



Pengenalan Kriptografi Kuantum (Quantum Cryptography) Versi 1.0

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

2025

PENGENALAN KRIPTOGRAFI KUANTUM (*QUANTUM CRYPTOGRAPHY*) 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

TIM PERUMUS

Pengarah : Tjahjo Khurniawan

Penanggung Jawab : Soetedjo Joewono

Tim Pereviu : Assoc. Prof. Dr.Eng Khoirul Anwar, S.T., M.Eng
(Telkom University)

Tim Penyusun :

1. Sari Agustini Hafman
2. Theresia Natalia
3. Mohamad Rahmadi
4. Yhufi Swastantri Gustiviana
5. Andreas Lugas

Penyunting :

1. Yhufi Swastantri Gustiviana
2. Mohamad Rahmadi
3. Andreas Lugas



PENGANTAR

Puji syukur kita panjatkan ke hadirat Tuhan Yang Maha Esa, karena atas rahmat dan karunia-Nya, dokumen *Pengenalan Kriptografi Kuantum (Quantum Cryptography) Versi 1.0* ini dapat diselesaikan. Dokumen ini disusun sebagai bagian dari upaya memperkuat landasan pengetahuan dan kesiapan nasional dalam menghadapi perkembangan teknologi masa depan.

Perkembangan pesat komputasi kuantum telah menghadirkan peluang sekaligus tantangan baru bagi keamanan informasi. Kemampuan komputasi kuantum yang melampaui paradigma komputasi klasik menuntut adanya transformasi menyeluruh terhadap mekanisme pengamanan data, khususnya pada sektor-sektor Infrastruktur Informasi Vital. Dalam menghadapi perkembangan ini, kriptografi kuantum, khususnya *Quantum Key Distribution* (QKD), menjadi salah satu teknologi kuantum yang menawarkan keamanan berbasis prinsip fisika kuantum. QKD tersebut kini berjalan beriringan dengan teknologi kriptografi pasca kuantum atau *Post-Quantum Cryptography* (PQC) yang kompatibel dengan infrastruktur yang ada saat ini.

Dokumen ini diharapkan dapat memberikan pemahaman awal mengenai konsep dasar, prinsip kerja, mekanisme protokol, dan penerapan QKD di berbagai sektor, sekaligus menegaskan komitmen dalam mendorong inovasi dan penguatan kapasitas keamanan siber dan sandi nasional. Saya berharap materi yang disajikan dalam dokumen ini dapat dimanfaatkan oleh seluruh pemangku kepentingan, baik di sektor pemerintah, industri, praktisi,



maupun akademisi, sebagai referensi teknis dan strategis dalam merumuskan kebijakan, penelitian, serta implementasi teknologi keamanan masa depan.

Saya menyampaikan apresiasi kepada seluruh jajaran BSSN, khususnya Deputy Bidang Strategi dan Kebijakan Keamanan Siber dan Sandi, serta para pakar dan mitra yang telah berkontribusi pada penyusunan dokumen ini. Saya mengajak seluruh pemangku kepentingan yang meliputi pemerintah, pelaku usaha, akademisi, dan masyarakat/komunitas, untuk memperkuat kolaborasi dalam mendukung implementasi teknologi kriptografi kuantum guna memperkuat keamanan siber nasional.

Harapan kami, panduan ini menjadi rujukan nasional dalam menjaga keamanan data strategis, memperkuat ketahanan siber Indonesia dan meningkatkan kepercayaan publik terhadap ruang digital kita. Semoga panduan ini memberikan manfaat yang nyata dalam membangun ekosistem keamanan informasi yang tangguh, aman, dan berdaulat di era komputasi kuantum.

Drs. Nugroho Sulistyo Budi, M.M., M.Han.

PROFESIONAL • ELABORATIF • RESPONSIF
INTEGRATIF • SOLID • AKUNTABEL

PERISAI

Kepala Badan Siber dan Sandi Negara

Desember 2025

PENGANTAR DEPUTI I



Puji syukur kita panjatkan ke hadirat Tuhan Yang Maha Esa, atas rahmat dan karunia-Nya, dokumen *Pengenalan Kriptografi Kuantum (Quantum Cryptography) Versi 1.0* ini dapat disusun dan diterbitkan sebagai salah satu langkah strategis dalam memperkuat ketahanan keamanan informasi nasional.

Kemajuan teknologi kuantum membawa peluang besar sekaligus tantangan baru bagi dunia keamanan siber. Kriptografi klasik kini menghadapi ancaman nyata dari kemampuan komputasi kuantum yang berpotensi memecahkan algoritma enkripsi yang selama ini dianggap aman. Dalam menghadapi era ini, teknologi kriptografi pasca kuantum atau *Post-Quantum Cryptography* (PQC) dan kriptografi kuantum, khususnya *Quantum Key Distribution* (QKD), menjadi dua pendekatan utama yang saling melengkapi. PQC bersifat praktis dan kompatibel dengan infrastruktur yang ada, sementara QKD menawarkan keamanan berbasis prinsip fisika kuantum.

Dokumen ini diharapkan dapat menjadi referensi awal bagi para pemangku kepentingan mulai dari regulator, peneliti, pengembang teknologi, dan praktisi keamanan siber dalam memahami konsep dasar, protokol, serta potensi penerapan QKD di berbagai sektor strategis. Dengan pemahaman yang selaras dan kolaborasi lintas sektor, Indonesia dapat mempersiapkan diri lebih baik dalam menghadapi tantangan komputasi kuantum serta memperkuat kedaulatan dan keamanan ruang siber nasional.

