |      |     |      |            |          |      |     |      |          |          |      |     |      |            |          |      |     |      |          |          |      |     |      |          |          |      |     |      |          |          |      |     |         |          |   |      |
| 842   | Cube          | $2^{78,6}$                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   | $2^{77}$   | [53]          |       |      |     |     |      |          |          |      |     |      |          |          |              |     |      |          |          |      |     |       |          |   |          |     |        |          |   |          |     |      |            |          |          |     |      |            |            |      |     |      |            |          |      |     |      |            |          |      |     |      |          |          |      |     |      |            |          |      |     |      |          |          |      |     |      |            |          |      |     |      |          |          |      |     |      |          |          |      |     |      |          |          |      |     |         |          |   |      |
| 842   | Cube          | $2^{78}$                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     | $2^{56}$   | [54]          |       |      |     |     |      |          |          |      |     |      |          |          |              |     |      |          |          |      |     |       |          |   |          |     |        |          |   |          |     |      |            |          |          |     |      |            |            |      |     |      |            |          |      |     |      |            |          |      |     |      |          |          |      |     |      |            |          |      |     |      |          |          |      |     |      |            |          |      |     |      |          |          |      |     |      |          |          |      |     |      |          |          |      |     |         |          |   |      |
| 843   | Cube          | $2^{79,6}$                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   | $2^{78}$   | [55]          |       |      |     |     |      |          |          |      |     |      |          |          |              |     |      |          |          |      |     |       |          |   |          |     |        |          |   |          |     |      |            |          |          |     |      |            |            |      |     |      |            |          |      |     |      |            |          |      |     |      |          |          |      |     |      |            |          |      |     |      |          |          |      |     |      |            |          |      |     |      |          |          |      |     |      |          |          |      |     |      |          |          |      |     |         |          |   |      |
| 843   | Cube          | $2^{77}$                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     | $2^{56}$   | [54]          |       |      |     |     |      |          |          |      |     |      |          |          |              |     |      |          |          |      |     |       |          |   |          |     |        |          |   |          |     |      |            |          |          |     |      |            |            |      |     |      |            |          |      |     |      |            |          |      |     |      |          |          |      |     |      |            |          |      |     |      |          |          |      |     |      |            |          |      |     |      |          |          |      |     |      |          |          |      |     |      |          |          |      |     |         |          |   |      |
| 844   | Cube          | $2^{79}$                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     | $2^{56}$   | [54]          |       |      |     |     |      |          |          |      |     |      |          |          |              |     |      |          |          |      |     |       |          |   |          |     |        |          |   |          |     |      |            |          |          |     |      |            |            |      |     |      |            |          |      |     |      |            |          |      |     |      |          |          |      |     |      |            |          |      |     |      |          |          |      |     |      |            |          |      |     |      |          |          |      |     |      |          |          |      |     |      |          |          |      |     |         |          |   |      |
| 845   | Cube          | $2^{79}$                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     | $2^{56}$   | [54]          |       |      |     |     |      |          |          |      |     |      |          |          |              |     |      |          |          |      |     |       |          |   |          |     |        |          |   |          |     |      |            |          |          |     |      |            |            |      |     |      |            |          |      |     |      |            |          |      |     |      |          |          |      |     |      |            |          |      |     |      |          |          |      |     |      |            |          |      |     |      |          |          |      |     |      |          |          |      |     |      |          |          |      |     |         |          |   |      |
| 855   | Cube **       | $2^{77}$                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     | -          | [56]          |       |      |     |     |      |          |          |      |     |      |          |          |              |     |      |          |          |      |     |       |          |   |          |     |        |          |   |          |     |      |            |          |          |     |      |            |            |      |     |      |            |          |      |     |      |            |          |      |     |      |          |          |      |     |      |            |          |      |     |      |          |          |      |     |      |            |          |      |     |      |          |          |      |     |      |          |          |      |     |      |          |          |      |     |         |          |   |      |

|                   |                 |                                                                                                                                                                                                                                                                                                                                                                                                    |
|-------------------|-----------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|                   |                 | <p>* Serangan tidak berhasil karena adanya kekeliruan dalam degenerasi menjadi distinguisher, sebagaimana ditunjukkan dalam [57,58].</p> <p>** Serangan tidak berhasil karena adanya kekeliruan dalam estimasi derajat, sebagaimana ditunjukkan dalam [51, 52].</p>                                                                                                                                |
| Analisis Performa | Perangkat Keras | Good dkk. [40] mengevaluasi kinerja implementasi perangkat keras Trivium menggunakan <i>standard cell library</i> 0,13 $\mu\text{m}$ . Trivium memiliki ukuran sirkuit 2.580 GE, frekuensi operasi maksimum 327,9 MHz, dan <i>throughput</i> 327,9 Mbps. Dengan konfigurasi paralel hingga 64 <i>state bit</i> , ukuran sirkuit meningkat menjadi 4.921 GE dengan <i>throughput</i> 22.299,6 Mbps. |
|                   | Perangkat Lunak | Implementasi perangkat lunak dievaluasi melalui FELICS [30]. Pada ARM Cortex-M3, <i>throughput</i> mencapai 49,4 <i>cycles/byte</i> lebih cepat dibandingkan ChaCha20. Namun, Trivium kurang sesuai untuk pemrosesan data pendek karena memerlukan inisialisasi sepanjang 7.195 <i>cycles</i> .                                                                                                    |

## B. *Lightweight Block Cipher*

Subbab ini berisi ringkasan algoritma *lightweight block cipher* yang terdapat dalam dokumen CRYPTREC *Cryptographic Technology Guideline - Lightweight Cryptography* [16] dan CRYPTREC *Cryptographic Technology Guideline (Lightweight Cryptography) 2023 Edition* [17] yang diterbitkan oleh CRYPTREC *Lightweight Cryptography Working Group*.

Ringkasan tersebut berisi informasi tentang profil algoritma, fitur, analisis keamanan, analisis performa pada perangkat keras dan/atau perangkat lunak, standardisasi dan informasi *open source* dari algoritma tersebut. Algoritma *lightweight block cipher* yang terdapat dalam subbab ini adalah CLEFIA, LED, LEA, Midori, Piccolo, PRESENT, PRINCE, SIMON, SPECK dan TWINE.

## 1. CLEFIA

|                   |                                                                                                                                                                                        |                                                                                                                                         |                                |                  |                 |            |      |
|-------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------|--------------------------------|------------------|-----------------|------------|------|
| Profil Algoritma  | Nama                                                                                                                                                                                   | CLEFIA                                                                                                                                  |                                |                  |                 |            |      |
|                   | Perancang                                                                                                                                                                              | Taizo Shirai, Kyoji Shiutani, Toru Akishita, Shibo Morial (Sony Corporation Japan), Tetsu Iwata (Nagoya University, Japan)              |                                |                  |                 |            |      |
|                   | Publikasi                                                                                                                                                                              | 2007 (FSE 2007)                                                                                                                         |                                |                  |                 |            |      |
|                   | Spesifikasi                                                                                                                                                                            | <a href="http://www.sony.net/Products/cryptography/clefia/">http://www.sony.net/Products/cryptography/clefia/</a> (Shirai et al., 2007) |                                |                  |                 |            |      |
| Fitur             | Perancang mengklaim bahwa algoritma CLEFIA memiliki performa tinggi baik pada implementasi perangkat lunak dan perangkat <i>keras</i> . CLEFIA memiliki fitur yang identik dengan AES. |                                                                                                                                         |                                |                  |                 |            |      |
|                   | Struktur                                                                                                                                                                               | GFN (4-line Type II Generalized Feistel Network)                                                                                        |                                |                  |                 |            |      |
|                   | Panjang blok (bit)                                                                                                                                                                     | 128                                                                                                                                     |                                |                  |                 |            |      |
|                   | Panjang kunci (bit)                                                                                                                                                                    | 128 (CLEFIA-128)                                                                                                                        | 192 (CLEFIA-192)               | 256 (CLEFIA-256) |                 |            |      |
|                   | Jumlah round                                                                                                                                                                           | 18                                                                                                                                      | 22                             | 26               |                 |            |      |
| Analisis keamanan | Status analisis keamanan CLEFIA ( <i>CPs: chosen plaintext, KPs: known plaintext</i> ) setelah September 2021:                                                                         |                                                                                                                                         |                                |                  |                 |            |      |
|                   | Algoritma                                                                                                                                                                              | Round yang dapat diserang                                                                                                               | Tipe                           | Waktu            | Data            | Memo ri    | Ref  |
|                   | CLEFIA-128                                                                                                                                                                             | 12                                                                                                                                      | <i>Integral</i>                | $2^{116,7}$      | $2^{113,0}$ CPs | N/A        | [59] |
|                   |                                                                                                                                                                                        | 13                                                                                                                                      | <i>Impossible Differential</i> | $2^{121,2}$      | $2^{117,8}$ CPs | $2^{86,8}$ | [60] |

|            |    |                                |             |                    |             |      |
|------------|----|--------------------------------|-------------|--------------------|-------------|------|
|            | 13 | <i>Impossible Differential</i> | $2^{114,6}$ | $2^{116,2}$<br>CPs | $2^{83,2}$  | [61] |
|            | 13 | <i>Truncated Differential</i>  | $2^{99,0}$  | $2^{99,0}$<br>CPs  | $2^{80,0}$  | [62] |
|            | 14 | <i>Truncated Differential</i>  | $2^{108,0}$ | $2^{100,0}$<br>CPs | $2^{101,3}$ | [62] |
| CLEFIA-192 | 13 | <i>Impossible Differential</i> | $2^{146,0}$ | $2^{119,8}$<br>CPs | $2^{120,0}$ | [63] |
|            | 13 | <i>Integral</i>                | $2^{180,5}$ | $2^{113,0}$<br>CPs | N/A         | [59] |
|            | 14 | <i>Zero-correlation Linear</i> | $2^{180,2}$ | $2^{127,5}$<br>KPs | $2^{115,0}$ | [64] |
|            | 14 | <i>Impossible Differential</i> | $2^{177,6}$ | $2^{118,9}$<br>CPs | N/A         | [65] |
|            | 14 | <i>Zero-correlation Linear</i> | $2^{173,9}$ | $2^{124,5}$<br>KPs | N/A         | [66] |
|            | 14 | <i>Integral</i>                | $2^{166,7}$ | $2^{128,0}$<br>CPs | N/A         | [66] |
|            | 14 | <i>Truncated Differential</i>  | $2^{135,0}$ | $2^{100,0}$<br>CPs | $2^{131,0}$ | [62] |
| CLEFIA-256 | 14 | <i>Impossible Differential</i> | $2^{212,0}$ | $2^{120,3}$<br>CPs | $2^{121,0}$ | [63] |
|            | 14 | <i>Integral</i>                | $2^{244,5}$ | $2^{113,0}$<br>CPs | N/A         | [59] |
|            | 15 | <i>Zero-correlation Linear</i> | $2^{244,2}$ | $2^{127,5}$<br>KPs | $2^{115,0}$ | [64] |
|            | 15 | <i>Impossible Differential</i> | $2^{242,1}$ | $2^{119,3}$<br>CPs | N/A         | [65] |
|            | 15 | <i>Zero-correlation Linear</i> | $2^{237,9}$ | $2^{124,5}$<br>KPs | N/A         | [66] |
|            | 15 | <i>Integral</i>                | $2^{230,7}$ | $2^{128,0}$<br>CPs | N/A         | [66] |
|            | 15 | <i>Truncated Differential</i>  | $2^{203,0}$ | $2^{100,0}$<br>CPs | $2^{139,0}$ | [62] |

Berdasarkan hasil kajian pada tabel di atas meskipun berbagai penelitian kriptanalisis telah dilakukan, hingga saat ini tidak terdapat serangan yang lebih efisien dibandingkan *exhaustive search* terhadap

|                      | <p>kunci rahasia tanpa memandang jumlah <i>round</i> yang digunakan. Serangan paling efektif yang diketahui adalah serangan <i>truncated differential</i> yang diusulkan oleh Li dkk. [62] pada tahun 2015, yang menyederhanakan algoritma CLEFIA menjadi 14 round. Varian CLEFIA-128, CLEFIA-192, dan CLEFIA-256 masing-masing disederhanakan menjadi 14 dan 15 round. Penyederhanaan ini memungkinkan serangan pemulihan kunci dilakukan dengan efisiensi yang lebih tinggi dibandingkan <i>exhaustive search</i> terhadap kunci rahasia.</p>                                                                                                                                                                                                                                                                                                                          |              |                            |              |                            |     |                  |       |     |    |      |                      |       |         |       |                      |       |    |       |      |           |            |            |                       |          |     |            |       |    |                |      |      |            |       |    |             |      |
|----------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------|----------------------------|--------------|----------------------------|-----|------------------|-------|-----|----|------|----------------------|-------|---------|-------|----------------------|-------|----|-------|------|-----------|------------|------------|-----------------------|----------|-----|------------|-------|----|----------------|------|------|------------|-------|----|-------------|------|
| Analisis Performa    | <p>Hasil evaluasi implementasi perangkat keras:</p> <table><tr><th>Algoritma</th><th>Area (GE)</th><th>Cycles/block</th><th>Throughput @ 100kHz (kbps)</th><th>Ref</th></tr><tr><td>CLEFIA-128 (Enc)</td><td>2.488</td><td>328</td><td>39</td><td rowspan="2">[67]</td></tr><tr><td>CLEFIA-192 (Enc/Dec)</td><td>2.604</td><td>328/320</td><td>39/40</td></tr><tr><td>CLEFIA-256 (Enc/Dec)</td><td>5.979</td><td>18</td><td>711,1</td><td>[69]</td></tr></table> <p>Hasil evaluasi implementasi perangkat lunak:</p> <table><tr><th>Algoritma</th><th>ROM (byte)</th><th>RAM (byte)</th><th>Cycles/byte (Enc/Dec)</th><th>Platform</th><th>Ref</th></tr><tr><td>CLEFIA-128</td><td>1.309</td><td>78</td><td>39.357/152.023</td><td>RL78</td><td rowspan="2">[69]</td></tr><tr><td>CLEFIA-128</td><td>2.025</td><td>64</td><td>4.337/4.477</td><td>RL78</td></tr></table> | Algoritma    | Area (GE)                  | Cycles/block | Throughput @ 100kHz (kbps) | Ref | CLEFIA-128 (Enc) | 2.488 | 328 | 39 | [67] | CLEFIA-192 (Enc/Dec) | 2.604 | 328/320 | 39/40 | CLEFIA-256 (Enc/Dec) | 5.979 | 18 | 711,1 | [69] | Algoritma | ROM (byte) | RAM (byte) | Cycles/byte (Enc/Dec) | Platform | Ref | CLEFIA-128 | 1.309 | 78 | 39.357/152.023 | RL78 | [69] | CLEFIA-128 | 2.025 | 64 | 4.337/4.477 | RL78 |
| Algoritma            | Area (GE)                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                | Cycles/block | Throughput @ 100kHz (kbps) | Ref          |                            |     |                  |       |     |    |      |                      |       |         |       |                      |       |    |       |      |           |            |            |                       |          |     |            |       |    |                |      |      |            |       |    |             |      |
| CLEFIA-128 (Enc)     | 2.488                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    | 328          | 39                         | [67]         |                            |     |                  |       |     |    |      |                      |       |         |       |                      |       |    |       |      |           |            |            |                       |          |     |            |       |    |                |      |      |            |       |    |             |      |
| CLEFIA-192 (Enc/Dec) | 2.604                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    | 328/320      | 39/40                      |              |                            |     |                  |       |     |    |      |                      |       |         |       |                      |       |    |       |      |           |            |            |                       |          |     |            |       |    |                |      |      |            |       |    |             |      |
| CLEFIA-256 (Enc/Dec) | 5.979                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    | 18           | 711,1                      | [69]         |                            |     |                  |       |     |    |      |                      |       |         |       |                      |       |    |       |      |           |            |            |                       |          |     |            |       |    |                |      |      |            |       |    |             |      |
| Algoritma            | ROM (byte)                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               | RAM (byte)   | Cycles/byte (Enc/Dec)      | Platform     | Ref                        |     |                  |       |     |    |      |                      |       |         |       |                      |       |    |       |      |           |            |            |                       |          |     |            |       |    |                |      |      |            |       |    |             |      |
| CLEFIA-128           | 1.309                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    | 78           | 39.357/152.023             | RL78         | [69]                       |     |                  |       |     |    |      |                      |       |         |       |                      |       |    |       |      |           |            |            |                       |          |     |            |       |    |                |      |      |            |       |    |             |      |
| CLEFIA-128           | 2.025                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    | 64           | 4.337/4.477                | RL78         |                            |     |                  |       |     |    |      |                      |       |         |       |                      |       |    |       |      |           |            |            |                       |          |     |            |       |    |                |      |      |            |       |    |             |      |
| Standarisasi         | ISO/IEC 29192-2 [5], IETF RFC 6114 [82]                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |              |                            |              |                            |     |                  |       |     |    |      |                      |       |         |       |                      |       |    |       |      |           |            |            |                       |          |     |            |       |    |                |      |      |            |       |    |             |      |

## 2. LED

|                  |             |                                                                                                            |
|------------------|-------------|------------------------------------------------------------------------------------------------------------|
| Profil Algoritma | Nama        | LED                                                                                                        |
|                  | Perancang   | Jian Guo (Institute for Infocomm Research, Singapore), Thomas Peyrin, Axel Poschmann (Nanyang Technologic) |
|                  | Publikasi   | 2011 (CHES 2011 [70])                                                                                      |
|                  | Spesifikasi | <a href="http://led.crypto.sg/home-1">http://led.crypto.sg/home-1</a>                                      |

|                     |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |                            |             |                |                    |      |        |                     |                |                  |                           |                      |                       |            |      |   |                            |            |                |            |      |   |                           |            |                |            |      |   |                           |          |                |            |      |   |                            |            |                |            |      |   |                |            |              |            |      |         |   |                           |             |                |            |      |   |                     |            |                |            |      |   |               |            |              |            |      |   |               |            |              |            |      |   |                |            |              |            |      |   |                |            |              |            |      |
|---------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------|-------------|----------------|--------------------|------|--------|---------------------|----------------|------------------|---------------------------|----------------------|-----------------------|------------|------|---|----------------------------|------------|----------------|------------|------|---|---------------------------|------------|----------------|------------|------|---|---------------------------|----------|----------------|------------|------|---|----------------------------|------------|----------------|------------|------|---|----------------|------------|--------------|------------|------|---------|---|---------------------------|-------------|----------------|------------|------|---|---------------------|------------|----------------|------------|------|---|---------------|------------|--------------|------------|------|---|---------------|------------|--------------|------------|------|---|----------------|------------|--------------|------------|------|---|----------------|------------|--------------|------------|------|
| Fitur               | <p>Perancang mengklaim bahwa algoritma LED memiliki kinerja implementasi perangkat lunak yang memadai dan menghilangkan penjadwalan kunci (<i>key scheduling</i>), tahan terhadap <i>related-key attacks</i>, dan disesuaikan untuk implementasi perangkat keras <i>lightweight</i>. Mirip dengan fungsi hash <i>lightweight</i> PHOTON, algoritma LED memiliki MDS serial sebagai struktur internal.</p> <table><tr><td>Struktur</td><td colspan="2">SPN</td></tr><tr><td>Panjang blok (bit)</td><td colspan="2">64</td></tr><tr><td>Panjang kunci (bit)</td><td>64<br/>(LED-64)</td><td>128<br/>(LED-128)</td></tr><tr><td>Jumlah <i>round</i></td><td>32 (8 <i>steps</i>)</td><td>48 (12 <i>steps</i>)</td></tr></table>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         | Struktur                   | SPN         |                | Panjang blok (bit) | 64   |        | Panjang kunci (bit) | 64<br>(LED-64) | 128<br>(LED-128) | Jumlah <i>round</i>       | 32 (8 <i>steps</i> ) | 48 (12 <i>steps</i> ) |            |      |   |                            |            |                |            |      |   |                           |            |                |            |      |   |                           |          |                |            |      |   |                            |            |                |            |      |   |                |            |              |            |      |         |   |                           |             |                |            |      |   |                     |            |                |            |      |   |               |            |              |            |      |   |               |            |              |            |      |   |                |            |              |            |      |   |                |            |              |            |      |
| Struktur            | SPN                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |                            |             |                |                    |      |        |                     |                |                  |                           |                      |                       |            |      |   |                            |            |                |            |      |   |                           |            |                |            |      |   |                           |          |                |            |      |   |                            |            |                |            |      |   |                |            |              |            |      |         |   |                           |             |                |            |      |   |                     |            |                |            |      |   |               |            |              |            |      |   |               |            |              |            |      |   |                |            |              |            |      |   |                |            |              |            |      |
| Panjang blok (bit)  | 64                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |                            |             |                |                    |      |        |                     |                |                  |                           |                      |                       |            |      |   |                            |            |                |            |      |   |                           |            |                |            |      |   |                           |          |                |            |      |   |                            |            |                |            |      |   |                |            |              |            |      |         |   |                           |             |                |            |      |   |                     |            |                |            |      |   |               |            |              |            |      |   |               |            |              |            |      |   |                |            |              |            |      |   |                |            |              |            |      |
| Panjang kunci (bit) | 64<br>(LED-64)                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      | 128<br>(LED-128)           |             |                |                    |      |        |                     |                |                  |                           |                      |                       |            |      |   |                            |            |                |            |      |   |                           |            |                |            |      |   |                           |          |                |            |      |   |                            |            |                |            |      |   |                |            |              |            |      |         |   |                           |             |                |            |      |   |                     |            |                |            |      |   |               |            |              |            |      |   |               |            |              |            |      |   |                |            |              |            |      |   |                |            |              |            |      |
| Jumlah <i>round</i> | 32 (8 <i>steps</i> )                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                | 48 (12 <i>steps</i> )      |             |                |                    |      |        |                     |                |                  |                           |                      |                       |            |      |   |                            |            |                |            |      |   |                           |            |                |            |      |   |                           |          |                |            |      |   |                            |            |                |            |      |   |                |            |              |            |      |         |   |                           |             |                |            |      |   |                     |            |                |            |      |   |               |            |              |            |      |   |               |            |              |            |      |   |                |            |              |            |      |   |                |            |              |            |      |
| Analisis keamanan   | <p>Status analisis keamanan LED dalam pengaturan kunci tunggal (CPs: <i>chosen plaintext</i>, KPs: <i>known plaintext</i>) setelah September 2021:</p> <table><tr><td>Algoritma</td><td>Step</td><td>Tipe</td><td>Waktu</td><td>Data</td><td>Memori</td><td>Ref</td></tr><tr><td rowspan="6">LED-64</td><td>2</td><td><i>Meet-in-the-Middle</i></td><td><math>2^{56,0}</math></td><td><math>2^{8,0}</math> CPs</td><td><math>2^{11,0}</math></td><td>[71]</td></tr><tr><td>2</td><td><i>Probabilistic Slide</i></td><td><math>2^{51,5}</math></td><td><math>2^{41,5}</math> KPs</td><td><math>2^{42,5}</math></td><td>[71]</td></tr><tr><td>2</td><td><i>Meet-in-the-Middle</i></td><td><math>2^{48,0}</math></td><td><math>2^{16,0}</math> CPs</td><td><math>2^{17,0}</math></td><td>[73]</td></tr><tr><td>2</td><td><i>Meet-in-the-Middle</i></td><td><math>2^{48}</math></td><td><math>2^{48,0}</math> KPs</td><td><math>2^{48,0}</math></td><td>[73]</td></tr><tr><td>2</td><td><i>Probabilistic Slide</i></td><td><math>2^{46,5}</math></td><td><math>2^{45,5}</math> KPs</td><td><math>2^{46,5}</math></td><td>[72]</td></tr><tr><td>3</td><td><i>Generic</i></td><td><math>2^{60,2}</math></td><td><math>2^{49}</math> KPs</td><td><math>2^{60,0}</math></td><td>[74]</td></tr><tr><td rowspan="6">LED-128</td><td>4</td><td><i>Meet-in-the-Middle</i></td><td><math>2^{112,0}</math></td><td><math>2^{16,0}</math> CPs</td><td><math>2^{60,0}</math></td><td>[71]</td></tr><tr><td>4</td><td><i>Differential</i></td><td><math>2^{96,0}</math></td><td><math>2^{64,0}</math> KPs</td><td><math>2^{64,0}</math></td><td>[75]</td></tr><tr><td>4</td><td><i>Slidex</i></td><td><math>2^{60,2}</math></td><td><math>2^{49}</math> KPs</td><td><math>2^{32,0}</math></td><td>[76]</td></tr><tr><td>6</td><td><i>Slidex</i></td><td><math>2^{60,2}</math></td><td><math>2^{49}</math> KPs</td><td><math>2^{59,0}</math></td><td>[76]</td></tr><tr><td>6</td><td><i>Generic</i></td><td><math>2^{60,2}</math></td><td><math>2^{49}</math> KPs</td><td><math>2^{60,0}</math></td><td>[74]</td></tr><tr><td>8</td><td><i>Generic</i></td><td><math>2^{60,2}</math></td><td><math>2^{49}</math> KPs</td><td><math>2^{60,0}</math></td><td>[74]</td></tr></table> <p>Status analisis keamanan LED dalam pengaturan <i>related-key</i> (CPs: <i>chosen plaintext</i>, KPs: <i>known plaintext</i>)</p> | Algoritma                  | Step        | Tipe           | Waktu              | Data | Memori | Ref                 | LED-64         | 2                | <i>Meet-in-the-Middle</i> | $2^{56,0}$           | $2^{8,0}$ CPs         | $2^{11,0}$ | [71] | 2 | <i>Probabilistic Slide</i> | $2^{51,5}$ | $2^{41,5}$ KPs | $2^{42,5}$ | [71] | 2 | <i>Meet-in-the-Middle</i> | $2^{48,0}$ | $2^{16,0}$ CPs | $2^{17,0}$ | [73] | 2 | <i>Meet-in-the-Middle</i> | $2^{48}$ | $2^{48,0}$ KPs | $2^{48,0}$ | [73] | 2 | <i>Probabilistic Slide</i> | $2^{46,5}$ | $2^{45,5}$ KPs | $2^{46,5}$ | [72] | 3 | <i>Generic</i> | $2^{60,2}$ | $2^{49}$ KPs | $2^{60,0}$ | [74] | LED-128 | 4 | <i>Meet-in-the-Middle</i> | $2^{112,0}$ | $2^{16,0}$ CPs | $2^{60,0}$ | [71] | 4 | <i>Differential</i> | $2^{96,0}$ | $2^{64,0}$ KPs | $2^{64,0}$ | [75] | 4 | <i>Slidex</i> | $2^{60,2}$ | $2^{49}$ KPs | $2^{32,0}$ | [76] | 6 | <i>Slidex</i> | $2^{60,2}$ | $2^{49}$ KPs | $2^{59,0}$ | [76] | 6 | <i>Generic</i> | $2^{60,2}$ | $2^{49}$ KPs | $2^{60,0}$ | [74] | 8 | <i>Generic</i> | $2^{60,2}$ | $2^{49}$ KPs | $2^{60,0}$ | [74] |
| Algoritma           | Step                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                | Tipe                       | Waktu       | Data           | Memori             | Ref  |        |                     |                |                  |                           |                      |                       |            |      |   |                            |            |                |            |      |   |                           |            |                |            |      |   |                           |          |                |            |      |   |                            |            |                |            |      |   |                |            |              |            |      |         |   |                           |             |                |            |      |   |                     |            |                |            |      |   |               |            |              |            |      |   |               |            |              |            |      |   |                |            |              |            |      |   |                |            |              |            |      |
| LED-64              | 2                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   | <i>Meet-in-the-Middle</i>  | $2^{56,0}$  | $2^{8,0}$ CPs  | $2^{11,0}$         | [71] |        |                     |                |                  |                           |                      |                       |            |      |   |                            |            |                |            |      |   |                           |            |                |            |      |   |                           |          |                |            |      |   |                            |            |                |            |      |   |                |            |              |            |      |         |   |                           |             |                |            |      |   |                     |            |                |            |      |   |               |            |              |            |      |   |               |            |              |            |      |   |                |            |              |            |      |   |                |            |              |            |      |
|                     | 2                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   | <i>Probabilistic Slide</i> | $2^{51,5}$  | $2^{41,5}$ KPs | $2^{42,5}$         | [71] |        |                     |                |                  |                           |                      |                       |            |      |   |                            |            |                |            |      |   |                           |            |                |            |      |   |                           |          |                |            |      |   |                            |            |                |            |      |   |                |            |              |            |      |         |   |                           |             |                |            |      |   |                     |            |                |            |      |   |               |            |              |            |      |   |               |            |              |            |      |   |                |            |              |            |      |   |                |            |              |            |      |
|                     | 2                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   | <i>Meet-in-the-Middle</i>  | $2^{48,0}$  | $2^{16,0}$ CPs | $2^{17,0}$         | [73] |        |                     |                |                  |                           |                      |                       |            |      |   |                            |            |                |            |      |   |                           |            |                |            |      |   |                           |          |                |            |      |   |                            |            |                |            |      |   |                |            |              |            |      |         |   |                           |             |                |            |      |   |                     |            |                |            |      |   |               |            |              |            |      |   |               |            |              |            |      |   |                |            |              |            |      |   |                |            |              |            |      |
|                     | 2                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   | <i>Meet-in-the-Middle</i>  | $2^{48}$    | $2^{48,0}$ KPs | $2^{48,0}$         | [73] |        |                     |                |                  |                           |                      |                       |            |      |   |                            |            |                |            |      |   |                           |            |                |            |      |   |                           |          |                |            |      |   |                            |            |                |            |      |   |                |            |              |            |      |         |   |                           |             |                |            |      |   |                     |            |                |            |      |   |               |            |              |            |      |   |               |            |              |            |      |   |                |            |              |            |      |   |                |            |              |            |      |
|                     | 2                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   | <i>Probabilistic Slide</i> | $2^{46,5}$  | $2^{45,5}$ KPs | $2^{46,5}$         | [72] |        |                     |                |                  |                           |                      |                       |            |      |   |                            |            |                |            |      |   |                           |            |                |            |      |   |                           |          |                |            |      |   |                            |            |                |            |      |   |                |            |              |            |      |         |   |                           |             |                |            |      |   |                     |            |                |            |      |   |               |            |              |            |      |   |               |            |              |            |      |   |                |            |              |            |      |   |                |            |              |            |      |
|                     | 3                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   | <i>Generic</i>             | $2^{60,2}$  | $2^{49}$ KPs   | $2^{60,0}$         | [74] |        |                     |                |                  |                           |                      |                       |            |      |   |                            |            |                |            |      |   |                           |            |                |            |      |   |                           |          |                |            |      |   |                            |            |                |            |      |   |                |            |              |            |      |         |   |                           |             |                |            |      |   |                     |            |                |            |      |   |               |            |              |            |      |   |               |            |              |            |      |   |                |            |              |            |      |   |                |            |              |            |      |
| LED-128             | 4                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   | <i>Meet-in-the-Middle</i>  | $2^{112,0}$ | $2^{16,0}$ CPs | $2^{60,0}$         | [71] |        |                     |                |                  |                           |                      |                       |            |      |   |                            |            |                |            |      |   |                           |            |                |            |      |   |                           |          |                |            |      |   |                            |            |                |            |      |   |                |            |              |            |      |         |   |                           |             |                |            |      |   |                     |            |                |            |      |   |               |            |              |            |      |   |               |            |              |            |      |   |                |            |              |            |      |   |                |            |              |            |      |
|                     | 4                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   | <i>Differential</i>        | $2^{96,0}$  | $2^{64,0}$ KPs | $2^{64,0}$         | [75] |        |                     |                |                  |                           |                      |                       |            |      |   |                            |            |                |            |      |   |                           |            |                |            |      |   |                           |          |                |            |      |   |                            |            |                |            |      |   |                |            |              |            |      |         |   |                           |             |                |            |      |   |                     |            |                |            |      |   |               |            |              |            |      |   |               |            |              |            |      |   |                |            |              |            |      |   |                |            |              |            |      |
|                     | 4                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   | <i>Slidex</i>              | $2^{60,2}$  | $2^{49}$ KPs   | $2^{32,0}$         | [76] |        |                     |                |                  |                           |                      |                       |            |      |   |                            |            |                |            |      |   |                           |            |                |            |      |   |                           |          |                |            |      |   |                            |            |                |            |      |   |                |            |              |            |      |         |   |                           |             |                |            |      |   |                     |            |                |            |      |   |               |            |              |            |      |   |               |            |              |            |      |   |                |            |              |            |      |   |                |            |              |            |      |
|                     | 6                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   | <i>Slidex</i>              | $2^{60,2}$  | $2^{49}$ KPs   | $2^{59,0}$         | [76] |        |                     |                |                  |                           |                      |                       |            |      |   |                            |            |                |            |      |   |                           |            |                |            |      |   |                           |          |                |            |      |   |                            |            |                |            |      |   |                |            |              |            |      |         |   |                           |             |                |            |      |   |                     |            |                |            |      |   |               |            |              |            |      |   |               |            |              |            |      |   |                |            |              |            |      |   |                |            |              |            |      |
|                     | 6                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   | <i>Generic</i>             | $2^{60,2}$  | $2^{49}$ KPs   | $2^{60,0}$         | [74] |        |                     |                |                  |                           |                      |                       |            |      |   |                            |            |                |            |      |   |                           |            |                |            |      |   |                           |          |                |            |      |   |                            |            |                |            |      |   |                |            |              |            |      |         |   |                           |             |                |            |      |   |                     |            |                |            |      |   |               |            |              |            |      |   |               |            |              |            |      |   |                |            |              |            |      |   |                |            |              |            |      |
|                     | 8                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   | <i>Generic</i>             | $2^{60,2}$  | $2^{49}$ KPs   | $2^{60,0}$         | [74] |        |                     |                |                  |                           |                      |                       |            |      |   |                            |            |                |            |      |   |                           |            |                |            |      |   |                           |          |                |            |      |   |                            |            |                |            |      |   |                |            |              |            |      |         |   |                           |             |                |            |      |   |                     |            |                |            |      |   |               |            |              |            |      |   |               |            |              |            |      |   |                |            |              |            |      |   |                |            |              |            |      |

|                       |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |                    |                            |                   |                            |      |              |     |        |     |              |                   |                   |                   |       |      |                    |                   |                   |                   |      |               |              |                   |                   |                   |           |      |             |          |     |        |                   |                |               |      |         |                   |                 |               |
|-----------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------|----------------------------|-------------------|----------------------------|------|--------------|-----|--------|-----|--------------|-------------------|-------------------|-------------------|-------|------|--------------------|-------------------|-------------------|-------------------|------|---------------|--------------|-------------------|-------------------|-------------------|-----------|------|-------------|----------|-----|--------|-------------------|----------------|---------------|------|---------|-------------------|-----------------|---------------|
|                       | <table><tr><td>Algoritma</td><td>Step</td><td>Type</td><td>Waktu</td><td>Data</td><td>Memori</td><td>Ref</td></tr><tr><td rowspan="3">LED-64</td><td>3</td><td>Differential</td><td>2<sup>60,0</sup></td><td>2<sup>60,0</sup></td><td>2<sup>60,0</sup></td><td>[75]</td></tr><tr><td>3</td><td>Meet-in-the-Middle</td><td>2<sup>49,0</sup></td><td>2<sup>49,0</sup></td><td>2<sup>59,0</sup></td><td>[73]</td></tr><tr><td>4</td><td>Differential</td><td>2<sup>63,0</sup></td><td>2<sup>63,0</sup></td><td>2<sup>63,0</sup></td><td>[75]</td></tr></table> <p>Berdasarkan hasil kajian pada tabel di atas, meskipun berbagai penelitian kriptanalisis telah dilakukan, hingga saat ini tidak terdapat serangan yang lebih efisien dibandingkan dengan <i>exhaustive search</i> terhadap kunci rahasia algoritma LED.</p>                                                                                            | Algoritma          | Step                       | Type              | Waktu                      | Data | Memori       | Ref | LED-64 | 3   | Differential | 2 <sup>60,0</sup> | 2 <sup>60,0</sup> | 2 <sup>60,0</sup> | [75]  | 3    | Meet-in-the-Middle | 2 <sup>49,0</sup> | 2 <sup>49,0</sup> | 2 <sup>59,0</sup> | [73] | 4             | Differential | 2 <sup>63,0</sup> | 2 <sup>63,0</sup> | 2 <sup>63,0</sup> | [75]      |      |             |          |     |        |                   |                |               |      |         |                   |                 |               |
| Algoritma             | Step                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 | Type               | Waktu                      | Data              | Memori                     | Ref  |              |     |        |     |              |                   |                   |                   |       |      |                    |                   |                   |                   |      |               |              |                   |                   |                   |           |      |             |          |     |        |                   |                |               |      |         |                   |                 |               |
| LED-64                | 3                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    | Differential       | 2 <sup>60,0</sup>          | 2 <sup>60,0</sup> | 2 <sup>60,0</sup>          | [75] |              |     |        |     |              |                   |                   |                   |       |      |                    |                   |                   |                   |      |               |              |                   |                   |                   |           |      |             |          |     |        |                   |                |               |      |         |                   |                 |               |
|                       | 3                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    | Meet-in-the-Middle | 2 <sup>49,0</sup>          | 2 <sup>49,0</sup> | 2 <sup>59,0</sup>          | [73] |              |     |        |     |              |                   |                   |                   |       |      |                    |                   |                   |                   |      |               |              |                   |                   |                   |           |      |             |          |     |        |                   |                |               |      |         |                   |                 |               |
|                       | 4                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    | Differential       | 2 <sup>63,0</sup>          | 2 <sup>63,0</sup> | 2 <sup>63,0</sup>          | [75] |              |     |        |     |              |                   |                   |                   |       |      |                    |                   |                   |                   |      |               |              |                   |                   |                   |           |      |             |          |     |        |                   |                |               |      |         |                   |                 |               |
| Analisis Performa     | <p>Hasil evaluasi implementasi perangkat keras:</p> <table><tr><td>Algoritma</td><td>Area (GE)</td><td>Cycles/block</td><td>Throughput @ 100kHz (kbps)</td><td>Ref</td></tr><tr><td>LED-64 (Enc)</td><td>966</td><td>1.248</td><td>5,1</td><td>[70]</td></tr><tr><td>LED-64 (Enc)</td><td>2.695</td><td>32</td><td>200,0</td><td>[77]</td></tr><tr><td>LED-128 (Enc)</td><td>1.265</td><td>1.872</td><td>3,4</td><td>[70]</td></tr><tr><td>LED-128 (Enc)</td><td>3.036</td><td>48</td><td>133,3</td><td>[77]</td></tr></table> <p>Hasil evaluasi implementasi perangkat lunak:</p> <table><tr><td>Algoritma</td><td>Type</td><td>Cycles/byte</td><td>Platform</td><td>Ref</td></tr><tr><td>LED-64</td><td>Table/VPI/Bitlice</td><td>76,0/48,1/13,1</td><td>Core i3 2367M</td><td rowspan="2">[79]</td></tr><tr><td>LED-128</td><td>Table/VPI/Bitlice</td><td>113,3/54,6/17,6</td><td>Core i3 2367M</td></tr></table> | Algoritma          | Area (GE)                  | Cycles/block      | Throughput @ 100kHz (kbps) | Ref  | LED-64 (Enc) | 966 | 1.248  | 5,1 | [70]         | LED-64 (Enc)      | 2.695             | 32                | 200,0 | [77] | LED-128 (Enc)      | 1.265             | 1.872             | 3,4               | [70] | LED-128 (Enc) | 3.036        | 48                | 133,3             | [77]              | Algoritma | Type | Cycles/byte | Platform | Ref | LED-64 | Table/VPI/Bitlice | 76,0/48,1/13,1 | Core i3 2367M | [79] | LED-128 | Table/VPI/Bitlice | 113,3/54,6/17,6 | Core i3 2367M |
| Algoritma             | Area (GE)                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            | Cycles/block       | Throughput @ 100kHz (kbps) | Ref               |                            |      |              |     |        |     |              |                   |                   |                   |       |      |                    |                   |                   |                   |      |               |              |                   |                   |                   |           |      |             |          |     |        |                   |                |               |      |         |                   |                 |               |
| LED-64 (Enc)          | 966                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  | 1.248              | 5,1                        | [70]              |                            |      |              |     |        |     |              |                   |                   |                   |       |      |                    |                   |                   |                   |      |               |              |                   |                   |                   |           |      |             |          |     |        |                   |                |               |      |         |                   |                 |               |
| LED-64 (Enc)          | 2.695                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                | 32                 | 200,0                      | [77]              |                            |      |              |     |        |     |              |                   |                   |                   |       |      |                    |                   |                   |                   |      |               |              |                   |                   |                   |           |      |             |          |     |        |                   |                |               |      |         |                   |                 |               |
| LED-128 (Enc)         | 1.265                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                | 1.872              | 3,4                        | [70]              |                            |      |              |     |        |     |              |                   |                   |                   |       |      |                    |                   |                   |                   |      |               |              |                   |                   |                   |           |      |             |          |     |        |                   |                |               |      |         |                   |                 |               |
| LED-128 (Enc)         | 3.036                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                | 48                 | 133,3                      | [77]              |                            |      |              |     |        |     |              |                   |                   |                   |       |      |                    |                   |                   |                   |      |               |              |                   |                   |                   |           |      |             |          |     |        |                   |                |               |      |         |                   |                 |               |
| Algoritma             | Type                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 | Cycles/byte        | Platform                   | Ref               |                            |      |              |     |        |     |              |                   |                   |                   |       |      |                    |                   |                   |                   |      |               |              |                   |                   |                   |           |      |             |          |     |        |                   |                |               |      |         |                   |                 |               |
| LED-64                | Table/VPI/Bitlice                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    | 76,0/48,1/13,1     | Core i3 2367M              | [79]              |                            |      |              |     |        |     |              |                   |                   |                   |       |      |                    |                   |                   |                   |      |               |              |                   |                   |                   |           |      |             |          |     |        |                   |                |               |      |         |                   |                 |               |
| LED-128               | Table/VPI/Bitlice                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    | 113,3/54,6/17,6    | Core i3 2367M              |                   |                            |      |              |     |        |     |              |                   |                   |                   |       |      |                    |                   |                   |                   |      |               |              |                   |                   |                   |           |      |             |          |     |        |                   |                |               |      |         |                   |                 |               |
| Informasi Open Source | <p>Implementasi tersedia di <i>website</i> LED</p> <p><a href="http://led.crypto.sg/software/lightweight-crypto-lib">http://led.crypto.sg/software/lightweight-crypto-lib</a></p> <p><a href="https://github.com/rb-anssi/lightweight-crypto-lib">https://github.com/rb-anssi/lightweight-crypto-lib</a></p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |                    |                            |                   |                            |      |              |     |        |     |              |                   |                   |                   |       |      |                    |                   |                   |                   |      |               |              |                   |                   |                   |           |      |             |          |     |        |                   |                |               |      |         |                   |                 |               |