Akhirnya, kami menyampaikan apresiasi kepada seluruh pihak yang telah berkontribusi dalam penyusunan dokumen ini. Semoga karya ini memberikan manfaat nyata dalam mendorong pengembangan dan implementasi teknologi kriptografi kuantum di Indonesia menuju ruang siber yang tangguh, aman, dan berdaulat.

Tjahjo Khurniawan

Deputi Bidang Strategi dan Kebijakan Keamanan Siber dan Sandi

Desember 2025



RINGKASAN EKSEKUTIF

Kriptografi klasik semakin rentan terhadap ancaman komputasi kuantum yang berpotensi memecahkan algoritma enkripsi yang ada. Untuk mengantisipasi hal tersebut, dikembangkan teknologi komunikasi aman pascakuantum (*post-quantum secure communication technologies*) yang dapat diterapkan melalui kriptografi pascakuantum (*post-quantum cryptography* (PQC)), kriptografi kuantum seperti distribusi kunci kuantum (*quantum key distribution* (QKD)), maupun kombinasi keduanya. PQC menawarkan solusi praktis yang kompatibel dengan infrastruktur digital saat ini, sedangkan QKD memberikan lapisan keamanan tambahan berbasis hukum fisika. Implementasi keduanya, baik secara terpisah maupun bersamaan, membentuk sistem pertahanan berlapis yang memperkuat ketahanan komunikasi terhadap ancaman komputasi kuantum di masa depan.

Sejalan dengan itu, teknologi kuantum saat ini menjadi tren teknologi, khususnya dalam bidang kriptografi dan sering menjadi bahasan penting dalam banyak forum ilmiah. Salah satu teknik kriptografi berbasis kuantum yang saat ini berkembang adalah *Quantum Key Distribution* (QKD), yaitu metode distribusi kunci kriptografi yang didasarkan pada prinsip-prinsip kuantum yang menawarkan keamanan berbasis prinsip fisika kuantum dan mampu melampaui batas-batas keamanan tradisional yang mengandalkan kompleksitas algoritma matematis. Protokol QKD secara umum dibagi menjadi tiga kategori, yaitu: (i) QKD berbasis foton tunggal, (ii) QKD berbasis keadaan koheren lemah, dan (iii) QKD berbasis foton yang saling terjerat (*entangled photon*). Dalam menghadapi tantangan teknologi kuantum di masa depan, pemahaman yang mendalam terhadap prinsip dasar dan implementasi kriptografi kuantum menjadi sangat penting.

Dokumen ini disusun sebagai pengenalan kepada pembaca terkait prinsip dasar informasi kuantum, protokol QKD, dan implementasi QKD. Secara struktural, dokumen ini terdiri atas lima bab. Bab I menjelaskan latar belakang, ruang lingkup, target audiens, dan sistematika penulisan. Bab II memberikan informasi tentang pengantar dan konsep dasar tentang

kriptografi kuantum, QKD, dan informasi kuantum. Bab III membahas tentang contoh protokol QKD yaitu protokol QKD berbasis foton tunggal, protokol QKD yang menggunakan keadaan koheren lemah, dan protokol QKD berbasis foton yang saling terjerat. Bab IV memberikan gambaran tentang tren jaringan modern menggunakan QKD yaitu contoh implementasi QKD di dalam jaringan 5G dan kuantum *repeater*. Bab V menutup dengan simpulan tentang pentingnya pemahaman terhadap konsep dasar informasi kuantum dalam menerapkan kriptografi kuantum.

Dokumen ini diharapkan menjadi referensi awal yang bermanfaat bagi para pemangku kepentingan, termasuk regulator, pengembang teknologi, peneliti, dan perancang sistem keamanan siber, dalam memahami prinsip-prinsip dasar dan protokol QKD. Dengan pemahaman yang selaras di antara para pemangku kepentingan diharapkan dapat mendorong kolaborasi lintas sektor untuk mendukung adopsi dan pengembangan teknologi QKD yang selaras dengan kebutuhan nasional. Lebih jauh, pemanfaatan dokumen ini diharapkan dapat mendukung harmonisasi kebijakan nasional, memperkuat ekosistem teknologi kuantum, serta meningkatkan ketahanan keamanan informasi Indonesia di masa depan.

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

DAFTAR ISI

PENGANTAR	iii
PENGANTAR DEPUTI I	v
RINGKASAN EKSEKUTIF	vii
DAFTAR ISI	ix
DAFTAR GAMBAR	x
DAFTAR TABEL	xi
BAB I PENDAHULUAN	1
A. RUANG LINGKUP	2
B. TARGET AUDIENS	3
C. RUJUKAN	4
D. SISTEMATIKA PENYUSUNAN DOKUMEN	5
BAB II PENGANTAR DAN KONSEP DASAR	6
A. KRIPTOGRAFI KUANTUM DAN <i>QUANTUM KEY DISTRIBUTION</i> (QKD)	7
B. PRINSIP DASAR INFORMASI KUANTUM	14
BAB III PROTOKOL QKD	23
A. PROTOKOL QKD BERBASIS FOTON TUNGGAL	25
B. PROTOKOL QKD BERBASIS KEADAAN KOHEREN LEMAH	33
C. PROTOKOL QKD BERBASIS FOTON YANG SALING TERJERAT	38
BAB IV TREN MODERN DALAM JARINGAN QKD	52
A. QKD DALAM JARINGAN 5G	53
B. <i>QUANTUM REPEATER</i> (<i>REPEATER KUANTUM</i>)	60
BAB V PENUTUP	62
REFERENSI	64

DAFTAR GAMBAR

Gambar 2.1 Contoh <i>entanglement</i> suatu foton	17
Gambar 3.1 Konsep dasar protokol QKD berbasis <i>entanglement</i>	24
Gambar 3.2 Protokol BB84	26
Gambar 3.3 Skematik Protokol COW	38
Gambar 3.4 Protokol E91	39
Gambar 3.5 Konsep <i>eavesdropping</i>	41
Gambar 3.6 Contoh perhitungan Protokol E91.....	42
Gambar 4.1 Struktur 5G: bagian fronthaul, midhaul, dan backhaul	54
Gambar 4.2 Evolusi RAN: (a) RAN terdistribusi; (b) Migrasi ke C-RAN; (c) Struktur C-RAN	56
Gambar 4.3 <i>Latency link budget</i> RTT lapisan-MAC di C-RAN	56
Gambar 4.4 Penerapan QKD dalam jaringan fronthaul seluler 5G	58



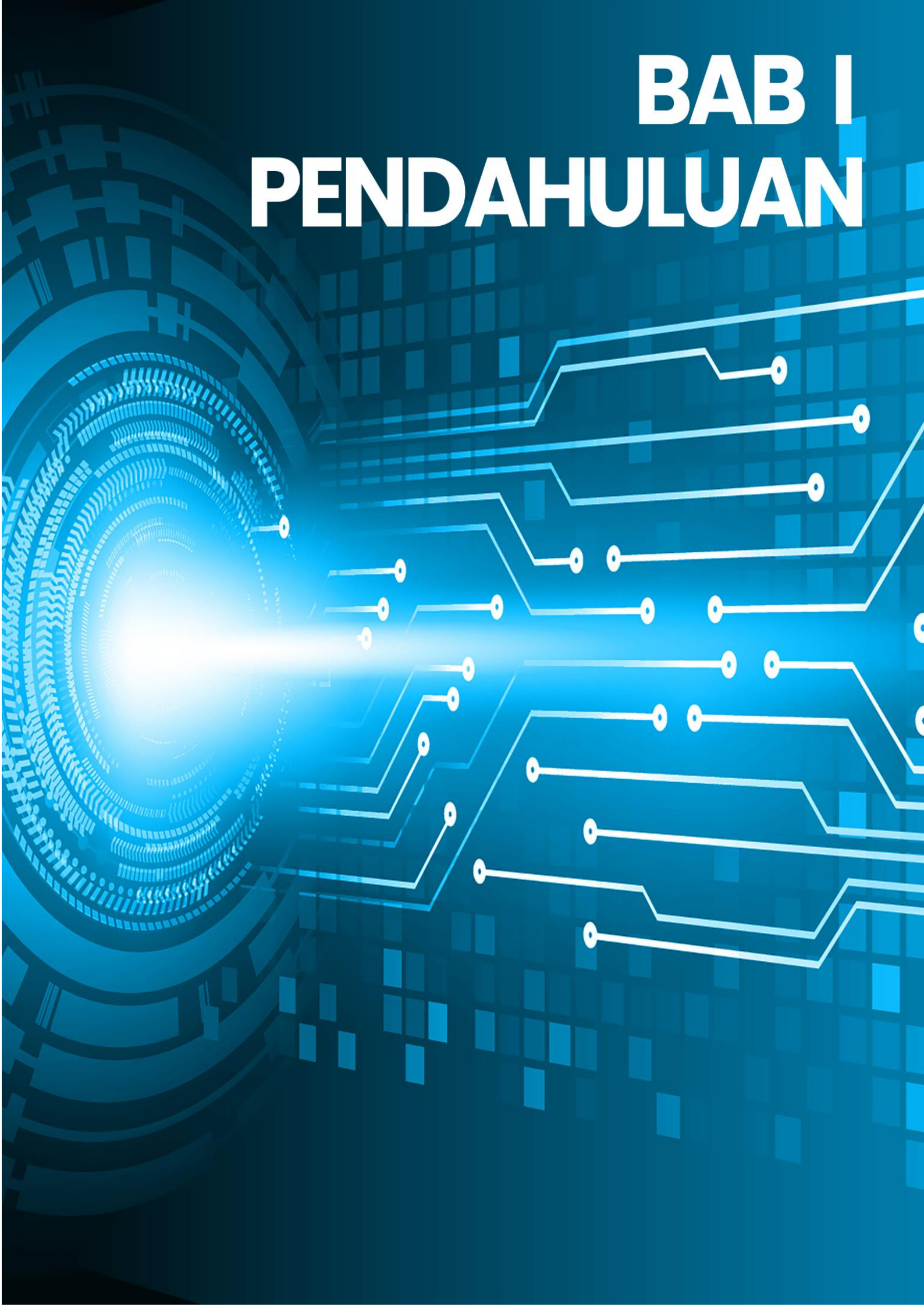
DAFTAR TABEL

Tabel 3.1 Basis pilihan Bob dan outcome pengukuran Bob.	28
Tabel 3.2 Cara kerja Protokol B92.	33
Tabel 3.3 Cara kerja protokol SARG04	34



BAB I

PENDAHULUAN



BAB I

PENDAHULUAN

Bab ini memberikan gambaran umum untuk memahami dokumen Pengenalan Kriptografi Kuantum (*Quantum Cryptography*). Bab ini terdiri atas 4 (empat) subbab yang membahas tentang ruang lingkup dokumen, target audiens, rujukan, dan sistematika penyusunan dokumen untuk memudahkan pemahaman.

A. RUANG LINGKUP

Kriptografi klasik dan kriptografi kuantum merupakan dua pendekatan yang sangat berbeda dalam menjaga keamanan data, namun keduanya saling melengkapi dalam menghadapi tantangan perlindungan informasi di dunia digital. Kriptografi klasik mengandalkan algoritma matematis untuk mengenkripsi dan mendekripsi informasi, dan selama ini terbukti efektif untuk berbagai aplikasi. Namun, kekuatan enkripsi klasik semakin terancam oleh kemajuan teknologi komputasi, khususnya komputasi kuantum yang berpotensi memecahkan algoritma klasik dengan efisiensi yang lebih tinggi dibandingkan komputer konvensional.