### 3. LEA

|                  |           |                                                                                                                  |
|------------------|-----------|------------------------------------------------------------------------------------------------------------------|
| Profil Algoritma | Nama      | LEA                                                                                                              |
|                  | Perancang | Deukjo Hong, Jung-Keun Lee, Dong-Chan Kim, Daesung Kwon, Kwon Ho Ryu, Dong-Geon Lee ( <i>Korea Electronics</i> ) |

|                                                                                                                                                                     |                                                                                                                            |                                                                          |                    |                        |                 |            |      |
|---------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------|--------------------|------------------------|-----------------|------------|------|
|                                                                                                                                                                     |                                                                                                                            | and Telecommunications Research Institute Korea, Sanyo University Korea) |                    |                        |                 |            |      |
|                                                                                                                                                                     | Publikasi                                                                                                                  | 2013 (WISA 2013 [80])                                                    |                    |                        |                 |            |      |
|                                                                                                                                                                     | Spesifikasi                                                                                                                | ISO/IEC 29192-2                                                          |                    |                        |                 |            |      |
| Fitur                                                                                                                                                               | Perancang menyatakan bahwa LEA dapat melakukan pemrosesan enkripsi berkecepatan tinggi dalam implementasi perangkat lunak. |                                                                          |                    |                        |                 |            |      |
|                                                                                                                                                                     | Struktur                                                                                                                   | Addition-Rotation-XOR (ARX) type                                         |                    |                        |                 |            |      |
|                                                                                                                                                                     | Panjang blok (bit)                                                                                                         | 128                                                                      |                    |                        |                 |            |      |
|                                                                                                                                                                     | Panjang kunci (bit)                                                                                                        | 128 (LEA-128)                                                            | 192 (LEA-192)      | 256 (LEA-256)          |                 |            |      |
|                                                                                                                                                                     | Jumlah round                                                                                                               | 24                                                                       | 28                 | 32                     |                 |            |      |
| Analisis keamanan                                                                                                                                                   | Status analisis keamanan LEA dalam pengaturan kunci tunggal (CPs: chosen plaintext):                                       |                                                                          |                    |                        |                 |            |      |
|                                                                                                                                                                     | Algoritma                                                                                                                  | Round                                                                    | Tipe               | Waktu                  | Data            | Memori     | Ref  |
|                                                                                                                                                                     | LEA-128                                                                                                                    | 12                                                                       | Differetial        | $2^{84,0}$             | $2^{100,0}$ CPs | $2^{84,1}$ | [80] |
|                                                                                                                                                                     |                                                                                                                            | 14                                                                       | Differetial        | $2^{124,0}$            | $2^{124,0}$ CPs | $2^{22,0}$ | [81] |
|                                                                                                                                                                     | LEA-192                                                                                                                    | 14                                                                       | Differetial        | $2^{124,0}$            | $2^{124,0}$ CPs | $2^{22,0}$ |      |
|                                                                                                                                                                     | LEA-256                                                                                                                    | 15                                                                       | Differetial        | $2^{252,0}$            | $2^{124,0}$ CPs | $2^{22,0}$ |      |
|                                                                                                                                                                     |                                                                                                                            |                                                                          |                    |                        |                 |            |      |
|                                                                                                                                                                     | Algoritma                                                                                                                  | Round                                                                    | Tipe               | Probabilitas atau Bias |                 | Ref        |      |
|                                                                                                                                                                     | LEA-128                                                                                                                    | 13                                                                       | Differetial        | $2^{-123,8}$           |                 | [81]       |      |
|                                                                                                                                                                     |                                                                                                                            | 11                                                                       | Linear             | $2^{-62}$              |                 | [80]       |      |
|                                                                                                                                                                     |                                                                                                                            | 14                                                                       | Differenial-Linear | $2^{-57}$              |                 | [80]       |      |
|                                                                                                                                                                     |                                                                                                                            | 14                                                                       | Boomerang          | $2^{-108}$             |                 | [82]       |      |
|                                                                                                                                                                     |                                                                                                                            | 16                                                                       | Boomerang          | $2^{-117,1}$           |                 | [82]       |      |
| Berdasarkan hasil kajian pada tabel di atas, meskipun berbagai penelitian kriptanalisis telah dilakukan, hingga saat ini tidak terdapat serangan yang lebih efisien |                                                                                                                            |                                                                          |                    |                        |                 |            |      |

|                   | <p>dibandingkan dengan <i>exhaustive search</i> terhadap algoritma LEA.</p> <p>Serangan terbaik pada <i>single-key setting</i> adalah <i>differential attack</i> yang dikemukakan oleh Song, dkk [81]. Serangan ini efektif terhadap versi tereduksi LEA, yaitu LEA-128 pada 14 dari 24 <i>round</i>, LEA-192 pada 14 dari 28 <i>round</i>, dan LEA-256 pada 15 dari 32 <i>round</i>, sehingga memungkinkan dilakukannya serangan <i>key recovery</i> yang lebih efisien dibandingkan pencarian menyeluruh. Sementara itu, serangan <i>distinguishing</i> paling efektif adalah <i>boomerang attack</i> yang diajukan oleh Kim, dkk [82], yang dapat membedakan LEA-128 tereduksi hingga 16 dari 24 <i>round</i>. Selain itu, sejumlah penelitian lain juga mengusulkan metode serangan tambahan, namun sejauh ini hanya berlaku pada <i>round</i> tereduksi dan tidak berimplikasi signifikan terhadap keamanan spesifikasi penuh LEA.</p>                               |              |                            |                         |                            |     |               |       |     |       |      |               |       |    |        |           |            |            |                       |          |     |         |     |    |          |            |      |         |   |   |         |            |         |   |   |            |                         |         |   |   |            |                    |
|-------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------|----------------------------|-------------------------|----------------------------|-----|---------------|-------|-----|-------|------|---------------|-------|----|--------|-----------|------------|------------|-----------------------|----------|-----|---------|-----|----|----------|------------|------|---------|---|---|---------|------------|---------|---|---|------------|-------------------------|---------|---|---|------------|--------------------|
| Analisis Performa | <p>Hasil evaluasi implementasi perangkat keras menunjukan:</p> <table><tr><th>Algoritma</th><th>Area (GE)</th><th>Cycles/block</th><th>Throughput @ 100kHz (kbps)</th><th>Ref</th></tr><tr><td>LEA-128 (Enc)</td><td>3.826</td><td>168</td><td>76,19</td><td rowspan="2">[80]</td></tr><tr><td>LEA-128 (Enc)</td><td>5.426</td><td>24</td><td>533,33</td></tr></table> <p>Hasil evaluasi implementasi perangkat lunak menunjukan:</p> <table><tr><th>Algoritma</th><th>ROM (byte)</th><th>RAM (byte)</th><th>Cycles/byte (Enc/Dec)</th><th>Platform</th><th>Ref</th></tr><tr><td>LEA-128</td><td>590</td><td>32</td><td>326,94/-</td><td>ARM926EJ-S</td><td rowspan="4">[81]</td></tr><tr><td>LEA-128</td><td>-</td><td>-</td><td>20,06/-</td><td>ARM926EJ-S</td></tr><tr><td>LEA-128</td><td>-</td><td>-</td><td>9,29/14,83</td><td>Intel Core 2 Quad Q6600</td></tr><tr><td>LEA-128</td><td>-</td><td>-</td><td>9,29/14,52</td><td>Intel Core i5-2500</td></tr></table> | Algoritma    | Area (GE)                  | Cycles/block            | Throughput @ 100kHz (kbps) | Ref | LEA-128 (Enc) | 3.826 | 168 | 76,19 | [80] | LEA-128 (Enc) | 5.426 | 24 | 533,33 | Algoritma | ROM (byte) | RAM (byte) | Cycles/byte (Enc/Dec) | Platform | Ref | LEA-128 | 590 | 32 | 326,94/- | ARM926EJ-S | [81] | LEA-128 | - | - | 20,06/- | ARM926EJ-S | LEA-128 | - | - | 9,29/14,83 | Intel Core 2 Quad Q6600 | LEA-128 | - | - | 9,29/14,52 | Intel Core i5-2500 |
| Algoritma         | Area (GE)                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 | Cycles/block | Throughput @ 100kHz (kbps) | Ref                     |                            |     |               |       |     |       |      |               |       |    |        |           |            |            |                       |          |     |         |     |    |          |            |      |         |   |   |         |            |         |   |   |            |                         |         |   |   |            |                    |
| LEA-128 (Enc)     | 3.826                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     | 168          | 76,19                      | [80]                    |                            |     |               |       |     |       |      |               |       |    |        |           |            |            |                       |          |     |         |     |    |          |            |      |         |   |   |         |            |         |   |   |            |                         |         |   |   |            |                    |
| LEA-128 (Enc)     | 5.426                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     | 24           | 533,33                     |                         |                            |     |               |       |     |       |      |               |       |    |        |           |            |            |                       |          |     |         |     |    |          |            |      |         |   |   |         |            |         |   |   |            |                         |         |   |   |            |                    |
| Algoritma         | ROM (byte)                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                | RAM (byte)   | Cycles/byte (Enc/Dec)      | Platform                | Ref                        |     |               |       |     |       |      |               |       |    |        |           |            |            |                       |          |     |         |     |    |          |            |      |         |   |   |         |            |         |   |   |            |                         |         |   |   |            |                    |
| LEA-128           | 590                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       | 32           | 326,94/-                   | ARM926EJ-S              | [81]                       |     |               |       |     |       |      |               |       |    |        |           |            |            |                       |          |     |         |     |    |          |            |      |         |   |   |         |            |         |   |   |            |                         |         |   |   |            |                    |
| LEA-128           | -                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         | -            | 20,06/-                    | ARM926EJ-S              |                            |     |               |       |     |       |      |               |       |    |        |           |            |            |                       |          |     |         |     |    |          |            |      |         |   |   |         |            |         |   |   |            |                         |         |   |   |            |                    |
| LEA-128           | -                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         | -            | 9,29/14,83                 | Intel Core 2 Quad Q6600 |                            |     |               |       |     |       |      |               |       |    |        |           |            |            |                       |          |     |         |     |    |          |            |      |         |   |   |         |            |         |   |   |            |                         |         |   |   |            |                    |
| LEA-128           | -                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         | -            | 9,29/14,52                 | Intel Core i5-2500      |                            |     |               |       |     |       |      |               |       |    |        |           |            |            |                       |          |     |         |     |    |          |            |      |         |   |   |         |            |         |   |   |            |                         |         |   |   |            |                    |

|              |                 |       |     |             |                      |  |
|--------------|-----------------|-------|-----|-------------|----------------------|--|
|              | LEA-128         | -     | -   | 8,85/14,50  | AMD Phenom II X4 965 |  |
|              | LEA-128         | -     | -   | 8,55/14.,05 | AMD Opteron 6176 SE  |  |
|              | LEA-128         | 9.674 | 832 | 103,59/-    | MCF5213              |  |
|              | LEA-128         | 704   | 32  | 829,25/-    | MCF5213              |  |
| Standarisasi | ISO/IEC 29192-2 |       |     |             |                      |  |

#### 4. Midori

|                   |                                                                                                                                                                   |                                                                                                                                                                                                                             |                                            |                 |            |          |
|-------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------|-----------------|------------|----------|
| Profil Algoritma  | Nama                                                                                                                                                              | Midori                                                                                                                                                                                                                      |                                            |                 |            |          |
|                   | Perancang                                                                                                                                                         | Subhadeep Banik, Andrey Bogdanov (Technical University of Denmark, Denmark), Takanori Isobe, Kyoji Shibutani, Harunaga Hiwatari, Toru Akishita (Sony Corporation, Japan), Francesco Regazzoni (University of Lugano, Swiss) |                                            |                 |            |          |
|                   | Publikasi                                                                                                                                                         | 2015 (ASIACRYPT 2015) [83]                                                                                                                                                                                                  |                                            |                 |            |          |
|                   | Spesifikasi                                                                                                                                                       | Dapat dilihat pada [83]                                                                                                                                                                                                     |                                            |                 |            |          |
| Fitur             | Para perancang mengklaim bahwa algoritma Midori memiliki konsumsi energi yang rendah, implementasi perangkat keras yang <i>compact</i> , dan latensi yang rendah. |                                                                                                                                                                                                                             |                                            |                 |            |          |
|                   | Struktur                                                                                                                                                          | SPN                                                                                                                                                                                                                         |                                            |                 |            |          |
|                   | Panjang blok (bit)                                                                                                                                                | 64 (Midori64)                                                                                                                                                                                                               |                                            | 128 (Midori128) |            |          |
|                   | Panjang kunci (bit)                                                                                                                                               | 128                                                                                                                                                                                                                         |                                            |                 |            |          |
|                   | Jumlah <i>round</i>                                                                                                                                               | 16                                                                                                                                                                                                                          |                                            | 20              |            |          |
|                   |                                                                                                                                                                   |                                                                                                                                                                                                                             |                                            |                 |            |          |
| Analisis keamanan | Status analisis keamanan Midori dalam pengaturan kunci tunggal                                                                                                    |                                                                                                                                                                                                                             |                                            |                 |            |          |
|                   | Algoritma                                                                                                                                                         | <i>Rounds</i>                                                                                                                                                                                                               | Tipe                                       | Waktu           | Data       | Ref      |
|                   | Midori64                                                                                                                                                          | 10                                                                                                                                                                                                                          | <i>Meet-in-the-Middle</i>                  | $2^{99,5}$      | $2^{61,5}$ | [84, 85] |
|                   |                                                                                                                                                                   | 11                                                                                                                                                                                                                          | <i>Meet-in-the-Middle</i>                  | $2^{122,0}$     | $2^{53,0}$ |          |
|                   |                                                                                                                                                                   | 12                                                                                                                                                                                                                          | <i>Meet-in-the-Middle</i>                  | $2^{125,5}$     | $2^{55,5}$ |          |
|                   |                                                                                                                                                                   | 16 (full)                                                                                                                                                                                                                   | <i>Invariant Subspace</i><br>( $2^{32}$ )* | $2^{16,0}$      | 2          | [86, 86] |

|           |    |                                |                                            |             |      |         |
|-----------|----|--------------------------------|--------------------------------------------|-------------|------|---------|
|           |    | 16 (full)                      | <i>Invariant Subspace</i><br>( $2^{64}$ )* | $2^{99,5}$  | 2    | [87,88] |
| Midori128 | 10 | <i>Impossible Differential</i> | $2^{199,0}$                                | $2^{118,6}$ | [89] |         |
|           | 10 | <i>Impossible Differential</i> | $2^{116,7}$                                | $2^{116,1}$ | [89] |         |
|           | 13 | <i>Truncated Differential</i>  | $2^{125,7}$                                | $2^{115,7}$ | [90] |         |
|           | 13 | <i>Truncated Differential</i>  | $2^{119,0}$                                | $2^{119,0}$ | [89] |         |

\* Catatan: serangan ini hanya bekerja jika digunakan sebuah kunci yang merupakan *weak key*.

Status analisis keamanan Midori dalam pengaturan *related-key*

|           |           |                     |            |             |      |
|-----------|-----------|---------------------|------------|-------------|------|
| Algoritma | Round     | Tipe                | Waktu      | Data        | Ref  |
| Midori64  | 14        | <i>Differential</i> | $2^{59,0}$ | $2^{116,0}$ | [91] |
|           | 16(full)  | <i>Differential</i> | $2^{23,8}$ | $2^{35,8}$  | [92] |
| Midori128 | 20 (full) | <i>Differential</i> | $2^{43,7}$ | $2^{43,7}$  | [92] |

Berdasarkan hasil kajian pada tabel di atas, meskipun berbagai penelitian kriptanalisis telah dilakukan, hingga saat ini tidak terdapat serangan yang lebih efisien dibandingkan dengan *exhaustive search* terhadap algoritma Midori.

|                     |                                              |           |              |                            |      |
|---------------------|----------------------------------------------|-----------|--------------|----------------------------|------|
| Analisis Performa   | Hasil evaluasi implementasi perangkat keras: |           |              |                            |      |
|                     | Algoritma                                    | Area (GE) | Cycles/block | Throughput @ 100kHz (kbps) | Ref  |
|                     | Midori64 (Enc)                               | 1.542     | 16           | 400,0                      | [83] |
|                     | Midori64 (Enc/Dec)                           | 2.450     | 16           | 400,0                      |      |
|                     | Midori128 (Enc)                              | 2.522     | 20           | 640,0                      |      |
| Midori128 (Enc/Dec) | 3.661                                        | 20        | 640,0        |                            |      |

## 5. Piccolo

|           |           |                                                                      |
|-----------|-----------|----------------------------------------------------------------------|
| Profil    | Nama      | Piccolo                                                              |
| Algoritma | Perancang | Kyoji Shibutani, Takanori Isobe, Harunaga Hiwatari, Atsushi Mitsuda, |

|                   |                                                                                                                                                                                                                                                                                                                                                                                                                   |                                                                                                                                                                                             |                         |                  |                |            |      |
|-------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------|------------------|----------------|------------|------|
|                   |                                                                                                                                                                                                                                                                                                                                                                                                                   | Toru Akishita, Taizo Shirai (Sony Corporation, Japan)                                                                                                                                       |                         |                  |                |            |      |
|                   | Publikasi                                                                                                                                                                                                                                                                                                                                                                                                         | 2011 (CHES 2011 [97])                                                                                                                                                                       |                         |                  |                |            |      |
|                   | Spesifikasi                                                                                                                                                                                                                                                                                                                                                                                                       | Kyoji Shibutani, Takanori Isobe, Harunaga Hiwatari, Atsushi Mitsuda, Toru Akishita, and Taizo Shirai. Piccolo: An ultra-lightweight blockcipher. In Preneel and Takagi, pages 342-357 [93]. |                         |                  |                |            |      |
| Fitur             | Para perancang mengklaim bahwa algoritma Piccolo cukup aman terhadap <i>related-key attack</i> , <i>meet-in-the-middle attack</i> , serta serangan konvensional, memiliki kinerja yang sangat tinggi dalam implementasi perangkat keras, terstruktur sehingga fungsi dekripsi dapat diimplementasikan tanpa menyebabkan <i>overhead</i> yang serius, dan unggul dalam hal bobot yang ringan dan efisiensi energi. |                                                                                                                                                                                             |                         |                  |                |            |      |
|                   | Struktur                                                                                                                                                                                                                                                                                                                                                                                                          | 4-line type-2 generalized Feistel type                                                                                                                                                      |                         |                  |                |            |      |
|                   | Panjang blok (bit)                                                                                                                                                                                                                                                                                                                                                                                                | 64                                                                                                                                                                                          |                         |                  |                |            |      |
|                   | Panjang kunci (bit)                                                                                                                                                                                                                                                                                                                                                                                               | 80 (Piccolo-80)                                                                                                                                                                             |                         | 128(Piccolo-128) |                |            |      |
|                   | Jumlah round                                                                                                                                                                                                                                                                                                                                                                                                      | 25                                                                                                                                                                                          |                         | 31               |                |            |      |
|                   | INTEGRATIF • SOLID • AKUNTABEL • INOVATIF                                                                                                                                                                                                                                                                                                                                                                         |                                                                                                                                                                                             |                         |                  |                |            |      |
| Analisis keamanan | Status analisis keamanan Piccolo dalam pengaturan kunci tunggal (CCs: <i>chosen ciphertext</i> , CPs: <i>chosen plaintext</i> )                                                                                                                                                                                                                                                                                   |                                                                                                                                                                                             |                         |                  |                |            |      |
|                   | Algoritma                                                                                                                                                                                                                                                                                                                                                                                                         | Rounds                                                                                                                                                                                      | Tipe                    | Waktu            | Data           | Memori     | Ref  |
|                   | Piccolo-80                                                                                                                                                                                                                                                                                                                                                                                                        | 12                                                                                                                                                                                          | Impossible Differential | $2^{55,2}$       | $2^{36,4}$ CCs | $2^{63,0}$ | [94] |
|                   |                                                                                                                                                                                                                                                                                                                                                                                                                   | 13                                                                                                                                                                                          | Impossible Differential | $2^{69,7}$       | $2^{43,3}$ CPs | $2^{62,0}$ | [94] |
|                   |                                                                                                                                                                                                                                                                                                                                                                                                                   | 14                                                                                                                                                                                          | Meet-in-the-Middle      | $2^{75,4}$       | $2^{43,3}$ CPs | $2^{73,5}$ | [95] |
|                   |                                                                                                                                                                                                                                                                                                                                                                                                                   | 14                                                                                                                                                                                          | Meet-in-the-Middle*     | $2^{73,0}$       | $2^{64,0}$     | $2^5$      | [96] |
|                   |                                                                                                                                                                                                                                                                                                                                                                                                                   | 14                                                                                                                                                                                          | Meet-in-the-Middle      | $2^{67,4}$       | $2^{52,0}$ CPs | $2^{64,9}$ | [96] |
| Piccolo-128       | 15                                                                                                                                                                                                                                                                                                                                                                                                                | Impossible Differential                                                                                                                                                                     | $2^{125,4}$             | $2^{58,7}$ CPs   | $2^{61,0}$     | [94]       |      |

|  |    |                            |             |                   |             |      |
|--|----|----------------------------|-------------|-------------------|-------------|------|
|  | 16 | <i>Meet-in-the-Middle</i>  | $2^{123,0}$ | $2^{43,0}$<br>CPs | $2^{113,5}$ | [95] |
|  | 17 | <i>Meet-in-the-Middle</i>  | $2^{126,9}$ | $2^{48,0}$<br>CPs | $2^{126,0}$ | [95] |
|  | 18 | <i>Meet-in-the-Middle</i>  | $2^{126,6}$ | $2^{52,0}$<br>CPs | $2^{125,3}$ | [97] |
|  | 21 | <i>Meet-in-the-Middle*</i> | $2^{121,0}$ | $2^{64,0}$        | $2^{6,0}$   | [96] |

- Catatan: Serangan ini membutuhkan *full codebook* atau lebih

Status analisis keamanan Piccolo dalam pengaturan *related-key*

| Algoritma   | Rounds | Tipe                            | Waktu       | Data        | Ref  |
|-------------|--------|---------------------------------|-------------|-------------|------|
| Piccolo-80  | 14     | <i>Impossible Differential*</i> | $2^{68,2}$  | $2^{68,2}$  | [98] |
| Piccolo-128 | 21     | <i>Impossible Differential*</i> | $2^{117,8}$ | $2^{117,8}$ | [98] |

Berdasarkan hasil kajian pada tabel di atas, meskipun berbagai penelitian kriptanalisis telah dilakukan, hingga saat ini tidak terdapat serangan yang lebih efisien dibandingkan dengan *exhaustive search* terhadap algoritma Piccolo.

| Analisis Performa     | Hasil evaluasi implementasi perangkat keras menunjukan:                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |                 |               |                            |      |           |           |              |                            |     |                  |          |      |             |      |                  |          |      |             |                  |                     |               |               |                   |             |                     |                 |                   |       |    |       |                   |       |     |      |
|-----------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------|---------------|----------------------------|------|-----------|-----------|--------------|----------------------------|-----|------------------|----------|------|-------------|------|------------------|----------|------|-------------|------------------|---------------------|---------------|---------------|-------------------|-------------|---------------------|-----------------|-------------------|-------|----|-------|-------------------|-------|-----|------|
|                       | <table><tr><th>Algoritma</th><th>Area (GE)</th><th>Cycles/block</th><th>Throughput @ 100kHz (kbps)</th><th>Ref</th></tr><tr><td>Piccolo-80 (Enc)</td><td>1.048</td><td>432</td><td>14,8</td><td rowspan="6">[93]</td></tr><tr><td>Piccolo-80 (Enc)</td><td>1.499</td><td>27</td><td>237,0</td></tr><tr><td>Piccolo-80 (Enc)</td><td>1.109</td><td>432</td><td>14,8</td></tr><tr><td>Piccolo-128 (Enc)</td><td>1.338</td><td>528</td><td>12,1</td></tr><tr><td>Piccolo-128 (Enc)</td><td>1.776</td><td>33</td><td>193,9</td></tr><tr><td>Piccolo-128 (Enc)</td><td>1.397</td><td>528</td><td>12,1</td></tr></table> |                 |               |                            |      | Algoritma | Area (GE) | Cycles/block | Throughput @ 100kHz (kbps) | Ref | Piccolo-80 (Enc) | 1.048    | 432  | 14,8        | [93] | Piccolo-80 (Enc) | 1.499    | 27   | 237,0       | Piccolo-80 (Enc) | 1.109               | 432           | 14,8          | Piccolo-128 (Enc) | 1.338       | 528                 | 12,1            | Piccolo-128 (Enc) | 1.776 | 33 | 193,9 | Piccolo-128 (Enc) | 1.397 | 528 | 12,1 |
|                       | Algoritma                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          | Area (GE)       | Cycles/block  | Throughput @ 100kHz (kbps) | Ref  |           |           |              |                            |     |                  |          |      |             |      |                  |          |      |             |                  |                     |               |               |                   |             |                     |                 |                   |       |    |       |                   |       |     |      |
|                       | Piccolo-80 (Enc)                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   | 1.048           | 432           | 14,8                       | [93] |           |           |              |                            |     |                  |          |      |             |      |                  |          |      |             |                  |                     |               |               |                   |             |                     |                 |                   |       |    |       |                   |       |     |      |
|                       | Piccolo-80 (Enc)                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   | 1.499           | 27            | 237,0                      |      |           |           |              |                            |     |                  |          |      |             |      |                  |          |      |             |                  |                     |               |               |                   |             |                     |                 |                   |       |    |       |                   |       |     |      |
|                       | Piccolo-80 (Enc)                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   | 1.109           | 432           | 14,8                       |      |           |           |              |                            |     |                  |          |      |             |      |                  |          |      |             |                  |                     |               |               |                   |             |                     |                 |                   |       |    |       |                   |       |     |      |
|                       | Piccolo-128 (Enc)                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  | 1.338           | 528           | 12,1                       |      |           |           |              |                            |     |                  |          |      |             |      |                  |          |      |             |                  |                     |               |               |                   |             |                     |                 |                   |       |    |       |                   |       |     |      |
|                       | Piccolo-128 (Enc)                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  | 1.776           | 33            | 193,9                      |      |           |           |              |                            |     |                  |          |      |             |      |                  |          |      |             |                  |                     |               |               |                   |             |                     |                 |                   |       |    |       |                   |       |     |      |
|                       | Piccolo-128 (Enc)                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  | 1.397           | 528           | 12,1                       |      |           |           |              |                            |     |                  |          |      |             |      |                  |          |      |             |                  |                     |               |               |                   |             |                     |                 |                   |       |    |       |                   |       |     |      |
|                       | Hasil evaluasi implementasi perangkat lunak menunjukan:                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |                 |               |                            |      |           |           |              |                            |     |                  |          |      |             |      |                  |          |      |             |                  |                     |               |               |                   |             |                     |                 |                   |       |    |       |                   |       |     |      |
|                       | <table><tr><th>Algoritma</th><th>Type</th><th>Cycles/byte</th><th>Platform</th><th>Ref</th></tr><tr><td>Piccolo-80</td><td>Bitslice</td><td>4,57</td><td>Core i7 870</td><td rowspan="2">[99]</td></tr><tr><td>Piccolo-128</td><td>Bitslice</td><td>5,52</td><td>Core i7 870</td></tr><tr><td>Piccolo-80</td><td>Table/VPI/ Bitslice</td><td>89,3/33,3/9,2</td><td>Core i3 2367M</td><td rowspan="2">[78]</td></tr><tr><td>Piccolo-128</td><td>Table/VPI/ Bitslice</td><td>103,6/41,6/10,9</td><td>Core i3 2367M</td></tr></table>                                                                                 |                 |               |                            |      | Algoritma | Type      | Cycles/byte  | Platform                   | Ref | Piccolo-80       | Bitslice | 4,57 | Core i7 870 | [99] | Piccolo-128      | Bitslice | 5,52 | Core i7 870 | Piccolo-80       | Table/VPI/ Bitslice | 89,3/33,3/9,2 | Core i3 2367M | [78]              | Piccolo-128 | Table/VPI/ Bitslice | 103,6/41,6/10,9 | Core i3 2367M     |       |    |       |                   |       |     |      |
|                       | Algoritma                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          | Type            | Cycles/byte   | Platform                   | Ref  |           |           |              |                            |     |                  |          |      |             |      |                  |          |      |             |                  |                     |               |               |                   |             |                     |                 |                   |       |    |       |                   |       |     |      |
|                       | Piccolo-80                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         | Bitslice        | 4,57          | Core i7 870                | [99] |           |           |              |                            |     |                  |          |      |             |      |                  |          |      |             |                  |                     |               |               |                   |             |                     |                 |                   |       |    |       |                   |       |     |      |
| Piccolo-128           | Bitslice                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           | 5,52            | Core i7 870   |                            |      |           |           |              |                            |     |                  |          |      |             |      |                  |          |      |             |                  |                     |               |               |                   |             |                     |                 |                   |       |    |       |                   |       |     |      |
| Piccolo-80            | Table/VPI/ Bitslice                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                | 89,3/33,3/9,2   | Core i3 2367M | [78]                       |      |           |           |              |                            |     |                  |          |      |             |      |                  |          |      |             |                  |                     |               |               |                   |             |                     |                 |                   |       |    |       |                   |       |     |      |
| Piccolo-128           | Table/VPI/ Bitslice                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                | 103,6/41,6/10,9 | Core i3 2367M |                            |      |           |           |              |                            |     |                  |          |      |             |      |                  |          |      |             |                  |                     |               |               |                   |             |                     |                 |                   |       |    |       |                   |       |     |      |
| Informasi Open Source | lightweight-crypto-lib<br><a href="https://github.com/rb-anssi/lightweight-crypto-lib">https://github.com/rb-anssi/lightweight-crypto-lib</a>                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |                 |               |                            |      |           |           |              |                            |     |                  |          |      |             |      |                  |          |      |             |                  |                     |               |               |                   |             |                     |                 |                   |       |    |       |                   |       |     |      |

## 6. PRESENT

|                  |                     |                                                                                                                                                                                                                                                                                                                                                                  |
|------------------|---------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Profil Algoritma | Nama                | PRESENT                                                                                                                                                                                                                                                                                                                                                          |
|                  | Perancang           | Andrey Bogdanov <sup>1</sup> , Lars R. Knudsen <sup>2</sup> , Gregor Leander <sup>1</sup> , Christof Paar <sup>1</sup> , Axel Poschmann <sup>1</sup> , Matthew J. B. Robshaw <sup>3</sup> , Yannick Seurin <sup>3</sup> , C. Vikkelsøe <sup>2</sup> (1: Ruhr-University Bochum, Germany, 2: Technical University of Denmark, Denmark, 3: France Telecom, France) |
|                  | Publikasi           | 2007 (CHES'07)                                                                                                                                                                                                                                                                                                                                                   |
| Spesifikasi      | Terdapat dalam [6]. |                                                                                                                                                                                                                                                                                                                                                                  |

|                   |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |                                    |                                    |                          |                          |                   |                |
|-------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------------------------------|------------------------------------|--------------------------|--------------------------|-------------------|----------------|
| Fitur             | Algoritma PRESENT memiliki performa tinggi dalam implementasi perangkat keras yang <i>compact</i> .                                                                                                                                                                                                                                                                                                                                                                                                                            |                                    |                                    |                          |                          |                   |                |
|                   | Struktur                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |                                    | SPN                                |                          |                          |                   |                |
|                   | Panjang blok (bit)                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |                                    | 64 bit                             |                          |                          |                   |                |
|                   | Panjang kunci (bit)                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |                                    | 80 bit                             |                          | 128 bit                  |                   |                |
|                   | Jumlah <i>round</i>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |                                    | 31                                 |                          |                          |                   |                |
| Analisis keamanan | Status analisis keamanan PRESENT dalam pengaturan kunci tunggal (KPs: <i>known plaintext</i> ):                                                                                                                                                                                                                                                                                                                                                                                                                                |                                    |                                    |                          |                          |                   |                |
|                   | Algoritma                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      | <i>Rounds</i>                      | Tipe                               | Waktu                    | Data                     | Memori            | Ref            |
|                   | PRESENT<br>-80                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 | 26                                 | <i>Multidimensional<br/>Linear</i> | 2 <sup>72,0</sup>        | 2 <sup>64,0</sup><br>KPs | 2 <sup>32,0</sup> | [100]          |
|                   |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                | 26                                 | <i>Multidimensional<br/>Linear</i> | 2 <sup>72,0</sup>        | 2 <sup>63,8</sup><br>KPs | 2 <sup>32,0</sup> | [100,<br>1051] |
|                   |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                | 26                                 | <i>Multidimensional<br/>Linear</i> | 2 <sup>71,8</sup>        | 2 <sup>60,8</sup><br>KPs | 2 <sup>44,0</sup> | [102]          |
|                   |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                | 26                                 | <i>Multidimensional<br/>Linear</i> | 2 <sup>68,6</sup>        | 2 <sup>63,0</sup><br>KPs | 2 <sup>48,0</sup> | [103]          |
|                   |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                | 26                                 | <i>Multidimensional<br/>Linear</i> | 2 <sup>68,2</sup>        | 2 <sup>61,1</sup><br>KPs | 2 <sup>44,0</sup> | [102]          |
|                   |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                | 27                                 | <i>Multidimensional<br/>Linear</i> | 2 <sup>77,3</sup>        | 2 <sup>63,8</sup><br>KPs | 2 <sup>48,0</sup> | [103]          |
|                   |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                | 27                                 | <i>Multidimensional<br/>Linear</i> | 2 <sup>74,0</sup>        | 2 <sup>64,0</sup><br>KPs | 2 <sup>67,0</sup> | [104]          |
|                   |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                | 27                                 | <i>Multidimensional<br/>Linear</i> | 2 <sup>72,0</sup>        | 2 <sup>63,4</sup><br>KPs | 2 <sup>44,0</sup> | [102]          |
|                   | 28                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             | <i>Multidimensional<br/>Linear</i> | 2 <sup>77,4</sup>                  | 2 <sup>64,0</sup><br>KPs | 2 <sup>51,0</sup>        | [102]             |                |
|                   | PRESENT<br>-128                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                | 28                                 | <i>Multidimensional<br/>Linear</i> | 2 <sup>122,0</sup>       | 2 <sup>64,0</sup><br>KPs | 2 <sup>84,6</sup> | [102]          |
|                   | <p>Hingga September 2021, berbagai penelitian kriptanalisis terhadap PRESENT telah dilakukan (ditunjukkan pada tabel di atas). Namun demikian, tidak ada serangan yang lebih efisien dibandingkan <i>brute force</i> terhadap spesifikasi penuh, kecuali pada kondisi tertentu (<i>known-key setting</i>). Dalam <i>single-key setting</i>, serangan terbaik adalah <i>multidimensional linear attack</i> yang diajukan oleh Flórez-Gutiérrez, dkk [102], efektif terhadap versi tereduksi 28 <i>round</i> dari PRESENT-80</p> |                                    |                                    |                          |                          |                   |                |

|                       | <p>dan PRESENT-128, serta memungkinkan <i>key recovery</i> lebih efisien daripada <i>exhaustive search</i>. Pada <i>known-key setting</i>, <i>truncated differential attack</i> yang dikemukakan oleh Blondeau, dkk [110] dapat diaplikasikan terhadap PRESENT-80 dan PRESENT-128 dengan 31 <i>round</i> penuh, tetapi hanya menghasilkan <i>distinguishing attack</i> tanpa kemampuan <i>key recovery</i>.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |              |                       |               |             |     |                  |      |     |      |       |                  |      |    |     |     |                   |      |     |      |       |                   |      |    |     |       |           |       |            |                       |          |     |                |          |      |     |             |             |            |                     |              |  |               |      |             |                     |              |  |               |      |           |            |            |                       |          |     |            |     |    |              |      |       |            |       |    |             |      |       |
|-----------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------|-----------------------|---------------|-------------|-----|------------------|------|-----|------|-------|------------------|------|----|-----|-----|-------------------|------|-----|------|-------|-------------------|------|----|-----|-------|-----------|-------|------------|-----------------------|----------|-----|----------------|----------|------|-----|-------------|-------------|------------|---------------------|--------------|--|---------------|------|-------------|---------------------|--------------|--|---------------|------|-----------|------------|------------|-----------------------|----------|-----|------------|-----|----|--------------|------|-------|------------|-------|----|-------------|------|-------|
| Analisis Performa     | <p>Hasil evaluasi implementasi perangkat keras:</p> <table><tr><th>Algoritma</th><th>Area (GE)</th><th>Cycles/block</th><th>Throughput</th><th>Ref</th></tr><tr><td>PRESENT-80 (Enc)</td><td>1000</td><td>563</td><td>11,4</td><td>[105]</td></tr><tr><td>PRESENT-80 (Enc)</td><td>1570</td><td>32</td><td>200</td><td>[6]</td></tr><tr><td>PRESENT-128 (Enc)</td><td>1391</td><td>559</td><td>11,4</td><td>[106]</td></tr><tr><td>PRESENT-128 (Enc)</td><td>1886</td><td>32</td><td>200</td><td>[106]</td></tr></table> <p>Hasil evaluasi implementasi perangkat lunak (<i>low-end CPU</i>):</p> <table><tr><th>Algoritma</th><th>Jenis</th><th>ROM (byte)</th><th>Cycles/byte (Enc/Dec)</th><th>Platform</th><th>Ref</th></tr><tr><td>PRESENT-80/128</td><td>Bitslice</td><td>5,79</td><td>512</td><td>Core i7 870</td><td>[107]<br/>23</td></tr><tr><td>PRESENT-80</td><td>Table/VPI/ Bitslice</td><td>72,6/35/17,4</td><td></td><td>Core i3 2367M</td><td>[78]</td></tr><tr><td>PRESENT-128</td><td>Table/VPI/ Bitslice</td><td>72,5/35/18,9</td><td></td><td>Core i3 2367M</td><td>[78]</td></tr></table> <p>Hasil evaluasi implementasi perangkat lunak (<i>low-end CPU</i>):</p> <table><tr><th>Algoritma</th><th>ROM (byte)</th><th>RAM (byte)</th><th>Cycles/byte (Enc/Dec)</th><th>Platform</th><th>Ref</th></tr><tr><td>PRESENT-80</td><td>512</td><td>62</td><td>1.634/60.834</td><td>RL78</td><td>[108]</td></tr><tr><td>PRESENT-80</td><td>1.855</td><td>48</td><td>9.007/8.920</td><td>RL78</td><td>[108]</td></tr></table> | Algoritma    | Area (GE)             | Cycles/block  | Throughput  | Ref | PRESENT-80 (Enc) | 1000 | 563 | 11,4 | [105] | PRESENT-80 (Enc) | 1570 | 32 | 200 | [6] | PRESENT-128 (Enc) | 1391 | 559 | 11,4 | [106] | PRESENT-128 (Enc) | 1886 | 32 | 200 | [106] | Algoritma | Jenis | ROM (byte) | Cycles/byte (Enc/Dec) | Platform | Ref | PRESENT-80/128 | Bitslice | 5,79 | 512 | Core i7 870 | [107]<br>23 | PRESENT-80 | Table/VPI/ Bitslice | 72,6/35/17,4 |  | Core i3 2367M | [78] | PRESENT-128 | Table/VPI/ Bitslice | 72,5/35/18,9 |  | Core i3 2367M | [78] | Algoritma | ROM (byte) | RAM (byte) | Cycles/byte (Enc/Dec) | Platform | Ref | PRESENT-80 | 512 | 62 | 1.634/60.834 | RL78 | [108] | PRESENT-80 | 1.855 | 48 | 9.007/8.920 | RL78 | [108] |
| Algoritma             | Area (GE)                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  | Cycles/block | Throughput            | Ref           |             |     |                  |      |     |      |       |                  |      |    |     |     |                   |      |     |      |       |                   |      |    |     |       |           |       |            |                       |          |     |                |          |      |     |             |             |            |                     |              |  |               |      |             |                     |              |  |               |      |           |            |            |                       |          |     |            |     |    |              |      |       |            |       |    |             |      |       |
| PRESENT-80 (Enc)      | 1000                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       | 563          | 11,4                  | [105]         |             |     |                  |      |     |      |       |                  |      |    |     |     |                   |      |     |      |       |                   |      |    |     |       |           |       |            |                       |          |     |                |          |      |     |             |             |            |                     |              |  |               |      |             |                     |              |  |               |      |           |            |            |                       |          |     |            |     |    |              |      |       |            |       |    |             |      |       |
| PRESENT-80 (Enc)      | 1570                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       | 32           | 200                   | [6]           |             |     |                  |      |     |      |       |                  |      |    |     |     |                   |      |     |      |       |                   |      |    |     |       |           |       |            |                       |          |     |                |          |      |     |             |             |            |                     |              |  |               |      |             |                     |              |  |               |      |           |            |            |                       |          |     |            |     |    |              |      |       |            |       |    |             |      |       |
| PRESENT-128 (Enc)     | 1391                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       | 559          | 11,4                  | [106]         |             |     |                  |      |     |      |       |                  |      |    |     |     |                   |      |     |      |       |                   |      |    |     |       |           |       |            |                       |          |     |                |          |      |     |             |             |            |                     |              |  |               |      |             |                     |              |  |               |      |           |            |            |                       |          |     |            |     |    |              |      |       |            |       |    |             |      |       |
| PRESENT-128 (Enc)     | 1886                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       | 32           | 200                   | [106]         |             |     |                  |      |     |      |       |                  |      |    |     |     |                   |      |     |      |       |                   |      |    |     |       |           |       |            |                       |          |     |                |          |      |     |             |             |            |                     |              |  |               |      |             |                     |              |  |               |      |           |            |            |                       |          |     |            |     |    |              |      |       |            |       |    |             |      |       |
| Algoritma             | Jenis                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      | ROM (byte)   | Cycles/byte (Enc/Dec) | Platform      | Ref         |     |                  |      |     |      |       |                  |      |    |     |     |                   |      |     |      |       |                   |      |    |     |       |           |       |            |                       |          |     |                |          |      |     |             |             |            |                     |              |  |               |      |             |                     |              |  |               |      |           |            |            |                       |          |     |            |     |    |              |      |       |            |       |    |             |      |       |
| PRESENT-80/128        | Bitslice                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   | 5,79         | 512                   | Core i7 870   | [107]<br>23 |     |                  |      |     |      |       |                  |      |    |     |     |                   |      |     |      |       |                   |      |    |     |       |           |       |            |                       |          |     |                |          |      |     |             |             |            |                     |              |  |               |      |             |                     |              |  |               |      |           |            |            |                       |          |     |            |     |    |              |      |       |            |       |    |             |      |       |
| PRESENT-80            | Table/VPI/ Bitslice                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        | 72,6/35/17,4 |                       | Core i3 2367M | [78]        |     |                  |      |     |      |       |                  |      |    |     |     |                   |      |     |      |       |                   |      |    |     |       |           |       |            |                       |          |     |                |          |      |     |             |             |            |                     |              |  |               |      |             |                     |              |  |               |      |           |            |            |                       |          |     |            |     |    |              |      |       |            |       |    |             |      |       |
| PRESENT-128           | Table/VPI/ Bitslice                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        | 72,5/35/18,9 |                       | Core i3 2367M | [78]        |     |                  |      |     |      |       |                  |      |    |     |     |                   |      |     |      |       |                   |      |    |     |       |           |       |            |                       |          |     |                |          |      |     |             |             |            |                     |              |  |               |      |             |                     |              |  |               |      |           |            |            |                       |          |     |            |     |    |              |      |       |            |       |    |             |      |       |
| Algoritma             | ROM (byte)                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 | RAM (byte)   | Cycles/byte (Enc/Dec) | Platform      | Ref         |     |                  |      |     |      |       |                  |      |    |     |     |                   |      |     |      |       |                   |      |    |     |       |           |       |            |                       |          |     |                |          |      |     |             |             |            |                     |              |  |               |      |             |                     |              |  |               |      |           |            |            |                       |          |     |            |     |    |              |      |       |            |       |    |             |      |       |
| PRESENT-80            | 512                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        | 62           | 1.634/60.834          | RL78          | [108]       |     |                  |      |     |      |       |                  |      |    |     |     |                   |      |     |      |       |                   |      |    |     |       |           |       |            |                       |          |     |                |          |      |     |             |             |            |                     |              |  |               |      |             |                     |              |  |               |      |           |            |            |                       |          |     |            |     |    |              |      |       |            |       |    |             |      |       |
| PRESENT-80            | 1.855                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      | 48           | 9.007/8.920           | RL78          | [108]       |     |                  |      |     |      |       |                  |      |    |     |     |                   |      |     |      |       |                   |      |    |     |       |           |       |            |                       |          |     |                |          |      |     |             |             |            |                     |              |  |               |      |             |                     |              |  |               |      |           |            |            |                       |          |     |            |     |    |              |      |       |            |       |    |             |      |       |
| Standarisasi          | <p>ISO/IEC 29192-2</p> <p>National Cybersecurity Authority (NCA), Qatar</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |              |                       |               |             |     |                  |      |     |      |       |                  |      |    |     |     |                   |      |     |      |       |                   |      |    |     |       |           |       |            |                       |          |     |                |          |      |     |             |             |            |                     |              |  |               |      |             |                     |              |  |               |      |           |            |            |                       |          |     |            |     |    |              |      |       |            |       |    |             |      |       |
| Informasi Open Source | <p>lightweight-crypto-lib</p> <p><a href="https://github.com/rb-anssi/lightweight-crypto-lib">https://github.com/rb-anssi/lightweight-crypto-lib</a></p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |              |                       |               |             |     |                  |      |     |      |       |                  |      |    |     |     |                   |      |     |      |       |                   |      |    |     |       |           |       |            |                       |          |     |                |          |      |     |             |             |            |                     |              |  |               |      |             |                     |              |  |               |      |           |            |            |                       |          |     |            |     |    |              |      |       |            |       |    |             |      |       |