Untuk menjawab tantangan tersebut, dikembangkan teknologi komunikasi aman pascakuantum (*post-quantum secure communication technologies*) yang dapat diterapkan melalui kriptografi pascakuantum (*post-quantum cryptography* (PQC)), kriptografi kuantum seperti distribusi kunci kuantum (*quantum key distribution* (QKD)), maupun kombinasi keduanya. PQC berfokus pada pengembangan algoritma matematis baru yang tahan terhadap serangan komputasi kuantum, namun tetap kompatibel dengan infrastruktur digital yang ada. Sementara itu, QKD memanfaatkan sifat – sifat unik partikel kuantum, seperti superposisi dan keterjeratan (*entanglement*) untuk menjamin keamanan distribusi kunci secara fisik serta mendeteksi adanya penyadapan.

Dengan demikian, PQC menyediakan solusi praktis dan implementatif untuk masa transisi menuju era kuantum, sedangkan QKD memberikan lapisan keamanan tambahan berbasis hukum fisika. Keduanya dapat diimplementasikan secara terpisah maupun bersamaan, sehingga membentuk sistem komunikasi berlapis yang memperkuat ketahanan keamanan informasi terhadap ancaman komputasi kuantum di masa depan. Dokumen ini memberikan penjelasan tentang:

1. Pengantar dan Konsep Dasar

Berisi informasi singkat mengenai kriptografi klasik, kriptografi kuantum, perbedaan antara kriptografi klasik dengan kriptografi kuantum khususnya QKD. Selain itu dokumen ini juga menjelaskan mengenai prinsip dasar komputasi kuantum yang menjadi dasar keamanan dalam QKD yaitu quantum bit (*qubit*), superposisi, *entanglement*, dan prinsip ketidakpastian (*uncertainty principles*).

2. Protokol QKD

Protokol QKD yang dijelaskan dalam dokumen ini terbagi dalam 3 (tiga) kategori, yaitu protokol QKD berbasis foton tunggal, protokol QKD berbasis keadaan koheren lemah dan protokol QKD berbasis foton yang saling terjerat (*entangled photon*).

3. Tren modern dalam jaringan QKD

Bagian ini akan menjelaskan gambaran penerapan QKD saat ini dalam jaringan 5G dan *repeater* kuantum.

B. TARGET AUDIENS

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

1. Para pengambil kebijakan yang berwenang menetapkan kebijakan keamanan siber dan sandi pada organisasinya untuk mendukung

kebijakan keamanan siber dan sandi nasional dan memastikan keamanan informasi dalam organisasi;

2. Para pihak yang terlibat dalam perumusan kebijakan keamanan siber dan sandi khususnya kebijakan terkait pertukaran kunci kriptografi yang menggunakan teknologi kuantum agar kebijakan yang dirumuskan selaras dengan perkembangan QKD;
3. Para profesional/praktisi keamanan siber dan sandi yang terlibat dalam pengembangan, penerapan, dan pemeliharaan sistem elektronik yang akan menerapkan QKD dalam pertukaran kunci kriptografi yang digunakan dalam sistem elektroniknya untuk memastikan sistem elektronik yang dikelola memenuhi standar keamanan yang berlaku internasional;
4. Para penyedia layanan dan/atau produk keamanan teknologi informasi yang memiliki kerja sama dengan para penyelenggara sistem elektronik dalam pengembangan sistem elektronik untuk memastikan layanan dan/atau produk telah sesuai dengan standar keamanan yang berlaku internasional.

C. RUJUKAN

Penyusunan dokumen ini mengacu pada beberapa rujukan, di antaranya:

1. ETSI GR QKD 007 V.1.1.1 *Quantum Key Distribution (QKD): Vocabulary*;
2. *Quantum Key Distribution Networks A Quality of Service Perspective*;
3. *Multi-photon Quantum Secure Communication*.

D. SISTEMATIKA PENYUSUNAN DOKUMEN

Untuk selanjutnya, dokumen ini disusun sebagai berikut:

BAB II. PENGANTAR DAN KONSEP DASAR

Bab ini berisi tentang kriptografi kuantum dan QKD dan prinsip dasar informasi kuantum.

BAB III. PROTOKOL QKD

Bab ini berisi informasi tentang 3 (tiga) kategori, yaitu protokol QKD berbasis foton tunggal, protokol QKD berbasis keadaan koheren lemah, dan protokol QKD berbasis *entangled photon*.

BAB IV. TREN MODERN DALAM JARINGAN QKD

Bab ini berisi tentang gambaran penerapan QKD saat ini dalam jaringan 5G dan *repeater* kuantum.

BAB V. PENUTUP

Bab ini berisi tentang simpulan dari seluruh isi dokumen.



The background is a deep blue field filled with a complex network of glowing, translucent blue lines that intersect to form a web-like pattern. A bright, circular light source is positioned in the center, emitting a strong glow and creating a lens flare effect. Numerous small, white, dust-like particles are scattered throughout the scene, particularly concentrated around the central light and the intersecting lines.

BAB II

PENGANTAR DAN

KONSEP DASAR

BAB II

PENGANTAR DAN KONSEP DASAR

Bab ini membahas tentang konsep dasar tentang kriptografi kuantum dan QKD, penerapan QKD di berbagai bidang, tantangan implementasi QKD, serta prinsip dasar informasi kuantum. Prinsip dasar ini menjadi landasan awal dalam memahami teknologi kuantum.

A. KRIPTOGRAFI KUANTUM DAN *QUANTUM KEY DISTRIBUTION* (QKD)

Kriptografi adalah studi untuk menjaga kerahasiaan informasi dengan metode dan teknik matematika yang berhubungan dengan aspek keamanan informasi seperti kerahasiaan, integritas data, autentikasi entitas, dan autentikasi asal data [1]. [2]. Sejarah kriptografi telah dimulai sejak ribuan tahun yang lalu, dimulai dari algoritma kriptografi sederhana seperti sistem Caesar pada masa Kekaisaran Romawi, hingga berkembang menjadi algoritma kriptografi berbasis matematika kompleks pada era digital. Seiring dengan kemajuan teknologi informasi, kriptografi telah menjadi komponen kunci dalam keamanan siber modern.

Sebagian besar sistem modern saat ini mengandalkan penggunaan kriptografi simetris dan asimetris secara bersamaan. Kriptografi simetris, seperti *Advanced Encryption Standard* (AES), menggunakan satu kunci yang sama untuk proses enkripsi dan dekripsi, dan dikenal karena efisiensinya dalam menangani data dalam jumlah besar. Namun, kelemahannya terletak pada proses distribusi kunci. Untuk mengatasi hal ini, kriptografi asimetris -seperti Rivest-Shamir-Adleman (RSA) dan Algoritma Diffie-Hellman digunakan dalam tahap awal komunikasi untuk mendistribusikan kunci secara aman. Kriptografi publik ini bergantung pada keberadaan fungsi satu arah, yaitu fungsi matematika yang mudah dihitung namun sangat sulit untuk dihitung terbalik tanpa informasi tambahan tertentu. Oleh karena itu, keamanan sistem-sistem ini sangat bergantung pada asumsi bahwa

fungsi satu arah tersebut benar-benar sulit untuk dihitung terbalik, meskipun hingga kini belum ada bukti matematis formal yang menjamin kekuatan fungsi-fungsi tersebut.

Secara khusus, perkembangan teknologi komputer kuantum membawa ancaman serius, karena algoritma kuantum seperti Shor's Algorithm mampu melakukan faktorisasi bilangan prima besar secara efisien, sehingga dapat melemahkan atau bahkan memecahkan skema enkripsi asimetris yang selama ini dianggap aman. Dengan demikian, teknik kriptografi konvensional yang digunakan saat ini masih memiliki kerentanan. Lebih jauh lagi, teknik kriptanalisis yang muncul di masa depan dapat diterapkan secara retroaktif, sehingga berpotensi membahayakan semua komunikasi dan data yang sebelumnya telah dianggap aman.

Fisika kuantum atau yang bisa juga disebut mekanika kuantum, telah membantu mengubah lanskap kriptografi dalam dua dekade terakhir, yaitu melalui pengenalan aplikasi mekanika kuantum untuk kriptografi yang kemudian disebut sebagai kriptografi kuantum. Berbeda dengan pendekatan konvensional yang bergantung pada kompleksitas matematika, kriptografi kuantum merupakan sistem kriptografi yang didasarkan pada prinsip-prinsip dasar fisika kuantum, seperti superposisi dan *entanglement*, untuk menyediakan transfer data yang aman secara mutlak (*unconditionally secure*) sampai saat ini.

Fisika kuantum adalah teori fundamental dalam fisika yang memberikan dasar untuk memahami sifat fisik alam pada tingkat atom dan subatomik [3]. IBM telah mendefinisikan kriptografi kuantum sebagai metode keamanan siber yang memanfaatkan prinsip-prinsip dasar dari mekanika kuantum (seperti superposisi dan *entanglement*) untuk mengenkripsi dan mengirimkan data secara aman [4]. Atas hal tersebut, maka dapat disimpulkan bahwa Kriptografi Kuantum adalah cabang kriptografi yang memanfaatkan prinsip-prinsip mekanika kuantum, seperti superposisi dan *entanglement*, untuk membangun

sistem kriptografi yang aman secara fundamental dan mengatasi keterbatasan kriptografi klasik. Salah satu aplikasi dari kriptografi kuantum adalah QKD, yang memungkinkan dua pihak untuk menghasilkan dan berbagi kunci enkripsi secara aman, bahkan jika ada penyadap di saluran komunikasi.

QKD adalah prosedur atau metode untuk menghasilkan dan mendistribusikan kunci kriptografi simetris dengan keamanan informasi teoretis berdasarkan teori informasi kuantum [5]. QKD merupakan sebuah metode revolusioner dalam bidang keamanan komunikasi data. Berbeda dengan metode kriptografi klasik yang bergantung pada kerumitan algoritma matematika, QKD memanfaatkan prinsip – prinsip fisika kuantum untuk mendistribusikan kunci kriptografi secara aman. Kunci ini kemudian digunakan untuk mengenkripsi dan mendekripsi data, sehingga komunikasi menjadi sangat sulit untuk disadap. QKD menyediakan kemampuan untuk mendeteksi keberadaan penyadap dengan memanfaatkan hukum kuantum yaitu *anti-cloning* [6].

QKD menggunakan serangkaian protokol yang memungkinkan pengembangan kunci rahasia awal, yang hanya diketahui oleh dua pihak yang terlibat dalam komunikasi, menjadi kunci yang lebih besar. Dengan asumsi yang wajar, kebocoran informasi ke dunia luar dari bit-bit yang baru dibuat dapat dibatasi seketat mungkin, sehingga menyediakan mekanisme untuk membuat kunci simetris dengan aman [7].

Dalam era digital saat ini, keamanan data menjadi semakin krusial. Serangan siber semakin canggih dan mengancam privasi serta integritas informasi. Berikut adalah beberapa alasan yang menjadikan QKD sebagai solusi yang sangat menjanjikan, yaitu:

1. QKD menawarkan tingkat keamanan yang jauh lebih tinggi dibandingkan dengan metode enkripsi klasik, sehingga ideal untuk melindungi data yang sangat sensitif.