## 7. PRINCE

|                     |                                                                                                                                                                                                                                                                                                                                                                                                                                    |                                                                                                                                                                                                                         |              |                |               |            |
|---------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------|----------------|---------------|------------|
| Profil<br>Algoritma | Nama                                                                                                                                                                                                                                                                                                                                                                                                                               | PRINCE                                                                                                                                                                                                                  |              |                |               |            |
|                     | Perancang                                                                                                                                                                                                                                                                                                                                                                                                                          | Julia Borghoff, Anne Canteaut, Tim Guneysu, Elif Bilge Kavun, Miroslav Knezevic, Lars R. Knudsen, Gregor Leander, Ventzislav Nikov, Christof Paar, Christian Rechberger, Peter Rombouts, Soren S. Thomsen, Tolga Yalcin |              |                |               |            |
|                     | Publikasi                                                                                                                                                                                                                                                                                                                                                                                                                          | 2012 (ASIACRYPT 2012 [109])                                                                                                                                                                                             |              |                |               |            |
| Spesifikasi         | Terdapat dalam [113]                                                                                                                                                                                                                                                                                                                                                                                                               |                                                                                                                                                                                                                         |              |                |               |            |
| Fitur               | Perancang mengklaim bahwa algoritma PRINCE memiliki latensi rendah dan <i>compact</i> dalam implementasi perangkat keras. Karena algoritma tersebut memiliki simetri yang disebut $\alpha$ – refleksi, yang berbeda dari <i>block cipher</i> pada umumnya, jika penyerang memiliki $2^n$ pasang <i>plaintext</i> dan <i>ciphertext</i> , keamanan yang dapat diklaim hanya $(127 \times n)$ -bit meskipun digunakan kunci 128-bit. |                                                                                                                                                                                                                         |              |                |               |            |
|                     | Struktur                                                                                                                                                                                                                                                                                                                                                                                                                           | SPN                                                                                                                                                                                                                     |              |                |               |            |
|                     | Panjang blok (bit)                                                                                                                                                                                                                                                                                                                                                                                                                 | 64                                                                                                                                                                                                                      |              |                |               |            |
|                     | Panjang kunci (bit)                                                                                                                                                                                                                                                                                                                                                                                                                | 128                                                                                                                                                                                                                     |              |                |               |            |
|                     | Jumlah <i>round</i>                                                                                                                                                                                                                                                                                                                                                                                                                | 12                                                                                                                                                                                                                      |              |                |               |            |
|                     | Analisis<br>keamanan                                                                                                                                                                                                                                                                                                                                                                                                               | Status analisis keamanan PRINCE (CPs: <i>chosen plaintext</i> , KPs: <i>known plaintext</i> ):                                                                                                                          |              |                |               |            |
| <i>Rounds</i>       |                                                                                                                                                                                                                                                                                                                                                                                                                                    | <i>Tipe</i>                                                                                                                                                                                                             | <i>Waktu</i> | <i>Data</i>    | <i>Memori</i> | <i>Ref</i> |
| 4                   |                                                                                                                                                                                                                                                                                                                                                                                                                                    | <i>Integral</i>                                                                                                                                                                                                         | $2^{64,0}$   | $2^{4,0}$ CPs  | $2^{4,0}$     | [111]      |
| 4                   |                                                                                                                                                                                                                                                                                                                                                                                                                                    | <i>Meet-in-the-Middle</i>                                                                                                                                                                                               | $2^{43,3}$   | $2^{5,0}$ KPs  | $2^{26,7}$    | [112]      |
| 6                   |                                                                                                                                                                                                                                                                                                                                                                                                                                    | <i>Meet-in-the-Middle</i>                                                                                                                                                                                               | $2^{101,1}$  | $2^{6,0}$ KPs  | $2^{34,0}$    | [112]      |
| 6                   |                                                                                                                                                                                                                                                                                                                                                                                                                                    | <i>Integral</i>                                                                                                                                                                                                         | $2^{41,0}$   | $2^{18,6}$ CPs | $2^{16,0}$    | [111]      |
| 6                   |                                                                                                                                                                                                                                                                                                                                                                                                                                    | <i>Meet-in-the-Middle</i>                                                                                                                                                                                               | $2^{33,7}$   | $2^{16,0}$ CPs | $2^{31,9}$    | [112,113]  |
| 6                   |                                                                                                                                                                                                                                                                                                                                                                                                                                    | <i>Differential</i>                                                                                                                                                                                                     | $2^{32,9}$   | $2^{14,9}$ CPs | $2^{27,0}$    | [112,113]  |
| 8                   |                                                                                                                                                                                                                                                                                                                                                                                                                                    | <i>Sieve in the Middle</i>                                                                                                                                                                                              | $2^{124,0}$  | $2^{1,0}$ KPs  | $2^{20}$      | [114]      |
| 8                   |                                                                                                                                                                                                                                                                                                                                                                                                                                    | <i>Meet-in-the-Middle</i>                                                                                                                                                                                               | $2^{60,0}$   | $2^{53,0}$ CPs | $2^{30,0}$    | [115]      |
| 8                   |                                                                                                                                                                                                                                                                                                                                                                                                                                    | <i>Meet-in-the-Middle</i>                                                                                                                                                                                               | $2^{60,7}$   | $2^{16,0}$ CPs | $2^{84,9}$    | [112,113]  |
| 10                  |                                                                                                                                                                                                                                                                                                                                                                                                                                    | <i>Meet-in-the-Middle</i>                                                                                                                                                                                               | $2^{68,0}$   | $2^{57,0}$ CPs | $2^{41,0}$    | [112,113]  |
| 10                  |                                                                                                                                                                                                                                                                                                                                                                                                                                    | <i>Multiple differential</i>                                                                                                                                                                                            | $2^{60,6}$   | $2^{57,9}$ CPs | $2^{61,5}$    | [116]      |

|                       | Berdasarkan hasil kajian pada tabel di atas, meskipun berbagai penelitian kriptanalisis telah dilakukan, hingga saat ini tidak terdapat serangan yang lebih efisien dibandingkan dengan <i>exhaustive search</i> terhadap algoritma PRINCE.                                                                                                                                                                                                                                                                                                                                                                                                                          |              |                       |              |            |     |                  |       |    |       |       |                  |       |   |        |     |           |            |            |                       |          |     |        |       |     |       |          |       |
|-----------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------|-----------------------|--------------|------------|-----|------------------|-------|----|-------|-------|------------------|-------|---|--------|-----|-----------|------------|------------|-----------------------|----------|-----|--------|-------|-----|-------|----------|-------|
| Analisis Performa     | <p>Hasil evaluasi implementasi perangkat keras:</p> <table><tr><th>Algoritma</th><th>Area (GE)</th><th>Cycles/block</th><th>Throughput</th><th>Ref</th></tr><tr><td>PRINCE (Enc/Dec)</td><td>2.953</td><td>12</td><td>533,3</td><td>[117]</td></tr><tr><td>PRINCE (Enc/Dec)</td><td>8.577</td><td>1</td><td>6400,0</td><td>[4]</td></tr></table> <p>Hasil evaluasi implementasi perangkat lunak (<i>low-end CPU</i>):</p> <table><tr><th>Algoritma</th><th>ROM (byte)</th><th>RAM (byte)</th><th>Cycles/byte (Enc/Dec)</th><th>Platform</th><th>Ref</th></tr><tr><td>PRINCE</td><td>2.382</td><td>220</td><td>225,4</td><td>Attiny85</td><td>[118]</td></tr></table> | Algoritma    | Area (GE)             | Cycles/block | Throughput | Ref | PRINCE (Enc/Dec) | 2.953 | 12 | 533,3 | [117] | PRINCE (Enc/Dec) | 8.577 | 1 | 6400,0 | [4] | Algoritma | ROM (byte) | RAM (byte) | Cycles/byte (Enc/Dec) | Platform | Ref | PRINCE | 2.382 | 220 | 225,4 | Attiny85 | [118] |
| Algoritma             | Area (GE)                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            | Cycles/block | Throughput            | Ref          |            |     |                  |       |    |       |       |                  |       |   |        |     |           |            |            |                       |          |     |        |       |     |       |          |       |
| PRINCE (Enc/Dec)      | 2.953                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                | 12           | 533,3                 | [117]        |            |     |                  |       |    |       |       |                  |       |   |        |     |           |            |            |                       |          |     |        |       |     |       |          |       |
| PRINCE (Enc/Dec)      | 8.577                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                | 1            | 6400,0                | [4]          |            |     |                  |       |    |       |       |                  |       |   |        |     |           |            |            |                       |          |     |        |       |     |       |          |       |
| Algoritma             | ROM (byte)                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           | RAM (byte)   | Cycles/byte (Enc/Dec) | Platform     | Ref        |     |                  |       |    |       |       |                  |       |   |        |     |           |            |            |                       |          |     |        |       |     |       |          |       |
| PRINCE                | 2.382                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                | 220          | 225,4                 | Attiny85     | [118]      |     |                  |       |    |       |       |                  |       |   |        |     |           |            |            |                       |          |     |        |       |     |       |          |       |
| Informasi Open Source | Kode sumber tidak disediakan di halaman web resmi. Namun, desainer akan menyediakan kode sumber perangkat keras (Verilog-HDL) dan perangkat lunak (C) bila diminta.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |              |                       |              |            |     |                  |       |    |       |       |                  |       |   |        |     |           |            |            |                       |          |     |        |       |     |       |          |       |

## 8. SIMON

|                  |                                                                                                                                                                                                                                                                                 |                                                                                                                             |
|------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------|
| Profil Algoritma | Nama                                                                                                                                                                                                                                                                            | SIMON                                                                                                                       |
|                  | Perancang                                                                                                                                                                                                                                                                       | Ray Beaulieu, Douglas Shors, Jason Smith, Stefan Treatman-Clark, Bryan Weeks, Louis Wingers (National Security Agency, USA) |
|                  | Publikasi                                                                                                                                                                                                                                                                       | 2013 (Cryptology ePrint Archive [119])                                                                                      |
| Spesifikasi      | Terdapat dalam [119]                                                                                                                                                                                                                                                            |                                                                                                                             |
| Fitur            | Perancang mengklaim bahwa algoritma SIMON mendukung berbagai panjang blok dan kunci serta memiliki bobot yang lebih ringan baik dalam implementasi perangkat keras maupun perangkat lunak, terutama dalam implementasi perangkat keras. SIMON dengan panjang blok $2n$ -bit dan |                                                                                                                             |

|                     |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |                         |             |             |       |      |     |         |     |                         |            |            |                    |    |              |            |            |       |    |              |            |            |       |                     |        |            |            |       |     |          |            |            |       |     |                     |            |            |       |    |                     |            |            |    |    |                     |            |            |  |         |    |                     |            |            |  |    |          |            |            |       |    |        |            |            |       |    |          |            |            |       |         |    |        |            |            |       |    |        |            |            |       |         |    |        |             |            |  |    |        |            |            |       |    |        |             |            |  |          |    |        |             |            |       |    |        |             |             |       |    |        |             |             |  |    |        |             |             |  |  |    |        |             |             |       |
|---------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------|-------------|-------------|-------|------|-----|---------|-----|-------------------------|------------|------------|--------------------|----|--------------|------------|------------|-------|----|--------------|------------|------------|-------|---------------------|--------|------------|------------|-------|-----|----------|------------|------------|-------|-----|---------------------|------------|------------|-------|----|---------------------|------------|------------|----|----|---------------------|------------|------------|--|---------|----|---------------------|------------|------------|--|----|----------|------------|------------|-------|----|--------|------------|------------|-------|----|----------|------------|------------|-------|---------|----|--------|------------|------------|-------|----|--------|------------|------------|-------|---------|----|--------|-------------|------------|--|----|--------|------------|------------|-------|----|--------|-------------|------------|--|----------|----|--------|-------------|------------|-------|----|--------|-------------|-------------|-------|----|--------|-------------|-------------|--|----|--------|-------------|-------------|--|--|----|--------|-------------|-------------|-------|
|                     | <p>panjang kunci <i>m-word</i> dinotasikan sebagai SIMON <math>2n/mn</math>. Misalnya, SIMON64/128 berarti SIMON dengan panjang blok 64 bit dan panjang kunci 128 bit.</p> <table><tr><td>Struktur</td><td colspan="10">Feistel</td></tr><tr><td>Panjang blok (bit)</td><td>32</td><td colspan="2">48</td><td colspan="2">64</td><td colspan="2">96</td><td colspan="3">128</td></tr><tr><td>Panjang kunci (bit)</td><td>64</td><td>72</td><td>96</td><td>96</td><td>128</td><td>96</td><td>144</td><td>128</td><td>192</td><td>256</td></tr><tr><td>Jumlah round</td><td>32</td><td colspan="2">36</td><td>42</td><td>44</td><td>52</td><td>54</td><td>68</td><td>69</td><td>72</td></tr></table>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              | Struktur                | Feistel     |             |       |      |     |         |     |                         |            |            | Panjang blok (bit) | 32 | 48           |            | 64         |       | 96 |              | 128        |            |       | Panjang kunci (bit) | 64     | 72         | 96         | 96    | 128 | 96       | 144        | 128        | 192   | 256 | Jumlah round        | 32         | 36         |       | 42 | 44                  | 52         | 54         | 68 | 69 | 72                  |            |            |  |         |    |                     |            |            |  |    |          |            |            |       |    |        |            |            |       |    |          |            |            |       |         |    |        |            |            |       |    |        |            |            |       |         |    |        |             |            |  |    |        |            |            |       |    |        |             |            |  |          |    |        |             |            |       |    |        |             |             |       |    |        |             |             |  |    |        |             |             |  |  |    |        |             |             |       |
| Struktur            | Feistel                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |                         |             |             |       |      |     |         |     |                         |            |            |                    |    |              |            |            |       |    |              |            |            |       |                     |        |            |            |       |     |          |            |            |       |     |                     |            |            |       |    |                     |            |            |    |    |                     |            |            |  |         |    |                     |            |            |  |    |          |            |            |       |    |        |            |            |       |    |          |            |            |       |         |    |        |            |            |       |    |        |            |            |       |         |    |        |             |            |  |    |        |            |            |       |    |        |             |            |  |          |    |        |             |            |       |    |        |             |             |       |    |        |             |             |  |    |        |             |             |  |  |    |        |             |             |       |
| Panjang blok (bit)  | 32                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              | 48                      |             | 64          |       | 96   |     | 128     |     |                         |            |            |                    |    |              |            |            |       |    |              |            |            |       |                     |        |            |            |       |     |          |            |            |       |     |                     |            |            |       |    |                     |            |            |    |    |                     |            |            |  |         |    |                     |            |            |  |    |          |            |            |       |    |        |            |            |       |    |          |            |            |       |         |    |        |            |            |       |    |        |            |            |       |         |    |        |             |            |  |    |        |            |            |       |    |        |             |            |  |          |    |        |             |            |       |    |        |             |             |       |    |        |             |             |  |    |        |             |             |  |  |    |        |             |             |       |
| Panjang kunci (bit) | 64                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              | 72                      | 96          | 96          | 128   | 96   | 144 | 128     | 192 | 256                     |            |            |                    |    |              |            |            |       |    |              |            |            |       |                     |        |            |            |       |     |          |            |            |       |     |                     |            |            |       |    |                     |            |            |    |    |                     |            |            |  |         |    |                     |            |            |  |    |          |            |            |       |    |        |            |            |       |    |          |            |            |       |         |    |        |            |            |       |    |        |            |            |       |         |    |        |             |            |  |    |        |            |            |       |    |        |             |            |  |          |    |        |             |            |       |    |        |             |             |       |    |        |             |             |  |    |        |             |             |  |  |    |        |             |             |       |
| Jumlah round        | 32                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              | 36                      |             | 42          | 44    | 52   | 54  | 68      | 69  | 72                      |            |            |                    |    |              |            |            |       |    |              |            |            |       |                     |        |            |            |       |     |          |            |            |       |     |                     |            |            |       |    |                     |            |            |    |    |                     |            |            |  |         |    |                     |            |            |  |    |          |            |            |       |    |        |            |            |       |    |          |            |            |       |         |    |        |            |            |       |    |        |            |            |       |         |    |        |             |            |  |    |        |            |            |       |    |        |             |            |  |          |    |        |             |            |       |    |        |             |             |       |    |        |             |             |  |    |        |             |             |  |  |    |        |             |             |       |
| Analisis keamanan   | <p>Status analisis keamanan SIMON dalam pengaturan kunci tunggal</p> <table><tr><td>Algoritma</td><td>Rounds</td><td>Type</td><td>Waktu</td><td>Data</td><td>Ref</td></tr><tr><td rowspan="8">SIMON32</td><td>20</td><td>Impossible Differential</td><td><math>2^{62,8}</math></td><td><math>2^{32,0}</math></td><td>[119]</td></tr><tr><td>21</td><td>Differential</td><td><math>2^{55,3}</math></td><td><math>2^{31,0}</math></td><td>[120]</td></tr><tr><td>22</td><td>Differential</td><td><math>2^{58,8}</math></td><td><math>2^{32,0}</math></td><td>[121]</td></tr><tr><td>23</td><td>Linear</td><td><math>2^{61,8}</math></td><td><math>2^{31,2}</math></td><td>[122]</td></tr><tr><td>24</td><td>Integral</td><td><math>2^{63,0}</math></td><td><math>2^{32,0}</math></td><td>[123]</td></tr><tr><td>24</td><td>Correlated Sequence</td><td><math>2^{61,8}</math></td><td><math>2^{31,2}</math></td><td>[124]</td></tr><tr><td>25</td><td>Correlated Sequence</td><td><math>2^{61,8}</math></td><td><math>2^{31,2}</math></td><td></td></tr><tr><td>26</td><td>Correlated Sequence</td><td><math>2^{61,8}</math></td><td><math>2^{31,2}</math></td><td></td></tr><tr><td rowspan="4">SIMON48</td><td>27</td><td>Correlated Sequence</td><td><math>2^{61,8}</math></td><td><math>2^{31,2}</math></td><td></td></tr><tr><td>24</td><td>Integral</td><td><math>2^{71,0}</math></td><td><math>2^{48,0}</math></td><td>[123]</td></tr><tr><td>24</td><td>Linear</td><td><math>2^{67,9}</math></td><td><math>2^{47,9}</math></td><td>[122]</td></tr><tr><td>25</td><td>Integral</td><td><math>2^{95,0}</math></td><td><math>2^{48,0}</math></td><td>[123]</td></tr><tr><td rowspan="2">SIMON64</td><td>25</td><td>Linear</td><td><math>2^{89,9}</math></td><td><math>2^{47,9}</math></td><td>[122]</td></tr><tr><td>30</td><td>Linear</td><td><math>2^{93,6}</math></td><td><math>2^{63,5}</math></td><td>[122]</td></tr><tr><td rowspan="3">SIMON96</td><td>31</td><td>Linear</td><td><math>2^{120,0}</math></td><td><math>2^{63,5}</math></td><td></td></tr><tr><td>37</td><td>Linear</td><td><math>2^{88,0}</math></td><td><math>2^{95,2}</math></td><td>[122]</td></tr><tr><td>38</td><td>Linear</td><td><math>2^{136,0}</math></td><td><math>2^{95,2}</math></td><td></td></tr><tr><td rowspan="4">SIMON128</td><td>45</td><td>Linear</td><td><math>2^{136,5}</math></td><td><math>2^{95,0}</math></td><td>[125]</td></tr><tr><td>49</td><td>Linear</td><td><math>2^{120,0}</math></td><td><math>2^{127,6}</math></td><td>[122]</td></tr><tr><td>51</td><td>Linear</td><td><math>2^{184,0}</math></td><td><math>2^{127,6}</math></td><td></td></tr><tr><td>53</td><td>Linear</td><td><math>2^{248,0}</math></td><td><math>2^{127,6}</math></td><td></td></tr><tr><td></td><td>56</td><td>Linear</td><td><math>2^{249,0}</math></td><td><math>2^{126,0}</math></td><td>[125]</td></tr></table> <p>Status analisis keamanan SIMON dalam pengaturan <i>related-key</i></p> | Algoritma               | Rounds      | Type        | Waktu | Data | Ref | SIMON32 | 20  | Impossible Differential | $2^{62,8}$ | $2^{32,0}$ | [119]              | 21 | Differential | $2^{55,3}$ | $2^{31,0}$ | [120] | 22 | Differential | $2^{58,8}$ | $2^{32,0}$ | [121] | 23                  | Linear | $2^{61,8}$ | $2^{31,2}$ | [122] | 24  | Integral | $2^{63,0}$ | $2^{32,0}$ | [123] | 24  | Correlated Sequence | $2^{61,8}$ | $2^{31,2}$ | [124] | 25 | Correlated Sequence | $2^{61,8}$ | $2^{31,2}$ |    | 26 | Correlated Sequence | $2^{61,8}$ | $2^{31,2}$ |  | SIMON48 | 27 | Correlated Sequence | $2^{61,8}$ | $2^{31,2}$ |  | 24 | Integral | $2^{71,0}$ | $2^{48,0}$ | [123] | 24 | Linear | $2^{67,9}$ | $2^{47,9}$ | [122] | 25 | Integral | $2^{95,0}$ | $2^{48,0}$ | [123] | SIMON64 | 25 | Linear | $2^{89,9}$ | $2^{47,9}$ | [122] | 30 | Linear | $2^{93,6}$ | $2^{63,5}$ | [122] | SIMON96 | 31 | Linear | $2^{120,0}$ | $2^{63,5}$ |  | 37 | Linear | $2^{88,0}$ | $2^{95,2}$ | [122] | 38 | Linear | $2^{136,0}$ | $2^{95,2}$ |  | SIMON128 | 45 | Linear | $2^{136,5}$ | $2^{95,0}$ | [125] | 49 | Linear | $2^{120,0}$ | $2^{127,6}$ | [122] | 51 | Linear | $2^{184,0}$ | $2^{127,6}$ |  | 53 | Linear | $2^{248,0}$ | $2^{127,6}$ |  |  | 56 | Linear | $2^{249,0}$ | $2^{126,0}$ | [125] |
| Algoritma           | Rounds                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          | Type                    | Waktu       | Data        | Ref   |      |     |         |     |                         |            |            |                    |    |              |            |            |       |    |              |            |            |       |                     |        |            |            |       |     |          |            |            |       |     |                     |            |            |       |    |                     |            |            |    |    |                     |            |            |  |         |    |                     |            |            |  |    |          |            |            |       |    |        |            |            |       |    |          |            |            |       |         |    |        |            |            |       |    |        |            |            |       |         |    |        |             |            |  |    |        |            |            |       |    |        |             |            |  |          |    |        |             |            |       |    |        |             |             |       |    |        |             |             |  |    |        |             |             |  |  |    |        |             |             |       |
| SIMON32             | 20                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              | Impossible Differential | $2^{62,8}$  | $2^{32,0}$  | [119] |      |     |         |     |                         |            |            |                    |    |              |            |            |       |    |              |            |            |       |                     |        |            |            |       |     |          |            |            |       |     |                     |            |            |       |    |                     |            |            |    |    |                     |            |            |  |         |    |                     |            |            |  |    |          |            |            |       |    |        |            |            |       |    |          |            |            |       |         |    |        |            |            |       |    |        |            |            |       |         |    |        |             |            |  |    |        |            |            |       |    |        |             |            |  |          |    |        |             |            |       |    |        |             |             |       |    |        |             |             |  |    |        |             |             |  |  |    |        |             |             |       |
|                     | 21                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              | Differential            | $2^{55,3}$  | $2^{31,0}$  | [120] |      |     |         |     |                         |            |            |                    |    |              |            |            |       |    |              |            |            |       |                     |        |            |            |       |     |          |            |            |       |     |                     |            |            |       |    |                     |            |            |    |    |                     |            |            |  |         |    |                     |            |            |  |    |          |            |            |       |    |        |            |            |       |    |          |            |            |       |         |    |        |            |            |       |    |        |            |            |       |         |    |        |             |            |  |    |        |            |            |       |    |        |             |            |  |          |    |        |             |            |       |    |        |             |             |       |    |        |             |             |  |    |        |             |             |  |  |    |        |             |             |       |
|                     | 22                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              | Differential            | $2^{58,8}$  | $2^{32,0}$  | [121] |      |     |         |     |                         |            |            |                    |    |              |            |            |       |    |              |            |            |       |                     |        |            |            |       |     |          |            |            |       |     |                     |            |            |       |    |                     |            |            |    |    |                     |            |            |  |         |    |                     |            |            |  |    |          |            |            |       |    |        |            |            |       |    |          |            |            |       |         |    |        |            |            |       |    |        |            |            |       |         |    |        |             |            |  |    |        |            |            |       |    |        |             |            |  |          |    |        |             |            |       |    |        |             |             |       |    |        |             |             |  |    |        |             |             |  |  |    |        |             |             |       |
|                     | 23                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              | Linear                  | $2^{61,8}$  | $2^{31,2}$  | [122] |      |     |         |     |                         |            |            |                    |    |              |            |            |       |    |              |            |            |       |                     |        |            |            |       |     |          |            |            |       |     |                     |            |            |       |    |                     |            |            |    |    |                     |            |            |  |         |    |                     |            |            |  |    |          |            |            |       |    |        |            |            |       |    |          |            |            |       |         |    |        |            |            |       |    |        |            |            |       |         |    |        |             |            |  |    |        |            |            |       |    |        |             |            |  |          |    |        |             |            |       |    |        |             |             |       |    |        |             |             |  |    |        |             |             |  |  |    |        |             |             |       |
|                     | 24                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              | Integral                | $2^{63,0}$  | $2^{32,0}$  | [123] |      |     |         |     |                         |            |            |                    |    |              |            |            |       |    |              |            |            |       |                     |        |            |            |       |     |          |            |            |       |     |                     |            |            |       |    |                     |            |            |    |    |                     |            |            |  |         |    |                     |            |            |  |    |          |            |            |       |    |        |            |            |       |    |          |            |            |       |         |    |        |            |            |       |    |        |            |            |       |         |    |        |             |            |  |    |        |            |            |       |    |        |             |            |  |          |    |        |             |            |       |    |        |             |             |       |    |        |             |             |  |    |        |             |             |  |  |    |        |             |             |       |
|                     | 24                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              | Correlated Sequence     | $2^{61,8}$  | $2^{31,2}$  | [124] |      |     |         |     |                         |            |            |                    |    |              |            |            |       |    |              |            |            |       |                     |        |            |            |       |     |          |            |            |       |     |                     |            |            |       |    |                     |            |            |    |    |                     |            |            |  |         |    |                     |            |            |  |    |          |            |            |       |    |        |            |            |       |    |          |            |            |       |         |    |        |            |            |       |    |        |            |            |       |         |    |        |             |            |  |    |        |            |            |       |    |        |             |            |  |          |    |        |             |            |       |    |        |             |             |       |    |        |             |             |  |    |        |             |             |  |  |    |        |             |             |       |
|                     | 25                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              | Correlated Sequence     | $2^{61,8}$  | $2^{31,2}$  |       |      |     |         |     |                         |            |            |                    |    |              |            |            |       |    |              |            |            |       |                     |        |            |            |       |     |          |            |            |       |     |                     |            |            |       |    |                     |            |            |    |    |                     |            |            |  |         |    |                     |            |            |  |    |          |            |            |       |    |        |            |            |       |    |          |            |            |       |         |    |        |            |            |       |    |        |            |            |       |         |    |        |             |            |  |    |        |            |            |       |    |        |             |            |  |          |    |        |             |            |       |    |        |             |             |       |    |        |             |             |  |    |        |             |             |  |  |    |        |             |             |       |
|                     | 26                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              | Correlated Sequence     | $2^{61,8}$  | $2^{31,2}$  |       |      |     |         |     |                         |            |            |                    |    |              |            |            |       |    |              |            |            |       |                     |        |            |            |       |     |          |            |            |       |     |                     |            |            |       |    |                     |            |            |    |    |                     |            |            |  |         |    |                     |            |            |  |    |          |            |            |       |    |        |            |            |       |    |          |            |            |       |         |    |        |            |            |       |    |        |            |            |       |         |    |        |             |            |  |    |        |            |            |       |    |        |             |            |  |          |    |        |             |            |       |    |        |             |             |       |    |        |             |             |  |    |        |             |             |  |  |    |        |             |             |       |
| SIMON48             | 27                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              | Correlated Sequence     | $2^{61,8}$  | $2^{31,2}$  |       |      |     |         |     |                         |            |            |                    |    |              |            |            |       |    |              |            |            |       |                     |        |            |            |       |     |          |            |            |       |     |                     |            |            |       |    |                     |            |            |    |    |                     |            |            |  |         |    |                     |            |            |  |    |          |            |            |       |    |        |            |            |       |    |          |            |            |       |         |    |        |            |            |       |    |        |            |            |       |         |    |        |             |            |  |    |        |            |            |       |    |        |             |            |  |          |    |        |             |            |       |    |        |             |             |       |    |        |             |             |  |    |        |             |             |  |  |    |        |             |             |       |
|                     | 24                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              | Integral                | $2^{71,0}$  | $2^{48,0}$  | [123] |      |     |         |     |                         |            |            |                    |    |              |            |            |       |    |              |            |            |       |                     |        |            |            |       |     |          |            |            |       |     |                     |            |            |       |    |                     |            |            |    |    |                     |            |            |  |         |    |                     |            |            |  |    |          |            |            |       |    |        |            |            |       |    |          |            |            |       |         |    |        |            |            |       |    |        |            |            |       |         |    |        |             |            |  |    |        |            |            |       |    |        |             |            |  |          |    |        |             |            |       |    |        |             |             |       |    |        |             |             |  |    |        |             |             |  |  |    |        |             |             |       |
|                     | 24                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              | Linear                  | $2^{67,9}$  | $2^{47,9}$  | [122] |      |     |         |     |                         |            |            |                    |    |              |            |            |       |    |              |            |            |       |                     |        |            |            |       |     |          |            |            |       |     |                     |            |            |       |    |                     |            |            |    |    |                     |            |            |  |         |    |                     |            |            |  |    |          |            |            |       |    |        |            |            |       |    |          |            |            |       |         |    |        |            |            |       |    |        |            |            |       |         |    |        |             |            |  |    |        |            |            |       |    |        |             |            |  |          |    |        |             |            |       |    |        |             |             |       |    |        |             |             |  |    |        |             |             |  |  |    |        |             |             |       |
|                     | 25                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              | Integral                | $2^{95,0}$  | $2^{48,0}$  | [123] |      |     |         |     |                         |            |            |                    |    |              |            |            |       |    |              |            |            |       |                     |        |            |            |       |     |          |            |            |       |     |                     |            |            |       |    |                     |            |            |    |    |                     |            |            |  |         |    |                     |            |            |  |    |          |            |            |       |    |        |            |            |       |    |          |            |            |       |         |    |        |            |            |       |    |        |            |            |       |         |    |        |             |            |  |    |        |            |            |       |    |        |             |            |  |          |    |        |             |            |       |    |        |             |             |       |    |        |             |             |  |    |        |             |             |  |  |    |        |             |             |       |
| SIMON64             | 25                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              | Linear                  | $2^{89,9}$  | $2^{47,9}$  | [122] |      |     |         |     |                         |            |            |                    |    |              |            |            |       |    |              |            |            |       |                     |        |            |            |       |     |          |            |            |       |     |                     |            |            |       |    |                     |            |            |    |    |                     |            |            |  |         |    |                     |            |            |  |    |          |            |            |       |    |        |            |            |       |    |          |            |            |       |         |    |        |            |            |       |    |        |            |            |       |         |    |        |             |            |  |    |        |            |            |       |    |        |             |            |  |          |    |        |             |            |       |    |        |             |             |       |    |        |             |             |  |    |        |             |             |  |  |    |        |             |             |       |
|                     | 30                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              | Linear                  | $2^{93,6}$  | $2^{63,5}$  | [122] |      |     |         |     |                         |            |            |                    |    |              |            |            |       |    |              |            |            |       |                     |        |            |            |       |     |          |            |            |       |     |                     |            |            |       |    |                     |            |            |    |    |                     |            |            |  |         |    |                     |            |            |  |    |          |            |            |       |    |        |            |            |       |    |          |            |            |       |         |    |        |            |            |       |    |        |            |            |       |         |    |        |             |            |  |    |        |            |            |       |    |        |             |            |  |          |    |        |             |            |       |    |        |             |             |       |    |        |             |             |  |    |        |             |             |  |  |    |        |             |             |       |
| SIMON96             | 31                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              | Linear                  | $2^{120,0}$ | $2^{63,5}$  |       |      |     |         |     |                         |            |            |                    |    |              |            |            |       |    |              |            |            |       |                     |        |            |            |       |     |          |            |            |       |     |                     |            |            |       |    |                     |            |            |    |    |                     |            |            |  |         |    |                     |            |            |  |    |          |            |            |       |    |        |            |            |       |    |          |            |            |       |         |    |        |            |            |       |    |        |            |            |       |         |    |        |             |            |  |    |        |            |            |       |    |        |             |            |  |          |    |        |             |            |       |    |        |             |             |       |    |        |             |             |  |    |        |             |             |  |  |    |        |             |             |       |
|                     | 37                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              | Linear                  | $2^{88,0}$  | $2^{95,2}$  | [122] |      |     |         |     |                         |            |            |                    |    |              |            |            |       |    |              |            |            |       |                     |        |            |            |       |     |          |            |            |       |     |                     |            |            |       |    |                     |            |            |    |    |                     |            |            |  |         |    |                     |            |            |  |    |          |            |            |       |    |        |            |            |       |    |          |            |            |       |         |    |        |            |            |       |    |        |            |            |       |         |    |        |             |            |  |    |        |            |            |       |    |        |             |            |  |          |    |        |             |            |       |    |        |             |             |       |    |        |             |             |  |    |        |             |             |  |  |    |        |             |             |       |
|                     | 38                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              | Linear                  | $2^{136,0}$ | $2^{95,2}$  |       |      |     |         |     |                         |            |            |                    |    |              |            |            |       |    |              |            |            |       |                     |        |            |            |       |     |          |            |            |       |     |                     |            |            |       |    |                     |            |            |    |    |                     |            |            |  |         |    |                     |            |            |  |    |          |            |            |       |    |        |            |            |       |    |          |            |            |       |         |    |        |            |            |       |    |        |            |            |       |         |    |        |             |            |  |    |        |            |            |       |    |        |             |            |  |          |    |        |             |            |       |    |        |             |             |       |    |        |             |             |  |    |        |             |             |  |  |    |        |             |             |       |
| SIMON128            | 45                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              | Linear                  | $2^{136,5}$ | $2^{95,0}$  | [125] |      |     |         |     |                         |            |            |                    |    |              |            |            |       |    |              |            |            |       |                     |        |            |            |       |     |          |            |            |       |     |                     |            |            |       |    |                     |            |            |    |    |                     |            |            |  |         |    |                     |            |            |  |    |          |            |            |       |    |        |            |            |       |    |          |            |            |       |         |    |        |            |            |       |    |        |            |            |       |         |    |        |             |            |  |    |        |            |            |       |    |        |             |            |  |          |    |        |             |            |       |    |        |             |             |       |    |        |             |             |  |    |        |             |             |  |  |    |        |             |             |       |
|                     | 49                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              | Linear                  | $2^{120,0}$ | $2^{127,6}$ | [122] |      |     |         |     |                         |            |            |                    |    |              |            |            |       |    |              |            |            |       |                     |        |            |            |       |     |          |            |            |       |     |                     |            |            |       |    |                     |            |            |    |    |                     |            |            |  |         |    |                     |            |            |  |    |          |            |            |       |    |        |            |            |       |    |          |            |            |       |         |    |        |            |            |       |    |        |            |            |       |         |    |        |             |            |  |    |        |            |            |       |    |        |             |            |  |          |    |        |             |            |       |    |        |             |             |       |    |        |             |             |  |    |        |             |             |  |  |    |        |             |             |       |
|                     | 51                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              | Linear                  | $2^{184,0}$ | $2^{127,6}$ |       |      |     |         |     |                         |            |            |                    |    |              |            |            |       |    |              |            |            |       |                     |        |            |            |       |     |          |            |            |       |     |                     |            |            |       |    |                     |            |            |    |    |                     |            |            |  |         |    |                     |            |            |  |    |          |            |            |       |    |        |            |            |       |    |          |            |            |       |         |    |        |            |            |       |    |        |            |            |       |         |    |        |             |            |  |    |        |            |            |       |    |        |             |            |  |          |    |        |             |            |       |    |        |             |             |       |    |        |             |             |  |    |        |             |             |  |  |    |        |             |             |       |
|                     | 53                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              | Linear                  | $2^{248,0}$ | $2^{127,6}$ |       |      |     |         |     |                         |            |            |                    |    |              |            |            |       |    |              |            |            |       |                     |        |            |            |       |     |          |            |            |       |     |                     |            |            |       |    |                     |            |            |    |    |                     |            |            |  |         |    |                     |            |            |  |    |          |            |            |       |    |        |            |            |       |    |          |            |            |       |         |    |        |            |            |       |    |        |            |            |       |         |    |        |             |            |  |    |        |            |            |       |    |        |             |            |  |          |    |        |             |            |       |    |        |             |             |       |    |        |             |             |  |    |        |             |             |  |  |    |        |             |             |       |
|                     | 56                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              | Linear                  | $2^{249,0}$ | $2^{126,0}$ | [125] |      |     |         |     |                         |            |            |                    |    |              |            |            |       |    |              |            |            |       |                     |        |            |            |       |     |          |            |            |       |     |                     |            |            |       |    |                     |            |            |    |    |                     |            |            |  |         |    |                     |            |            |  |    |          |            |            |       |    |        |            |            |       |    |          |            |            |       |         |    |        |            |            |       |    |        |            |            |       |         |    |        |             |            |  |    |        |            |            |       |    |        |             |            |  |          |    |        |             |            |       |    |        |             |             |       |    |        |             |             |  |    |        |             |             |  |  |    |        |             |             |       |