QKD memanfaatkan prinsip ketidakpastian Heisenberg yang menyatakan bahwa kita tidak dapat mengukur semua sifat partikel kuantum secara simultan dengan akurasi yang tinggi. Setiap upaya untuk mengukur (*measure*) atau menyalin informasi kuantum akan mengubah keadaan kuantum itu sendiri, sehingga perubahan ini dapat terdeteksi oleh pengirim dan penerima.

2. QKD menawarkan perlindungan terhadap ancaman perkembangan komputer kuantum yang berpotensi untuk memecahkan kriptografi klasik saat ini
3. Kunci yang dihasilkan oleh QKD hanya digunakan sekali, sehingga tidak dapat digunakan kembali oleh penyerang.

Kunci yang dihasilkan oleh QKD bersifat sekali pakai (*one-time pad*). Setelah digunakan untuk mengenkripsi pesan, kunci tersebut dibuang dan digantikan dengan kunci baru. Hal ini membuat sistem sangat aman, karena bahkan jika kunci berhasil disadap, informasi yang diperoleh tidak dapat digunakan untuk memecahkan pesan lain

4. Setiap upaya penyadapan dapat langsung terdeteksi karena proses penyadapan dapat mengganggu keadaan kuantum partikel (*quantum state*).

Jika ada pihak ketiga yang mencoba menyadap komunikasi, tindakan ini akan mengganggu keadaan kuantum foton, sehingga *quantum state* kolaps dan dapat terdeteksi oleh Alice dan Bob.

5. QKD dapat diterapkan pada berbagai skala, mulai dari jaringan kecil hingga jaringan yang sangat besar.

Dalam konteks yang lebih luas, QKD berperan penting dalam melindungi data sensitif seperti transaksi keuangan, komunikasi pemerintah, dan data pribadi.

Berikut adalah contoh penerapan QKD yaitu:

1. Perbankan dan Keuangan:
 - a. QKD dapat digunakan untuk mengamankan transaksi keuangan Online, seperti transfer uang dan pembayaran Online. Dengan QKD, informasi sensitif seperti nomor kartu kredit dan data pribadi pelanggan akan terenkripsi dengan sangat kuat, sehingga sulit bagi penyerang untuk mengaksesnya.
 - b. QKD dapat mengamankan komunikasi antara lembaga keuangan dan bursa saham, memastikan integritas data perdagangan, dan mencegah manipulasi pasar.
2. Pemerintah dan Militer
 - a. Pemerintah dan militer sering kali perlu berkomunikasi secara rahasia, terutama dalam hal intelijen dan operasi militer. QKD dapat memastikan bahwa komunikasi yang dilakukan tetap aman dan tidak dapat disadap oleh pihak yang tidak berwenang.
 - b. QKD dapat digunakan untuk mengamankan infrastruktur kritis seperti jaringan listrik, komunikasi, dan transportasi. Ini akan mencegah serangan siber yang dapat menyebabkan gangguan yang luas.
3. Kesehatan
 - a. Rekam medis elektronik mengandung informasi sensitif tentang pasien. QKD dapat mengamankan data ini, sehingga mencegah kebocoran informasi medis yang dapat membahayakan privasi pasien.
 - b. QKD dapat mengamankan komunikasi antara dokter dan pasien, terutama saat dilakukan melalui telekonferensi.

4. Akademisi dan Penelitian Ilmiah

- a. Laboratorium nasional sering kali melakukan penelitian yang bersifat rahasia. QKD dapat mengamankan komunikasi antara para peneliti dan melindungi hasil penelitian mereka.
- b. QKD dapat memfasilitasi kolaborasi ilmiah internasional yang aman, terutama dalam bidang-bidang seperti fisika partikel dan astronomi.

5. *Virtual Private Network* (VPN) Kuantum

- a. VPN kuantum menggunakan QKD untuk mengamankan koneksi jarak jauh, memungkinkan pengguna untuk mengakses jaringan pribadi secara aman dari mana saja.
- b. VPN kuantum dapat melindungi data perusahaan yang sensitif dari serangan siber.

Walaupun menawarkan tingkat keamanan yang belum pernah terjadi sebelumnya, implementasi dan operasional QKD menghadapi beberapa tantangan signifikan, di antaranya:

1. Jarak dan Infrastruktur

Salah satu batasan utama dari QKD adalah jarak efektif distribusi kunci. Pada jarak beberapa ratus kilometer, efisiensi transmisi melalui serat optik mulai berkurang, yang mengakibatkan penurunan kinerja. Selain itu, infrastruktur yang diperlukan untuk QKD, termasuk sumber foton tunggal dan detektor foton sangat sensitif, umumnya mahal dan memerlukan teknologi canggih. Memperluas cakupan jaringan QKD akan memerlukan investasi besar-besaran dalam infrastruktur ini dan solusi inovatif untuk meningkatkan jangkauan transmisi.

2. Integrasi dengan Teknologi Saat Ini

Integrasi QKD dengan sistem jaringan yang ada merupakan tantangan teknis. Kompatibilitas dengan infrastruktur komunikasi

yang ada memerlukan pengembangan perangkat keras khusus yang bisa memfasilitasi distribusi kunci kuantum tanpa mengganggu operasi jaringan konvensional. Selain itu, skala besar penerapan QKD membutuhkan penyesuaian besar pada protokol jaringan dan mungkin menimbulkan masalah logistik dan teknis.