|                       | <table><tr><th>Algoritma</th><th>Rounds</th><th>Tipe</th><th>Waktu</th><th>Data</th><th>Ref</th></tr><tr><td>SIMON32</td><td>23</td><td>Linear</td><td>2<sup>46,7</sup></td><td>2<sup>46,3</sup></td><td rowspan="5">[126]</td></tr><tr><td>SIMON48</td><td>28</td><td>Linear</td><td>2<sup>71,1</sup></td><td>2<sup>70,9</sup></td></tr><tr><td>SIMON64</td><td>34</td><td>Linear</td><td>2<sup>95,5</sup></td><td>2<sup>96,3</sup></td></tr><tr><td rowspan="2">SIMON128</td><td>55</td><td>Linear</td><td>2<sup>175,0</sup></td><td>2<sup>174,7</sup></td></tr><tr><td>62</td><td>Linear</td><td>2<sup>190,8</sup></td><td>2<sup>190,4</sup></td></tr></table>                                                                                                                                                                                                                                                                                                                                                                                               | Algoritma    | Rounds                | Tipe               | Waktu      | Data | Ref        | SIMON32 | 23    | Linear | 2 <sup>46,7</sup> | 2 <sup>46,3</sup> | [126] | SIMON48 | 28  | Linear       | 2 <sup>71,1</sup> | 2 <sup>70,9</sup> | SIMON64 | 34           | Linear | 2 <sup>95,5</sup> | 2 <sup>96,3</sup> | SIMON128  | 55         | Linear     | 2 <sup>175,0</sup>    | 2 <sup>174,7</sup> | 62  | Linear     | 2 <sup>190,8</sup> | 2 <sup>190,4</sup> |     |          |       |             |     |   |     |          |              |     |   |     |          |              |     |   |     |          |
|-----------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------|-----------------------|--------------------|------------|------|------------|---------|-------|--------|-------------------|-------------------|-------|---------|-----|--------------|-------------------|-------------------|---------|--------------|--------|-------------------|-------------------|-----------|------------|------------|-----------------------|--------------------|-----|------------|--------------------|--------------------|-----|----------|-------|-------------|-----|---|-----|----------|--------------|-----|---|-----|----------|--------------|-----|---|-----|----------|
| Algoritma             | Rounds                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          | Tipe         | Waktu                 | Data               | Ref        |      |            |         |       |        |                   |                   |       |         |     |              |                   |                   |         |              |        |                   |                   |           |            |            |                       |                    |     |            |                    |                    |     |          |       |             |     |   |     |          |              |     |   |     |          |              |     |   |     |          |
| SIMON32               | 23                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              | Linear       | 2 <sup>46,7</sup>     | 2 <sup>46,3</sup>  | [126]      |      |            |         |       |        |                   |                   |       |         |     |              |                   |                   |         |              |        |                   |                   |           |            |            |                       |                    |     |            |                    |                    |     |          |       |             |     |   |     |          |              |     |   |     |          |              |     |   |     |          |
| SIMON48               | 28                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              | Linear       | 2 <sup>71,1</sup>     | 2 <sup>70,9</sup>  |            |      |            |         |       |        |                   |                   |       |         |     |              |                   |                   |         |              |        |                   |                   |           |            |            |                       |                    |     |            |                    |                    |     |          |       |             |     |   |     |          |              |     |   |     |          |              |     |   |     |          |
| SIMON64               | 34                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              | Linear       | 2 <sup>95,5</sup>     | 2 <sup>96,3</sup>  |            |      |            |         |       |        |                   |                   |       |         |     |              |                   |                   |         |              |        |                   |                   |           |            |            |                       |                    |     |            |                    |                    |     |          |       |             |     |   |     |          |              |     |   |     |          |              |     |   |     |          |
| SIMON128              | 55                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              | Linear       | 2 <sup>175,0</sup>    | 2 <sup>174,7</sup> |            |      |            |         |       |        |                   |                   |       |         |     |              |                   |                   |         |              |        |                   |                   |           |            |            |                       |                    |     |            |                    |                    |     |          |       |             |     |   |     |          |              |     |   |     |          |              |     |   |     |          |
|                       | 62                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              | Linear       | 2 <sup>190,8</sup>    | 2 <sup>190,4</sup> |            |      |            |         |       |        |                   |                   |       |         |     |              |                   |                   |         |              |        |                   |                   |           |            |            |                       |                    |     |            |                    |                    |     |          |       |             |     |   |     |          |              |     |   |     |          |              |     |   |     |          |
|                       | <p>Berdasarkan hasil kajian pada tabel di atas, meskipun berbagai penelitian kriptanalisis telah dilakukan, hingga saat ini tidak terdapat serangan yang lebih efisien dibandingkan dengan <i>exhaustive search</i> terhadap semua varian algoritma SIMON.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |              |                       |                    |            |      |            |         |       |        |                   |                   |       |         |     |              |                   |                   |         |              |        |                   |                   |           |            |            |                       |                    |     |            |                    |                    |     |          |       |             |     |   |     |          |              |     |   |     |          |              |     |   |     |          |
| Analisis Performa     | <p>Hasil evaluasi implementasi perangkat keras:</p> <table><tr><th>Algoritma</th><th>Area (GE)</th><th>Cycles/block</th><th>Throughput</th><th>Ref</th></tr><tr><td>SIMON64/96</td><td>809</td><td>1.455</td><td>4,4</td><td rowspan="4">[119]</td></tr><tr><td>SIMON64/128</td><td>958</td><td>1.524</td><td>4,2</td></tr><tr><td>SIMON128/128</td><td>1.234</td><td>4.414</td><td>2,9</td></tr><tr><td>SIMON128/256</td><td>1.782</td><td>4.923</td><td>2,6</td></tr></table> <p>Hasil evaluasi implementasi perangkat lunak (<i>low-end CPU</i>):</p> <table><tr><th>Algoritma</th><th>ROM (byte)</th><th>RAM (byte)</th><th>Cycles/byte (Enc/Dec)</th><th>Platform</th><th>Ref</th></tr><tr><td>SIMON64/96</td><td>274</td><td>0</td><td>239</td><td>ATtiny45</td><td rowspan="4">[119]</td></tr><tr><td>SIMON64/128</td><td>282</td><td>0</td><td>250</td><td>ATtiny45</td></tr><tr><td>SIMON128/128</td><td>732</td><td>0</td><td>376</td><td>ATtiny45</td></tr><tr><td>SIMON128/256</td><td>764</td><td>0</td><td>398</td><td>ATtiny45</td></tr></table> | Algoritma    | Area (GE)             | Cycles/block       | Throughput | Ref  | SIMON64/96 | 809     | 1.455 | 4,4    | [119]             | SIMON64/128       | 958   | 1.524   | 4,2 | SIMON128/128 | 1.234             | 4.414             | 2,9     | SIMON128/256 | 1.782  | 4.923             | 2,6               | Algoritma | ROM (byte) | RAM (byte) | Cycles/byte (Enc/Dec) | Platform           | Ref | SIMON64/96 | 274                | 0                  | 239 | ATtiny45 | [119] | SIMON64/128 | 282 | 0 | 250 | ATtiny45 | SIMON128/128 | 732 | 0 | 376 | ATtiny45 | SIMON128/256 | 764 | 0 | 398 | ATtiny45 |
| Algoritma             | Area (GE)                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       | Cycles/block | Throughput            | Ref                |            |      |            |         |       |        |                   |                   |       |         |     |              |                   |                   |         |              |        |                   |                   |           |            |            |                       |                    |     |            |                    |                    |     |          |       |             |     |   |     |          |              |     |   |     |          |              |     |   |     |          |
| SIMON64/96            | 809                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             | 1.455        | 4,4                   | [119]              |            |      |            |         |       |        |                   |                   |       |         |     |              |                   |                   |         |              |        |                   |                   |           |            |            |                       |                    |     |            |                    |                    |     |          |       |             |     |   |     |          |              |     |   |     |          |              |     |   |     |          |
| SIMON64/128           | 958                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             | 1.524        | 4,2                   |                    |            |      |            |         |       |        |                   |                   |       |         |     |              |                   |                   |         |              |        |                   |                   |           |            |            |                       |                    |     |            |                    |                    |     |          |       |             |     |   |     |          |              |     |   |     |          |              |     |   |     |          |
| SIMON128/128          | 1.234                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           | 4.414        | 2,9                   |                    |            |      |            |         |       |        |                   |                   |       |         |     |              |                   |                   |         |              |        |                   |                   |           |            |            |                       |                    |     |            |                    |                    |     |          |       |             |     |   |     |          |              |     |   |     |          |              |     |   |     |          |
| SIMON128/256          | 1.782                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           | 4.923        | 2,6                   |                    |            |      |            |         |       |        |                   |                   |       |         |     |              |                   |                   |         |              |        |                   |                   |           |            |            |                       |                    |     |            |                    |                    |     |          |       |             |     |   |     |          |              |     |   |     |          |              |     |   |     |          |
| Algoritma             | ROM (byte)                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      | RAM (byte)   | Cycles/byte (Enc/Dec) | Platform           | Ref        |      |            |         |       |        |                   |                   |       |         |     |              |                   |                   |         |              |        |                   |                   |           |            |            |                       |                    |     |            |                    |                    |     |          |       |             |     |   |     |          |              |     |   |     |          |              |     |   |     |          |
| SIMON64/96            | 274                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             | 0            | 239                   | ATtiny45           | [119]      |      |            |         |       |        |                   |                   |       |         |     |              |                   |                   |         |              |        |                   |                   |           |            |            |                       |                    |     |            |                    |                    |     |          |       |             |     |   |     |          |              |     |   |     |          |              |     |   |     |          |
| SIMON64/128           | 282                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             | 0            | 250                   | ATtiny45           |            |      |            |         |       |        |                   |                   |       |         |     |              |                   |                   |         |              |        |                   |                   |           |            |            |                       |                    |     |            |                    |                    |     |          |       |             |     |   |     |          |              |     |   |     |          |              |     |   |     |          |
| SIMON128/128          | 732                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             | 0            | 376                   | ATtiny45           |            |      |            |         |       |        |                   |                   |       |         |     |              |                   |                   |         |              |        |                   |                   |           |            |            |                       |                    |     |            |                    |                    |     |          |       |             |     |   |     |          |              |     |   |     |          |              |     |   |     |          |
| SIMON128/256          | 764                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             | 0            | 398                   | ATtiny45           |            |      |            |         |       |        |                   |                   |       |         |     |              |                   |                   |         |              |        |                   |                   |           |            |            |                       |                    |     |            |                    |                    |     |          |       |             |     |   |     |          |              |     |   |     |          |              |     |   |     |          |
| Informasi Open Source | <p>Tim SIMON dan SPECK telah merilis perangkat lunak domain publik yang mengimplementasikan beberapa versi SIMON dan SPECK untuk berbagai platform [77]. Kontribusi terhadap kerangka kerja pembandingan FELICS [127] menyediakan implementasi SIMON dan SPECK ukuran blok 64-bit yang dioptimalkan untuk mikrokontroler AVR, MSP430, dan ARM Cortex M. Kontribusi terhadap kerangka kerja pembandingan SUPERCOP [128] menyediakan implementasi SIMON dan SPECK ukuran blok 64 dan 128-bit yang dioptimalkan untuk CPU kelas atas seperti X86 dan ARM Cortex A. Pencarian di Internet mengungkap sejumlah</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                   |              |                       |                    |            |      |            |         |       |        |                   |                   |       |         |     |              |                   |                   |         |              |        |                   |                   |           |            |            |                       |                    |     |            |                    |                    |     |          |       |             |     |   |     |          |              |     |   |     |          |              |     |   |     |          |

|  |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |
|--|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|  | <p>proyek perangkat lunak <i>open source</i> lainnya yang mengimplementasikan SIMON atau SPECK. Namun, mereka tidak termasuk dalam pustaka kriptografi yang digunakan secara luas seperti OpenSSL.</p> <p>[1] <a href="https://iadgov.github.io/simon-speck/implementations/">https://iadgov.github.io/simon-speck/implementations/</a></p> <p>[2] <a href="https://www.cryptolux.org/index.php/FELICS">https://www.cryptolux.org/index.php/FELICS</a></p> <p>[3] <a href="https://bench.cr.yp.to/supercop.html">https://bench.cr.yp.to/supercop.html</a></p> <p>[4] <a href="https://rweather.github.io/arduinolibs/crypto.html">https://rweather.github.io/arduinolibs/crypto.html</a></p> <p>[5] <a href="http://cppcrypto.sourceforge.net/">http://cppcrypto.sourceforge.net/</a></p> |
|--|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|

## 9. SPECK

|                     |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |          |         |     |    |     |     |     |     |  |  |  |                    |    |    |  |    |  |    |  |     |  |  |                     |    |    |    |    |     |    |     |     |     |     |              |    |  |    |    |    |    |    |    |    |
|---------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------|---------|-----|----|-----|-----|-----|-----|--|--|--|--------------------|----|----|--|----|--|----|--|-----|--|--|---------------------|----|----|----|----|-----|----|-----|-----|-----|-----|--------------|----|--|----|----|----|----|----|----|----|
| Profil              | Nama                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            | SPECK                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |          |         |     |    |     |     |     |     |  |  |  |                    |    |    |  |    |  |    |  |     |  |  |                     |    |    |    |    |     |    |     |     |     |     |              |    |  |    |    |    |    |    |    |    |
| Algoritma           | Perancang                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       | Ray Beaulieu, Douglas Shors, Jason Smith, Stefan Treatman-Clark, Bryan Weeks, Louis Wingers (NSA, USA)                                                                                                                                                                                                                                                                                                                                                                                                                  |          |         |     |    |     |     |     |     |  |  |  |                    |    |    |  |    |  |    |  |     |  |  |                     |    |    |    |    |     |    |     |     |     |     |              |    |  |    |    |    |    |    |    |    |
|                     | Publikasi                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       | 2013 (Cryptology ePrint Archive [119])                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |          |         |     |    |     |     |     |     |  |  |  |                    |    |    |  |    |  |    |  |     |  |  |                     |    |    |    |    |     |    |     |     |     |     |              |    |  |    |    |    |    |    |    |    |
| Spesifikasi         | Terdapat dalam [123].                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |          |         |     |    |     |     |     |     |  |  |  |                    |    |    |  |    |  |    |  |     |  |  |                     |    |    |    |    |     |    |     |     |     |     |              |    |  |    |    |    |    |    |    |    |
| Fitur               | <p>Perancang mengklaim bahwa algoritma SPECK mendukung berbagai panjang blok dan kunci serta memiliki bobot yang lebih ringan baik dalam implementasi perangkat keras maupun perangkat lunak, terutama dalam implementasi perangkat lunak. Mirip dengan SIMON, SPECK dengan panjang blok <math>2n</math>-bit dan panjang kunci <math>m</math>-word dinotasikan sebagai SPECK <math>2n/mn</math>. Misalnya, SPECK 64/128 berarti SPECK dengan panjang blok 64 bit dan panjang kunci 128 bit.</p> |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |          |         |     |    |     |     |     |     |  |  |  |                    |    |    |  |    |  |    |  |     |  |  |                     |    |    |    |    |     |    |     |     |     |     |              |    |  |    |    |    |    |    |    |    |
|                     |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |          |         |     |    |     |     |     |     |  |  |  |                    |    |    |  |    |  |    |  |     |  |  |                     |    |    |    |    |     |    |     |     |     |     |              |    |  |    |    |    |    |    |    |    |
|                     |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |          |         |     |    |     |     |     |     |  |  |  |                    |    |    |  |    |  |    |  |     |  |  |                     |    |    |    |    |     |    |     |     |     |     |              |    |  |    |    |    |    |    |    |    |
|                     |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |          |         |     |    |     |     |     |     |  |  |  |                    |    |    |  |    |  |    |  |     |  |  |                     |    |    |    |    |     |    |     |     |     |     |              |    |  |    |    |    |    |    |    |    |
|                     |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 | <table><tr><td>Struktur</td><td colspan="10">Feistel</td></tr><tr><td>Panjang blok (bit)</td><td>32</td><td colspan="2">48</td><td colspan="2">64</td><td colspan="2">96</td><td colspan="3">128</td></tr><tr><td>Panjang kunci (bit)</td><td>64</td><td>72</td><td>96</td><td>96</td><td>128</td><td>96</td><td>144</td><td>128</td><td>192</td><td>256</td></tr><tr><td>Jumlah round</td><td colspan="2">22</td><td>23</td><td>26</td><td>27</td><td>28</td><td>29</td><td>32</td><td>33</td><td>34</td></tr></table> | Struktur | Feistel |     |    |     |     |     |     |  |  |  | Panjang blok (bit) | 32 | 48 |  | 64 |  | 96 |  | 128 |  |  | Panjang kunci (bit) | 64 | 72 | 96 | 96 | 128 | 96 | 144 | 128 | 192 | 256 | Jumlah round | 22 |  | 23 | 26 | 27 | 28 | 29 | 32 | 33 |
| Struktur            | Feistel                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |          |         |     |    |     |     |     |     |  |  |  |                    |    |    |  |    |  |    |  |     |  |  |                     |    |    |    |    |     |    |     |     |     |     |              |    |  |    |    |    |    |    |    |    |
| Panjang blok (bit)  | 32                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              | 48                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |          | 64      |     | 96 |     | 128 |     |     |  |  |  |                    |    |    |  |    |  |    |  |     |  |  |                     |    |    |    |    |     |    |     |     |     |     |              |    |  |    |    |    |    |    |    |    |
| Panjang kunci (bit) | 64                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              | 72                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      | 96       | 96      | 128 | 96 | 144 | 128 | 192 | 256 |  |  |  |                    |    |    |  |    |  |    |  |     |  |  |                     |    |    |    |    |     |    |     |     |     |     |              |    |  |    |    |    |    |    |    |    |
| Jumlah round        | 22                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         | 23       | 26      | 27  | 28 | 29  | 32  | 33  | 34  |  |  |  |                    |    |    |  |    |  |    |  |     |  |  |                     |    |    |    |    |     |    |     |     |     |     |              |    |  |    |    |    |    |    |    |    |

|                   |                                                               |        |              |             |             |       |
|-------------------|---------------------------------------------------------------|--------|--------------|-------------|-------------|-------|
| Analisis keamanan | Status analisis keamanan SPECK dalam pengaturan kunci tunggal |        |              |             |             |       |
|                   | Algoritma                                                     | Rounds | Type         | Waktu       | Data        | Ref   |
|                   | Speck32                                                       | 14     | Differential | $2^{63,0}$  | $2^{31,0}$  | [129] |
|                   |                                                               | 14     | Differential | $2^{61,4}$  | $2^{29,4}$  | [130] |
|                   | Speck48                                                       | 14     | Differential | $2^{65,0}$  | $2^{41,0}$  | [129] |
|                   |                                                               | 15     | Differential | $2^{89,0}$  | $2^{41,0}$  |       |
|                   |                                                               | 15     | Differential | $2^{68,3}$  | $2^{44,3}$  | [130] |
|                   |                                                               | 16     | Differential | $2^{92,3}$  | $2^{44,3}$  |       |
|                   | Speck64                                                       | 18     | Differential | $2^{93,0}$  | $2^{61,0}$  | [129] |
|                   |                                                               | 19     | Differential | $2^{125,0}$ | $2^{61,0}$  | [130] |
|                   |                                                               | 19     | Differential | $2^{92,6}$  | $2^{60,8}$  | [129] |
|                   |                                                               | 20     | Differential | $2^{124,6}$ | $2^{60,8}$  | [130] |
|                   | Speck96                                                       | 16     | Differential | $2^{85,0}$  | $2^{85,0}$  | [129] |
|                   |                                                               | 17     | Differential | $2^{133,0}$ | $2^{85,0}$  |       |
|                   |                                                               | 20     | Differential | $2^{94,9}$  | $2^{94,9}$  | [130] |
|                   |                                                               | 23     | Differential | $2^{142,9}$ | $2^{94,9}$  |       |
|                   |                                                               |        |              |             |             |       |
|                   | Speck128                                                      | 17     | Differential | $2^{113,0}$ | $2^{113,0}$ | [129] |
|                   |                                                               | 18     | Differential | $2^{177,0}$ | $2^{113,0}$ |       |
|                   |                                                               | 19     | Differential | $2^{241,0}$ | $2^{113,0}$ |       |
|                   |                                                               | 23     | Differential | $2^{124,4}$ | $2^{124,4}$ | [130] |
|                   |                                                               | 24     | Differential | $2^{188,4}$ | $2^{124,4}$ |       |
|                   |                                                               | 25     | Differential | $2^{252,4}$ | $2^{124,4}$ |       |

Berdasarkan hasil kajian pada tabel di atas, meskipun berbagai penelitian kriptanalisis telah dilakukan hingga tahun 2021, namun tidak terdapat serangan yang lebih efisien dibandingkan dengan *exhaustive search* terhadap semua varian algoritma SPECK.

|                       |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |            |              |                       |          |       |
|-----------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------|--------------|-----------------------|----------|-------|
| Analisis Performa     | Hasil evaluasi implementasi perangkat keras:                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |            |              |                       |          |       |
|                       | Algoritma                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      | Area (GE)  | Cycles/block | Throughput            | Ref      |       |
|                       | SPECK64/96                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     | 860        | 1.778        | 3,6                   | [119]    |       |
|                       | SPECK64/128                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    | 996        | 1.882        | 3,4                   |          |       |
|                       | SPECK128/128                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   | 1.280      | 4.267        | 3,0                   |          |       |
| SPECK128/256          | 1.840                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          | 4.571      | 2,8          |                       |          |       |
| Informasi Open Source | Hasil evaluasi implementasi perangkat lunak (low-end CPU):                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |            |              |                       |          |       |
|                       | Algoritma                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      | ROM (byte) | RAM (byte)   | Cycles/byte (Enc/Dec) | Platform | Ref   |
|                       | SPECK64/96                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     | 182        | 0            | 144                   | ATtiny45 | [119] |
|                       | SPECK64/128                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    | 186        | 0            | 150                   | ATtiny45 |       |
|                       | SPECK128/128                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   | 396        | 0            | 167                   | ATtiny45 |       |
| SPECK128/256          | 412                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            | 0          | 177          | ATtiny45              |          |       |
|                       | <p>Tim SIMON dan SPECK telah merilis perangkat lunak domain publik yang mengimplementasikan beberapa versi SIMON dan SPECK untuk berbagai platform [77]. Kontribusi terhadap kerangka kerja perbandingan FELICS [127] menyediakan implementasi SIMON dan SPECK ukuran blok 64-bit yang dioptimalkan untuk mikrokontroler AVR, MSP430, dan ARM Cortex M. Kontribusi terhadap kerangka kerja perbandingan SUPERCOP [128] menyediakan implementasi SIMON dan SPECK ukuran blok 64 dan 128-bit yang dioptimalkan untuk CPU kelas atas seperti X86 dan ARM Cortex A. Pencarian di Internet mengungkap sejumlah proyek perangkat lunak open source lainnya yang mengimplementasikan SIMON atau SPECK. Namun, mereka tidak termasuk dalam pustaka kriptografi yang digunakan secara luas seperti OpenSSL.</p> <p>[1] <a href="https://iadgov.github.io/simon-speck/implementations/">https://iadgov.github.io/simon-speck/implementations/</a></p> <p>[2] <a href="https://www.cryptolux.org/index.php/FELICS">https://www.cryptolux.org/index.php/FELICS</a></p> <p>[3] <a href="https://bench.cr.yp.to/supercop.html">https://bench.cr.yp.to/supercop.html</a></p> <p>[4] <a href="https://rweather.github.io/arduinoilibs/crypto.html">https://rweather.github.io/arduinoilibs/crypto.html</a></p> |            |              |                       |          |       |

|  |                                                                                       |
|--|---------------------------------------------------------------------------------------|
|  | [5] <a href="http://cppcrypto.sourceforge.net/">http://cppcrypto.sourceforge.net/</a> |
|--|---------------------------------------------------------------------------------------|

## 10. TWINE

|                     |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |                                                                                  |  |          |                             |  |                    |    |  |                     |               |                 |              |    |  |
|---------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------|--|----------|-----------------------------|--|--------------------|----|--|---------------------|---------------|-----------------|--------------|----|--|
| Profil<br>Algoritma | Nama                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             | TWINE                                                                            |  |          |                             |  |                    |    |  |                     |               |                 |              |    |  |
|                     | Perancang                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        | Tomoyasu Suzaki, Kazuhiko Minematsu, Sumio Morioka, Eita Kobayashi (NEC, Jepang) |  |          |                             |  |                    |    |  |                     |               |                 |              |    |  |
|                     | Publikasi                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        | 2011 (ECRYPT Workshop on Lightweight Cryptography, SAC 2012 [131])               |  |          |                             |  |                    |    |  |                     |               |                 |              |    |  |
| Spesifikasi         | terdapat di website:<br><a href="http://jpn.nec.com/rd/crl/code/research/image/twine_SAC_full_v5.pdf">http://jpn.nec.com/rd/crl/code/research/image/twine_SAC_full_v5.pdf</a> , dan dalam [131]                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |                                                                                  |  |          |                             |  |                    |    |  |                     |               |                 |              |    |  |
| Fitur               | <p>Perancang mengklaim bahwa algoritma TWINE memiliki bobot yang ringan dalam implementasi perangkat keras dan implementasi perangkat lunak dalam berbagai CPU mulai dari <i>low-end</i> hingga <i>high-end</i>. Algoritma TWINE menggunakan pengacakan blok (<i>shuffle block</i>) yang lebih baik yang diusulkan oleh para perancang di FSE 2010 untuk meningkatkan keamanan.</p> <table><tr><td>Struktur</td><td colspan="2">16-line generalized Feistel</td></tr><tr><td>Panjang blok (bit)</td><td colspan="2">64</td></tr><tr><td>Panjang kunci (bit)</td><td>80 (TWINE-80)</td><td>128 (TWINE-128)</td></tr><tr><td>Jumlah round</td><td colspan="2">36</td></tr></table> |                                                                                  |  | Struktur | 16-line generalized Feistel |  | Panjang blok (bit) | 64 |  | Panjang kunci (bit) | 80 (TWINE-80) | 128 (TWINE-128) | Jumlah round | 36 |  |
| Struktur            | 16-line generalized Feistel                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |                                                                                  |  |          |                             |  |                    |    |  |                     |               |                 |              |    |  |
| Panjang blok (bit)  | 64                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |                                                                                  |  |          |                             |  |                    |    |  |                     |               |                 |              |    |  |
| Panjang kunci (bit) | 80 (TWINE-80)                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    | 128 (TWINE-128)                                                                  |  |          |                             |  |                    |    |  |                     |               |                 |              |    |  |
| Jumlah round        | 36                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |                                                                                  |  |          |                             |  |                    |    |  |                     |               |                 |              |    |  |

| Analisis keamanan   | <p>Status analisis keamanan TWINE dalam pengaturan kunci tunggal (CPs: <i>chosen plaintext</i>, KPs: <i>known plaintext</i>)</p> <table><tr><th>Algoritma</th><th>Rounds</th><th>Tipe</th><th>Waktu</th><th>Data</th><th>Memori</th><th>Ref</th></tr><tr><td rowspan="2">TWINE-80</td><td>23</td><td><i>Impossible Differential</i></td><td><math>2^{79,1}</math></td><td><math>2^{57,9}</math> CPs</td><td><math>2^{84,1}</math></td><td>[132]</td></tr><tr><td>23</td><td><i>Multidimensional ZC Linear</i></td><td><math>2^{73,0}</math></td><td><math>2^{62,1}</math> KPs</td><td><math>2^{60,0}</math></td><td>[133]</td></tr><tr><td rowspan="4">TWINE-128</td><td>25</td><td><i>Meet-in-the-Middle</i></td><td><math>2^{124,7}</math></td><td><math>2^{48,0}</math> CPs</td><td><math>2^{109,0}</math></td><td>[134]</td></tr><tr><td>25</td><td><i>Impossible Differential</i></td><td><math>2^{124,5}</math></td><td><math>2^{59,1}</math> CPs</td><td><math>2^{78,1}</math></td><td>[134]</td></tr><tr><td>25</td><td><i>Multidimensional ZC Linear</i></td><td><math>2^{122,1}</math></td><td><math>2^{62,1}</math> KPs</td><td><math>2^{60,0}</math></td><td>[135]</td></tr><tr><td>25</td><td><i>Multidimensional ZC Linear</i></td><td><math>2^{119,0}</math></td><td><math>2^{62,1}</math> KPs</td><td><math>2^{60,0}</math></td><td>[133]</td></tr></table> <p>Berdasarkan hasil kajian pada tabel di atas, meskipun berbagai penelitian kriptanalisis telah dilakukan hingga tahun 2021, namun tidak terdapat serangan yang lebih efisien dibandingkan dengan <i>exhaustive search</i> terhadap semua varian algoritma TWINE-80 dan TWINE-128.</p> | Algoritma                         | Rounds                | Tipe           | Waktu       | Data  | Memori         | Ref   | TWINE-80 | 23    | <i>Impossible Differential</i> | $2^{79,1}$     | $2^{57,9}$ CPs | $2^{84,1}$ | [132] | 23                 | <i>Multidimensional ZC Linear</i> | $2^{73,0}$ | $2^{62,1}$ KPs | $2^{60,0}$      | [133] | TWINE-128 | 25    | <i>Meet-in-the-Middle</i> | $2^{124,7}$ | $2^{48,0}$ CPs | $2^{109,0}$ | [134]     | 25   | <i>Impossible Differential</i> | $2^{124,5}$ | $2^{59,1}$ CPs | $2^{78,1}$   | [134]                           | 25         | <i>Multidimensional ZC Linear</i> | $2^{122,1}$ | $2^{62,1}$ KPs | $2^{60,0}$ | [135]      | 25                    | <i>Multidimensional ZC Linear</i> | $2^{119,0}$ | $2^{62,1}$ KPs | $2^{60,0}$ | [133] |         |           |       |          |     |     |             |           |
|---------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------|-----------------------|----------------|-------------|-------|----------------|-------|----------|-------|--------------------------------|----------------|----------------|------------|-------|--------------------|-----------------------------------|------------|----------------|-----------------|-------|-----------|-------|---------------------------|-------------|----------------|-------------|-----------|------|--------------------------------|-------------|----------------|--------------|---------------------------------|------------|-----------------------------------|-------------|----------------|------------|------------|-----------------------|-----------------------------------|-------------|----------------|------------|-------|---------|-----------|-------|----------|-----|-----|-------------|-----------|
| Algoritma           | Rounds                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              | Tipe                              | Waktu                 | Data           | Memori      | Ref   |                |       |          |       |                                |                |                |            |       |                    |                                   |            |                |                 |       |           |       |                           |             |                |             |           |      |                                |             |                |              |                                 |            |                                   |             |                |            |            |                       |                                   |             |                |            |       |         |           |       |          |     |     |             |           |
| TWINE-80            | 23                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  | <i>Impossible Differential</i>    | $2^{79,1}$            | $2^{57,9}$ CPs | $2^{84,1}$  | [132] |                |       |          |       |                                |                |                |            |       |                    |                                   |            |                |                 |       |           |       |                           |             |                |             |           |      |                                |             |                |              |                                 |            |                                   |             |                |            |            |                       |                                   |             |                |            |       |         |           |       |          |     |     |             |           |
|                     | 23                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  | <i>Multidimensional ZC Linear</i> | $2^{73,0}$            | $2^{62,1}$ KPs | $2^{60,0}$  | [133] |                |       |          |       |                                |                |                |            |       |                    |                                   |            |                |                 |       |           |       |                           |             |                |             |           |      |                                |             |                |              |                                 |            |                                   |             |                |            |            |                       |                                   |             |                |            |       |         |           |       |          |     |     |             |           |
| TWINE-128           | 25                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  | <i>Meet-in-the-Middle</i>         | $2^{124,7}$           | $2^{48,0}$ CPs | $2^{109,0}$ | [134] |                |       |          |       |                                |                |                |            |       |                    |                                   |            |                |                 |       |           |       |                           |             |                |             |           |      |                                |             |                |              |                                 |            |                                   |             |                |            |            |                       |                                   |             |                |            |       |         |           |       |          |     |     |             |           |
|                     | 25                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  | <i>Impossible Differential</i>    | $2^{124,5}$           | $2^{59,1}$ CPs | $2^{78,1}$  | [134] |                |       |          |       |                                |                |                |            |       |                    |                                   |            |                |                 |       |           |       |                           |             |                |             |           |      |                                |             |                |              |                                 |            |                                   |             |                |            |            |                       |                                   |             |                |            |       |         |           |       |          |     |     |             |           |
|                     | 25                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  | <i>Multidimensional ZC Linear</i> | $2^{122,1}$           | $2^{62,1}$ KPs | $2^{60,0}$  | [135] |                |       |          |       |                                |                |                |            |       |                    |                                   |            |                |                 |       |           |       |                           |             |                |             |           |      |                                |             |                |              |                                 |            |                                   |             |                |            |            |                       |                                   |             |                |            |       |         |           |       |          |     |     |             |           |
|                     | 25                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  | <i>Multidimensional ZC Linear</i> | $2^{119,0}$           | $2^{62,1}$ KPs | $2^{60,0}$  | [133] |                |       |          |       |                                |                |                |            |       |                    |                                   |            |                |                 |       |           |       |                           |             |                |             |           |      |                                |             |                |              |                                 |            |                                   |             |                |            |            |                       |                                   |             |                |            |       |         |           |       |          |     |     |             |           |
| Analisis Performa   | <p>Hasil evaluasi implementasi perangkat keras:</p> <table><tr><th>Algoritma</th><th>Area (GE)</th><th>Cycles/block</th><th>Throughput</th><th>Ref</th></tr><tr><td>TWINE-80 (Enc)</td><td>1.503</td><td>36</td><td>177,8</td><td rowspan="5">[131]</td></tr><tr><td>TWINE-80 (Enc)</td><td>1.011</td><td>393</td><td>16,3</td></tr><tr><td>TWINE-80 (Enc/Dec)</td><td>1.799</td><td>36</td><td>177,8</td></tr><tr><td>TWINE-128 (Enc)</td><td>1.866</td><td>36</td><td>177,8</td></tr><tr><td>TWINE-128 (Enc/Dec)</td><td>2.285</td><td>36</td><td>177,8</td></tr></table> <p>Hasil evaluasi implementasi perangkat keras (<i>high-end CPU</i>):</p> <table><tr><th>Algoritma</th><th>Type</th><th>Cycles/byte (Enc/Dec)</th><th>Platform</th><th>Ref</th></tr><tr><td>TWINE-80/128</td><td><i>Bitslice (Single/Double)</i></td><td>11,10/5,55</td><td>Core i7 2600S</td><td>[131]</td></tr></table> <p>Hasil evaluasi implementasi perangkat lunak (<i>low-end CPU</i>):</p> <table><tr><th>Algoritma</th><th>ROM (byte)</th><th>RAM (byte)</th><th>Cycles/byte (Enc/Dec)</th><th>Platform</th><th>Ref</th></tr><tr><td>TWINE-80</td><td>2.294</td><td>386</td><td>163/163</td><td>Atmega163</td><td rowspan="2">[131]</td></tr><tr><td>TWINE-80</td><td>792</td><td>191</td><td>2.350/2.337</td><td>Atmega163</td></tr></table>                                                                                                                                                                                                                                                                                                                                  | Algoritma                         | Area (GE)             | Cycles/block   | Throughput  | Ref   | TWINE-80 (Enc) | 1.503 | 36       | 177,8 | [131]                          | TWINE-80 (Enc) | 1.011          | 393        | 16,3  | TWINE-80 (Enc/Dec) | 1.799                             | 36         | 177,8          | TWINE-128 (Enc) | 1.866 | 36        | 177,8 | TWINE-128 (Enc/Dec)       | 2.285       | 36             | 177,8       | Algoritma | Type | Cycles/byte (Enc/Dec)          | Platform    | Ref            | TWINE-80/128 | <i>Bitslice (Single/Double)</i> | 11,10/5,55 | Core i7 2600S                     | [131]       | Algoritma      | ROM (byte) | RAM (byte) | Cycles/byte (Enc/Dec) | Platform                          | Ref         | TWINE-80       | 2.294      | 386   | 163/163 | Atmega163 | [131] | TWINE-80 | 792 | 191 | 2.350/2.337 | Atmega163 |
| Algoritma           | Area (GE)                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           | Cycles/block                      | Throughput            | Ref            |             |       |                |       |          |       |                                |                |                |            |       |                    |                                   |            |                |                 |       |           |       |                           |             |                |             |           |      |                                |             |                |              |                                 |            |                                   |             |                |            |            |                       |                                   |             |                |            |       |         |           |       |          |     |     |             |           |
| TWINE-80 (Enc)      | 1.503                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               | 36                                | 177,8                 | [131]          |             |       |                |       |          |       |                                |                |                |            |       |                    |                                   |            |                |                 |       |           |       |                           |             |                |             |           |      |                                |             |                |              |                                 |            |                                   |             |                |            |            |                       |                                   |             |                |            |       |         |           |       |          |     |     |             |           |
| TWINE-80 (Enc)      | 1.011                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               | 393                               | 16,3                  |                |             |       |                |       |          |       |                                |                |                |            |       |                    |                                   |            |                |                 |       |           |       |                           |             |                |             |           |      |                                |             |                |              |                                 |            |                                   |             |                |            |            |                       |                                   |             |                |            |       |         |           |       |          |     |     |             |           |
| TWINE-80 (Enc/Dec)  | 1.799                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               | 36                                | 177,8                 |                |             |       |                |       |          |       |                                |                |                |            |       |                    |                                   |            |                |                 |       |           |       |                           |             |                |             |           |      |                                |             |                |              |                                 |            |                                   |             |                |            |            |                       |                                   |             |                |            |       |         |           |       |          |     |     |             |           |
| TWINE-128 (Enc)     | 1.866                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               | 36                                | 177,8                 |                |             |       |                |       |          |       |                                |                |                |            |       |                    |                                   |            |                |                 |       |           |       |                           |             |                |             |           |      |                                |             |                |              |                                 |            |                                   |             |                |            |            |                       |                                   |             |                |            |       |         |           |       |          |     |     |             |           |
| TWINE-128 (Enc/Dec) | 2.285                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               | 36                                | 177,8                 |                |             |       |                |       |          |       |                                |                |                |            |       |                    |                                   |            |                |                 |       |           |       |                           |             |                |             |           |      |                                |             |                |              |                                 |            |                                   |             |                |            |            |                       |                                   |             |                |            |       |         |           |       |          |     |     |             |           |
| Algoritma           | Type                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                | Cycles/byte (Enc/Dec)             | Platform              | Ref            |             |       |                |       |          |       |                                |                |                |            |       |                    |                                   |            |                |                 |       |           |       |                           |             |                |             |           |      |                                |             |                |              |                                 |            |                                   |             |                |            |            |                       |                                   |             |                |            |       |         |           |       |          |     |     |             |           |
| TWINE-80/128        | <i>Bitslice (Single/Double)</i>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     | 11,10/5,55                        | Core i7 2600S         | [131]          |             |       |                |       |          |       |                                |                |                |            |       |                    |                                   |            |                |                 |       |           |       |                           |             |                |             |           |      |                                |             |                |              |                                 |            |                                   |             |                |            |            |                       |                                   |             |                |            |       |         |           |       |          |     |     |             |           |
| Algoritma           | ROM (byte)                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          | RAM (byte)                        | Cycles/byte (Enc/Dec) | Platform       | Ref         |       |                |       |          |       |                                |                |                |            |       |                    |                                   |            |                |                 |       |           |       |                           |             |                |             |           |      |                                |             |                |              |                                 |            |                                   |             |                |            |            |                       |                                   |             |                |            |       |         |           |       |          |     |     |             |           |
| TWINE-80            | 2.294                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               | 386                               | 163/163               | Atmega163      | [131]       |       |                |       |          |       |                                |                |                |            |       |                    |                                   |            |                |                 |       |           |       |                           |             |                |             |           |      |                                |             |                |              |                                 |            |                                   |             |                |            |            |                       |                                   |             |                |            |       |         |           |       |          |     |     |             |           |
| TWINE-80            | 792                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 | 191                               | 2.350/2.337           | Atmega163      |             |       |                |       |          |       |                                |                |                |            |       |                    |                                   |            |                |                 |       |           |       |                           |             |                |             |           |      |                                |             |                |              |                                 |            |                                   |             |                |            |            |                       |                                   |             |                |            |       |         |           |       |          |     |     |             |           |

|           |                                                                                                                         |
|-----------|-------------------------------------------------------------------------------------------------------------------------|
| Informasi | Solusi IoT Industri NEC <i>Engineering: Secure Sensors</i>                                                              |
| Open      | <a href="http://jpn.nec.com/engsl/pro/securesensor/index.html">http://jpn.nec.com/engsl/pro/securesensor/index.html</a> |
| Source    | <a href="http://www.nec-eng.co.jp/press/161024press.html">http://www.nec-eng.co.jp/press/161024press.html</a>           |
|           | NEC Store Video Surveillance Cloud Service                                                                              |
|           | <a href="http://jpn.nec.com/press/201604/20160421_02.html">http://jpn.nec.com/press/201604/20160421_02.html</a>         |
|           | NEC ExpEther 40G                                                                                                        |
|           | <a href="http://jpn.nec.com/press/201511/20151109_01.html">http://jpn.nec.com/press/201511/20151109_01.html</a>         |

### C. *Lightweight Fungsi Hash*

Subbab ini berisi ringkasan algoritma *lightweight* fungsi *hash* yang terdapat dalam CryptoLUX kelompok penelitian kriptologi di *Security and Trust interdisciplinary center* dan *Departement of Computer Science* pada *University of Luxembourg*. Selain itu, ringkasan algoritma *lighweifht* fungsi *hash* juga diambil dari dokumen CRYPTREC *Cryptographic Technology Guideline - Lightweight Cryptography* [16] dan CRYPTREC *Cryptographic Technology Guideline (Lightweight Cryptography) 2023 Edition* [17] yang diterbitkan oleh CRYPTREC *Lightweight Cryptography Working Group*. Ringkasan ini berisi informasi mengenai profil algoritma, analisis performa pada perangkat keras dan/atau perangkat lunak, standarisasi serta ketersediaan *open source*. Algoritma *lightweight* fungsi *hash* yang dibahas dalam subbab ini meliputi ARMADILO, DM-PRESENT, GLUON, Lesamnta-LW, PHOTON, QUARK, SipHash-2-4, SPN-Hash, dan SPONGENT.