3. Laju (*rate*) dan Efisiensi

Rate dalam distribusi kunci oleh QKD cenderung lebih rendah dibandingkan dengan metode distribusi kunci klasik. Hal ini bisa menjadi penghambat dalam situasi yang memerlukan pertukaran kunci yang sangat banyak. Sumber daya yang diperlukan untuk menjaga keamanan kuantum juga bisa mengurangi efisiensi transmisi data, mengingat kebutuhan untuk frekuensi pertukaran kunci yang tinggi untuk menjaga keamanan komunikasi.

4. Ancaman Keamanan

Meskipun QKD secara teoretis tahan terhadap banyak serangan, implementasi nyata QKD mungkin memiliki celah keamanan yang bisa dimanfaatkan oleh pihak berbahaya. Misalnya, perangkat keras seperti detektor atau sumber foton dapat diserang, memungkinkan pihak ketiga untuk mendapatkan informasi tentang kunci. Kemajuan di bidang komputasi kuantum juga berpotensi mengembangkan teknik baru yang dapat mengancam keamanan sistem QKD.

5. Regulasi dan Standardisasi

Penerapan QKD di tingkat global akan membutuhkan pengembangan regulasi dan standardisasi yang jelas. Hal ini termasuk protokol keamanan, spesifikasi teknis, dan kesepakatan internasional mengenai penggunaan QKD. Standardisasi akan membantu memastikan keamanan, keandalan, dan kompatibilitas sistem QKD dengan berbagai infrastruktur teknologi dan regulasi di berbagai negara.

Dengan mengatasi tantangan-tantangan ini, QKD dapat memainkan peran penting dalam memperkuat keamanan informasi global. Namun, kerja sama internasional yang luas, inovasi teknologi, dan kesiapan untuk investasi dalam penelitian serta pengembangan infrastruktur baru akan diperlukan.

B. PRINSIP DASAR INFORMASI KUANTUM

Untuk memahami prinsip dan penerapan kriptografi kuantum khususnya QKD, pembaca harus terlebih dahulu memiliki pemahaman dasar tentang konsep dan fenomena dasar dalam mekanika kuantum. Pembahasan lengkap mengenai mekanika kuantum berada di luar cakupan bab ini. Bab ini membahas beberapa gagasan utama yang penting untuk memahami kriptografi kuantum.

Mekanika kuantum adalah cabang Fisika yang mempelajari perilaku materi pada tingkat atom dan sub-atom. Prinsip-prinsip unik dalam mekanika kuantum inilah yang menjadi dasar keamanan dalam QKD. Berikut adalah beberapa konsep kunci yang mendasari QKD:

1. *Quantum Bit (Qubit)*

Qubit atau bit kuantum merupakan unit dasar informasi dalam komputasi kuantum. *Qubit* merupakan satuan informasi kuantum, yang digambarkan oleh vektor keadaan dalam sistem mekanika kuantum dua tingkat, yang secara formal setara dengan ruang vektor dua dimensi pada bilangan kompleks [5]. Berbeda dengan bit klasik yang hanya dapat memiliki nilai 0 atau 1 pada satu waktu, *qubit* dapat berada dalam superposisi kuantum dari kedua keadaan tersebut secara simultan, sehingga dapat merepresentasikan 0, 1, atau kombinasi linear dari keduanya dalam satu waktu. Selain superposisi, *qubit* juga dapat terjerat (*entangled*) dengan *qubit* lainnya, menciptakan korelasi kuantum sehingga memungkinkan *qubit* yang terhubung untuk saling mempengaruhi secara instan, terlepas dari jarak yang memisahkannya.

Qubit ini dapat dicontohkan dengan kejadian perputaran koin. Pada perputaran ini akan terdapat kondisi saat koin berada dalam superposisi untuk keadaan Gambar atau Angka. Begitu kita mengukur (*measure*) dengan cara memegangnya, koin akan kolaps menuju salah satu keadaan saja (Gambar saja atau Angka saja). Dalam QKD, *qubit* dapat direalisasikan dengan polarisasi foton. Foton dapat terpolarisasi secara horizontal $|0\rangle$ atau vertikal $|1\rangle$, atau dalam superposisi antara kedua polarisasi tersebut.

2. Superposisi

Superposisi adalah kemampuan suatu sistem kuantum untuk berada dalam beberapa keadaan sekaligus sampai dilakukannya proses berikutnya termasuk pengukuran. Superposisi dapat dicontohkan melalui fenomena saat sebuah partikel kuantum seperti elektron atau foton berada dalam dua keadaan, misalnya $|0\rangle$ dan $|1\rangle$. Menurut prinsip superposisi, partikel tersebut dapat berada dalam kombinasi linear antara kedua keadaan ini sampai dilakukannya pengukuran. Dalam konteks ini, $|0\rangle$ dan $|1\rangle$ merepresentasikan dua keadaan dasar (*basis states*) dari suatu sistem kuantum, seperti spin elektron (atas/bawah) atau polarisasi foton (vertikal/horizontal).

Eksperimen celah ganda (*double slit experiment*) adalah salah satu eksperimen paling terkenal yang menggambarkan prinsip superposisi. Dalam eksperimen ini, sebuah partikel (seperti elektron atau foton) dilewatkan melalui dua celah kecil, dan kemudian detektor digunakan untuk mengamati pola yang dihasilkan di layar.

Hasilnya adalah:

- a. Tanpa Pengamatan: Ketika tidak ada pengamatan untuk menentukan melalui celah mana partikel melewati, partikel tampak melewati kedua celah sekaligus dan menciptakan pola interferensi di layar detektor, yang merupakan bukti dari superposisi kuantum dan menunjukkan bahwa kuantum memiliki sifat gelombang.