#### 1. ARMADILO

|           |           |                                                                                                                                                                                                                                                               |
|-----------|-----------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Profil    | Nama      | ARMADILO                                                                                                                                                                                                                                                      |
| Algoritma | Perancang | Stephane Badel (EPFL, Lausanne, Switzerland), Nilay Dagtekin (EPFL, Lausanne, Switzerland), Jorge Nakahara Jr (EPFL, Lausanne, Switzerland), Khaled Ouaf (EPFL, Lausanne, Switzerland), Nicolas Reffe ( Oridao, Montpellier, France), Pouyan Sepehrdad (EPFL, |

|                           |              |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |                  |     |     |     |     |     |     |             |     |     |    |    |   |     |             |     |     |     |    |   |     |             |     |     |     |    |    |     |             |     |     |     |    |    |     |             |     |     |     |     |    |     |
|---------------------------|--------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------------|-----|-----|-----|-----|-----|-----|-------------|-----|-----|----|----|---|-----|-------------|-----|-----|-----|----|---|-----|-------------|-----|-----|-----|----|----|-----|-------------|-----|-----|-----|----|----|-----|-------------|-----|-----|-----|-----|----|-----|
|                           |              | Lausanne, Switzerland), Petr Susil (EPFL, Lausanne, Switzerland), Serge Vaudenay (EPFL, Lausanne, Switzerland). (Badel dkk., 2010)                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |                  |     |     |     |     |     |     |             |     |     |    |    |   |     |             |     |     |     |    |   |     |             |     |     |     |    |    |     |             |     |     |     |    |    |     |             |     |     |     |     |    |     |
|                           | Publikasi    | CHES 2010                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |                  |     |     |     |     |     |     |             |     |     |    |    |   |     |             |     |     |     |    |   |     |             |     |     |     |    |    |     |             |     |     |     |    |    |     |             |     |     |     |     |    |     |
|                           | Spesifikasi  | <a href="https://www.iacr.org/archive/ches2010/62250388/62250388.pdf">https://www.iacr.org/archive/ches2010/62250388/62250388.pdf</a> [136]                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |                  |     |     |     |     |     |     |             |     |     |    |    |   |     |             |     |     |     |    |   |     |             |     |     |     |    |    |     |             |     |     |     |    |    |     |             |     |     |     |     |    |     |
|                           | Standarisasi | -                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    |                  |     |     |     |     |     |     |             |     |     |    |    |   |     |             |     |     |     |    |   |     |             |     |     |     |    |    |     |             |     |     |     |    |    |     |             |     |     |     |     |    |     |
| Karakteristik kriptografi | Fitur        | <p>ARMADILO memiliki struktur Merkle-Damgaard dengan berbagai konfigurasi sesuai parameter internal. ARMADILO memiliki lima variasi (lihat tabel di bawah).</p> <table><tr><td>ARMADILO- Vektor</td><td><math>k</math></td><td><math>j</math></td><td><math>c</math></td><td><math>m</math></td><td><math>r</math></td><td><math>t</math></td></tr><tr><td>ARMADILO -A</td><td>128</td><td>128</td><td>80</td><td>48</td><td>6</td><td>128</td></tr><tr><td>ARMADILO -B</td><td>192</td><td>192</td><td>128</td><td>64</td><td>9</td><td>192</td></tr><tr><td>ARMADILO -C</td><td>240</td><td>240</td><td>160</td><td>80</td><td>10</td><td>240</td></tr><tr><td>ARMADILO -D</td><td>228</td><td>228</td><td>192</td><td>96</td><td>12</td><td>228</td></tr><tr><td>ARMADILO -E</td><td>384</td><td>384</td><td>256</td><td>128</td><td>15</td><td>384</td></tr></table> <p>Dengan <math>k</math>: ukuran register internal, <math>j</math>: jumlah bit permutasi yang digunakan dalam fungsi, <math>c</math>: panjang keluaran, <math>m</math>: panjang blok input, <math>r</math>: jumlah iterasi minimal yang diproses, dan <math>t</math>: jumlah bit keluaran</p> <p>ARMADILLO memetakan nilai awal <math>C</math> dan blok pesan <math>U_i</math> menjadi dua nilai, yaitu <math>(Vc, Vt) = \text{ARMADILLO}(C, U_i)</math>. Secara definisi, <math>C</math> dan <math>Vc</math> masing-masing terdiri dari <math>c</math> bit, sedangkan <math>Vt</math> dan setiap blok <math>U_i</math> terdiri dari <math>m</math> bit, dan register <math>X_{\text{inter}}</math> berukuran <math>k = c + m</math> bit. ARMADILLO didefinisikan oleh parameter bilangan bulat <math>c, m, j = c + m</math>, serta dua permutasi tetap <math>\sigma_0</math> dan <math>\sigma_1</math> pada himpunan <math>\{1, 2, \dots, 2k\}</math>.</p> | ARMADILO- Vektor | $k$ | $j$ | $c$ | $m$ | $r$ | $t$ | ARMADILO -A | 128 | 128 | 80 | 48 | 6 | 128 | ARMADILO -B | 192 | 192 | 128 | 64 | 9 | 192 | ARMADILO -C | 240 | 240 | 160 | 80 | 10 | 240 | ARMADILO -D | 228 | 228 | 192 | 96 | 12 | 228 | ARMADILO -E | 384 | 384 | 256 | 128 | 15 | 384 |
| ARMADILO- Vektor          | $k$          | $j$                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  | $c$              | $m$ | $r$ | $t$ |     |     |     |             |     |     |    |    |   |     |             |     |     |     |    |   |     |             |     |     |     |    |    |     |             |     |     |     |    |    |     |             |     |     |     |     |    |     |
| ARMADILO -A               | 128          | 128                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  | 80               | 48  | 6   | 128 |     |     |     |             |     |     |    |    |   |     |             |     |     |     |    |   |     |             |     |     |     |    |    |     |             |     |     |     |    |    |     |             |     |     |     |     |    |     |
| ARMADILO -B               | 192          | 192                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  | 128              | 64  | 9   | 192 |     |     |     |             |     |     |    |    |   |     |             |     |     |     |    |   |     |             |     |     |     |    |    |     |             |     |     |     |    |    |     |             |     |     |     |     |    |     |
| ARMADILO -C               | 240          | 240                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  | 160              | 80  | 10  | 240 |     |     |     |             |     |     |    |    |   |     |             |     |     |     |    |   |     |             |     |     |     |    |    |     |             |     |     |     |    |    |     |             |     |     |     |     |    |     |
| ARMADILO -D               | 228          | 228                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  | 192              | 96  | 12  | 228 |     |     |     |             |     |     |    |    |   |     |             |     |     |     |    |   |     |             |     |     |     |    |    |     |             |     |     |     |    |    |     |             |     |     |     |     |    |     |
| ARMADILO -E               | 384          | 384                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  | 256              | 128 | 15  | 384 |     |     |     |             |     |     |    |    |   |     |             |     |     |     |    |   |     |             |     |     |     |    |    |     |             |     |     |     |    |    |     |             |     |     |     |     |    |     |

|                   | Analisis keamanan                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     | Berdasarkan analisis dalam makalah <i>Practical Cryptanalysis of ARMADILLO2</i> [137], ARMADILLO tidak tahan terhadap serangan <i>local-linearization</i> . Serangan ini memanfaatkan kelemahan struktural pada mekanisme difusi yang lemah dan transposisi bit bergantung data, sehingga penyerang dapat memodelkan sebagian operasi internal sebagai transformasi linear lokal. Dengan pendekatan ini, penyerang berhasil membangun serangan <i>semi-free-start collision</i> pada fungsi hash ARMADILLO secara praktis dengan kompleksitas rendah, menunjukkan bahwa desain ARMADILLO tidak mampu mempertahankan karakteristik non-linearitas yang memadai untuk menahan analisis linear tingkat lanjut seperti <i>local-linearization</i> . |                   |               |                         |                   |               |             |               |       |          |         |             |               |        |             |         |             |               |        |         |         |             |               |         |          |         |             |                |         |          |         |
|-------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------|---------------|-------------------------|-------------------|---------------|-------------|---------------|-------|----------|---------|-------------|---------------|--------|-------------|---------|-------------|---------------|--------|---------|---------|-------------|---------------|---------|----------|---------|-------------|----------------|---------|----------|---------|
| Analisis performa | <p>Implementasi perangkat keras (menggunakan CMOS 0,18 <math>\mu\text{m}</math> dengan pustaka <i>standard-cell</i> komersial (blok logika siap pakai), menggunakan <i>Synopsys Design Compiler</i> untuk menyintesis desain digital dan menghitung <i>wire load</i> secara akurat [136].</p> <p>Untuk hasil sintesis pada 1 MHz.</p> <p>Hasil Implementasi N=1:</p> <table><tr><th>ARMADILO - Vector</th><th>Area (GE)</th><th>Power (<math>\mu\text{W}</math>)</th><th>Throughput (kbps)</th><th>Latency (clk)</th></tr><tr><td>ARMADILO -A</td><td>3.972 / 2.923</td><td>69/44</td><td>109 / 27</td><td>128/176</td></tr><tr><td>ARMADILO -B</td><td>6.598 / 4.353</td><td>117/65</td><td>1.000 / 250</td><td>192/256</td></tr><tr><td>ARMADILO -C</td><td>8.231 / 5.406</td><td>146/83</td><td>100/250</td><td>240/320</td></tr><tr><td>ARMADILO -D</td><td>8.650 / 6.554</td><td>177/102</td><td>100 / 25</td><td>288/384</td></tr><tr><td>ARMADILO -E</td><td>13.344 / 8.653</td><td>228/137</td><td>100 / 25</td><td>384/512</td></tr></table> |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 | ARMADILO - Vector | Area (GE)     | Power ( $\mu\text{W}$ ) | Throughput (kbps) | Latency (clk) | ARMADILO -A | 3.972 / 2.923 | 69/44 | 109 / 27 | 128/176 | ARMADILO -B | 6.598 / 4.353 | 117/65 | 1.000 / 250 | 192/256 | ARMADILO -C | 8.231 / 5.406 | 146/83 | 100/250 | 240/320 | ARMADILO -D | 8.650 / 6.554 | 177/102 | 100 / 25 | 288/384 | ARMADILO -E | 13.344 / 8.653 | 228/137 | 100 / 25 | 384/512 |
| ARMADILO - Vector | Area (GE)                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             | Power ( $\mu\text{W}$ )                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         | Throughput (kbps) | Latency (clk) |                         |                   |               |             |               |       |          |         |             |               |        |             |         |             |               |        |         |         |             |               |         |          |         |             |                |         |          |         |
| ARMADILO -A       | 3.972 / 2.923                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         | 69/44                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           | 109 / 27          | 128/176       |                         |                   |               |             |               |       |          |         |             |               |        |             |         |             |               |        |         |         |             |               |         |          |         |             |                |         |          |         |
| ARMADILO -B       | 6.598 / 4.353                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         | 117/65                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          | 1.000 / 250       | 192/256       |                         |                   |               |             |               |       |          |         |             |               |        |             |         |             |               |        |         |         |             |               |         |          |         |             |                |         |          |         |
| ARMADILO -C       | 8.231 / 5.406                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         | 146/83                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          | 100/250           | 240/320       |                         |                   |               |             |               |       |          |         |             |               |        |             |         |             |               |        |         |         |             |               |         |          |         |             |                |         |          |         |
| ARMADILO -D       | 8.650 / 6.554                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         | 177/102                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         | 100 / 25          | 288/384       |                         |                   |               |             |               |       |          |         |             |               |        |             |         |             |               |        |         |         |             |               |         |          |         |             |                |         |          |         |
| ARMADILO -E       | 13.344 / 8.653                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        | 228/137                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         | 100 / 25          | 384/512       |                         |                   |               |             |               |       |          |         |             |               |        |             |         |             |               |        |         |         |             |               |         |          |         |             |                |         |          |         |

|                                                                                |               |                     |                   |                              |
|--------------------------------------------------------------------------------|---------------|---------------------|-------------------|------------------------------|
| Hasil Implementasi N=4                                                         |               |                     |                   |                              |
| ARMADILO - Vector                                                              | Area (GE)     | Power ( $\mu W$ )   | Throughput (kbps) | Latency (clk)                |
| ARMADILO -A                                                                    | 5.770/4.030   | 133/77              | 1.500/1.090       | 32/44                        |
| ARMADILO -B                                                                    | 9.709/6.025   | 237/118             | 1.333/1.000       | 48/64                        |
| ARMADILO -C                                                                    | 12.217/7.492  | 300/158             | 1.333/1.000       | 60/80                        |
| ARMADILO -D                                                                    | 14.641/8.999  | 368/183             | 1.333/1.000       | 72/96                        |
| ARMADILO -E                                                                    | 19.669/11.914 | 513/251             | 1.333/1.000       | 96/128                       |
| Dengan N: jumlah permutasi yang dilakukan per siklus jam pada fungsi permutasi |               |                     |                   |                              |
| Implementasi untuk fungsi hash dengan <i>throughput</i> pada 100 kHz           |               |                     |                   |                              |
| ARMADILO - Vector                                                              | Area (GE)     | Time (cycles/block) | Throughput (kbps) | FOM (nanobit/cycle. $GE^2$ ) |
| ARMADILO -A                                                                    | 4.030/2.923   | 44/176              | 109/27            | 67,17/31,92                  |
| ARMADILO -B                                                                    | 6.025/4353    | 64/256              | 1.000/250         | 27,55/13,19                  |
| ARMADILO -C                                                                    | 7.492/5.406   | 80/320              | 100/25            | 17,81/8,55                   |
| ARMADILO -D                                                                    | 8.999/6554    | 96/384              | 100/25            | 12,35/5,82                   |
| ARMADILO -E                                                                    | 11.914/8.653  | 128/512             | 100/25            | 7,05/3,34                    |
| Implementasi untuk enkripsi dengan <i>throughput</i> pada 100 kHz              |               |                     |                   |                              |
| ARMADILO - Vector                                                              | Area (GE)     | Time (cycles/block) | Throughput (kbps) | FOM (nanobit/cycle. $GE^2$ ) |
| ARMADILO -A                                                                    | 4.030/2.923   | 44/176              | 291/73            | 179,12/85,12                 |
| ARMADILO -B                                                                    | 6.025/4353    | 64/256              | 300/75            | 82,64/39,58                  |
| ARMADILO -C                                                                    | 7.492/5.406   | 80/320              | 300/75            | 53,45/25,66                  |
| ARMADILO -D                                                                    | 8.999/6554    | 96/384              | 300/75            | 37,04/17,46                  |
| ARMADILO -E                                                                    | 11.914/8.653  | 128/512             | 300/75            | 21,13/10,02                  |

## 2. DM-PRESENT

|                  |             |                                                                                               |
|------------------|-------------|-----------------------------------------------------------------------------------------------|
| Profil Algoritma | Nama        | DM-PRESENT                                                                                    |
|                  | Perancang   | Axel York Poschmann (University Bochum, Germany) (Technology, 2009)                           |
|                  | Publikasi   | <a href="https://eprint.iacr.org/2009/516.pdf">https://eprint.iacr.org/2009/516.pdf</a> [138] |
|                  | Spesifikasi | <a href="https://eprint.iacr.org/2009/516.pdf">https://eprint.iacr.org/2009/516.pdf</a> [138] |

|                           | Standarisasi      | -                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |  |     |     |               |    |    |                |    |     |
|---------------------------|-------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--|-----|-----|---------------|----|----|----------------|----|-----|
| Karakteristik kriptografi | Fitur             | <p>DM-PRESENT memiliki struktur Merkle-Damgaard dengan berbagai konfigurasi sesuai parameter internal. DM-PRESENT memiliki dua variasi (lihat tabel di bawah).</p> <table border="1"> <thead> <tr> <th></th><th><math>n</math></th><th><math>r</math></th></tr> </thead> <tbody> <tr> <td>DM-PRESENT-80</td><td>64</td><td>80</td></tr> <tr> <td>DM-PRESENT-128</td><td>64</td><td>128</td></tr> </tbody> </table> <p>dengan <math>n</math>: panjang keluaran, dan <math>r</math>: panjang blok input</p> <p>DM-PRESENT memetakan variabel rantai <math>H_i</math> berukuran 64 bit dan blok pesan <math>M_i</math> menjadi nilai baru <math>H_i'</math> menggunakan konstruksi <i>Davies-Meyer</i> dengan persamaan <math>H_i' = E M_i(H_i) \oplus H_i</math>, di mana <math>E</math> merepresentasikan enkripsi menggunakan cipher PRESENT-80 atau PRESENT-128.</p> |  | $n$ | $r$ | DM-PRESENT-80 | 64 | 80 | DM-PRESENT-128 | 64 | 128 |
|                           | $n$               | $r$                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |  |     |     |               |    |    |                |    |     |
| DM-PRESENT-80             | 64                | 80                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    |  |     |     |               |    |    |                |    |     |
| DM-PRESENT-128            | 64                | 128                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |  |     |     |               |    |    |                |    |     |
|                           | Analisis keamanan | <p>Berdasarkan makalah <i>Multi-differential Cryptanalysis on Reduced DM-PRESENT-80: Collisions and Other Differential Properties</i> [139], DM-PRESENT-80 tidak mampu mempertahankan ketahanan yang memadai terhadap serangan multi-differential, khususnya pada versi dengan jumlah <i>round</i> yang direduksi. Penelitian tersebut menunjukkan bahwa penyerang dapat menemukan collision pada 12 <i>round</i> DM-PRESENT-80 dengan kompleksitas sekitar <math>2^{29,18}</math>, jauh lebih rendah dari ekspektasi <i>brute-force</i> <math>2^{64}</math>. Selain itu, mereka juga berhasil membangun <i>distinguisher</i> terhadap hingga 18</p>                                                                                                                                                                                                                  |  |     |     |               |    |    |                |    |     |

|                   |                                             |                                                                                                                                                                                                                                                                                                                                                                        |                                      |                          |
|-------------------|---------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------|--------------------------|
|                   |                                             | <i>round</i> , yang mengindikasikan bahwa struktur internal DM-PRESENT-80 masih menampilkan pola diferensial terdeteksi meskipun jumlah <i>round</i> -nya diperbanyak. Hasil ini menegaskan bahwa margin keamanan DM-PRESENT-80 terhadap serangan multi-differential relatif sempit dan tidak cukup kuat untuk menjamin keamanan pada jumlah <i>round</i> yang rendah. |                                      |                          |
| Analisis performa | Implementansi perangkat keras (proses ASIC) |                                                                                                                                                                                                                                                                                                                                                                        |                                      |                          |
|                   |                                             | <i>Area</i> (GE)                                                                                                                                                                                                                                                                                                                                                       | <i>power consumption</i> ( $\mu W$ ) | <i>Throughput</i> (kbps) |
|                   | DM-PRESENT-80                               | 2.213 / 1.600                                                                                                                                                                                                                                                                                                                                                          | 6,28 / 1,83                          | 242,42 / 14,63           |
|                   | DM-PRESENT-128                              | 2.530 / 1.886                                                                                                                                                                                                                                                                                                                                                          | 7,49 / 2,94                          | 387,88 / 22,9            |

### 3. GLUON

|                  |              |                                                                                                                                                                                                                                                                                            |
|------------------|--------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Profil Algoritma | Nama         | GLUON                                                                                                                                                                                                                                                                                      |
|                  | Perancang    | Thierry P. Berger (Universit e de Limoges 123 avenue Albert Thomas, France), Joffrey D'Hayer (Universit e de Lyon, INRIA), Kevin Marquet (Universit e de Lyon, INRIA), Marine Minier (Universit e de Lyon, INRIA), Ga el Thomas (Universit e de Limoges 123 avenue Albert Thomas, France). |
|                  | Publikasi    | AFRICACRYPT 2012                                                                                                                                                                                                                                                                           |
|                  | Spesifikasi  | <a href="https://link.springer.com/chapter/10.1007/978-3-642-31410-0_19">https://link.springer.com/chapter/10.1007/978-3-642-31410-0_19</a> [140]                                                                                                                                          |
|                  | Standarisasi | -                                                                                                                                                                                                                                                                                          |
|                  | Fitur        | GLUON memiliki struktur sponge dengan berbagai konfigurasi sesuai parameter internal.                                                                                                                                                                                                      |

|                           |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |       |     |      |     |     |           |   |     |     |     |           |    |     |     |     |            |    |     |     |     |
|---------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------|-----|------|-----|-----|-----------|---|-----|-----|-----|-----------|----|-----|-----|-----|------------|----|-----|-----|-----|
| Karakteristik kriptografi | <p>Terdapat tiga variasi GLUON (lihat tabel di bawah).</p> <table><tr><td>GLUON</td><td><math>r</math></td><td><math>cp</math></td><td><math>b</math></td><td><math>N</math></td></tr><tr><td>GLUON -64</td><td>8</td><td>128</td><td>136</td><td>128</td></tr><tr><td>GLUON -80</td><td>16</td><td>160</td><td>176</td><td>160</td></tr><tr><td>GLUON -112</td><td>32</td><td>224</td><td>256</td><td>224</td></tr></table> <p>dengan <math>r</math>: panjang blok input, <math>cp</math>: panjang keluaran dan <math>b</math>: ukuran fungsi <math>f</math>, <math>N</math>: ukuran blok register</p> <p>Laju dari konstruksi sponge yang terkait adalah <math>r</math>, dengan kapasitas <math>cp = (w - 2) \times r</math>, dan ukuran fungsi <math>f</math> adalah <math>b = r + cp</math>. Fungsi <math>f</math> terbagi menjadi dua bagian, yaitu bagian eksternal yang terdiri dari kata pertama sepanjang <math>r</math>-bit dari masukan, dan bagian internal yang terdiri dari <math>(w - 2)</math> kata <math>r</math>-bit berikutnya dari masukan. Pada tahap absorbing, setiap kata pesan <math>p_i</math> dengan panjang <math>r</math>-bit di-xor dengan kata <math>r</math>-bit pertama dari register utama FCSR. Selanjutnya, kata <math>r</math>-bit pertama ini menjadi keluaran pada tahap squeezing.</p> | GLUON | $r$ | $cp$ | $b$ | $N$ | GLUON -64 | 8 | 128 | 136 | 128 | GLUON -80 | 16 | 160 | 176 | 160 | GLUON -112 | 32 | 224 | 256 | 224 |
| GLUON                     | $r$                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            | $cp$  | $b$ | $N$  |     |     |           |   |     |     |     |           |    |     |     |     |            |    |     |     |     |
| GLUON -64                 | 8                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              | 128   | 136 | 128  |     |     |           |   |     |     |     |           |    |     |     |     |            |    |     |     |     |
| GLUON -80                 | 16                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             | 160   | 176 | 160  |     |     |           |   |     |     |     |           |    |     |     |     |            |    |     |     |     |
| GLUON -112                | 32                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             | 224   | 256 | 224  |     |     |           |   |     |     |     |           |    |     |     |     |            |    |     |     |     |
| Analisis keamanan         | <p>Berdasarkan analisis dalam makalah <i>Collision Spectrum, Entropy Loss, T-Sponges, and Cryptanalysis of GLUON-64</i> [141], GLUON-64 menunjukkan tingkat resistansi kriptografis yang rendah terhadap <i>iterated preimage attack</i> pada <i>full hash function</i>. Kelemahan ini disebabkan oleh penggunaan fungsi pembaruan internal yang non-injektif dan</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |       |     |      |     |     |           |   |     |     |     |           |    |     |     |     |            |    |     |     |     |

|                   |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |               |                   |               |                   |           |      |    |       |           |        |    |    |            |      |    |       |        |                        |           |        |           |       |            |       |
|-------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------|-------------------|---------------|-------------------|-----------|------|----|-------|-----------|--------|----|----|------------|------|----|-------|--------|------------------------|-----------|--------|-----------|-------|------------|-------|
|                   | <p>memiliki <i>collision probability spectrum</i> (CPS) tinggi. CPS yang tinggi menyebabkan banyak <i>state</i> internal memiliki beberapa <i>preimage</i>, sehingga ukuran ruang <i>state</i> menyusut secara signifikan selama iterasi, khususnya saat memproses pesan panjang dengan blok-blok identik di bagian akhir. Akibatnya, kompleksitas pencarian <i>preimage</i> penuh menurun dari klaim ideal <math>2^{128}</math> menjadi sekitar <math>2^{105,32}</math>, yang menunjukkan bahwa GLUON-64 tidak memberikan tingkat keamanan <i>preimage</i> setara tingkat keamanan yang diklaim dan rentan pada skenario pesan panjang berpola.</p> <p>[141]</p>                    |               |                   |               |                   |           |      |    |       |           |        |    |    |            |      |    |       |        |                        |           |        |           |       |            |       |
| Analisis performa | <p>Implementasi perangkat keras (ASIC synthetisor Cadence RTL version RC10.1.101 (32- bits version)</p> <table><tr><td></td><td>Area (GE)</td><td>Latency (clk)</td><td>Throughput (kbps)</td></tr><tr><td>GLUON -64</td><td>2071</td><td>66</td><td>12,12</td></tr><tr><td>GLUON -80</td><td>2799,3</td><td>50</td><td>32</td></tr><tr><td>GLUON -112</td><td>4724</td><td>55</td><td>58,18</td></tr></table> <p>Implementasi perangkat lunak (Intel Core 2 Duo @ 2.66 GHz)</p> <table><tr><td>Varian</td><td>performa (cycles/byte)</td></tr><tr><td>GLUON -64</td><td>1.7319</td></tr><tr><td>GLUON -80</td><td>8.523</td></tr><tr><td>GLUON -112</td><td>1.951</td></tr></table> |               | Area (GE)         | Latency (clk) | Throughput (kbps) | GLUON -64 | 2071 | 66 | 12,12 | GLUON -80 | 2799,3 | 50 | 32 | GLUON -112 | 4724 | 55 | 58,18 | Varian | performa (cycles/byte) | GLUON -64 | 1.7319 | GLUON -80 | 8.523 | GLUON -112 | 1.951 |
|                   | Area (GE)                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            | Latency (clk) | Throughput (kbps) |               |                   |           |      |    |       |           |        |    |    |            |      |    |       |        |                        |           |        |           |       |            |       |
| GLUON -64         | 2071                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 | 66            | 12,12             |               |                   |           |      |    |       |           |        |    |    |            |      |    |       |        |                        |           |        |           |       |            |       |
| GLUON -80         | 2799,3                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               | 50            | 32                |               |                   |           |      |    |       |           |        |    |    |            |      |    |       |        |                        |           |        |           |       |            |       |
| GLUON -112        | 4724                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 | 55            | 58,18             |               |                   |           |      |    |       |           |        |    |    |            |      |    |       |        |                        |           |        |           |       |            |       |
| Varian            | performa (cycles/byte)                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |               |                   |               |                   |           |      |    |       |           |        |    |    |            |      |    |       |        |                        |           |        |           |       |            |       |
| GLUON -64         | 1.7319                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |               |                   |               |                   |           |      |    |       |           |        |    |    |            |      |    |       |        |                        |           |        |           |       |            |       |
| GLUON -80         | 8.523                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |               |                   |               |                   |           |      |    |       |           |        |    |    |            |      |    |       |        |                        |           |        |           |       |            |       |
| GLUON -112        | 1.951                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |               |                   |               |                   |           |      |    |       |           |        |    |    |            |      |    |       |        |                        |           |        |           |       |            |       |

#### 4. LESAMNTA-LW

|                  |           |                                                                               |
|------------------|-----------|-------------------------------------------------------------------------------|
| Profil Algoritma | Nama      | LESAMNTA-LW                                                                   |
|                  | Perancang | Shoichi Hirose ( <i>Graduate School of Engineering, University of Fukui</i> ) |

|                           |                   |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |
|---------------------------|-------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|                           |                   | <p>3-9-1, Bunkyo, Fukui 910-8507, Jepang), Kota Ideguchi (<i>Systems Development Laboratory, Hitachi, Ltd. 292 Yoshida-cho, Totsuka-ku, Yokohama, Kanagawa 244-0817, Jepang</i>), Hidenori Kuwakado (<i>Graduate School of Engineering, Kobe University 1-1 Rokkodai, Nada, Kobe 657-8501, Jepang</i>), Bart Preneel dan Hirotaka Yoshida (<i>Department of Electrical Engineering ESAT/SCD-COSIC, Katholieke Universiteit Leuven Kasteelpark Arenberg 10, B-3001 Heverlee, Belgia</i>)</p> |
|                           | Publikasi         | ICICS 2010                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |
|                           | Spesifikasi       | <a href="https://link.springer.com/chapter/10.1007/978-3-642-24209-0_10">https://link.springer.com/chapter/10.1007/978-3-642-24209-0_10</a> [142]                                                                                                                                                                                                                                                                                                                                           |
|                           | Standarisasi      | ISO/IEC 29192-5                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |
| Karakteristik kriptografi | Fitur             | <p>LESAMNTA-LW memiliki struktur Merkle-Damgaard dengan berbagai konfigurasi sesuai parameter internal. ISO/IEC 29192 menetapkan panjang blok 256-bit dengan ukuran kunci 128-bit.</p> <p>Fungsi kompresi LESAMNTA-LW dibangun dari <i>block cipher</i> berbasis AES yang mana pengurangan keamanannya dapat dibuktikan.</p>                                                                                                                                                                |
|                           | Analisis keamanan | <p>Belum ada kerentanan kritis yang dilaporkan, tetapi karena hasil analisis masih terbatas memungkinkan adanya kerentanan potensial.</p> <p>Untuk pengaturan kunci tunggal, serangan terbaik adalah serangan integral yang diajukan oleh Shiba dkk. [143] pada 2021. Serangan ini</p>                                                                                                                                                                                                      |

|                       | <p>memungkinkan pemulihan kunci dilakukan lebih efisien daripada <i>brute-force</i> pada Lesamnta-LW-BC yang disederhanakan menjadi 20 <i>round</i>. Selain itu, serangan diferensial oleh Hirose dkk. [144] pada 2020 memungkinkan serangan identifikasi dijalankan secara efisien pada versi Lesamnta-LW-BC yang dipangkas menjadi 29 <i>round</i>.</p> <p>Sementara itu, pada pengaturan kunci yang diketahui, serangan terbaik adalah serangan <i>zero-sum</i> yang diajukan oleh Shiba dkk. pada 2021. Serangan ini memungkinkan identifikasi secara efisien pada Lesamnta-LW-BC yang dipangkas menjadi 47 <i>round</i>. Perlu dicatat bahwa semua serangan identifikasi ini tidak menurunkan keamanan dasar fungsi hash.</p> |                            |               |                     |                            |                   |                            |       |      |        |       |       |    |            |             |          |    |         |                        |   |      |                            |
|-----------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------|---------------|---------------------|----------------------------|-------------------|----------------------------|-------|------|--------|-------|-------|----|------------|-------------|----------|----|---------|------------------------|---|------|----------------------------|
| Analisis performa     | <p>Implementasi perangkat keras (<i>Low-Area ASIC</i>)</p> <table><tr><th>Logic Process</th><th>Area (Kgates)</th><th>Throughput (Mbit/s)</th><th>Clock (MHz)</th><th>Throughput / AREA</th><th>Throughput @30MHz (Mbit/s)</th></tr><tr><td>90 nm</td><td>8,24</td><td>125,55</td><td>188,3</td><td>15,31</td><td>20</td></tr></table> <p>Implementasi LESAMNTA-LW pada perangkat lunak</p> <table><tr><th>RAM (byte)</th><th>Cycles/byte</th><th>Platform</th></tr><tr><td>50</td><td>1.650,9</td><td>Renesas H8 (8-bit CPU)</td></tr><tr><td>-</td><td>39,5</td><td>Intel Core i5 (32-bit CPU)</td></tr></table>                                                                                                                 | Logic Process              | Area (Kgates) | Throughput (Mbit/s) | Clock (MHz)                | Throughput / AREA | Throughput @30MHz (Mbit/s) | 90 nm | 8,24 | 125,55 | 188,3 | 15,31 | 20 | RAM (byte) | Cycles/byte | Platform | 50 | 1.650,9 | Renesas H8 (8-bit CPU) | - | 39,5 | Intel Core i5 (32-bit CPU) |
| Logic Process         | Area (Kgates)                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      | Throughput (Mbit/s)        | Clock (MHz)   | Throughput / AREA   | Throughput @30MHz (Mbit/s) |                   |                            |       |      |        |       |       |    |            |             |          |    |         |                        |   |      |                            |
| 90 nm                 | 8,24                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               | 125,55                     | 188,3         | 15,31               | 20                         |                   |                            |       |      |        |       |       |    |            |             |          |    |         |                        |   |      |                            |
| RAM (byte)            | Cycles/byte                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        | Platform                   |               |                     |                            |                   |                            |       |      |        |       |       |    |            |             |          |    |         |                        |   |      |                            |
| 50                    | 1.650,9                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            | Renesas H8 (8-bit CPU)     |               |                     |                            |                   |                            |       |      |        |       |       |    |            |             |          |    |         |                        |   |      |                            |
| -                     | 39,5                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               | Intel Core i5 (32-bit CPU) |               |                     |                            |                   |                            |       |      |        |       |       |    |            |             |          |    |         |                        |   |      |                            |
| Informasi Open Source | <p><a href="https://github.com/kuwakado/Lesamnta-LW">https://github.com/kuwakado/Lesamnta-LW</a></p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |                            |               |                     |                            |                   |                            |       |      |        |       |       |    |            |             |          |    |         |                        |   |      |                            |

## 5. PHOTON

| Profil Algoritma          | Nama         | PHOTON                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |      |  |                    |     |     |      |                 |    |    |    |                  |     |    |    |                  |     |    |    |                  |     |    |    |                  |     |
|---------------------------|--------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------|--|--------------------|-----|-----|------|-----------------|----|----|----|------------------|-----|----|----|------------------|-----|----|----|------------------|-----|----|----|------------------|-----|
|                           | Perancang    | Jian Guo ( <i>Institute for Infocomm Research</i> , Singapura), Thomas Peyrin ( <i>Nanyang Technological University</i> , Singapura), Axel Poschmann ( <i>Nanyang Technological University</i> , Singapura).                                                                                                                                                                                                                                                                            |      |  |                    |     |     |      |                 |    |    |    |                  |     |    |    |                  |     |    |    |                  |     |    |    |                  |     |
|                           | Publikasi    | CRYPTO 2011                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |      |  |                    |     |     |      |                 |    |    |    |                  |     |    |    |                  |     |    |    |                  |     |    |    |                  |     |
|                           | Spesifikasi  | <a href="https://sites.google.com/site/photonhashfunction/">https://sites.google.com/site/photonhashfunction/</a> [142]                                                                                                                                                                                                                                                                                                                                                                 |      |  |                    |     |     |      |                 |    |    |    |                  |     |    |    |                  |     |    |    |                  |     |    |    |                  |     |
|                           | Standarisasi | ISO/IEC 29192-5 [150]                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |      |  |                    |     |     |      |                 |    |    |    |                  |     |    |    |                  |     |    |    |                  |     |    |    |                  |     |
| Karakteristik kriptografi | Fitur        | PHOTON memiliki struktur Sponge dengan berbagai konfigurasi sesuai parameter internal. ISO/IEC 29192 menetapkan lima variasi (lihat tabel di bawah).                                                                                                                                                                                                                                                                                                                                    |      |  |                    |     |     |      |                 |    |    |    |                  |     |    |    |                  |     |    |    |                  |     |    |    |                  |     |
|                           |              | <table><tr><th>PHOTON<br/><math>n/r/r'</math></th><th><math>n</math></th><th><math>r</math></th><th><math>r'</math></th></tr><tr><td>PHOTON-80/20/16</td><td>80</td><td>20</td><td>16</td></tr><tr><td>PHOTON-128/16/16</td><td>128</td><td>16</td><td>16</td></tr><tr><td>PHOTON-160/36/36</td><td>160</td><td>36</td><td>36</td></tr><tr><td>PHOTON-224/32/32</td><td>224</td><td>32</td><td>32</td></tr><tr><td>PHOTON-256/32/32</td><td>256</td><td>32</td><td>32</td></tr></table> |      |  | PHOTON<br>$n/r/r'$ | $n$ | $r$ | $r'$ | PHOTON-80/20/16 | 80 | 20 | 16 | PHOTON-128/16/16 | 128 | 16 | 16 | PHOTON-160/36/36 | 160 | 36 | 36 | PHOTON-224/32/32 | 224 | 32 | 32 | PHOTON-256/32/32 | 256 |
| PHOTON<br>$n/r/r'$        | $n$          | $r$                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     | $r'$ |  |                    |     |     |      |                 |    |    |    |                  |     |    |    |                  |     |    |    |                  |     |    |    |                  |     |
| PHOTON-80/20/16           | 80           | 20                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      | 16   |  |                    |     |     |      |                 |    |    |    |                  |     |    |    |                  |     |    |    |                  |     |    |    |                  |     |
| PHOTON-128/16/16          | 128          | 16                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      | 16   |  |                    |     |     |      |                 |    |    |    |                  |     |    |    |                  |     |    |    |                  |     |    |    |                  |     |
| PHOTON-160/36/36          | 160          | 36                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      | 36   |  |                    |     |     |      |                 |    |    |    |                  |     |    |    |                  |     |    |    |                  |     |    |    |                  |     |
| PHOTON-224/32/32          | 224          | 32                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      | 32   |  |                    |     |     |      |                 |    |    |    |                  |     |    |    |                  |     |    |    |                  |     |    |    |                  |     |
| PHOTON-256/32/32          | 256          | 32                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      | 32   |  |                    |     |     |      |                 |    |    |    |                  |     |    |    |                  |     |    |    |                  |     |    |    |                  |     |
|                           |              | dengan $n$ : panjang keluaran, $r$ : panjang blok input dan $r'$ : panjang blok keluaran                                                                                                                                                                                                                                                                                                                                                                                                |      |  |                    |     |     |      |                 |    |    |    |                  |     |    |    |                  |     |    |    |                  |     |    |    |                  |     |
|                           |              | Permutasi internal PHOTON mirip AES terdiri atas empat langkah berulang, yaitu                                                                                                                                                                                                                                                                                                                                                                                                          |      |  |                    |     |     |      |                 |    |    |    |                  |     |    |    |                  |     |    |    |                  |     |    |    |                  |     |

|                   |                                              | <i>AddConstants</i> , <i>SubCells</i> , <i>ShiftRows</i> , dan <i>MixColumnsSerial</i> selama 12 <i>round</i> . Pada langkah <i>SubCells</i> digunakan S-box PRESENT 4-bit .                                                                                                                                                                                                                                                                                                                                                                                                                     |                          |                  |                      |                          |                 |           |         |            |                  |             |         |            |                  |             |           |        |                  |             |           |            |                  |             |         |            |
|-------------------|----------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------|------------------|----------------------|--------------------------|-----------------|-----------|---------|------------|------------------|-------------|---------|------------|------------------|-------------|-----------|--------|------------------|-------------|-----------|------------|------------------|-------------|---------|------------|
|                   | Analisis keamanan                            | <p>Belum ada kerentanan kritis yang dilaporkan, tetapi karena hasil analisis masih terbatas memungkinkan adanya kerentanan potensial.</p> <p>Serangan terbaik adalah serangan <i>zero-sum</i> yang diajukan oleh Wang dkk. [147, 148] pada 2017. Serangan ini memungkinkan serangan identifikasi dilakukan secara efisien terhadap substitusi kriptografis PHOTON-80 yang disederhanakan menjadi 11 <i>round</i>, serta substitusi kriptografis PHOTON-128/160/224 dengan spesifikasi penuh. Namun, serangan identifikasi terhadap PHOTON tidak mengancam standar keamanan wajib fungsi hash</p> |                          |                  |                      |                          |                 |           |         |            |                  |             |         |            |                  |             |           |        |                  |             |           |            |                  |             |         |            |
| Analisis performa | Implementansi perangkat keras (proses 180nm) |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |                          |                  |                      |                          |                 |           |         |            |                  |             |         |            |                  |             |           |        |                  |             |           |            |                  |             |         |            |
|                   |                                              | <table><tr><th></th><th><i>Area</i> (GE)</th><th><i>Latency</i> (clk)</th><th><i>Throughput</i> (kbps)</th></tr><tr><td>PHOTON-80/20/16</td><td>865/1.168</td><td>708/132</td><td>2,82/15,15</td></tr><tr><td>PHOTON-128/16/16</td><td>1.122/1.708</td><td>996/156</td><td>1,61/10,26</td></tr><tr><td>PHOTON-160/36/36</td><td>1.396/2.117</td><td>1.332/180</td><td>2,7/20</td></tr><tr><td>PHOTON-224/32/32</td><td>1.735/2.786</td><td>1.716/204</td><td>1,86/15,69</td></tr><tr><td>PHOTON-256/32/32</td><td>2.177/4.362</td><td>996/156</td><td>3,21/20,51</td></tr></table>               |                          | <i>Area</i> (GE) | <i>Latency</i> (clk) | <i>Throughput</i> (kbps) | PHOTON-80/20/16 | 865/1.168 | 708/132 | 2,82/15,15 | PHOTON-128/16/16 | 1.122/1.708 | 996/156 | 1,61/10,26 | PHOTON-160/36/36 | 1.396/2.117 | 1.332/180 | 2,7/20 | PHOTON-224/32/32 | 1.735/2.786 | 1.716/204 | 1,86/15,69 | PHOTON-256/32/32 | 2.177/4.362 | 996/156 | 3,21/20,51 |
|                   | <i>Area</i> (GE)                             | <i>Latency</i> (clk)                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             | <i>Throughput</i> (kbps) |                  |                      |                          |                 |           |         |            |                  |             |         |            |                  |             |           |        |                  |             |           |            |                  |             |         |            |
| PHOTON-80/20/16   | 865/1.168                                    | 708/132                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          | 2,82/15,15               |                  |                      |                          |                 |           |         |            |                  |             |         |            |                  |             |           |        |                  |             |           |            |                  |             |         |            |
| PHOTON-128/16/16  | 1.122/1.708                                  | 996/156                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          | 1,61/10,26               |                  |                      |                          |                 |           |         |            |                  |             |         |            |                  |             |           |        |                  |             |           |            |                  |             |         |            |
| PHOTON-160/36/36  | 1.396/2.117                                  | 1.332/180                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        | 2,7/20                   |                  |                      |                          |                 |           |         |            |                  |             |         |            |                  |             |           |        |                  |             |           |            |                  |             |         |            |
| PHOTON-224/32/32  | 1.735/2.786                                  | 1.716/204                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        | 1,86/15,69               |                  |                      |                          |                 |           |         |            |                  |             |         |            |                  |             |           |        |                  |             |           |            |                  |             |         |            |
| PHOTON-256/32/32  | 2.177/4.362                                  | 996/156                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          | 3,21/20,51               |                  |                      |                          |                 |           |         |            |                  |             |         |            |                  |             |           |        |                  |             |           |            |                  |             |         |            |

|                                 |                                                                                                                                     |                                    |
|---------------------------------|-------------------------------------------------------------------------------------------------------------------------------------|------------------------------------|
|                                 | Implementasi perangkat lunak (Intel Core i7 @1,6 GHz)                                                                               |                                    |
|                                 |                                                                                                                                     | Implementasi teroptimasi<br>32 bit |
|                                 | PHOTON-80/20/16                                                                                                                     | 95                                 |
|                                 | PHOTON-128/16/16                                                                                                                    | 156                                |
|                                 | PHOTON-160/36/36                                                                                                                    | 116                                |
|                                 | PHOTON-224/32/32                                                                                                                    | 227                                |
|                                 | PHOTON-256/32/32                                                                                                                    | 135                                |
| Informasi<br><i>Open Source</i> | <a href="https://sites.google.com/site/photonhashfunction/downloads">https://sites.google.com/site/photonhashfunction/downloads</a> |                                    |

## 6. QUARK

|                              |              |                                                                                                                                                                                                                                                                                               |     |       |     |      |     |         |   |     |     |     |     |         |    |     |     |     |     |         |    |     |     |
|------------------------------|--------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----|-------|-----|------|-----|---------|---|-----|-----|-----|-----|---------|----|-----|-----|-----|-----|---------|----|-----|-----|
| Profil<br>Algoritma          | Nama         | QUARK                                                                                                                                                                                                                                                                                         |     |       |     |      |     |         |   |     |     |     |     |         |    |     |     |     |     |         |    |     |     |
|                              | Perancang    | Jean-Philippe Aumasson ( <i>Nagravision SA, Cheseaux, Swiss</i> ), Luca Henzen ( <i>ETH Zurich, Swiss</i> ), Willi Meier ( <i>FHNW, Windisch, Swiss</i> ), Maria Naya-Plasencia ( <i>FHNW, Windisch, Swiss</i> )                                                                              |     |       |     |      |     |         |   |     |     |     |     |         |    |     |     |     |     |         |    |     |     |
|                              | Publikasi    | CHES 2010                                                                                                                                                                                                                                                                                     |     |       |     |      |     |         |   |     |     |     |     |         |    |     |     |     |     |         |    |     |     |
|                              | Spesifikasi  | <a href="http://aumasson.jp/quark/">http://aumasson.jp/quark/</a> [149]                                                                                                                                                                                                                       |     |       |     |      |     |         |   |     |     |     |     |         |    |     |     |     |     |         |    |     |     |
|                              | Standarisasi | -                                                                                                                                                                                                                                                                                             |     |       |     |      |     |         |   |     |     |     |     |         |    |     |     |     |     |         |    |     |     |
| Karakteristik<br>kriptografi | Fitur        | QUARK memiliki struktur sponge dan berbagai konfigurasi sesuai dengan parameter internal. Permutasi QUARK dirancang dengan menggabungkan keunggulan Grain dan <i>block cipher</i> KATAN. Keluarga QUARK terdiri dari tiga varian, yaitu U-QUARK, D-QUARK, dan S-QUARK (lihat tabel di bawah). |     |       |     |      |     |         |   |     |     |     |     |         |    |     |     |     |     |         |    |     |     |
|                              |              |                                                                                                                                                                                                                                                                                               | $r$ | $c$   | $b$ | $4b$ | $n$ | U-QUARK | 8 | 128 | 136 | 544 | 136 | D-QUARK | 16 | 160 | 176 | 704 | 176 | S-QUARK | 32 | 224 | 256 |
|                              | $r$          | $c$                                                                                                                                                                                                                                                                                           | $b$ | $4b$  | $n$ |      |     |         |   |     |     |     |     |         |    |     |     |     |     |         |    |     |     |
| U-QUARK                      | 8            | 128                                                                                                                                                                                                                                                                                           | 136 | 544   | 136 |      |     |         |   |     |     |     |     |         |    |     |     |     |     |         |    |     |     |
| D-QUARK                      | 16           | 160                                                                                                                                                                                                                                                                                           | 176 | 704   | 176 |      |     |         |   |     |     |     |     |         |    |     |     |     |     |         |    |     |     |
| S-QUARK                      | 32           | 224                                                                                                                                                                                                                                                                                           | 256 | 1.024 | 256 |      |     |         |   |     |     |     |     |         |    |     |     |     |     |         |    |     |     |

|                   |                                                                                                                                                                                                                                                                                                                                                   | Dengan Rate ( $r$ ): jumlah bit yang diproses dalam setiap siklus, Capacity ( $c$ ) panjang keluaran: Width ( $b$ ): ukuran total dari internal state, Round ( $4b$ ): jumlah iterasi, Digest ( $n$ ): panjang blok keluaran.                                                                                                                                                                                                                                                                                                  |                   |               |                   |         |             |        |            |         |             |        |            |         |             |         |            |  |
|-------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------|---------------|-------------------|---------|-------------|--------|------------|---------|-------------|--------|------------|---------|-------------|---------|------------|--|
|                   | Analisis keamanan                                                                                                                                                                                                                                                                                                                                 | <p>Belum ada kerentanan kritis yang dilaporkan, tetapi karena hasil analisis masih terbatas memungkinkan adanya kerentanan potensial.</p> <p>Serangan terbaik adalah serangan diferensial bersyarat yang diajukan oleh Yang dkk [150]. pada 2018. Serangan ini memungkinkan serangan identifikasi dilakukan secara efisien terhadap U/D/S-QUARK yang disederhanakan menjadi 155, 166, dan 259 <i>round</i>. Namun, serangan identifikasi terhadap QUARK secara prinsip tidak mengancam standar keamanan wajib fungsi hash.</p> |                   |               |                   |         |             |        |            |         |             |        |            |         |             |         |            |  |
| Analisis performa | Implementansi perangkat keras (proses 0,18 $\mu$ m)                                                                                                                                                                                                                                                                                               |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |                   |               |                   |         |             |        |            |         |             |        |            |         |             |         |            |  |
|                   | <table><tr><th></th><th>Area (GE)</th><th>Latency (clk)</th><th>Throughput (kbps)</th></tr><tr><td>U-QUARK</td><td>1.379/2.392</td><td>544/68</td><td>1,47/11,76</td></tr><tr><td>D-QUARK</td><td>1.702/2.819</td><td>704/88</td><td>2,27/18,18</td></tr><tr><td>S-QUARK</td><td>2.296/4.640</td><td>1024/64</td><td>3,13/50,00</td></tr></table> |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                | Area (GE)         | Latency (clk) | Throughput (kbps) | U-QUARK | 1.379/2.392 | 544/68 | 1,47/11,76 | D-QUARK | 1.702/2.819 | 704/88 | 2,27/18,18 | S-QUARK | 2.296/4.640 | 1024/64 | 3,13/50,00 |  |
|                   | Area (GE)                                                                                                                                                                                                                                                                                                                                         | Latency (clk)                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  | Throughput (kbps) |               |                   |         |             |        |            |         |             |        |            |         |             |         |            |  |
| U-QUARK           | 1.379/2.392                                                                                                                                                                                                                                                                                                                                       | 544/68                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         | 1,47/11,76        |               |                   |         |             |        |            |         |             |        |            |         |             |         |            |  |
| D-QUARK           | 1.702/2.819                                                                                                                                                                                                                                                                                                                                       | 704/88                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         | 2,27/18,18        |               |                   |         |             |        |            |         |             |        |            |         |             |         |            |  |
| S-QUARK           | 2.296/4.640                                                                                                                                                                                                                                                                                                                                       | 1024/64                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        | 3,13/50,00        |               |                   |         |             |        |            |         |             |        |            |         |             |         |            |  |

## 7. SipHash-2-4

|                  |              |                                                                                                                 |
|------------------|--------------|-----------------------------------------------------------------------------------------------------------------|
| Profil Algoritma | Nama         | SipHash-2-4                                                                                                     |
|                  | Perancang    | Jean-Philippe Aumasson (NAGRA Swiss), Daniel J. Bernstein ( <i>University of Illinois at Chicago, Chicago</i> ) |
|                  | Publikasi    | INDOCRYPT 12                                                                                                    |
|                  | Spesifikasi  | <a href="https://eprint.iacr.org/2012/351.pdf">https://eprint.iacr.org/2012/351.pdf</a> [151]                   |
|                  | Standarisasi | -                                                                                                               |

|                           |                   |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |
|---------------------------|-------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Karakteristik kriptografi | Fitur             | SipHash-2-4 memiliki struktur sponge dan berbagai konfigurasi sesuai dengan parameter internal. SipHash-2-4 adalah fungsi hash dengan panjang hash 128 bit dan panjang keluaran 64 bit. Batas panjang pesan yang dapat diterima adalah 2039 byte, yang lebih pendek dibandingkan dengan fungsi hash umum.                                                                                                                                                                                                                                                                                                                                                                                                     |
|                           | Analisis keamanan | <p>Belum ada kerentanan kritis yang dilaporkan, tetapi karena hasil analisis masih terbatas memungkinkan adanya kerentanan potensial.</p> <p>Serangan terbaik terhadap SipHash-2-4 adalah serangan diferensial yang diusulkan oleh Dobraunig dkk. [152] pada tahun 2014, yang menemukan jalur diferensial dengan probabilitas karakteristik diferensial <math>2^{-236,3}</math>. Namun, karena serangan <i>brute-force</i> lebih efisien, hasil ini tidak mengancam keamanan SipHash. Serangan terbaik terhadap SipHash yang hanya menyederhanakan fase kompresi adalah serangan diferensial yang diusulkan oleh Xin dkk. [153] pada tahun 2019, meskipun hasil ini pun tidak mengancam keamanan SipHash.</p> |
| Analisis performa         |                   | <p>SipHash-2-4 diuji pada implementasi ASIC dengan pengukuran kebutuhan logika dalam satuan GE, Untuk arsitektur kompak, total GE sekitar 3.700 GE. Untuk arsitektur berkecepatan tinggi, total GE sekitar 13.500 GE.</p> <p>SipHash-2-4 diuji pada arsitektur amd64 memiliki hasil throughput antara 1,5 hingga 3 cycles/byte. Pengukuran</p>                                                                                                                                                                                                                                                                                                                                                                |

|                                                                            |                   |       |       |      |      |      |      |      |      |
|----------------------------------------------------------------------------|-------------------|-------|-------|------|------|------|------|------|------|
| kecepatan SipHash-2-4 untuk pesan pendek dapat dilihat pada tabel dibawah. |                   |       |       |      |      |      |      |      |      |
| Pesan yang dikirim                                                         | Panjang byte data | 8     | 16    | 24   | 32   | 40   | 48   | 56   | 64   |
| “bulldozer”                                                                | Cycles            | 124   | 141   | 156  | 171  | 188  | 203  | 218  | 234  |
|                                                                            | Cycles/byte       | 12,5  | 8,81  | 6,5  | 5,34 | 4,7  | 4,23 | 3,89 | 3,66 |
| “ishmael”                                                                  | Cycles            | 123   | 134   | 145  | 158  | 170  | 182  | 192  | 204  |
|                                                                            | Cycles/byte       | 15,38 | 8,38  | 6    | 4,94 | 4,25 | 3,79 | 3,43 | 3,19 |
| “latour”                                                                   | Cycles            | 135   | 144   | 162  | 171  | 189  | 207  | 216  | 225  |
|                                                                            | Cycles/byte       | 16,88 | 10,29 | 6,75 | 5,34 | 4,5  | 4,31 | 3,86 | 2,52 |

## 8. SPN-Hash

|                           |              |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |       |     |     |     |     |          |              |   |   |     |     |     |     |              |   |   |     |     |     |     |              |    |   |       |     |     |     |
|---------------------------|--------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------|-----|-----|-----|-----|----------|--------------|---|---|-----|-----|-----|-----|--------------|---|---|-----|-----|-----|-----|--------------|----|---|-------|-----|-----|-----|
| Profil Algoritma          | Nama         | SPN-Hash                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |       |     |     |     |     |          |              |   |   |     |     |     |     |              |   |   |     |     |     |     |              |    |   |       |     |     |     |
|                           | Perancang    | Jiali Choy (DSO <i>National Laboratories</i> , 20 <i>Science Park Drive</i> , Singapura), Huihui Yap (DSO <i>National Laboratories</i> , 20 <i>Science Park Drive</i> , Singapura), Khoongming Khoo (DSO <i>National Laboratories</i> , 20 <i>Science Park Drive</i> , Singapura), Jian Guo ( <i>Institute for Infocomm Research</i> , A*STAR, Singapura), Thomas Peyrin ( <i>Nanyang Technological University</i> , Singapura), Axel Poschmann ( <i>Nanyang Technological University</i> , Singapura), Chik How Tan ( <i>National University of Singapore</i> ) |       |     |     |     |     |          |              |   |   |     |     |     |     |              |   |   |     |     |     |     |              |    |   |       |     |     |     |
|                           | Publikasi    | AFRICACRYPT 12                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |       |     |     |     |     |          |              |   |   |     |     |     |     |              |   |   |     |     |     |     |              |    |   |       |     |     |     |
|                           | Spesifikasi  | <a href="https://eprint.iacr.org/2012/234.pdf">https://eprint.iacr.org/2012/234.pdf</a> [154]                                                                                                                                                                                                                                                                                                                                                                                                                                                                    |       |     |     |     |     |          |              |   |   |     |     |     |     |              |   |   |     |     |     |     |              |    |   |       |     |     |     |
|                           | Standarisasi | -                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |       |     |     |     |     |          |              |   |   |     |     |     |     |              |   |   |     |     |     |     |              |    |   |       |     |     |     |
| Karakteristik kriptografi | Fitur        | SPN-Hash memiliki struktur sponge mode operasi JH dengan berbagai konfigurasi sesuai parameter internal. Terdapat dua variasi SPN-Hash (lihat tabel di bawah).                                                                                                                                                                                                                                                                                                                                                                                                   |       |     |     |     |     |          |              |   |   |     |     |     |     |              |   |   |     |     |     |     |              |    |   |       |     |     |     |
|                           |              |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  | n     | m   | b   | r   | c   | keluaran | SPN-Hash-128 | 8 | 4 | 256 | 128 | 128 | 128 | SPN-Hash-256 | 8 | 8 | 512 | 256 | 256 | 256 | SPN-Hash-512 | 16 | 8 | 1.024 | 512 | 512 | 512 |
|                           |              |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  | n     | m   | b   | r   | c   | keluaran |              |   |   |     |     |     |     |              |   |   |     |     |     |     |              |    |   |       |     |     |     |
|                           |              | SPN-Hash-128                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     | 8     | 4   | 256 | 128 | 128 | 128      |              |   |   |     |     |     |     |              |   |   |     |     |     |     |              |    |   |       |     |     |     |
|                           |              | SPN-Hash-256                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     | 8     | 8   | 512 | 256 | 256 | 256      |              |   |   |     |     |     |     |              |   |   |     |     |     |     |              |    |   |       |     |     |     |
| SPN-Hash-512              | 16           | 8                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                | 1.024 | 512 | 512 | 512 |     |          |              |   |   |     |     |     |     |              |   |   |     |     |     |     |              |    |   |       |     |     |     |
|                           |              |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |       |     |     |     |     |          |              |   |   |     |     |     |     |              |   |   |     |     |     |     |              |    |   |       |     |     |     |
|                           |              |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |       |     |     |     |     |          |              |   |   |     |     |     |     |              |   |   |     |     |     |     |              |    |   |       |     |     |     |
|                           |              |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |       |     |     |     |     |          |              |   |   |     |     |     |     |              |   |   |     |     |     |     |              |    |   |       |     |     |     |

|                   |                                                  |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |                   |                             |               |                   |                             |              |               |        |             |            |              |               |          |              |           |
|-------------------|--------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------|-----------------------------|---------------|-------------------|-----------------------------|--------------|---------------|--------|-------------|------------|--------------|---------------|----------|--------------|-----------|
|                   |                                                  | <p>dengan <math>n</math>: jumlah byte/bundle, <math>m</math>: jumlah bundle <math>b</math>: lebar, <math>r</math>:laju, <math>c</math>: kapasitas.</p> <p>SPN-Hash beroperasi pada sebuah state dengan ukuran <math>b = r + c</math> bit. <math>b</math> disebut sebagai lebar, <math>r</math> adalah laju, dan <math>c</math> adalah kapasitas. Desain kami adalah konstruksi iteratif sederhana yang didasarkan pada permutasi panjang tetap yang tidak terkunci <math>P</math>, di mana <math>r = c</math>. State internal dari <math>P</math> dapat direpresentasikan oleh matriks <math>n \times m</math> dari sel 8-bit, di mana <math>n</math> adalah jumlah byte dalam satu bundle, dan <math>m</math> adalah jumlah bundle. Dengan demikian, <math>P</math> beroperasi pada lebar <math>b = 8nm</math> bit, laju dan kapasitas masing-masing adalah <math>4nm</math>-bit, dan keluarannya adalah nilai hash <math>4nm</math>-bit.</p> |                   |                             |               |                   |                             |              |               |        |             |            |              |               |          |              |           |
|                   | Analisis keamanan                                | Belum ada kerentanan kritis yang dilaporkan, tetapi karena hasil analisis masih terbatas memungkinkan adanya kerentanan potensial.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |                   |                             |               |                   |                             |              |               |        |             |            |              |               |          |              |           |
| Analisis performa | Implementansi perangkat keras (EMC 0.18 $\mu$ m) |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |                   |                             |               |                   |                             |              |               |        |             |            |              |               |          |              |           |
|                   |                                                  | <table><tr><td></td><td>Area (GE)</td><td>Latency (clk)</td><td>Throughput (kbps)</td><td>FOM (nbps/GE<sup>2</sup>)</td></tr><tr><td>SPN-Hash-128</td><td>2.777 / 4.600</td><td>990/45</td><td>36,1 / 55,7</td><td>2.338/2627</td></tr><tr><td>SPN-Hash-256</td><td>4.625 / 8.500</td><td>2.380/70</td><td>35,8 / 111,3</td><td>837/1.541</td></tr></table>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    |                   | Area (GE)                   | Latency (clk) | Throughput (kbps) | FOM (nbps/GE <sup>2</sup> ) | SPN-Hash-128 | 2.777 / 4.600 | 990/45 | 36,1 / 55,7 | 2.338/2627 | SPN-Hash-256 | 4.625 / 8.500 | 2.380/70 | 35,8 / 111,3 | 837/1.541 |
|                   | Area (GE)                                        | Latency (clk)                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  | Throughput (kbps) | FOM (nbps/GE <sup>2</sup> ) |               |                   |                             |              |               |        |             |            |              |               |          |              |           |
| SPN-Hash-128      | 2.777 / 4.600                                    | 990/45                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         | 36,1 / 55,7       | 2.338/2627                  |               |                   |                             |              |               |        |             |            |              |               |          |              |           |
| SPN-Hash-256      | 4.625 / 8.500                                    | 2.380/70                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       | 35,8 / 111,3      | 837/1.541                   |               |                   |                             |              |               |        |             |            |              |               |          |              |           |

## 9. SPONGENT

|           |           |                                                                                                                                                                                                                                                                                                                                           |
|-----------|-----------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Profil    | Nama      | SPONGENT                                                                                                                                                                                                                                                                                                                                  |
| Algoritma | Perancang | Andrey Bogdanov ( <i>Katholieke Universiteit Leuven, ESAT/COSIC and IBBT, Belgia</i> ),<br>Miroslav Knežević ( <i>NXP Semiconductors, Leuven, Belgia</i> ), Gregor Leander ( <i>DTU Mathematics, Technical University of Denmark</i> ),<br>Deniz Toz ( <i>Katholieke Universiteit Leuven, ESAT/COSIC and IBBT, Belgia</i> ), Kerem Varıcı |

|                           |              | (Katholieke Universiteit Leuven, ESAT/COSIC and IBBT, Belgia), Ingrid Verbauwhede (Katholieke Universiteit Leuven, ESAT/COSIC and IBBT, Belgia).                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |                   |     |     |     |                   |    |    |   |                    |    |     |    |                     |     |     |   |                      |     |     |     |                      |     |     |    |                     |     |     |    |                      |     |     |     |                      |     |     |    |                      |     |     |     |                      |     |     |     |                      |     |     |    |                      |     |     |     |                      |     |     |     |
|---------------------------|--------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------|-----|-----|-----|-------------------|----|----|---|--------------------|----|-----|----|---------------------|-----|-----|---|----------------------|-----|-----|-----|----------------------|-----|-----|----|---------------------|-----|-----|----|----------------------|-----|-----|-----|----------------------|-----|-----|----|----------------------|-----|-----|-----|----------------------|-----|-----|-----|----------------------|-----|-----|----|----------------------|-----|-----|-----|----------------------|-----|-----|-----|
|                           | Publikasi    | CHES 11                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |                   |     |     |     |                   |    |    |   |                    |    |     |    |                     |     |     |   |                      |     |     |     |                      |     |     |    |                     |     |     |    |                      |     |     |     |                      |     |     |    |                      |     |     |     |                      |     |     |     |                      |     |     |    |                      |     |     |     |                      |     |     |     |
|                           | Spesifikasi  | <a href="https://www.iacr.org/archive/ches2011/69170311/69170311.pdf">https://www.iacr.org/archive/ches2011/69170311/69170311.pdf</a> [155]                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |                   |     |     |     |                   |    |    |   |                    |    |     |    |                     |     |     |   |                      |     |     |     |                      |     |     |    |                     |     |     |    |                      |     |     |     |                      |     |     |    |                      |     |     |     |                      |     |     |     |                      |     |     |    |                      |     |     |     |                      |     |     |     |
|                           | Standarisasi | ISO/IEC 29192-5 [146]                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |                   |     |     |     |                   |    |    |   |                    |    |     |    |                     |     |     |   |                      |     |     |     |                      |     |     |    |                     |     |     |    |                      |     |     |     |                      |     |     |    |                      |     |     |     |                      |     |     |     |                      |     |     |    |                      |     |     |     |                      |     |     |     |
| Karakteristik kriptografi | Fitur        | <p>SPONGENT memiliki struktur sponge yang menggunakan permutasi tipe PRESENT dan berbagai konfigurasi sesuai dengan parameter internal. Para perancang telah menunjukkan 13 variasi (lihat tabel di bawah), dan lima di antaranya telah distandardisasi sebagai ISO/IEC 29192-5 (* pada tabel).</p> <table><tr><th>SPONGENT-<math>n/c/r</math></th><th><math>n</math></th><th><math>c</math></th><th><math>r</math></th></tr><tr><td>SPONGENT-88/80/8*</td><td>88</td><td>80</td><td>8</td></tr><tr><td>SPONGENT-88/176/88</td><td>88</td><td>176</td><td>88</td></tr><tr><td>SPONGENT-128/128/8*</td><td>128</td><td>128</td><td>8</td></tr><tr><td>SPONGENT-128/256/128</td><td>128</td><td>256</td><td>128</td></tr><tr><td>SPONGENT-160/160/16*</td><td>160</td><td>160</td><td>16</td></tr><tr><td>SPONGENT-160/160/80</td><td>160</td><td>160</td><td>80</td></tr><tr><td>SPONGENT-160/320/160</td><td>160</td><td>320</td><td>160</td></tr><tr><td>SPONGENT-224/224/16*</td><td>224</td><td>224</td><td>16</td></tr><tr><td>SPONGENT-224/224/112</td><td>224</td><td>224</td><td>112</td></tr><tr><td>SPONGENT-224/448/224</td><td>224</td><td>448</td><td>224</td></tr><tr><td>SPONGENT-256/256/16*</td><td>256</td><td>256</td><td>16</td></tr><tr><td>SPONGENT-256/256/128</td><td>256</td><td>256</td><td>128</td></tr><tr><td>SPONGENT-256/512/256</td><td>256</td><td>512</td><td>256</td></tr></table> <p>dengan <math>n</math>: panjang keluaran, <math>c</math>: kapasitas dan <math>r</math>: panjang blok input</p> | SPONGENT- $n/c/r$ | $n$ | $c$ | $r$ | SPONGENT-88/80/8* | 88 | 80 | 8 | SPONGENT-88/176/88 | 88 | 176 | 88 | SPONGENT-128/128/8* | 128 | 128 | 8 | SPONGENT-128/256/128 | 128 | 256 | 128 | SPONGENT-160/160/16* | 160 | 160 | 16 | SPONGENT-160/160/80 | 160 | 160 | 80 | SPONGENT-160/320/160 | 160 | 320 | 160 | SPONGENT-224/224/16* | 224 | 224 | 16 | SPONGENT-224/224/112 | 224 | 224 | 112 | SPONGENT-224/448/224 | 224 | 448 | 224 | SPONGENT-256/256/16* | 256 | 256 | 16 | SPONGENT-256/256/128 | 256 | 256 | 128 | SPONGENT-256/512/256 | 256 | 512 | 256 |
| SPONGENT- $n/c/r$         | $n$          | $c$                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   | $r$               |     |     |     |                   |    |    |   |                    |    |     |    |                     |     |     |   |                      |     |     |     |                      |     |     |    |                     |     |     |    |                      |     |     |     |                      |     |     |    |                      |     |     |     |                      |     |     |     |                      |     |     |    |                      |     |     |     |                      |     |     |     |
| SPONGENT-88/80/8*         | 88           | 80                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    | 8                 |     |     |     |                   |    |    |   |                    |    |     |    |                     |     |     |   |                      |     |     |     |                      |     |     |    |                     |     |     |    |                      |     |     |     |                      |     |     |    |                      |     |     |     |                      |     |     |     |                      |     |     |    |                      |     |     |     |                      |     |     |     |
| SPONGENT-88/176/88        | 88           | 176                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   | 88                |     |     |     |                   |    |    |   |                    |    |     |    |                     |     |     |   |                      |     |     |     |                      |     |     |    |                     |     |     |    |                      |     |     |     |                      |     |     |    |                      |     |     |     |                      |     |     |     |                      |     |     |    |                      |     |     |     |                      |     |     |     |
| SPONGENT-128/128/8*       | 128          | 128                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   | 8                 |     |     |     |                   |    |    |   |                    |    |     |    |                     |     |     |   |                      |     |     |     |                      |     |     |    |                     |     |     |    |                      |     |     |     |                      |     |     |    |                      |     |     |     |                      |     |     |     |                      |     |     |    |                      |     |     |     |                      |     |     |     |
| SPONGENT-128/256/128      | 128          | 256                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   | 128               |     |     |     |                   |    |    |   |                    |    |     |    |                     |     |     |   |                      |     |     |     |                      |     |     |    |                     |     |     |    |                      |     |     |     |                      |     |     |    |                      |     |     |     |                      |     |     |     |                      |     |     |    |                      |     |     |     |                      |     |     |     |
| SPONGENT-160/160/16*      | 160          | 160                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   | 16                |     |     |     |                   |    |    |   |                    |    |     |    |                     |     |     |   |                      |     |     |     |                      |     |     |    |                     |     |     |    |                      |     |     |     |                      |     |     |    |                      |     |     |     |                      |     |     |     |                      |     |     |    |                      |     |     |     |                      |     |     |     |
| SPONGENT-160/160/80       | 160          | 160                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   | 80                |     |     |     |                   |    |    |   |                    |    |     |    |                     |     |     |   |                      |     |     |     |                      |     |     |    |                     |     |     |    |                      |     |     |     |                      |     |     |    |                      |     |     |     |                      |     |     |     |                      |     |     |    |                      |     |     |     |                      |     |     |     |
| SPONGENT-160/320/160      | 160          | 320                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   | 160               |     |     |     |                   |    |    |   |                    |    |     |    |                     |     |     |   |                      |     |     |     |                      |     |     |    |                     |     |     |    |                      |     |     |     |                      |     |     |    |                      |     |     |     |                      |     |     |     |                      |     |     |    |                      |     |     |     |                      |     |     |     |
| SPONGENT-224/224/16*      | 224          | 224                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   | 16                |     |     |     |                   |    |    |   |                    |    |     |    |                     |     |     |   |                      |     |     |     |                      |     |     |    |                     |     |     |    |                      |     |     |     |                      |     |     |    |                      |     |     |     |                      |     |     |     |                      |     |     |    |                      |     |     |     |                      |     |     |     |
| SPONGENT-224/224/112      | 224          | 224                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   | 112               |     |     |     |                   |    |    |   |                    |    |     |    |                     |     |     |   |                      |     |     |     |                      |     |     |    |                     |     |     |    |                      |     |     |     |                      |     |     |    |                      |     |     |     |                      |     |     |     |                      |     |     |    |                      |     |     |     |                      |     |     |     |
| SPONGENT-224/448/224      | 224          | 448                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   | 224               |     |     |     |                   |    |    |   |                    |    |     |    |                     |     |     |   |                      |     |     |     |                      |     |     |    |                     |     |     |    |                      |     |     |     |                      |     |     |    |                      |     |     |     |                      |     |     |     |                      |     |     |    |                      |     |     |     |                      |     |     |     |
| SPONGENT-256/256/16*      | 256          | 256                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   | 16                |     |     |     |                   |    |    |   |                    |    |     |    |                     |     |     |   |                      |     |     |     |                      |     |     |    |                     |     |     |    |                      |     |     |     |                      |     |     |    |                      |     |     |     |                      |     |     |     |                      |     |     |    |                      |     |     |     |                      |     |     |     |
| SPONGENT-256/256/128      | 256          | 256                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   | 128               |     |     |     |                   |    |    |   |                    |    |     |    |                     |     |     |   |                      |     |     |     |                      |     |     |    |                     |     |     |    |                      |     |     |     |                      |     |     |    |                      |     |     |     |                      |     |     |     |                      |     |     |    |                      |     |     |     |                      |     |     |     |
| SPONGENT-256/512/256      | 256          | 512                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   | 256               |     |     |     |                   |    |    |   |                    |    |     |    |                     |     |     |   |                      |     |     |     |                      |     |     |    |                     |     |     |    |                      |     |     |     |                      |     |     |    |                      |     |     |     |                      |     |     |     |                      |     |     |    |                      |     |     |     |                      |     |     |     |

|                       |                                                                                                                         |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |               |                   |
|-----------------------|-------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------|-------------------|
|                       | Analisis keamanan                                                                                                       | Belum ada kerentanan kritis yang dilaporkan, tetapi karena hasil analisis masih terbatas memungkinkan adanya kerentanan potensial.<br><br>Serangan terbaik adalah serangan diferensial yang dipangkas yang diajukan oleh Zhang dkk. [156] pada 2017. Serangan ini memungkinkan serangan identifikasi dilakukan secara efisien terhadap variasi penyederhanaan substitusi kriptografis SPONGENT. Namun, serangan identifikasi pada SPONGENT tidak mengancam standar keamanan wajib fungsi hash. |               |                   |
| Analisis performa     | Implementasi perangkat keras (proses 130nm)                                                                             |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |               |                   |
|                       |                                                                                                                         | Area (GE)                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      | Latency (clk) | Throughput (kbps) |
|                       | SPONGENT-88/80/8                                                                                                        | 738/1127                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       | 990/45        | 0.81/17.78        |
|                       | SPONGENT-128/128/8                                                                                                      | 1060/1687                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      | 2380/70       | 0.34/11.43        |
|                       | SPONGENT-160/160/16                                                                                                     | 1329/2190                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      | 3960/90       | 0.40/17.78        |
|                       | SPONGENT-224/224/16                                                                                                     | 1728/2903                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      | 7200/120      | 0.22/13.33        |
|                       | SPONGENT-256/256/16                                                                                                     | 1950/3281                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      | 9520/140      | 0.17/11.43        |
| Informasi Open Source | <a href="https://sites.google.com/site/spongenthash/downloads">https://sites.google.com/site/spongenthash/downloads</a> |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |               |                   |

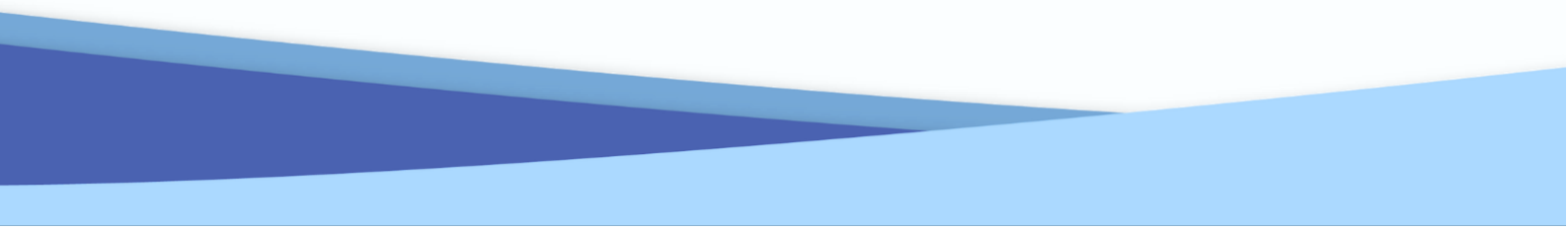


# BAB IV

## PENUTUP



KESIMPULAN UMUM PANDUAN KRIPTOGRAFI  
*LIGHTWEIGHT*



## BAB IV PENUTUP

Kriptografi *lightweight* telah menjadi komponen penting dalam pengamanan perangkat dengan sumber daya terbatas, seperti sensor, perangkat IoT, RFID, dan sistem tertanam. Dokumen ini memaparkan konsep dasar, prinsip desain, serta contoh algoritma *lightweight* yang mewakili tiga kategori utama: *stream cipher* (misalnya Trivium, Grain v1), *block cipher* (misalnya PRESENT, CLEFIA), dan fungsi *hash* (misalnya SPONGENT, GLUON-64). Tujuan utamanya adalah menghadirkan solusi kriptografi yang efisien dalam penggunaan daya, area perangkat keras, dan waktu proses, sekaligus tetap menjaga keamanan data.

Evaluasi terhadap beberapa algoritma yang dikaji menunjukkan bahwa efisiensi tinggi tidak selalu sejalan dengan keamanan tinggi. Beberapa algoritma *lightweight* yang pernah diusulkan ternyata memiliki margin keamanan kecil terhadap serangan kriptanalisis modern. Misalnya, GLUON-64 terbukti rentan terhadap *iterated preimage attack* karena tingginya *collision probability spectrum* (CPS), yang menyebabkan kompleksitas pencarian *preimage* penuh turun dari klaim ideal  $2^{128}$  menjadi sekitar  $2^{105,32}$ . Algoritma ARMADILLO2 gagal mempertahankan non-linearitas terhadap teknik *local-linearization*, memungkinkan serangan *semi-free-start collision* secara praktis. Sementara itu, DM-PRESENT-80 menunjukkan kelemahan terhadap serangan *multi-differential*, dengan *collision* pada 12 *round* (kompleksitas  $2^{29,18}$  dan *distinguisher* hingga 18 *round*). Hasil-hasil ini menggarisbawahi perlunya pengujian menyeluruh terhadap keamanan algoritma sebelum digunakan secara luas.

Sebagai penutup, pengembangan dan pemilihan algoritma kriptografi *lightweight* harus memperhatikan keseimbangan antara efisiensi dan ketahanan kriptografis. Algoritma harus ringan secara komputasional, tetapi juga cukup kuat menghadapi berbagai jenis serangan seperti *collision*, *preimage*, dan *differential attacks*. Diperlukan kolaborasi berkelanjutan antara peneliti, pengembang, dan lembaga standardisasi untuk

mengevaluasi, memperbaiki, dan memperbarui algoritma yang ada sesuai dengan hasil penelitian terkini. Hanya melalui pendekatan berbasis bukti dan evaluasi berkelanjutan, implementasi kriptografi *lightweight* dapat memberikan perlindungan andal pada ekosistem perangkat dengan sumber daya terbatas.



## LAMPIRAN

### CONTOH IMPLEMENTASI KRIPTOGRAFI *LIGHTWEIGHT* DALAM BAHASA PEMROGRAMAN

Berikut ini adalah beberapa contoh implementasi kriptografi *lightweight* dalam Bahasa pemrograman.

#### A. Implementasi SPECK 64 dan SPECK 128

Berikut adalah implementasi SPECK 64 dan SPECK 128 berdasarkan dokumen SIMON and SPECK *Implementation Guide* yang ditulis oleh Ray Beaulieu, Douglas Shors, Jason Smith, Stefan Treatman-Clark, Bryan Weeks, dan Louis Wingers dari *National Security Agency* yang dapat diunduh pada halaman <https://nsacyber.github.io/simon-speck/implementations/ImplementationGuide1.1.pdf>.

Implementasi SPECK 64 adalah sebagai berikut :

```
#define ER32(x,y,k) (x=ROTR32(x,8), x+=y, x^=k,  
y=ROTL32(y,3), y^=x)  
#define DR32(x,y,k) (y^=x, y=ROTR32(y,3), x^=k, x-=y,  
x=ROTL32(x,8))  
  
void Speck6496KeySchedule(u32 K[],u32 rk[])  
{  
    u32 i,C=K[2],B=K[1],A=K[0];  
  
    for(i=0;i<26;){  
        rk[i]=A; ER32(B,A,i++);  
        rk[i]=A; ER32(C,A,i++);  
    }  
}  
  
void Speck6496Encrypt(u32 Pt[],u32 Ct[],u32 rk[])  
{  
    u32 i;  
    Ct[0]=Pt[0]; Ct[1]=Pt[1];  
    for(i=0;i<26;){ ER32(Ct[1],Ct[0],rk[i++]);  
    }  
}
```

```

void Speck6496Decrypt(u32 Pt[],u32 Ct[],u32 rk[])
{
    int i;

    Pt[0]=Ct[0]; Pt[1]=Ct[1];
    for(i=25;i>=0;) DR32(Pt[1],Pt[0],rk[i--]);
}

void Speck64128KeySchedule(u32 K[],u32 rk[])
{
    u32 i,D=K[3],C=K[2],B=K[1],A=K[0];
    for(i=0;i<27;){
        rk[i]=A; ER32(B,A,i++);
        rk[i]=A; ER32(C,A,i++);
        rk[i]=A; ER32(D,A,i++);
    }
}

void Speck64128Encrypt(u32 Pt[],u32 Ct[],u32 rk[])
{
    u32 i;

    Ct[0]=Pt[0]; Ct[1]=Pt[1];
    for(i=0;i<27;) ER32(Ct[1],Ct[0],rk[i++]);
}

void Speck64128Decrypt(u32 Pt[],u32 Ct[],u32 rk[])
{
    int i;

    Pt[0]=Ct[0]; Pt[1]=Ct[1];
    for(i=26;i>=0;) DR32(Pt[1],Pt[0],rk[i--]);
}

```

Implementasi SPECK 128 adalah sebagai berikut :

```

#define ER64(x,y,k) (x=ROTR64(x,8), x+=y, x^=k, y=ROTL64(y,3),
y^=x)

```

```

#define  DR64(x,y,k)  (y^=x,   y=ROTR64(y,3),   x^=k,   x-=y,
x=ROTL64(x,8))

void Speck128128KeySchedule(u64 K[],u64 rk[])
{
    u64 i,B=K[1],A=K[0];

    for(i=0;i<31;){
        rk[i]=A;
        ER64(B,A,i++);
    }
    rk[i]=A;
}

void Speck128128Encrypt(u64 Pt[],u64 Ct[],u64 rk[])
{
    u64 i;

    Ct[0]=Pt[0]; Ct[1]=Pt[1];
    for(i=0;i<32;) ER64(Ct[1],Ct[0],rk[i++]);
}

void Speck128128Decrypt(u64 Pt[],u64 Ct[],u64 rk[])
{
    int i;
    Pt[0]=Ct[0]; Pt[1]=Ct[1];
    for(i=31;i>=0;) DR64(Pt[1],Pt[0],rk[i--]);
}

void Speck128192KeySchedule(u64 K[],u64 rk[])
{
    u64 i,C=K[2],B=K[1],A=K[0];

    for(i=0;i<32;){
        rk[i]=A; ER64(B,A,i++);
        rk[i]=A; ER64(C,A,i++);
    }
    rk[i]=A;
}

```

```

}

void Speck128192Encrypt(u64 Pt[],u64 Ct[],u64 rk[])
{
    u64 i;

    Ct[0]=Pt[0]; Ct[1]=Pt[1];
    for(i=0;i<33;) ER64(Ct[1],Ct[0],rk[i++]);
}

void Speck128192Decrypt(u64 Pt[],u64 Ct[],u64 rk[])
{
    int i;

    Pt[0]=Ct[0]; Pt[1]=Ct[1];
    for(i=32;i>=0;) DR64(Pt[1],Pt[0],rk[i--]);
}

void Speck128256KeySchedule(u64 K[],u64 rk[])
{
    u64 i,D=K[3],C=K[2],B=K[1],A=K[0];

    for(i=0;i<33;){
        rk[i]=A; ER64(B,A,i++);
        rk[i]=A; ER64(C,A,i++);
        rk[i]=A; ER64(D,A,i++);
    }
    rk[i]=A;
}

void Speck128256Encrypt(u64 Pt[],u64 Ct[],u64 rk[])
{
    u64 i;

    Ct[0]=Pt[0]; Ct[1]=Pt[1];
    for(i=0;i<34;) ER64(Ct[1],Ct[0],rk[i++]);
}

```

```

void Speck128256Decrypt(u64 Pt[],u64 Ct[],u64 rk[])
{
    int i;

    Pt[0]=Ct[0]; Pt[1]=Ct[1];
    for(i=33;i>=0;) DR64(Pt[1],Pt[0],rk[i--]);
}

```

## B. Implementasi PRESENT

Berikut adalah implementasi PRESENT dalam bahasa pemrograman C yang dapat diunduh pada halaman [https://www.oryx-embedded.com/doc/present\\_8c\\_source.html](https://www.oryx-embedded.com/doc/present_8c_source.html).

```

/**
 * @file present.c
 * @brief PRESENT encryption algorithm
 *
 * @section License
 *
 * SPDX-License-Identifier: GPL-2.0-or-later
 *
 * Copyright (C) 2010-2025 Oryx Embedded SARL. All rights reserved.
 *
 * This file is part of CycloneCRYPTO Open.
 *
 * This program is free software; you can redistribute it and/or
 * modify it under the terms of the GNU General Public License
 * as published by the Free Software Foundation; either version
 * 2
 * of the License, or (at your option) any later version.
 *
 * This program is distributed in the hope that it will be
 * useful,

```

```

* but WITHOUT ANY WARRANTY; without even the implied warranty
of
* MERCHANTABILITY or FITNESS FOR A PARTICULAR PURPOSE. See
the
* GNU General Public License for more details.
*
* You should have received a copy of the GNU General Public
License
* along with this program; if not, write to the Free Software
Foundation,
* Inc., 51 Franklin Street, Fifth Floor, Boston, MA 02110-
1301, USA.
*
* @section Description
*
* PRESENT is an ultra-lightweight block cipher
*
* @author Oryx Embedded SARL (www.oryx-embedded.com)
* @version 2.5.0
**/

//Switch to the appropriate trace level
#define TRACE_LEVEL_CRYPTOTRACE_LEVEL

//Dependencies
#include "core/crypto.h"
#include "cipher/present.h"

//Check crypto library configuration
#if (PRESENT_SUPPORT == ENABLED)

//S-box
static const uint8_t sbbox[16] =
{
    0x0C, 0x05, 0x06, 0x0B, 0x09, 0x00, 0x0A, 0x0D, 0x03, 0x0E,
    0x0F, 0x08, 0x04, 0x07, 0x01, 0x02
};

```

```

//Inverse S-box
static const uint8_t isbox[256] =
{
    0x55, 0x5E, 0x5F, 0x58, 0x5C, 0x51, 0x52, 0x5D, 0x5B, 0x54,
    0x56, 0x53, 0x50, 0x57, 0x59, 0x5A,
    0xE5, 0xEE, 0xEF, 0xE8, 0xEC, 0xE1, 0xE2, 0xED, 0xEB, 0xE4,
    0xE6, 0xE3, 0xE0, 0xE7, 0xE9, 0xEA,
    0xF5, 0xFE, 0xFF, 0xF8, 0xFC, 0xF1, 0xF2, 0xFD, 0xFB, 0xF4,
    0xF6, 0xF3, 0xF0, 0xF7, 0xF9, 0xFA,
    0x85, 0x8E, 0x8F, 0x88, 0x8C, 0x81, 0x82, 0x8D, 0x8B, 0x84,
    0x86, 0x83, 0x80, 0x87, 0x89, 0x8A,
    0xC5, 0xCE, 0xCF, 0xC8, 0xCC, 0xC1, 0xC2, 0xCD, 0xCB, 0xC4,
    0xC6, 0xC3, 0xC0, 0xC7, 0xC9, 0xCA,
    0x15, 0x1E, 0x1F, 0x18, 0x1C, 0x11, 0x12, 0x1D, 0x1B, 0x14,
    0x16, 0x13, 0x10, 0x17, 0x19, 0x1A,
    0x25, 0x2E, 0x2F, 0x28, 0x2C, 0x21, 0x22, 0x2D, 0x2B, 0x24,
    0x26, 0x23, 0x20, 0x27, 0x29, 0x2A,
    0xD5, 0xDE, 0xDF, 0xD8, 0xDC, 0xD1, 0xD2, 0xDD, 0xDB, 0xD4,
    0xD6, 0xD3, 0xD0, 0xD7, 0xD9, 0xDA,
    0xB5, 0xBE, 0xBF, 0xB8, 0xBC, 0xB1, 0xB2, 0xBD, 0xBB, 0xB4,
    0xB6, 0xB3, 0xB0, 0xB7, 0xB9, 0xBA,
    0x45, 0x4E, 0x4F, 0x48, 0x4C, 0x41, 0x42, 0x4D, 0x4B, 0x44,
    0x46, 0x43, 0x40, 0x47, 0x49, 0x4A,
    0x65, 0x6E, 0x6F, 0x68, 0x6C, 0x61, 0x62, 0x6D, 0x6B, 0x64,
    0x66, 0x63, 0x60, 0x67, 0x69, 0x6A,
    0x35, 0x3E, 0x3F, 0x38, 0x3C, 0x31, 0x32, 0x3D, 0x3B, 0x34,
    0x36, 0x33, 0x30, 0x37, 0x39, 0x3A,
    0x05, 0x0E, 0x0F, 0x08, 0x0C, 0x01, 0x02, 0x0D, 0x0B, 0x04,
    0x06, 0x03, 0x00, 0x07, 0x09, 0x0A,
    0x75, 0x7E, 0x7F, 0x78, 0x7C, 0x71, 0x72, 0x7D, 0x7B, 0x74,
    0x76, 0x73, 0x70, 0x77, 0x79, 0x7A,
    0x95, 0x9E, 0x9F, 0x98, 0x9C, 0x91, 0x92, 0x9D, 0x9B, 0x94,
    0x96, 0x93, 0x90, 0x97, 0x99, 0x9A,
    0xA5, 0xAE, 0xAF, 0xA8, 0xAC, 0xA1, 0xA2, 0xAD, 0xAB, 0xA4,
    0xA6, 0xA3, 0xA0, 0xA7, 0xA9, 0xAA,
};

```

```

//Inverse bit permutation
static const uint32_t ipbox[256] =
{
    0x00000000, 0x00000001, 0x00000010, 0x00000011, 0x00000100,
0x00000101, 0x00000110, 0x00000111,
    0x00001000, 0x00001001, 0x00001010, 0x00001011, 0x00001100,
0x00001101, 0x00001110, 0x00001111,
    0x00010000, 0x00010001, 0x00010010, 0x00010011, 0x00010100,
0x00010101, 0x00010110, 0x00010111,
    0x00011000, 0x00011001, 0x00011010, 0x00011011, 0x00011100,
0x00011101, 0x00011110, 0x00011111,
    0x00100000, 0x00100001, 0x00100010, 0x00100011, 0x00100100,
0x00100101, 0x00100110, 0x00100111,
    0x00101000, 0x00101001, 0x00101010, 0x00101011, 0x00101100,
0x00101101, 0x00101110, 0x00101111,
    0x00110000, 0x00110001, 0x00110010, 0x00110011, 0x00110100,
0x00110101, 0x00110110, 0x00110111,
    0x00111000, 0x00111001, 0x00111010, 0x00111011, 0x00111100,
0x00111101, 0x00111110, 0x00111111,
    0x01000000, 0x01000001, 0x01000010, 0x01000011, 0x01000100,
0x01000101, 0x01000110, 0x01000111,
    0x01001000, 0x01001001, 0x01001010, 0x01001011, 0x01001100,
0x01001101, 0x01001110, 0x01001111,
    0x01010000, 0x01010001, 0x01010010, 0x01010011, 0x01010100,
0x01010101, 0x01010110, 0x01010111,
    0x01011000, 0x01011001, 0x01011010, 0x01011011, 0x01011100,
0x01011101, 0x01011110, 0x01011111,
    0x01100000, 0x01100001, 0x01100010, 0x01100011, 0x01100100,
0x01100101, 0x01100110, 0x01100111,
    0x01101000, 0x01101001, 0x01101010, 0x01101011, 0x01101100,
0x01101101, 0x01101110, 0x01101111,
    0x01110000, 0x01110001, 0x01110010, 0x01110011, 0x01110100,
0x01110101, 0x01110110, 0x01110111,
    0x01111000, 0x01111001, 0x01111010, 0x01111011, 0x01111100,
0x01111101, 0x01111110, 0x01111111,

```

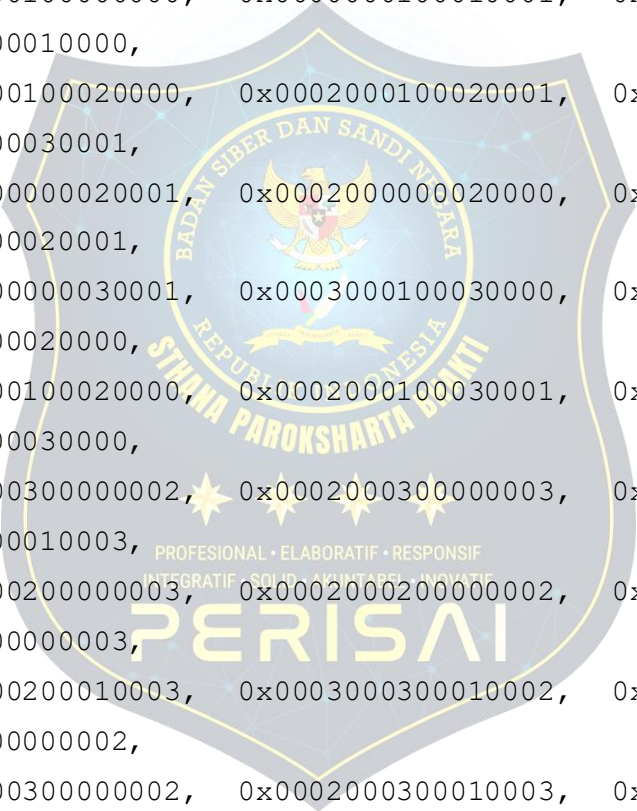
```

        0x10000000, 0x10000001, 0x10000010, 0x10000011, 0x10000100,
        0x10000101, 0x10000110, 0x10000111,
        0x10001000, 0x10001001, 0x10001010, 0x10001011, 0x10001100,
        0x10001101, 0x10001110, 0x10001111,
        0x10010000, 0x10010001, 0x10010010, 0x10010011, 0x10010100,
        0x10010101, 0x10010110, 0x10010111,
        0x10011000, 0x10011001, 0x10011010, 0x10011011, 0x10011100,
        0x10011101, 0x10011110, 0x10011111,
        0x10100000, 0x10100001, 0x10100010, 0x10100011, 0x10100100,
        0x10100101, 0x10100110, 0x10100111,
        0x10101000, 0x10101001, 0x10101010, 0x10101011, 0x10101100,
        0x10101101, 0x10101110, 0x10101111,
        0x10110000, 0x10110001, 0x10110010, 0x10110011, 0x10110100,
        0x10110101, 0x10110110, 0x10110111,
        0x10111000, 0x10111001, 0x10111010, 0x10111011, 0x10111100,
        0x10111101, 0x10111110, 0x10111111,
        0x11000000, 0x11000001, 0x11000010, 0x11000011, 0x11000100,
        0x11000101, 0x11000110, 0x11000111,
        0x11001000, 0x11001001, 0x11001010, 0x11001011, 0x11001100,
        0x11001101, 0x11001110, 0x11001111,
        0x11010000, 0x11010001, 0x11010010, 0x11010011, 0x11010100,
        0x11010101, 0x11010110, 0x11010111,
        0x11011000, 0x11011001, 0x11011010, 0x11011011, 0x11011100,
        0x11011101, 0x11011110, 0x11011111,
        0x11100000, 0x11100001, 0x11100010, 0x11100011, 0x11100100,
        0x11100101, 0x11100110, 0x11100111,
        0x11101000, 0x11101001, 0x11101010, 0x11101011, 0x11101100,
        0x11101101, 0x11101110, 0x11101111,
        0x11110000, 0x11110001, 0x11110010, 0x11110011, 0x11110100,
        0x11110101, 0x11110110, 0x11110111,
        0x11111000, 0x11111001, 0x11111010, 0x11111011, 0x11111100,
        0x11111101, 0x11111110, 0x11111111
    };

    //Combined S-box and bit permutation
    static const uint64_t spbox[256] =
    {

```

|                     |                     |                     |
|---------------------|---------------------|---------------------|
| 0x0003000300000000, | 0x0002000300000001, | 0x0002000300010000, |
| 0x0003000200010001, |                     |                     |
| 0x0003000200000001, | 0x0002000200000000, | 0x0003000200010000, |
| 0x0003000300000001, |                     |                     |
| 0x0002000200010001, | 0x0003000300010000, | 0x0003000300010001, |
| 0x0003000200000000, |                     |                     |
| 0x0002000300000000, | 0x0002000300010001, | 0x0002000200000001, |
| 0x0002000200010000, |                     |                     |
| 0x0001000300000002, | 0x0000000300000003, | 0x0000000300010002, |
| 0x0001000200010003, |                     |                     |
| 0x0001000200000003, | 0x0000000200000002, | 0x0001000200010002, |
| 0x0001000300000003, |                     |                     |
| 0x0000000200010003, | 0x0001000300010002, | 0x0001000300010003, |
| 0x0001000200000002, |                     |                     |
| 0x0000000300000002, | 0x0000000300010003, | 0x0000000200000003, |
| 0x0000000200010002, |                     |                     |
| 0x0001000300020000, | 0x0000000300020001, | 0x0000000300030000, |
| 0x0001000200030001, |                     |                     |
| 0x0001000200020001, | 0x0000000200020000, | 0x0001000200030000, |
| 0x0001000300020001, |                     |                     |
| 0x0000000200030001, | 0x0001000300030000, | 0x0001000300030001, |
| 0x0001000200020000, |                     |                     |
| 0x0000000300020000, | 0x0000000300030001, | 0x0000000200020001, |
| 0x0000000200030000, |                     |                     |
| 0x0003000100020002, | 0x0002000100020003, | 0x0002000100030002, |
| 0x0003000000030003, |                     |                     |
| 0x0003000000020003, | 0x0002000000020002, | 0x0003000000030002, |
| 0x0003000100020003, |                     |                     |
| 0x0002000000030003, | 0x0003000100030002, | 0x0003000100030003, |
| 0x0003000000020002, |                     |                     |
| 0x0002000100020002, | 0x0002000100030003, | 0x0002000000020003, |
| 0x0002000000030002, |                     |                     |
| 0x0003000100000002, | 0x0002000100000003, | 0x0002000100010002, |
| 0x0003000000010003, |                     |                     |
| 0x0003000000000003, | 0x0002000000000002, | 0x0003000000010002, |
| 0x0003000100000003, |                     |                     |



0x0002000000010003, 0x0003000100010002, 0x0003000100010003,  
 0x0003000000000002,  
 0x0002000100000002, 0x0002000100010003, 0x0002000000000003,  
 0x0002000000010002,  
 0x0001000100000000, 0x0000000100000001, 0x0000000100010000,  
 0x00010000000010001,  
 0x0001000000000001, 0x0000000000000000, 0x00010000000010000,  
 0x0001000100000001,  
 0x00000000000010001, 0x0001000100010000, 0x0001000100010001,  
 0x0001000000000000,  
 0x0000000100000000, 0x0000000100010001, 0x0000000000000001,  
 0x00000000000010000,  
 0x0003000100020000, 0x0002000100020001, 0x0002000100030000,  
 0x00030000000030001,  
 0x00030000000020001, 0x00020000000020000, 0x00030000000030000,  
 0x0003000100020001,  
 0x00020000000030001, 0x0003000100030000, 0x0003000100030001,  
 0x00030000000020000,  
 0x0002000100020000, 0x0002000100030001, 0x00020000000020001,  
 0x00020000000030000,  
 0x0003000300000002, 0x0002000300000003, 0x0002000300010002,  
 0x0003000200010003,  
 0x0003000200000003, 0x0002000200000002, 0x0003000200010002,  
 0x0003000300000003,  
 0x0002000200010003, 0x0003000300010002, 0x0003000300010003,  
 0x0003000200000002,  
 0x0002000300000002, 0x0002000300010003, 0x0002000200000003,  
 0x0002000200010002,  
 0x0001000100020002, 0x0000000100020003, 0x0000000100030002,  
 0x00010000000030003,  
 0x00010000000020003, 0x00000000000020002, 0x00010000000030002,  
 0x0001000100020003,  
 0x00000000000030003, 0x0001000100030002, 0x0001000100030003,  
 0x00010000000020002,  
 0x0000000100020002, 0x0000000100030003, 0x00000000000020003,  
 0x00000000000030002,

|                     |                     |                     |
|---------------------|---------------------|---------------------|
| 0x0003000300020000, | 0x0002000300020001, | 0x0002000300030000, |
| 0x0003000200030001, |                     |                     |
| 0x0003000200020001, | 0x0002000200020000, | 0x0003000200030000, |
| 0x0003000300020001, |                     |                     |
| 0x0002000200030001, | 0x0003000300030000, | 0x0003000300030001, |
| 0x0003000200020000, |                     |                     |
| 0x0002000300020000, | 0x0002000300030001, | 0x0002000200020001, |
| 0x0002000200030000, |                     |                     |
| 0x0003000300020002, | 0x0002000300020003, | 0x0002000300030002, |
| 0x0003000200030003, |                     |                     |
| 0x0003000200020003, | 0x0002000200020002, | 0x0003000200030002, |
| 0x0003000300020003, |                     |                     |
| 0x0002000200030003, | 0x0003000300030002, | 0x0003000300030003, |
| 0x0003000200020002, |                     |                     |
| 0x0002000300020002, | 0x0002000300030003, | 0x0002000200020003, |
| 0x0002000200030002, |                     |                     |
| 0x0003000100000000, | 0x0002000100000001, | 0x0002000100010000, |
| 0x0003000000010001, |                     |                     |
| 0x0003000000000001, | 0x0002000000000000, | 0x0003000000010000, |
| 0x0003000100000001, |                     |                     |
| 0x0002000000010001, | 0x0003000100010000, | 0x0003000100010001, |
| 0x0003000000000000, |                     |                     |
| 0x0002000100000000, | 0x0002000100010001, | 0x0002000000000001, |
| 0x0002000000010000, |                     |                     |
| 0x0001000300000000, | 0x0000000300000001, | 0x0000000300010000, |
| 0x0001000200010001, |                     |                     |
| 0x0001000200000001, | 0x0000000200000000, | 0x0001000200010000, |
| 0x0001000300000001, |                     |                     |
| 0x0000000200010001, | 0x0001000300010000, | 0x0001000300010001, |
| 0x0001000200000000, |                     |                     |
| 0x0000000300000000, | 0x0000000300010001, | 0x0000000200000001, |
| 0x0000000200010000, |                     |                     |
| 0x0001000300020002, | 0x0000000300020003, | 0x0000000300030002, |
| 0x0001000200030003, |                     |                     |
| 0x0001000200020003, | 0x0000000200020002, | 0x0001000200030002, |
| 0x0001000300020003, |                     |                     |

```

    0x0000000200030003, 0x0001000300030002, 0x0001000300030003,
    0x0001000200020002,
    0x0000000300020002, 0x0000000300030003, 0x0000000200020003,
    0x0000000200030002,
    0x0001000100000002, 0x0000000100000003, 0x0000000100010002,
    0x00010000000010003,
    0x0001000000000003, 0x0000000000000002, 0x00010000000010002,
    0x0001000100000003,
    0x00000000000010003, 0x0001000100010002, 0x0001000100010003,
    0x0001000000000002,
    0x0000000100000002, 0x0000000100010003, 0x0000000000000003,
    0x00000000000010002,
    0x0001000100020000, 0x0000000100020001, 0x0000000100030000,
    0x00010000000030001,
    0x00010000000020001, 0x000000000000020000, 0x00010000000030000,
    0x0001000100020001,
    0x00000000000030001, 0x0001000100030000, 0x0001000100030001,
    0x00010000000020000,
    0x0000000100020000, 0x0000000100030001, 0x00000000000020001,
    0x00000000000030000
};

//Common interface for encryption algorithms
const CipherAlgo presentCipherAlgo =
{
    "PRESENT",
    sizeof(PresentContext),
    CIPHER_ALGO_TYPE_BLOCK,
    PRESENT_BLOCK_SIZE,
    (CipherAlgoInit) presentInit,
    NULL,
    NULL,
    (CipherAlgoEncryptBlock) presentEncryptBlock,
    (CipherAlgoDecryptBlock) presentDecryptBlock,
    (CipherAlgoDeinit) presentDeinit
};

```

```

/**
 * @brief Key expansion
 * @param[in] context Pointer to the PRESENT context to
initialize
 * @param[in] key Pointer to the key
 * @param[in] keyLen Length of the key
 * @return Error code
 **/

error_t presentInit(PresentContext *context, const uint8_t *key,
size_t keyLen)
{
    uint_t i;
    uint64_t t;
    uint64_t kl;
    uint64_t kh;

    //Check parameters
    if(context == NULL || key == NULL)
        return ERROR_INVALID_PARAMETER;

    //Check key length
    if(keyLen != 10 && keyLen != 16)
        return ERROR_INVALID_KEY_LENGTH;

    //PRESENT can take keys of either 80 or 128 bits
    if(keyLen == 10)
    {
        //Copy the 80-bit key
        kh = LOAD16BE(key);
        kl = LOAD64BE(key + 2);

        //Save the 64 leftmost bits of K
        context->ks[0] = (kh << 48) | (kl >> 16);

        //Generate round keys

```

```

for(i = 1; i <= 31; i++)
{
//The key register is rotated by 61 bit positions to the left
t = kh & 0xFFFF;
kh = (kl >> 3) & 0xFFFF;
kl = (kl << 61) | (t << 45) | (kl >> 19);

//The left-most four bits are passed through the S-box
t = sbbox[(kh >> 12) & 0x0F];
kh = (kh & 0x0FFF) | (t << 12);

//The round counter value i is XOR-ed with bits 19, 18, 17,
16, 15 of K
kl ^= (uint64_t) i << 15;

//Save the 64 leftmost bits of K
context->ks[i] = (kh << 48) | (kl >> 16);
}
}
else
{
//Copy the 128-bit key
kh = LOAD64BE(key);
kl = LOAD64BE(key + 8);

//Save the 64 leftmost bits of K
context->ks[0] = kh;

//Generate round keys
for(i = 1; i <= 31; i++)
{
//The key register is rotated by 61 bit positions to the left
t = kh;
kh = (t << 61) | (kl >> 3);
kl = (kl << 61) | (t >> 3);

//The left-most eight bits are passed through two S-boxes

```

```

t = sbbox[(kh >> 56) & 0x0F];
kh = (kh & 0xF0FFFFFFFFFFFFFF) | (t << 56);
t = sbbox[(kh >> 60) & 0x0F];
kh = (kh & 0x0FFFFFFFFFFFFFFF) | (t << 60);

//The round counter value i is XOR-ed with bits 66, 65, 64,
63, 62 of K
kh ^= (uint64_t) i >> 2;
kl ^= (uint64_t) i << 62;

//Save the 64 leftmost bits of K
context->ks[i] = kh;
}
}

//Successful initialization
return NO_ERROR;
}

/**
 * @brief Encrypt a 8-byte block using PRESENT algorithm
 * @param[in] context Pointer to the PRESENT context
 * @param[in] input Plaintext block to encrypt
 * @param[out] output Ciphertext block resulting from
encryption
 */

void presentEncryptBlock(PresentContext *context, const uint8_t
*input,
uint8_t *output)
{
uint_t i;
uint64_t s;
uint64_t t;
uint64_t state;

```

```

//Copy the plaintext to the 64-bit state
state = LOAD64BE(input);

//Initial round key addition
state ^= context->ks[0];

//The encryption consists of 31 rounds
for(i = 1; i <= 31; i++)
{
//Apply S-box and bit permutation
s = spbox[state & 0xFF];
t = spbox[(state >> 8) & 0xFF];
s |= ROL64(t, 2);
t = spbox[(state >> 16) & 0xFF];
s |= ROL64(t, 4);
t = spbox[(state >> 24) & 0xFF];
s |= ROL64(t, 6);
t = spbox[(state >> 32) & 0xFF];
s |= ROL64(t, 8);
t = spbox[(state >> 40) & 0xFF];
s |= ROL64(t, 10);
t = spbox[(state >> 48) & 0xFF];
s |= ROL64(t, 12);
t = spbox[(state >> 56) & 0xFF];
s |= ROL64(t, 14);

//Add round key
state = s ^ context->ks[i];
}

//The final state is then copied to the output
STORE64BE(state, output);
}

/**
 * @brief Decrypt a 8-byte block using PRESENT algorithm

```

```

    * @param[in] context Pointer to the PRESENT context
    * @param[in] input Ciphertext block to decrypt
    * @param[out] output Plaintext block resulting from decryption
    **/

void presentDecryptBlock(PresentContext *context, const uint8_t
*input,
    uint8_t *output)
{
    uint_t i;
    uint64_t s;
    uint64_t t;
    uint64_t state;

    //Copy the ciphertext to the 64-bit state
    state = LOAD64BE(input);

    //The decryption consists of 31 rounds
    for(i = 31; i > 0; i--)
    {
        //Add round key
        state ^= context->ks[i];

        //Apply inverse bit permutation
        s = ipbox[state & 0xFF];
        t = ipbox[(state >> 8) & 0xFF];
        s |= ROL64(t, 32);
        t = ipbox[(state >> 16) & 0xFF];
        s |= ROL64(t, 1);
        t = ipbox[(state >> 24) & 0xFF];
        s |= ROL64(t, 33);
        t = ipbox[(state >> 32) & 0xFF];
        s |= ROL64(t, 2);
        t = ipbox[(state >> 40) & 0xFF];
        s |= ROL64(t, 34);
        t = ipbox[(state >> 48) & 0xFF];
        s |= ROL64(t, 3);
    }
}

```

```

t = ipbox[(state >> 56) & 0xFF];
s |= ROL64(t, 35);

//Apply inverse S-box
state = isbox[s & 0xFF];
t = isbox[(s >> 8) & 0xFF];
state |= ROL64(t, 8);
t = isbox[(s >> 16) & 0xFF];
state |= ROL64(t, 16);
t = isbox[(s >> 24) & 0xFF];
state |= ROL64(t, 24);
t = isbox[(s >> 32) & 0xFF];
state |= ROL64(t, 32);
t = isbox[(s >> 40) & 0xFF];
state |= ROL64(t, 40);
t = isbox[(s >> 48) & 0xFF];
state |= ROL64(t, 48);
t = isbox[(s >> 56) & 0xFF];
state |= ROL64(t, 56);
}

//Final round key addition
state ^= context->ks[0];

//The final state is then copied to the output
STORE64BE(state, output);
}

/**
 * @brief Release PRESENT context
 * @param[in] context Pointer to the PRESENT context
 */

void presentDeinit(PresentContext *context)
{
    //Clear PRESENT context

```

```

    osMemset(context, 0, sizeof(PresentContext));
}

#endif

```

### C. Implementasi SIMON 64 dan SIMON 128

Berikut adalah implementasi SIMON 64 dan SIMON 128 berdasarkan dokumen *SIMON and SPECK Implementation Guide* yang ditulis oleh Ray Beaulieu, Douglas Shors, Jason Smith, Stefan Treatman-Clark, Bryan Weeks, dan Louis Wingers dari *National Security Agency* yang dapat diunduh pada halaman <https://nsacyber.github.io/simon-speck/implementations/ImplementationGuide1.1.pdf>.

Implementasi SIMON 64 adalah sebagai berikut.

```

#define f32(x) ((ROTL32(x,1) & ROTL32(x,8)) ^ ROTL32(x,2))
#define R32x2(x,y,k1,k2) (y^=f32(x), y^=k1, x^=f32(y), x^=k2)

void Simon6496KeySchedule(u32 K[],u32 rk[])
{
    u32 i,c=0xffffffffc;
    u64 z=0x7369f885192c0ef5LL;

    rk[0]=K[0]; rk[1]=K[1]; rk[2]=K[2];

    for(i=3;i<42;i++){
        rk[i]=c^(z&1)^rk[i-3]^ROTR32(rk[i-1],3)^ROTR32(rk[i-1],4);
        z>>=1;
    }
}

void Simon6496Encrypt(u32 Pt[],u32 Ct[],u32 rk[])
{
    u32 i;

    Ct[1]=Pt[1]; Ct[0]=Pt[0];
    for(i=0;i<42;) R32x2(Ct[1],Ct[0],rk[i++],rk[i++]);
}

```

```

}

void Simon6496Decrypt(u32 Pt[],u32 Ct[],u32 rk[])
{
    int i;

    Pt[1]=Ct[1]; Pt[0]=Ct[0];
    for(i=41;i>=0;) R32x2(Pt[0],Pt[1],rk[i--],rk[i--]);
}

void Simon64128KeySchedule(u32 K[],u32 rk[])
{
    u32 i,c=0xffffffffc;
    u64 z=0xfc2ce51207a635dbLL;

    rk[0]=K[0]; rk[1]=K[1]; rk[2]=K[2]; rk[3]=K[3];

    for(i=4;i<44;i++){
        rk[i]=c^(z&1)^rk[i-4]^ROTR32(rk[i-1],3)^rk[i-3]
        ^ROTR32(rk[i-1],4)^ROTR32(rk[i-3],1);
        z>>=1;
    }
}

void Simon64128Encrypt(u32 Pt[],u32 Ct[],u32 rk[])
{
    u32 i;

    Ct[1]=Pt[1]; Ct[0]=Pt[0];
    for(i=0;i<44;) R32x2(Ct[1],Ct[0],rk[i++],rk[i++]);
}

void Simon64128Decrypt(u32 Pt[],u32 Ct[],u32 rk[])
{
    int i;

    Pt[1]=Ct[1]; Pt[0]=Ct[0];
    for(i=43;i>=0;) R32x2(Pt[0],Pt[1],rk[i--],rk[i--]);
}

```

```
}
```

Implementasi SIMON 128 adalah sebagai berikut.

```
void Simon128128KeySchedule(u64 K[],u64 rk[])
{
    u64 i,B=K[1],A=K[0];
    u64 c=0xffffffffffffffffcLL, z=0x7369f885192c0ef5LL;

    for(i=0;i<64;){
        rk[i++]=A; A^=c^(z&1)^ROTR64(B,3)^ROTR64(B,4); z>>=1;
        rk[i++]=B; B^=c^(z&1)^ROTR64(A,3)^ROTR64(A,4); z>>=1;
    }

    rk[64]=A; A^=c^1^ROTR64(B,3)^ROTR64(B,4);
    rk[65]=B; B^=c^0^ROTR64(A,3)^ROTR64(A,4);
    rk[66]=A; rk[67]=B;
}

void Simon128128Encrypt(u64 Pt[],u64 Ct[],u64 rk[])
{
    u64 i;

    Ct[0]=Pt[0]; Ct[1]=Pt[1];
    for(i=0;i<68;i+=2) R64x2(Ct[1],Ct[0],rk[i],rk[i+1]);
}

void Simon128128Decrypt(u64 Pt[],u64 Ct[],u64 rk[])
{
    int i;

    Pt[0]=Ct[0]; Pt[1]=Ct[1];
    for(i=67;i>=0;i-=2) R64x2(Pt[0],Pt[1],rk[i],rk[i-1]);
}

void Simon128192KeySchedule(u64 K[],u64 rk[])
{

```

```

u64 i,C=K[2],B=K[1],A=K[0];
u64 c=0xffffffffffffffffcLL, z=0xfc2ce51207a635dbLL;

for(i=0;i<63;){
    rk[i++]=A; A^=c^(z&1)^ROTR64(C,3)^ROTR64(C,4); z>>=1;
    rk[i++]=B; B^=c^(z&1)^ROTR64(A,3)^ROTR64(A,4); z>>=1;
    rk[i++]=C; C^=c^(z&1)^ROTR64(B,3)^ROTR64(B,4); z>>=1;
}
rk[63]=A; A^=c^1^ROTR64(C,3)^ROTR64(C,4);
rk[64]=B; B^=c^0^ROTR64(A,3)^ROTR64(A,4);
rk[65]=C; C^=c^1^ROTR64(B,3)^ROTR64(B,4);
rk[66]=A; rk[67]=B; rk[68]=C;
}

void Simon128192Encrypt(u64 Pt[],u64 Ct[],u64 rk[])
{
    u64 i,t;

    Ct[0]=Pt[0]; Ct[1]=Pt[1];
    for(i=0;i<68;i+=2) R64x2(Ct[1],Ct[0],rk[i],rk[i+1]);
    t=Ct[1]; Ct[1]=Ct[0]^f(Ct[1]^rk[68]); Ct[0]=t;
}

void Simon128192Decrypt(u64 Pt[],u64 Ct[],u64 rk[])
{
    int i;
    u64 t;

    Pt[0]=Ct[0]; Pt[1]=Ct[1];
    t=Pt[0]; Pt[0]=Pt[1]^f(Pt[0]^rk[68]); Pt[1]=t;
    for(i=67;i>=0;i--) R64x2(Pt[0],Pt[1],rk[i],rk[i-1]);
}

void Simon128256KeySchedule(u64 K[],u64 rk[])
{
    u64 i,D=K[3],C=K[2],B=K[1],A=K[0];
    u64 c=0xffffffffffffffffcLL, z=0xfdc94c3a046d678bLL;

```

```

for(i=0;i<64;){
    rk[i++]=A;
    A^=c^(z&1)^ROTR64(D,3)^ROTR64(D,4)^B^ROTR64(B,1); z>>=1;
    rk[i++]=B;
    B^=c^(z&1)^ROTR64(A,3)^ROTR64(A,4)^C^ROTR64(C,1); z>>=1;
    rk[i++]=C;
    C^=c^(z&1)^ROTR64(B,3)^ROTR64(B,4)^D^ROTR64(D,1); z>>=1;
    rk[i++]=D;
    D^=c^(z&1)^ROTR64(C,3)^ROTR64(C,4)^A^ROTR64(A,1); z>>=1;
}
rk[64]=A; A^=c^0^ROTR64(D,3)^ROTR64(D,4)^B^ROTR64(B,1);
rk[65]=B; B^=c^1^ROTR64(A,3)^ROTR64(A,4)^C^ROTR64(C,1);
rk[66]=C; C^=c^0^ROTR64(B,3)^ROTR64(B,4)^D^ROTR64(D,1);
rk[67]=D; D^=c^0^ROTR64(C,3)^ROTR64(C,4)^A^ROTR64(A,1);
rk[68]=A; rk[69]=B; rk[70]=C; rk[71]=D;
}
void Simon128256Encrypt(u64 Pt[],u64 Ct[],u64 rk[])
{
    u64 i;

    Ct[0]=Pt[0]; Ct[1]=Pt[1];
    for(i=0;i<72;i+=2) R64x2(Ct[1],Ct[0],rk[i],rk[i+1]);
}

void Simon128256Decrypt(u64 Pt[],u64 Ct[],u64 rk[])
{
    int i;

    Pt[0]=Ct[0]; Pt[1]=Ct[1];
    for(i=71;i>=0;i-=2) R64x2(Pt[0],Pt[1],rk[i],rk[i-1]);
}

```

#### D. Implementasi ChaCha 20

Berikut adalah implementasi referensi ChaCha20 dalam bahasa pemrograman C yang dapat diunduh pada halaman <https://cr.yp.to/streamciphers/timings/estreambench/submissions/salsa20/chacha8/ref/chacha.c>

```

/*
chacha-ref.c version 20080118
D. J. Bernstein
Public domain.
*/

#include "ecrypt-sync.h"

#define ROTATE(v,c) (ROTL32(v,c))
#define XOR(v,w) ((v) ^ (w))
#define PLUS(v,w) (U32V((v) + (w)))
#define PLUSONE(v) (PLUS((v),1))

#define QUARTERROUND(a,b,c,d) \
    x[a] = PLUS(x[a],x[b]); x[d] = ROTATE(XOR(x[d],x[a]),16); \
    x[c] = PLUS(x[c],x[d]); x[b] = ROTATE(XOR(x[b],x[c]),12); \
    x[a] = PLUS(x[a],x[b]); x[d] = ROTATE(XOR(x[d],x[a]), 8); \
    x[c] = PLUS(x[c],x[d]); x[b] = ROTATE(XOR(x[b],x[c]), 7);

static void salsa20_wordtobyte(u8 output[64],const u32 input[16])
{
    u32 x[16];
    int i;

    for (i = 0;i < 16;++i) x[i] = input[i];
    for (i = 8;i > 0;i -= 2) {
        QUARTERROUND( 0, 4, 8,12)
        QUARTERROUND( 1, 5, 9,13)
        QUARTERROUND( 2, 6,10,14)
        QUARTERROUND( 3, 7,11,15)
        QUARTERROUND( 0, 5,10,15)
        QUARTERROUND( 1, 6,11,12)
        QUARTERROUND( 2, 7, 8,13)
        QUARTERROUND( 3, 4, 9,14)
    }
    for (i = 0;i < 16;++i) x[i] = PLUS(x[i],input[i]);
    for (i = 0;i < 16;++i) U32TO8_LITTLE(output + 4 * i,x[i]);
}

```

```

}

void ECRYPT_init(void)
{
    return;
}

static const char sigma[16] = "expand 32-byte k";
static const char tau[16] = "expand 16-byte k";

void ECRYPT_keysetup(ECRYPT_ctx *x, const u8 *k, u32 kbits, u32
ivbits)
{
    const char *constants;

    x->input[4] = U8TO32_LITTLE(k + 0);
    x->input[5] = U8TO32_LITTLE(k + 4);
    x->input[6] = U8TO32_LITTLE(k + 8);
    x->input[7] = U8TO32_LITTLE(k + 12);
    if (kbits == 256) { /* recommended */
        k += 16;
        constants = sigma;
    } else { /* kbits == 128 */
        constants = tau;
    }

    x->input[8] = U8TO32_LITTLE(k + 0);
    x->input[9] = U8TO32_LITTLE(k + 4);
    x->input[10] = U8TO32_LITTLE(k + 8);
    x->input[11] = U8TO32_LITTLE(k + 12);
    x->input[0] = U8TO32_LITTLE(constants + 0);
    x->input[1] = U8TO32_LITTLE(constants + 4);
    x->input[2] = U8TO32_LITTLE(constants + 8);
    x->input[3] = U8TO32_LITTLE(constants + 12);
}

void ECRYPT_ivsetup(ECRYPT_ctx *x, const u8 *iv)
{

```

```

x->input[12] = 0;
x->input[13] = 0;
x->input[14] = U8TO32_LITTLE(iv + 0);
x->input[15] = U8TO32_LITTLE(iv + 4);
}

void ECRYPT_encrypt_bytes(ECRYPT_ctx *x, const u8 *m, u8 *c, u32
bytes)
{
    u8 output[64];
    int i;

    if (!bytes) return;
    for (;;) {
        salsa20_wordtobyte(output, x->input);
        x->input[12] = PLUSONE(x->input[12]);
        if (!x->input[12]) {
            x->input[13] = PLUSONE(x->input[13]);
            /* stopping at 2^70 bytes per nonce is user's responsibility
*/
        }
        if (bytes <= 64) {
            for (i = 0; i < bytes; ++i) c[i] = m[i] ^ output[i];
            return;
        }
        for (i = 0; i < 64; ++i) c[i] = m[i] ^ output[i];
        bytes -= 64;
        c += 64;
        m += 64;
    }
}

void ECRYPT_decrypt_bytes(ECRYPT_ctx *x, const u8 *c, u8 *m, u32
bytes)
{
    ECRYPT_encrypt_bytes(x, c, m, bytes);
}

```

```

void ECRYPT_keystream_bytes(ECRYPT_ctx *x,u8 *stream,u32 bytes)
{
    u32 i;
    for (i = 0;i < bytes;++i) stream[i] = 0;
    ECRYPT_encrypt_bytes(x,stream,stream,bytes);
}

```

## E. Implementasi SPONGENT

Berikut adalah implementasi referensi SPONGENT menggunakan python yang dapat diunduh pada halaman <https://github.com/joostrijneveld/readable-crypto/blob/master/hashfunctions/SPONGENT.py>

```

#!/usr/bin/env python

import math

SBOX = [0xE, 0xD, 0xB, 0x0, 0x2, 0x1, 0x4, 0xF,
        0x7, 0xA, 0x8, 0x5, 0x9, 0xC, 0x3, 0x6]

class SPONGENT(object):

    def __init__(self, n=88, c=80, r=8, R=45):
        self.n = n
        self.c = c
        self.r = r
        self.R = R
        self.LFSRsize = math.ceil(math.log2(R))
        self.LFSRmask = int('1' * self.LFSRsize, 2)
        self.reset_LFSR()

    def initialise(self, m, prefix_zeros=0):
        m = m << 1 | 1

```

```

length = len(bin(m)) - 2 + prefix_zeros # -2 for 0b prefix
m <= self.r - length % self.r
N = math.ceil((prefix_zeros + length) / self.r)
return m, N

def sBoxLayer(self, state):
    for i in range(0, (self.r + self.c), 4):
        word = (state >> i) & 0xF
        state = state & ~(0xF << i) | (SBOX[word] << i)
    return state

def pLayer(self, state):
    b = self.r + self.c

    def Pb(j):
        if j <= b - 2:
            return (j * b//4) % (b - 1)
        return b - 1

    oldstate = state
    for j in range(b):
        state = state & ~(0x1 << Pb(j)) | ((oldstate >> j) &
0x1) << Pb(j)
    return state

def reset_LFSR(self):
    self.LFSR = {88: int('000101', 2),
                  128: int('1111010', 2),
                  160: int('1000101', 2),
                  224: int('0000001', 2),
                  256: int('10011110', 2)}[self.n]

def lCounter(self):
    z = lambda i: (self.LFSR >> i-1) & 0x1
    if self.n == 88:
        x = z(6) ^ z(5)
    elif self.n in [128, 160, 224]:

```

```

        x = z(7) ^ z(6)
    elif self.n == 256:
        x = z(8) ^ z(4) ^ z(3) ^ z(2)
    self.LFSR = (self.LFSR << 1 | x) & self.LFSRmask

def P(self, s):
    self.reset_LFSR()
    for _ in range(1, self.R+1):
        tmp = self.LFSR
        revLFSR = 0
        for _ in range(self.LFSRsize):
            revLFSR = revLFSR << 1 | tmp & 0x1
            tmp >>= 1
        s = (revLFSR << (self.r + self.c - self.LFSRsize)) ^
s ^ self.LFSR
        self.lCounter()
        s = self.sBoxLayer(s)
        s = self.pLayer(s)
    return s

# The necessity of this function is not clear in the SPONGENT
article
# It follows from the test vectors produced by the reference
implementation
# The message blocks are reversed on a per-byte basis; this
shows for r > 8
def reverse_block(self, block):
    result = 0
    for _ in range(self.r//8):
        result = result << 8 | block & 0xFF
        block >>= 8
    return result

def absorb(self, m, N):
    mblocks = []
    for i in range(N):
        mblocks.append(m & int('1' * self.r, 2))

```

```

        m >>= self.r
    s = 0
    for mblock in reversed(mblocks):
        s = s ^ self.reverse_block(mblock)
        s = self.P(s)
    return s

def squeeze(self, s):
    result = 0x0
    for i in range(self.n // self.r - 1):
        result = result | self.reverse_block(s & int('1' *
self.r, 2))
        result <<= self.r
        s = self.P(s)
    result = result | self.reverse_block(s & int('1' * self.r,
2))
    return result

def hash(self, m, prefix_zeros=0):
    m, N = self.initialise(m, prefix_zeros)
    s = self.absorb(m, N)
    return self.squeeze(s)

```

## REFERENSI

- [1] ISO/IEC, "ISO/IEC 29192-1:2012 — Information Technology — Security techniques — Lightweight Cryptography —Part 1: General", 2012.
- [2] ISO/IEC, "ISO/IEC 29192-3:2012 — *Information technology — Security techniques — Lightweight cryptography Part 3: Stream ciphers*", 2012.
- [3] BSN, "SNI ISO/IEC 18033-4:2011 Teknologi informasi — Teknik keamanan — Algoritma enkripsi — Bagian 4: Penyandian alir", 2011.
- [4] BSN, "SNI ISO/IEC 18033-3:2010 Teknologi informasi — Teknik keamanan — Algoritma enkripsi — Bagian 3: Penyandian blok", 2010.
- [5] ISO/IEC, "ISO/IEC 29192-2:2012 — Information technology — Lightweight cryptography —Part 2: Block ciphers", 2012.
- [6] A. Bogdanov, L.R. Knudsen, G. Leander, C. Paar, A. Poschmann, M.J.B. Robshaw, Y. Seurin, C. Vikkelsøe, "PRESENT: An Ultra-Lightweight Block Cipher", *Cryptographic Hardware and Embedded Systems – CHES 2007, Lecture Notes in Computer Science*. Vol.4727. pages 450–466, 2007.
- [7] B. Schneier, "NIST Hash Workshop Liveblogging", [Online], Available: [https://www.schneier.com/blog/archives/2005/11/nist\\_hash\\_works\\_4.html](https://www.schneier.com/blog/archives/2005/11/nist_hash_works_4.html), 2005.
- [8] A. J. Menezes, P. C. Van Oorschot, and S. A. Vanstone, "Handbook of Applied Cryptography, 1st ed", Boca Raton, FL, USA.: CRC press, 1997.
- [9] BSN, "SNI ISO/IEC 10118-1:2016 Teknologi informasi, Teknik keamanan — Fungsi-hash — Bagian. 1: Umum", 2016.
- [10] G. Bertoni, J. Daemen, M. Peeters, and G. Van Assche, "Cryptographic sponge functions", [Online], Available: <https://keccak.team/files/CSF-0.1.pdf>, 2011.
- [11] J. Katz and Y. Lindell, "Introduction to Modern Cryptography", Chapman and Hall/CRC Press, 2007.
- [12] B. Preneel. "Davies\_Meyer hash function in Encyclopedia of Cryptography and Security", H. C. A. van Tilborg, Ed. Boston, MA, page136-136, USA: Springer, 2005.

- [13] B.T. Hammad, N. Jamil, M.E. Rusli, and M.R. Z'aba, "A Survey of Lightweight Cryptographic Hash Function", International Journal of Scientific & Engineering Research Volume 8, Issue 7, 2017.
- [14] K. A. McKay, L. Bassham, M.S. Turan, and N. Mouha, "NISTIR 8114 Report on Lightweight Cryptography", 2017.
- [15] A.Y. Poschmann, "Lightweight Cryptography: Cryptographic Engineering for a Pervasive World", Ph.D. Thesis, Ruhr University Bochum, <http://d-nb.info/996578153>, 2009.
- [16] CRYPTREC Lightweight Cryptography Working Group, "CRYPTREC Cryptographic Technology Guideline (Lightweight Cryptography)", 2017.
- [17] CRYPTREC Lightweight Cryptography Working Group, "2023 Edition CRYPTREC Cryptographic Technology Guideline (Lightweight Cryptography)", 2024.
- [18] D. J. Bernstein. Chacha, a variant of Salsa20, "In The State of the Art of Stream Ciphers", SASC 2008, ECRYPT, 2008.
- [19] Y. Nir and A. Langley, "ChaCha20 and Poly1305 for IETF Protocols, volume RFC4493 of Request For Comments", <https://tools.ietf.org/html/rfc7539>, May 2015.
- [20] J.P. Aumasson, S. Fischer, S. Khazaei, W. Meier, and C. Rechberger, "New Features of Latin Dances: Analysis of Salsa, ChaCha, and Rumba", In Kaisa Nyberg, editor, Fast Software Encryption, 15th International Workshop, FSE 2008, Lausanne, Switzerland, February 10-13, 2008, Revised Selected Papers, volume 5086 of Lecture Notes in Computer Science, pages 470–488. Springer, 2008.
- [21] Z. Shi, B. Zhang, D. Feng, and W. Wu, "Improved Key Recovery Attacks on Reduced-Round Salsa20 and ChaCha", In Taekyoung Kwon, Mun-Kyu Lee, and Daesung Kwon, editors, Information Security and Cryptology - ICISC 2012 - 15th International Conference, Seoul, Korea, November 28-30, 2012, Revised Selected Papers, volume 7839 of Lecture Notes in Computer Science, pages 337–351, Springer, 2012.

- [22] A.R. Choudhuri and S. Maitra, “Significantly Improved Multi-bit Differentials for Reduced Round Salsa and ChaCha”, IACR Trans. Symmetric Cryptol., pages 261–287, 2016.
- [23] M. Coutinho and T. C. Souza Neto, “New Multi-bit Differentials to Improve Attacks Against ChaCha”, IACR Cryptol. ePrint Arch., 2020.
- [24] C. Beierle, G. Leander, and Y. Todo, “Improved Differential-Linear Attacks with Applications to ARX Ciphers”, In Daniele Micciancio and Thomas Ristenpart, editors, Advances in Cryptology - CRYPTO 2020 - 40th Annual International Cryptology Conference, CRYPTO 2020, Santa Barbara, CA, USA, August 17-21, 2020, Proceedings, Part III, volume 12172 of Lecture Notes in Computer Science, pages 329–358. Springer, 2020.
- [25] M. Coutinho and T. C. Souza Neto, “Improved Linear Approximations to ARX Ciphers and Attacks Against ChaCha”, IACR Cryptol. ePrint Arch., pages 224, 2021.
- [26] S. Maitra, “Chosen IV cryptanalysis on reduced round ChaCha and Salsa”, Discret.Appl. Math., pages 88–97, 2016.
- [27] S. Miyashita, R. Ito, and A. Miyaji, “PNB-focused Differential Cryptanalysis of ChaCha Stream Cipher”, IACR Cryptol. ePrint Arch., 2021.
- [28] M. Coutinho and T. C. Souza Neto, “Improved Linear Approximations to ARX Ciphers and Attacks Against ChaCha”, In Anne Canteaut and Francois-Xavier Standaert, editors, Advances in Cryptology - EUROCRYPT 2021 - 40th Annual International Conference on the Theory and Applications of Cryptographic Techniques, Zagreb, Croatia, October 17-21, 2021, Proceedings, Part I, volume 12696 of Lecture Notes in Computer Science, pages 711–740, Springer, 2021.
- [29] Ebacs: Ecrypt benchmarking of cryptographic systems. <http://bench.cr.yp.to/results-stream.html>.
- [30] Felics stream ciphers brief results. [https://www.cryptolux.org/index.php/FELICS\\_Stream\\_Ciphers\\_Brief\\_Results](https://www.cryptolux.org/index.php/FELICS_Stream_Ciphers_Brief_Results).

- [31] L. Ding, C. Jin, and J. Guan. "Slide attack on standard stream cipher Enocoro-80 in the related-key chosen IV setting", *Pervasive Mob. Comput.*, pages 224–23, 2015.
- [32] Y. Funabiki, Y. Todo, T. Isobe, and M. Morii, "Security evaluation of Enocoro-128v2 against Cube attack", In *Symposium on Cryptography and Information Security, SCIS2019*, 2B1-1, 2019.
- [33] N. Shibayama, Y. Igarashi, and T. Kaneko, "Higher-Order Differential Characteristics of the Stream Cipher Enocoro-128v2", In: *Symposium on Cryptography and Information Security (SCIS2021)*, Paper 1B1-4, 2021.
- [34] D. Watanabe, K. Ideguchi, J. Kitahara, K. Muto, H. Furuichi, and T. Kaneko, "Enocoro-80: A hardware oriented stream cipher", In *Second International Workshop on Advances in Information Security*, 2008.
- [35] S. Mikami and D. Watanabe, "Software and hardware implementation and evaluation of stream cipher Enocoro-128v2", In *Computer Security Symposium, CSS2012*, pages 742-748, 2012.
- [36] C. Berbain, H. Gilbert, and A. Maximov, "Cryptanalysis of Grain", In M. Robshaw, editor, *Fast Software Encryption, FSE'06*, volume 4047 of *Lecture Notes in Computer Science*, pages 15-29, Springer-Verlag, 2006.
- [37] I. Dinur and A. Shamir, "Breaking Grain-128 with dynamic cube attack", In A. Joux, editor, *Fast Software Encryption, FSE 2011*, volume 6733 of *Lecture Notes in Computer Science*, pages 167-187, Springer, 2011.
- [38] B. Zhang, C. Xu, and W. Meier, "Fast Near Collision Attack on the Grain v1 Stream Cipher", In Jesper Buus Nielsen and Vincent Rijmen, editors, *Advances in Cryptology - EUROCRYPT 2018 - 37th Annual International Conference on the Theory and Applications of Cryptographic Techniques*, Tel Aviv, Israel, April 29 - May 3, 2018 *Proceedings, Part II*, volume 10821 of *Lecture Notes in Computer Science*, pages 771–802, Springer, 2018.
- [39] Y. Todo, T. Isobe, W. Meier, K. Aoki, and B. Zhang, "Fast Correlation Attack Revisited - Cryptanalysis on Full Grain-128a, Grain-128, and

- Grain-v1”, In Hovav Shacham and Alexandra Boldyreva, editors, Advances in Cryptology – CRYPTO 2018 - 38th Annual International Cryptology Conference, Santa Barbara, CA, USA, August 19-23, 2018, Proceedings, Part II, volume 10992 of Lecture Notes in Computer Science, pages 129–159, Springer, 2018.
- [40] T. Good and M. Benaissa, “Hardware performance of eStream phase-III stream cipher candidates”, In The State of the Art of Stream Ciphers, SASC 2008, 2008.
- [41] L. Ding, C. Jin, J. Guan, and C. Qi, “New Treatment of the BSW Sampling and Its Applications to Stream Ciphers”, In David Pointcheval and Damien Vergnaud, editors, Progress in Cryptology - AFRICACRYPT 2014 - 7th International Conference on Cryptology in Africa, Marrakesh, Morocco, May 28-30, 2014, Proceedings, volume 8469 of Lecture Notes in Computer Science, pages 136–146, Springer, 2014.
- [42] L. Ding, D. Gu, and L. Wang, “New Key Recovery Attack on the MICKEY Family of Stream Ciphers”, In Bazhong Shen, Baocang Wang, Jinguang Han, and Yong Yu, editors, International Conference on Frontiers in Cyber Security - FCS 2019, volume 1105 of Communications in Computer and Information Science, pages 239–249, Springer, 2019.
- [43] A.r Maximov and A. Biryukov, “Two trivial attacks on Trivium”, In Carlisle Adams and Ali Miri Michael Wiener, editors, Selected Areas in Cryptography, 14th International Workshop, SAC 2007, volume 4876 of Lecture Notes in Computer Science, pages 36-55, Springer Berlin Heidelberg, 2007.
- [44] P.A. Fouque and T. Vannet, “Improving key recovery to 784 and 799 rounds of trivium using optimized cube attacks”, In Shiho Moriai, editor, Fast Software Encryption, FSE 2013, volume 8424 of Lecture Notes in Computer Science, pages 502-517, Springer Berlin Heidelberg, 2013.
- [45] Y. Todo, T. Isobe, Y. Hao, and W. Meier, “Cube Attacks on Non-Blackbox Polynomials Based on Division Property”, In Jonathan Katz and Hovav Shacham, editors, Advances in Cryptology - CRYPTO 2017 - 37th Annual International Cryptology Conference, Santa Barbara, CA, USA,

- August 20-24, 2017, Proceedings, Part III, volume 10403 of Lecture Notes in Computer Science, pages 250–279, Springer, 2017.
- [46] S. Wang, B. Hu, J. Guan, K. Zhang, and T. Shi, “MILP-aided Method of Searching Division Property Using Three Subsets and Applications”, In Steven D. Galbraith and Shiho Moriai, editors, Advances in Cryptology - ASIACRYPT 2019 - 25th International Conference on the Theory and Application of Cryptology and Information Security, Kobe, Japan, December 8-12, 2019, Proceedings, Part III, volume 11923 of Lecture Notes in Computer Science, pages 398–427, Springer, 2019.
- [47] C.D. Ye and T. Tian, “Revisit Division Property Based Cube Attacks: Key-Recovery or Distinguishing Attacks?”, IACR Trans. Symmetric Cryptol, pages 81–102, 2019.
- [48] M. Liu, J. Yang, W. Wang, and D. Lin, “Correlation Cube Attacks: From Weak-Key Distinguisher to Key Recovery”, In Jesper Buus Nielsen and Vincent Rijmen, editors, Advances in Cryptology - EUROCRYPT 2018 - 37th Annual International Conference on the Theory and Applications of Cryptographic Techniques, Tel Aviv, Israel, April 29 - May 3, 2018 Proceedings, Part II, volume 10821 of Lecture Notes in Computer Science, pages 715–744, Springer, 2018.
- [49] Y. Hao, T. Isobe, L. Jiao, C. Li, W. Meier, Y. Todo, and Q. Wang, “Improved Division Property Based Cube Attacks Exploiting Algebraic Properties of Superpoly”, IEEE Trans. Computers, pages 1470–1486, 2019.
- [50] Q. Wang, Y. Hao, Y. Todo, C. Li, T. Isobe, and W. Meier, “Improved Division Property Based Cube Attacks Exploiting Algebraic Properties of Superpoly”, In Hovav Shacham and Alexandra Boldyreva, editors, Advances in Cryptology - CRYPTO 2018 - 38th Annual International Cryptology Conference, Santa Barbara, CA, USA, August 19-23, 2018, Proceedings, Part I, volume 10991 of Lecture Notes in Computer Science, pages 275–305, Springer, 2018.
- [51] Y. Hao, G. Leander, W. Meier, Y. Todo, and Q. Wang, “Modeling for Three-Subset Division Property Without Unknown Subset - Improved Cube Attacks Against Trivium and Grain-128AEAD”, In Anne Canteaut

- and Yuval Ishai, editors, *Advances in Cryptology - EUROCRYPT 2020 - 39th Annual International Conference on the Theory and Applications of Cryptographic Techniques*, Zagreb, Croatia, May 10-14, 2020, Proceedings, Part I, volume 12105 of *Lecture Notes in Computer Science*, pages 466–495, Springer, 2020.
- [52] Y. Hao, Gr. Leander, W. Meier, Y.e Todo, and Q. Wang, “Modeling for Three-Subset Division Property without Unknown Subset”, *J. Cryptol.*, 2021.
- [53] K. Hu, S. Sun, M. Wang, and Q. Wang, “An Algebraic Formulation of the Division Property: Revisiting Degree Evaluations, Cube Attacks, and Key-Independent Sums”, In Shiho Moriai and Huaxiong Wang, editors, *Advances in Cryptology - ASIACRYPT 2020 - 26th International Conference on the Theory and Application of Cryptology and Information Security*, Daejeon, South Korea, December 7-11, 2020, Proceedings, Part I, volume 12491 of *Lecture Notes in Computer Science*, pages 446–476, 2020.
- [54] K. Hu, S. Sun, Y. Todo, M. Wang, and Q. Wang, “Massive Superpoly Recovery with Nested Monomial Predictions”, *IACR Cryptol. ePrint Arch.*, 2021:1225, (accepted on *Advances in Cryptology - ASIACRYPT 2021 - 27th International Conference on the Theory and Application of Cryptology and Information Security*), 2021.
- [55] Y. Sun, “Cube Attack against 843-Round Trivium”, *IACR Cryptol. ePrint Arch.*, pages 547, 2021.
- [56] X. Fu, X. Wang, X. Dong, and W. Meier, “A Key-Recovery Attack on 855-round Trivium”, In Hovav Shacham and Alexandra Boldyreva, editors, *Advances in Cryptology - CRYPTO 2018 - 38th Annual International Cryptology Conference*, Santa Barbara, CA, USA, August 19-23, 2018, Proceedings, Part II, volume 10992 of *Lecture Notes in Computer Science*, pages 160–184, Springer, 2018.
- [57] S. Wang, B. Hu, J. Guan, K. Zhang, and T. Shi, “MILP-aided Method of Searching Division Property Using Three Subsets and Applications”, In Steven D. Galbraith and Shiho Moriai, editors, *Advances in Cryptology - ASIACRYPT 2019 - 25th International Conference on the Theory and*

- Application of Cryptology and Information Security, Kobe, Japan, December 8-12, 2019, Proceedings, Part III, volume 11923 of Lecture Notes in Computer Science, pages 398–427, Springer, 2019.
- [58] C.D. Ye and T. Tian, “Revisit Division Property Based Cube Attacks: Key-Recovery or Distinguishing Attacks?”, IACR Trans. Symmetric Cryptol., pages 81–102, 2019.
  - [59] Y. Li, W. Wu, and L. Zhang, “Improved Integral Attacks on Reduced-Round CLEFIA Block Cipher”, In Souhwan Jung and Moti Yung, editors, Information Security Applications - 12th International Workshop, WISA 2011, Jeju Island, Korea, August 22-24, 2011, Revised Selected Papers, volume 7115 of Lecture Notes in Computer Science, pages 28–39, Springer, 2011.
  - [60] H. Mala, M. Dakhilalian, and M. Shakiba, “Impossible Differential Attacks on 13-Round CLEFIA-128”, J. Comput. Sci. Technol., pages 744–750, 2011.
  - [61] C. Boura, M.N. Plasencia, and V. Suder, “Scrutinizing and Improving Impossible Differential Attacks: Applications to CLEFIA, Camellia, LBlock and Simon”, In Palash Sarkar and Tetsu Iwata, editors, Advances in Cryptology - ASIACRYPT 2014 - 20th International Conference on the Theory and Application of Cryptology and Information Security, Kaoshiung, Taiwan, R.O.C., December 7-11, 2014. Proceedings, Part I, volume 8873 of Lecture Notes in Computer Science, pages 179–199, Springer, 2014.
  - [62] L. Li, K. Jia, X. Wang, and X. Dong, “Meet-in-the-Middle Technique for Truncated Differential and Its Applications to CLEFIA and Camellia”, In Gregor Leander, editor, Fast Software Encryption - 22nd International Workshop, FSE 2015, Istanbul, Turkey, March 8-11, 2015, Revised Selected Papers, volume 9054 of Lecture Notes in Computer Science, pages 48–70, Springer, 2015.
  - [63] Y. Tsunoo, E. Tsujihara, M. Shigeri, T. Saito, T. Suzaki, and H. Kubo, “Impossible differential cryptanalysis of CLEFIA”, In Kaisa Nyberg, editor, Fast Software Encryption, 15th International Workshop, FSE 2008, Lausanne, Switzerland, February 10-13, 2008, Revised Selected

- Papers, volume 5086 of Lecture Notes in Computer Science, pages 398–411, Springer, 2008.
- [64] A. Bogdanov, H. Geng, M. Wang, L. Wen, and B. Collard, “Zero-Correlation Linear Cryptanalysis with FFT and Improved Attacks on ISO Standards Camellia and CLEFIA”, In Tanja Lange, Kristin E. Lauter, and Petr Lisonek, editors, Selected Areas in Cryptography - SAC 2013 - 20th International Conference, Burnaby, BC, Canada, August 14-16, 2013, Revised Selected Papers, volume 8282 of Lecture Notes in Computer Science, pages 306–323, Springer, 2013.
- [65] C. Tezcan and A.A. Selcuk, “Improved improbable differential attacks on ISO standard CLEFIA: Expansion technique revisited”, Inf. Process. Lett., pages 136–143, 2016.
- [66] W. Yi, B.Wu, S. Chen, and D. Lin, “Improved Integral and Zero correlation Linear Cryptanalysis of CLEFIA Block Cipher”, In Kefei Chen, Dongdai Lin, and Moti Yung, editors, Information Security and Cryptology - 12th International Conference, Inscrypt 2016, Beijing, China, November 4-6, 2016, Revised Selected Papers, volume 10143 of Lecture Notes in Computer Science, pages 33–46, Springer, 2016.
- [67] T. Akishita and H. Hiwatari, “Very compact hardware implementations of the block-cipher CLEFIA”, In Ali Miri and Serge Vaudenay, editors, Selected Areas in Cryptography - 18th International Workshop, SAC 2011, Toronto, ON, Canada, August 11-12, 2011, Revised Selected Papers, volume 7118 of Lecture Notes in Computer Science, pages 278–292, Springer, 2011.
- [68] T. Shirai, K. Shibutani, T. Akishita, S. Moriai, and T. Iwata, “The 128-bit blockcipher CLEFIA (extended abstract)”, In Alex Biryukov, editor, Fast Software Encryption, 14th International Workshop, FSE 2007, Luxembourg, Luxembourg, March 26-28, 2007, Revised Selected Papers, volume 4593 of Lecture Notes in Computer Science, pages 181–195, Springer, 2007.
- [69] M. Matsui and Y. Murakami, “Minimalism of software implementation – extensive performance analysis of symmetric primitives on the RL78 microcontroller”, In Shiho Moriai, editor, Fast Software Encryption -

- 20th International Workshop, FSE 2013, Singapore, March 11-13, 2013, Revised Selected Papers, volume 8424 of Lecture Notes in Computer Science, pages 393-409, Springer, 2013.
- [70] J. Guo, T. Peyrin, A. Poschmann, and M.J.B. Robshaw, "The LED Block Cipher", In B. Preneel and T. Takagi, editors, Cryptographic Hardware and Embedded Systems - CHES 2011, volume 6917 of LNCS, pages 326-341, Springer, 2011.
- [71] T. Isobe and K. Shibutani, "Security Analysis of the Lightweight Block Ciphers XTEA, LED and Piccolo", In Willy Susilo, Yi Mu, and Jennifer Seberry, editors, Information Security and Privacy - 17th Australasian Conference, ACISP 2012, Wollongong, NSW, Australia, July 9-11, 2012, Proceedings, volume 7372 of Lecture Notes in Computer Science, pages 71-86, Springer, 2012.
- [72] H. Soleimany, "Probabilistic Slide Cryptanalysis and Its Applications to LED-64 and Zorro", In Carlos Cid and Christian Rechberger, editors, Fast Software Encryption - 21st International Workshop, FSE 2014, London, UK, March 3-5, 2014, Revised Selected Papers, volume 8540 of Lecture Notes in Computer Science, pages 373-389, Springer, 2014.
- [73] I. Dinur, O. Dunkelman, N. Keller, and A. Shamir, "Improved Linear Sieving Techniques with Applications to Step-Reduced LED-64", In Carlos Cid and Christian Rechberger, editors, Fast Software Encryption - 21st International Workshop, FSE 2014, London, UK, March 3-5, 2014, Revised Selected Papers, volume 8540 of Lecture Notes in Computer Science, pages 390-410, Springer, 2014.
- [74] I. Dinur, O. Dunkelman, N. Keller, and A. Shamir, "Key Recovery Attacks on 3-round Even-Mansour, 8-step LED-128, and Full AES2", In Kazue Sako and Palash Sarkar, editors, Advances in Cryptology - ASIACRYPT 2013 - 19th International Conference on the Theory and Application of Cryptology and Information Security, Bengaluru, India, December 1-5, 2013, Proceedings, Part I, volume 8269 of Lecture Notes in Computer Science, pages 337-356, Springer, 2013.
- [75] F. Mendel, V. Rijmen, D. Toz, and K. Varici, "Differential Analysis of the LED Block Cipher", In Xiaoyun Wang and Kazue Sako, editors,

- Advances in Cryptology - ASIACRYPT 2012 - 18th International Conference on the Theory and Application of Cryptology and Information Security, Beijing, China, December 2-6, 2012, Proceedings, volume 7658 of Lecture Notes in Computer Science, pages 190–207, Springer, 2012.
- [76] I. Nikolic, L. Wang, and S. Wu, “Cryptanalysis of Round-Reduced LED”, In Shiho Moriai, editor, Fast Software Encryption - 20th International Workshop, FSE 2013, Singapore, March 11-13, 2013, Revised Selected Papers, volume 8424 of Lecture Notes in Computer Science, pages 112–129, Springer, 2013.
- [77] “The LED block cipher”, Available from <https://sites.google.com/site/ledblockcipher/hardware>, December 2013.
- [78] R. Benadjila, J. Guo, V. Lomne, and T. Peyrin, “Implementing lightweight block ciphers on x86 architectures”, In International Conference on Selected Areas in Cryptography, pages 324–351, Springer, 2013.
- [79] M. Katagi, “The 128-Bit Blockcipher CLEFIA RFC 6114 (Mar 2011)”, <https://www.rfc-editor.org/info/rfc6114>, 2011.
- [80] D. Hong, J.K. Lee, D.C. Kim, D. Kwon, K.H. Ryu, and D. Lee, “LEA: A 128-Bit Block Cipher for Fast Encryption on Common Processors”, In Yongdae Kim, Heejo Lee, and Adrian Perrig, editors, Information Security Applications - 14th International Workshop, WISA 2013, Jeju Island, Korea, August 19-21, 2013, Revised Selected Papers, volume 8267 of Lecture Notes in Computer Science, pages 3–27, Springer, 2013.
- [81] L. Song, Z. Huang, and Q. Yang, “Automatic Differential Analysis of ARX Block Ciphers with Application to SPECK and LEA”, In Joseph K. Liu and Ron Steinfeld, editors, Information Security and Privacy - 21st Australasian Conference, ACISP 2016, Melbourne, VIC, Australia, July 4-6, 2016, Proceedings, Part II, volume 9723 of Lecture Notes in Computer Science, pages 379–394, Springer, 2016.

- [82] D. Kim, D. Kwon, and J. Song, "Efficient Computation of Boomerang Connection Probability for ARX-Based Block Ciphers with Application to SPECK and LEA", *IEICE Trans. Fundam. Electron. Commun. Comput. Sci.*, pages 677–685, 2020.
- [83] S. Banik, A. Bogdanov, T. Isobe, K. Shibutani, H. Hiwatari, T. Akishita, and F. Regazzoni, "Midori: A block cipher for low energy", In Tetsu Iwata and Jung Hee Cheon, editors, *Advances in Cryptology - ASIACRYPT 2015 - 21st International Conference on the Theory and Application of Cryptology and Information Security*, Auckland, New Zealand, November 29 - December 3, 2015, Proceedings, Part II, volume 9453 of *Lecture Notes in Computer Science*, pages 411–436, Springer, 2015.
- [84] L. Lin and W. Wu, "Meet-in-the-Middle Attacks on Reduced-Round Midori-64", *IACR Cryptol. ePrint Arch.*, 2015.
- [85] L. Lin and W. Wu, "Meet-in-the-Middle Attacks on Reduced-Round Midori64", *IACR Trans. Symmetric Cryptol.*, pages 215–239, 2017.
- [86] J. Guo, J. Jean, I. Nikolic, K. Qiao, Y. Sasaki, and S.M. Sim, "Invariant Subspace Attack Against Midori64 and The Resistance Criteria for S-box Designs", *IACR Trans. Symmetric Cryptol.*, pages 33–56, 2016.
- [87] L. Sun, W. Wang, and M. Wang, "Accelerating the Search of Differential and Linear Characteristics with the SAT Method", *IACR Trans. Symmetric Cryptol.*, pages 269–315, 2021.
- [88] Y. Todo, G. Leander, and Y. Sasaki, "Nonlinear Invariant Attack: Practical Attack on Full SCREAM, iSCREAM, and Midori64", *J. Cryptol.*, pages 1383–1422, 2019.
- [89] Z. Chen, H.g Chen, and X. Wang, "Cryptanalysis of Midori128 Using Impossible Differential Techniques", In Feng Bao, Liqun Chen, Robert H. Deng, and Guojun Wang, editors, *Information Security Practice and Experience - 12th International Conference, ISPEC 2016, Zhangjiajie, China, November 16-18, 2016, Proceedings*, volume 10060 of *Lecture Notes in Computer Science*, pages 1–12, 2016.
- [90] M. Tolba, A. Abdelkhalek, and A. M. Youssef, "Truncated and Multiple Differential Cryptanalysis of Reduced Round Midori128", In Matt Bishop and Anderson C. A. Nascimento, editors, *Information Security -*

- 19th International Conference, ISC 2016, Honolulu, HI, USA, September 3-6, 2016, Proceedings, volume 9866 of Lecture Notes in Computer Science, pages 3–17, Springer, 2016.
- [91] X. Dong and Y. Shen, “Cryptanalysis of Reduced-Round Midori64 Block Cipher”, IACR Cryptol. ePrint Arch., 2016.
- [92] D. G erault and P. Lafourcade, “Related-Key Cryptanalysis of Midori”, In Orr Dunkelman and Somitra Kumar Sanadhya, editors, Progress in Cryptology – INDOCRYPT 2016 - 17th International Conference on Cryptology in India, Kolkata, India, December 11-14, 2016, Proceedings, volume 10095 of Lecture Notes in Computer Science, pages 287–304, 2016.
- [93] K. Shibutani, T. Isobe, H. Hiwatari, A. Mitsuda, T. Akishita, and T. Shirai, “Piccolo: An ultra-lightweight blockcipher”, In Cryptographic Hardware and Embedded Systems - CHES 2011 - 13th International Workshop, Nara, Japan, September 28 - October 1, 2011, Proceedings, pages 342–357, 2011.
- [94] S.A. Azimi, Z. Ahmadian, J. Mohajeri, and M.R. Aref, “Impossible differential cryptanalysis of Piccolo lightweight block cipher”, In 11th International ISC Conference on Information Security and Cryptology, ISCISC 2014, Tehran, Iran, September 3-4, 2014, pages 89–94, IEEE, 2014.
- [95] M. Tolba, A. Abdelkhalek, and A. M. Youssef, “Meet-in-the-Middle Attacks on Reduced Round Piccolo”, In Tim Guneysu, Gregor Leander, and Amir Moradi, editors, Lightweight Cryptography for Security and Privacy - 4th International Workshop, Light-Sec 2015, Bochum, Germany, September 10-11, 2015, Revised Selected Papers, volume 9542 of Lecture Notes in Computer Science, pages 3–20, Springer, 2015.
- [96] T. Isobe and K. Shibutani, “Security Analysis of the Lightweight Block Ciphers XTEA, LED and Piccolo”, In Willy Susilo, Yi Mu, and Jennifer Seberry, editors, Information Security and Privacy - 17th Australasian Conference, ACISP 2012, Wollongong, NSW, Australia, July 9-11, 2012,

- Proceedings, volume 7372 of Lecture Notes in Computer Science, pages 71–86, Springer, 2012
- [97] Y. Liu, L. Cheng, Z. Liu, W. Li, Q. Wang, and D. Gu, “Improved meet-in-the-middle attacks on reduced-round Piccolo”, *Sci. China Inf. Sci.*, 61(3):032108:1–032108:13, 2018.
- [98] M. Minier, “On the Security of Piccolo Lightweight Block Cipher against Related-Key Impossible Differentials”, In Goutam Paul and Serge Vaudenay, editors, *Progress in Cryptology - INDOCRYPT 2013 - 14th International Conference on Cryptology in India*, Mumbai, India, December 7-10, 2013, Proceedings, volume 8250 of Lecture Notes in Computer Science, pages 308–318, Springer, 2013.
- [99] S. Matsuda and S. Moriai, “Lightweight cryptography for the cloud: Exploit the power of bitslice implementation”, In Emmanuel Prouff and Patrick Schaumont, editors, *Cryptographic Hardware and Embedded Systems - CHES 2012 - 14th International Workshop*, Leuven, Belgium, September 9-12, 2012, Proceedings, volume 7428 of Lecture Notes in Computer Science, pages 408-425, Springer, 2012.
- [100] C. Blondeau and K. Nyberg, “Improved Parameter Estimates for Correlation and Capacity Deviates in Linear Cryptanalysis”, *IACR Trans. Symmetric Cryptol*, pages 162–191, 2016.
- [101] J.Y. Cho, “Linear Cryptanalysis of Reduced-Round PRESENT”, In Josef Pieprzyk, editor, *Topics in Cryptology - CT-RSA 2010*, The Cryptographers’ Track at the RSA Conference 2010, San Francisco, CA, USA, March 1-5, 2010, Proceedings, volume 5985 of Lecture Notes in Computer Science, pages 302–317, Springer, 2010.
- [102] A.F. Guti  rrez and M.N. Plasencia, “Improving Key-Recovery in Linear Attacks: Application to 28-Round PRESENT”, In Anne Canteaut and Yuval Ishai, editors, *Advances in Cryptology - EUROCRYPT 2020 - 39th Annual International Conference on the Theory and Applications of Cryptographic Techniques*, Zagreb, Croatia, May 10-14, 2020, Proceedings, Part I, volume 12105 of Lecture Notes in Computer Science, pages 221–249, Springer, 2020.

- [103] An. Bogdanov, E. Tischhauser, and P.S. Vejre, “Multivariate Profiling of Hulls for Linear Cryptanalysis”, *IACR Trans. Symmetric Cryptol.*, pages 101–125, 2018.
- [104] L. Zheng and S.W. Zhang, “FFT-based multidimensional linear attack on PRESENT using the 2-bit-fixed characteristic”, *Secur. Commun. Networks*, pages 3535–3545, 2015.
- [105] C. Rolfes, A. Poschmann, G. Leander, and C. Paar, “Ultra-lightweight implementations for smart devices - security for 1000 gate equivalents”, In Gilles Grimaud and Francois-Xavier Standaert, editors, *Smart Card Research and Advanced Applications*, 8th IFIP WG 8.8/11.2 International Conference, CARDIS 2008, London, UK, September 8–11, 2008. Proceedings, volume 5189 of *Lecture Notes in Computer Science*, pages 89–103, Springer, 2008.
- [106] R. Benadjila, J. Guo, V. Lomne, and T. Peyrin, “Implementing lightweight block ciphers on x86 architectures”, In: Lange, T., Lauter, K., Lisoněk, P. (eds) *Selected Areas in Cryptography - SAC 2013*, *Lecture Notes in Computer Science*, vol 8282, Springer, Berlin, Heidelberg, 2014, [https://doi.org/10.1007/978-3-662-43414-7\\_17](https://doi.org/10.1007/978-3-662-43414-7_17).
- [107] S. Matsuda and S. Moriai, “Lightweight cryptography for the cloud: Exploit the power of bitslice implementation”, In Emmanuel Prouff and Patrick Schaumont, editors, *Cryptographic Hardware and Embedded Systems - CHES 2012 - 14th International Workshop*, Leuven, Belgium, September 9–12, 2012, Proceedings, volume 7428 of *Lecture Notes in Computer Science*, pages 408–425, Springer, 2012.
- [108] M. Matsui and Y. Murakami, “Minimalism of software implementation – extensive performance analysis of symmetric primitives on the RL78 microcontroller”, In Shiho Moriai, editor, *Fast Software Encryption - 20th International Workshop, FSE 2013, Singapore, March 11–13, 2013, Revised Selected Papers*, volume 8424 of *Lecture Notes in Computer Science*, pages 393–409, Springer, 2013.
- [109] J. Borghoff, A. Canteaut, T. Guneysu, E.B. Kavun, M. Knezevic, L.R. Knudsen, G. Leander, V. Nikov, C. Paar, C. Rechberger, P. Rombouts, S.S. Thomsen, and T. Yalcin, “PRINCE - A low-latency block cipher for

- pervasive computing applications - extended abstract”, In Xiaoyun Wang and Kazue Sako, editors, Advances in Cryptology - ASIACRYPT 2012 - 18th International Conference on the Theory and Application of Cryptology and Information Security, Beijing, China, December 2-6, 2012, Proceedings, volume 7658 of Lecture Notes in Computer Science, pages 208-225, Springer, 2012.
- [110] C.Blondeau, T. Peyrin, L. Wang, “Known-Key Distinguisher on Full PRESENT”, In: Gennaro, R., Robshaw, M. (eds.) Advances in Cryptology - CRYPTO 2015 - 35th Annual Cryptology Conference, Santa Barbara, CA, USA, August 16-20, 2015, Proceedings, Part I. Lecture Notes in Computer Science, vol. 9215, pages 455–474, Springer, 2015, [https://doi.org/10.1007/978-3-662-47989-6\\_22](https://doi.org/10.1007/978-3-662-47989-6_22)
- [111] J. Jean, I. Nikolic, T. Peyrin, L. Wang, and S. Wu, “Security Analysis of PRINCE”, In Shiho Moriai, editor, Fast Software Encryption - 20th International Workshop, FSE 2013, Singapore, March 11-13, 2013. Revised Selected Papers, volume 8424 of Lecture Notes in Computer Science, pages 92–111, Springer, 2013.
- [112] P. Derbez and L. Perrin, “Meet-in-the-Middle Attacks and Structural Analysis of Round-Reduced PRINCE”, J. Cryptol., pages 1184–1215, 2020.
- [113] P. Derbez and L. Perrin, “Meet-in-the-middle attacks and structural analysis of round-reduced PRINCE”, In Gregor Leander, editor, Fast Software Encryption - 22nd International Workshop, FSE 2015, Istanbul, Turkey, March 8-11, 2015, Revised Selected Papers, volume 9054 of Lecture Notes in Computer Science, pages 190–216, Springer, 2015.
- [114] A. Canteaut, M.N. Plasencia, and B. Vayssiere, “Sieve-in-the-Middle: Improved MITM Attacks”, In Ran Canetti and Juan A. Garay, editors, Advances in Cryptology - CRYPTO 2013 - 33rd Annual Cryptology Conference, Santa Barbara, CA, USA, August 18-22, 2013, Proceedings, Part I, volume 8042 of Lecture Notes in Computer Science, pages 222–240, Springer, 2013.

- [115] L. Li, K. Jia, and X. Wang, "Improved Meet-in-the-Middle Attacks on AES-192 and PRINCE", IACR Cryptol. ePrint Arch., 2013.
- [116] A. Canteaut, T. Fuhr, H. Gilbert, M.N. Plasencia, and J.R. Reinhard, "Multiple Differential Cryptanalysis of Round-Reduced PRINCE:", In Carlos Cid and Christian Rechberger, editors, Fast Software Encryption - 21st International Workshop, FSE 2014, London, UK, March 3-5, 2014, Revised Selected Papers, volume 8540 of Lecture Notes in Computer Science, pages 591–610, Springer, 2013.
- [117] L. Batina, A. Das, B. Ege, E.B. Kavun, N. Mentens, C. Paar, I. Verbauwhede, and T. Yalcin, "Dietary recommendations for lightweight block ciphers: Power, energy and area analysis of recently developed architectures", In Michael Hutter and Jhorn-Marc Schmidt, editors, Radio Frequency Identification - Security and Privacy Issues 9th International Workshop, RFIDsec 2013, Graz, Austria, July 9-11, 2013, Revised Selected Papers, volume 8262 of Lecture Notes in Computer Science, pages 103-112, Springer, 2013.
- [118] K. Papapagiannopoulos, "High throughput in slices: The case of present, PRINCE and KATAN64 ciphers", In Nitesh Saxena and Ahmad-Reza Sadeghi, editors, Radio Frequency Identification: Security and Privacy Issues - 10th International Workshop, RFIDSec 2014, Oxford, UK, July 21-23, 2014, Revised Selected Papers, volume 8651 of Lecture Notes in Computer Science, pages 137-155, Springer, 2014.
- [119] R. Beaulieu, D. Shors, J. Smith, S.T. Clark, B. Weeks, and L. Wingers, "The SIMON and SPECK families of lightweight block ciphers", IACR Cryptology ePrint Archive, 2013.
- [120] P. Derbez and P.A. Fouque, "Automatic Search of Meet-in-the-Middle and Impossible Differential Attacks", In Matthew Robshaw and Jonathan Katz, editors, Advances in Cryptology - CRYPTO 2016 - 36th Annual International Cryptology Conference, Santa Barbara, CA, USA, August 14-18, 2016, Proceedings, Part II, volume 9815 of Lecture Notes in Computer Science, pages 157–184, Springer, 2016.
- [121] K. Qiao, L. Hu, and S. Sun, "Differential Analysis on Simeck and SIMON with Dynamic Key-Guessing Techniques", In Olivier Camp, Steven

- Furnell, and Paolo Mori, editors, Information Systems Security and Privacy - Second International Conference, ICISSP 2016, Rome, Italy, February 19-21, 2016, Revised Selected Papers, volume 691 of Communications in Computer and Information Science, pages 64–85, Springer, 2016.
- [122] H. Chen and X. Wang, “Improved Linear Hull Attack on Round-Reduced Simon with Dynamic Key-Guessing Techniques”, In Thomas Peyrin, editor, Fast Software Encryption - 23rd International Conference, FSE 2016, Bochum, Germany, March 20-23, 2016, Revised Selected Papers, volume 9783 of Lecture Notes in Computer Science, pages 428–449, Springer, 2016.
- [123] Z. Chu, H. Chen, X. Wang, X. Dong, and L. Li, “Improved Integral Attacks on SIMON32 and SIMON48 with Dynamic Key-Guessing Techniques”, Secur. Commun. Networks, pages 1–11, 2018.
- [124] R. Rohit and G. Gong, “Correlated Sequence Attack on Reduced-Round Simon-32/64 and Simeck-32/64”, IACR Cryptol. ePrint Arch., 2018.
- [125] G. Leurent, C. Pernot, and A. Schrottenloher, “Clustering Effect in Simon and Simeck”, IACR Cryptol. ePrint Arch., 2021. (accepted on Advances in Cryptology - ASIACRYPT 2021 - 27th International Conference on the Theory and Application of Cryptology and Information Security).
- [126] J.K. Lee, B. Koo, and W.H. Kim, “A General Framework for the Related-Key Linear Attack Against Block Ciphers with Linear Key Schedules”, In Kenneth G. Paterson and Douglas Stebila, editors, Selected Areas in Cryptography – SAC 2019 - 26th International Conference, Waterloo, ON, Canada, August 12-16, 2019, Revised Selected Papers, volume 11959 of Lecture Notes in Computer Science, pages 194–224, Springer, 2019.
- [127] T. Akishita and H. Hiwatari, “Very compact hardware implementations of the block cipher CLEFIA”, In Ali Miri and Serge Vaudenay, editors, Selected Areas in Cryptography -18th International Workshop, SAC 2011, Toronto, Canada, August 11-12, 2011, Revised Selected Papers,

- volume 7118 of Lecture Notes in Computer Science, pages 278-292, Springer, 2011.
- [128] S. Banik, A. Bogdanov, T. Isobe, K. Shibutani, H. Hiwatari, T. Akishita, and F. Regazzoni, “Midori: A block cipher for low energy”, In Tetsu Iwata and Jung Hee Cheon, editors, *Advances in Cryptology - ASIACRYPT 2015 - 21st International Conference on the Theory and Application of Cryptology and Information Security*, Auckland, New Zealand, November 29 - December 3, 2015, Proceedings, Part II, volume 9453 of Lecture Notes in Computer Science, pages 411-436, Springer, 2015.
- [129] I. Dinur, “Improved Differential Cryptanalysis of Round-Reduced Speck”, In Antoine Joux and Amr M. Youssef, editors, *Selected Areas in Cryptography - SAC 2014 - 21st International Conference*, Montreal, QC, ON, Canada, August 14-15, 2014, Revised Selected Papers, volume 8781 of Lecture Notes in Computer Science, pages 147-164, Springer, 2014.
- [130] L. Song, Z. Huang, and Q. Yang, “Automatic Differential Analysis of ARX Block Ciphers with Application to SPECK and LEA”, In Joseph K. Liu and Ron Steinfeld, editors, *Information Security and Privacy - 21st Australasian Conference, ACISP 2016*, Melbourne, VIC, Australia, July 4-6, 2016, Proceedings, Part II, volume 9723 of Lecture Notes in Computer Science, pages 379-394, Springer, 2016.
- [131] T. Suzaki, K. Minematsu, S. Morioka, and E. Kobayashi, “TWINE : A lightweight block cipher for multiple platforms”, In Lars R. Knudsen and Huapeng Wu, editors, *Selected Areas in Cryptography*, 19th International Conference, SAC 2012, Windsor, ON, Canada, August 15-16, 2012, Revised Selected Papers, volume 7707 of Lecture Notes in Computer Science, pages 339-354, Springer, 2012.
- [132] X. Zheng and K. Jia, “Impossible Differential Attack on Reduced-Round TWINE”, In Hyang-Sook Lee and Dong-Guk Han, editors, *Information Security and Cryptology - ICISC 2013 - 16th International Conference*, Seoul, Korea, November 27-29, 2013, Revised Selected Papers, volume 8565 of Lecture Notes in Computer Science, pages 123-143, Springer, 2013.

- [133] L. Lin, W. Wu, and Y. Zheng, “Automatic Search for Key-Bridging Technique: Applications to LBlock and TWINE”, In Thomas Peyrin, editor, Fast Software Encryption - 23rd International Conference, FSE 2016, Bochum, Germany, March 20-23, 2016, Revised Selected Papers, volume 9783 of Lecture Notes in Computer Science, pages 247–267, Springer, 2016.
- [134] A. Biryukov, P. Derbez, and L. Perrin, “Differential Analysis and Meet-in-the-Middle Attack Against Round-Reduced TWINE”, In Gregor Leander, editor, Fast Software Encryption - 22nd International Workshop, FSE 2015, Istanbul, Turkey, March 8-11, 2015, Revised Selected Papers, volume 9054 of Lecture Notes in Computer Science, pages 3–27, Springer, 2015.
- [135] Y. Wang and W. Wu, “Improved Multidimensional Zero-Correlation Linear Cryptanalysis and Applications to LBlock and TWINE”, In Willy Susilo and Yi Mu, editors, Information Security and Privacy - 19th Australasian Conference, ACISP 2014, Wollongong, NSW, Australia, July 7-9, 2014. Proceedings, volume 8544 of Lecture Notes in Computer Science, pages 1–16, Springer, 2014.
- [136] S. Badel, N. Dağtekin, J. Nakahara Jr, K. Ouafi, N. Reffé, P. Sepehrdad, & S. Vaudenay, “ARMADILLO: a multi-purpose cryptographic primitive dedicated to hardware”, In Cryptographic Hardware and Embedded Systems, CHES 2010, 2010, <https://www.iacr.org/archive/ches2010/62250388/62250388.pdf>.
- [137] M.N. Plasencia, & T. Peyrin, “Practical cryptanalysis of ARMADILLO2”, In Fast Software Encryption 2012, pages 146-162, 2012, <https://www.iacr.org/archive/fse2012/75490147/75490147.pdf>.
- [138] A. Poschmann, “Lightweight Cryptography: Cryptographic Engineering for a Pervasive World”, PhD Thesis from Faculty of Electrical Engineering and Information Technology Ruhr-University Bochum, Germany, 2009, <https://eprint.iacr.org/2009/516.pdf>.
- [139] T. Koyama, Y. Sasaki, & N. Kunihiro, “Multi-differential cryptanalysis on reduced DM-PRESENT-80: collisions and other differential properties”, In Information Security and Cryptology–ICISC 2012, pages

- 352-367, 2012, [https://link.springer.com/chapter/10.1007/978-3-642-37682-5\\_25](https://link.springer.com/chapter/10.1007/978-3-642-37682-5_25).
- [140] T.P. Berger, J. D'Hayer, K. Marquet, M. Minier, & G. Thomas, "The GLUON family: a lightweight Hash function family based on FCSRs", In Progress in Cryptology-AFRICACRYPT 2012, pages 306-323, 2012, [https://link.springer.com/chapter/10.1007/978-3-642-31410-0\\_19](https://link.springer.com/chapter/10.1007/978-3-642-31410-0_19).
- [141] L. Perrin, & D. Khovratovich, "Collision Spectrum, Entropy Loss, T-Sponges, and Cryptanalysis of GLUON-64", In Fast Software Encryption 2014 (to appear), 2014, <https://eprint.iacr.org/2014/223.pdf>.
- [142] S. Hirose, K. Ideguchi, H. Kuwakado, T. Owada, B. Preneel, & H. Yoshida, "A lightweight 256-bit hash function for hardware and low-end devices: Lesamnta-LW", In International Conference on Information Security and Cryptology 2010, pages 151-168, Springer Berlin Heidelberg, 2010, [https://link.springer.com/chapter/10.1007/978-3-642-24209-0\\_10](https://link.springer.com/chapter/10.1007/978-3-642-24209-0_10).
- [143] R. Shiba, K. Sakamoto, F. Liu, K. Minematsu, T. Isobe, "Integral and Impossible Differential Attacks on the Reduced-Round Lesamnta-LW-BC", SCIS2021, 1B1-2, 2021.
- [144] S. Hirose, Y. Sasaki, H. Yoshida, "Lesamnta-LW Revisited: Improved Security Analysis of Primitive and New PRF Mode", In: Conti, M., Zhou, J., Casalicchio, E., Spognardi, A. (eds.) Applied Cryptography and Network Security - 18th International Conference, ACNS 2020, Rome, Italy, October 19-22, 2020, Proceedings, Part I. Lecture Notes in Computer Science, vol. 12146, pages 89-109, Springer, 2020, [https://doi.org/10.1007/978-3-030-57808-4\\_5](https://doi.org/10.1007/978-3-030-57808-4_5).
- [145] J. Guo, T. Peyrin, & A. Poschmann, "The PHOTON family of lightweight hash functions", In Advances in Cryptology-CRYPTO 2011, pages 222-239, Springer Berlin Heidelberg, 2011, <https://sites.google.com/site/photonhashfunction/>.
- [146] ISO/IEC, 2016. ISO/IEC 29192-5:2016 Information technology — Security techniques — Lightweight Cryptography —Part 5: Hash-functions, Geneva:ISO, 2016.

- [147] Q. Wang, L. Grassi, C. Rechberger, “Zero-Sum Partitions of PHOTON Permutations”, IACR Cryptol. ePrint Arch. 2017, 2017, <https://eprint.iacr.org/2017/1211>.
- [148] Q. Wang, L. Grassi, C. Rechberger, “Zero-Sum Partitions of PHOTON Permutations”, In: Smart, N.P. (ed.) Topics in Cryptology - CT-RSA 2018 - The Cryptographers’ Track at the RSA Conference 2018, San Francisco, CA, USA, April 16-20, 2018, Proceedings. Lecture Notes in Computer Science, vol. 10808, pages 279–299, Springer, 2018, [https://doi.org/10.1007/978-3-319-76953-0\\_15](https://doi.org/10.1007/978-3-319-76953-0_15).
- [149] J.P. Aumasson, L. Henzen, W. Meier, & M.N. Plasencia, “Quark: A lightweight hash”, Journal of cryptology, pages 313-339, 2013, <http://aumasson.jp/quark/>.
- [150] J. Yang, M. Liu, D. Lin, W. Wang, “Symbolic-Like Computation and Conditional Differential Cryptanalysis of QUARK”, In: Inomata, A., Yasuda, K. (eds.) Advances in Information and Computer Security - 13th International Workshop on Security, IWSEC 2018, Sendai, Japan, September 3-5, 2018, Proceedings Lecture Notes in Computer Science, vol. 11049, pages 244–261, Springer, 2018, [https://doi.org/10.1007/978-3-319-97916-8\\_16](https://doi.org/10.1007/978-3-319-97916-8_16).
- [151] J.P. Aumasson, & D.J. Bernstein, “SipHash: a fast short-input PRF”, In Progress in Cryptology-INDOCRYPT 2012, pages 489-508, Springer Berlin Heidelberg, 2012, <https://eprint.iacr.org/2012/351.pdf>.
- [152] C. Dobraunig, F. Mendel, M. Schlaffer, “Differential Cryptanalysis of SipHash”, In: Joux, A., Youssef, A.M. (eds.) Selected Areas in Cryptography - SAC 2014 - 21st International Conference, Montreal, QC, Canada, August 14- 15, 2014, Revised Selected Papers, Lecture Notes in Computer Science, vol. 8781, pages 165–182, Springer. 2014, [https://doi.org/10.1007/978-3-319-13051-4\\_10](https://doi.org/10.1007/978-3-319-13051-4_10).
- [153] W. Xin, Y. Liu, B. Sun, C. Li, “Improved Cryptanalysis on SipHash”, In: Mu, Y., Deng, R.H., Huang, X. (eds.) Cryptology and Network Security - 18th International Conference, CANS 2019, Fuzhou, China, October 25-27, 2019, Proceedings. Lecture Notes in Computer Science, vol.

- 11829, pages 61–79, Springer, 2019, [https://doi.org/10.1007/978-3-030-31578-8\\_4](https://doi.org/10.1007/978-3-030-31578-8_4).
- [154] J. Choy, H. Yap, K. Khoo, J. Guo, T. Peyrin, A. Poschmann, & C.H. Tan, “SPN-hash: improving the provable resistance against differential collision attacks”, In Progress in Cryptology-AFRICACRYPT 2012, pages 270-286, Springer Berlin Heidelberg, 2012, <https://eprint.iacr.org/2012/234.pdf>.
- [155] A. Bogdanov, M. Knežević, G. Leander, D. Toz, K. Varıcı, & I. Verbauwhede, “SPONGENT: A lightweight hash function”, In Cryptographic Hardware and Embedded Systems–CHES 2011, pages 312-325, Springer Berlin Heidelberg, 2011, <https://www.iacr.org/archive/ches2011/69170311/69170311.pdf>.
- [156] G. Zhang, M. Liu, “A distinguisher on PRESENT-like permutations with application to SPONGENT”, Sci. China Inf. Sci. 60(7), 72101 (2017), <https://doi.org/10.1007/s11432>.





**BADAN SIBER  
DAN SANDI  
NEGARA**



**Deputi Bidang Strategi dan Kebijakan Keamanan Siber dan Sandi  
Badan Siber dan Sandi Negara**

Jl. Cijayanti No. 70, Kec. Babakan Madang, Kabupaten Bogor

**2025**

**PUBLIK**