- b. Dengan Pengamatan: Namun, ketika pengamatan dilakukan untuk melihat melalui celah mana partikel melewati, pola interferensi menghilang, dan partikel hanya melewati satu celah tertentu dan menunjukkan bahwa kuantum memiliki sifat partikel.

Eksperimen ini menunjukkan bahwa hingga diukur, partikel dapat berada dalam superposisi dari melewati kedua celah sekaligus. Namun, pengukuran memaksa partikel untuk "memilih" satu jalur, yang disebut "keruntuhan fungsi gelombang" (*wave function collapse*).

Dalam mekanika kuantum, keadaan suatu sistem fisik direpresentasikan oleh vektor di dalam ruang Hilbert. Prinsip superposisi menyatakan bahwa jika $|\psi_1\rangle$ dan $|\psi_2\rangle$ adalah dua keadaan kuantum yang mungkin dari sistem tersebut, maka setiap keadaan yang mungkin dari sistem $|\psi\rangle$ dapat diwakili sebagai kombinasi linear antara kedua keadaan ini:

$$|\psi\rangle = \alpha |\psi_1\rangle + \beta |\psi_2\rangle$$

dengan:

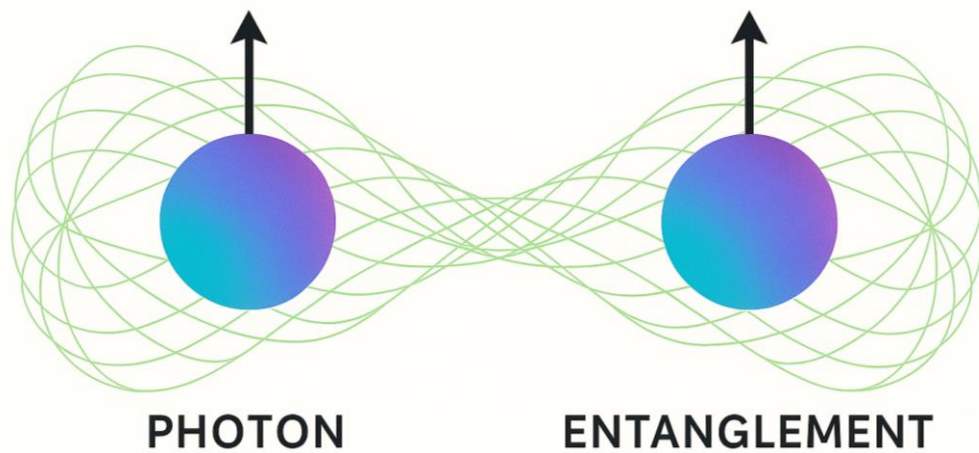
α dan β adalah amplitude yang bernilai bilangan real atau kompleks dan memenuhi $\alpha^2 + \beta^2 = 1$.

$|\alpha|^2$ dan $|\beta|^2$ mewakili probabilitas relatif untuk menemukan sistem dalam keadaan $|\psi_1\rangle$ atau $|\psi_2\rangle$ jika dilakukan pengukuran pada basis $\{|\psi_1\rangle, |\psi_2\rangle\}$.

3. Keterjeratan (*Entanglement*)

Entanglement dalam QKD merupakan sifat sistem mekanika kuantum yang menunjukkan korelasi antara dua sistem fisik yang tidak dapat dijelaskan oleh Fisika klasik [5]. *Entanglement* adalah fenomena kuantum saat dua atau lebih partikel saling terikat sedemikian rupa sehingga keadaan kuantum satu partikel sangat bergantung pada keadaan kuantum partikel lainnya, bahkan jika

partikel-partikel ini dipisahkan oleh jarak yang sangat jauh. Gambar 2.1 menunjukkan contoh *entanglement* foton.



Gambar 2.1 Contoh *entanglement* suatu foton dibuat menggunakan AI.

Keunggulan penggunaan *entanglement* dalam QKD adalah jaminan keamanan yang sangat kuat terhadap serangan oleh komputer klasik maupun kuantum, karena keamanan ini berdasarkan pada sifat-sifat dasar dari mekanika kuantum. Dengan adanya prinsip *entanglement* ini, penyadap juga dapat dideteksi dengan mudah. Hal ini dikarenakan apabila seorang penyadap akan mengambil informasi yang sedang dikomunikasikan pada suatu partikel kuantum, hal ini akan memengaruhi partikel kuantum yang lain, sehingga pengirim atau penerima akan lebih mudah mendeteksi adanya penyadapan.

4. Prinsip Ketidakpastian (*Uncertainty Principle*)

Prinsip ketidakpastian menyatakan bahwa kita tidak dapat mengetahui secara pasti nilai sepasang variabel Fisika komplementer, seperti posisi dan momentum, secara bersamaan. Semakin akurat kita mengukur satu variabel, semakin tidak akurat pengukuran kita terhadap variabel lainnya. Prinsip ini memastikan bahwa setiap upaya untuk mengukur sifat kuantum dari sebuah partikel akan mengganggu keadaan kuantum partikel tersebut. Hal

ini membuat sangat sulit bagi pihak ketiga untuk menyadap jalur komunikasi kuantum tanpa terdeteksi.

5. Teorema anti-cloning (*No-Cloning Theorem*)

Teorema anti-cloning (*No-Cloning Theorem*) adalah sebuah prinsip dasar dalam mekanika kuantum yang menyatakan bahwa: *“Tidak mungkin membuat salinan sempurna dari suatu keadaan kuantum yang tidak diketahui secara umum.”*[9]. Dengan kata lain, jika memiliki sebuah *qubit* dalam suatu keadaan yang tidak diketahui, maka tidak ada proses fisik yang bisa menggandakan (*copy*) keadaan tersebut tanpa mengubah atau merusaknya. Jika ada suatu keadaan kuantum $|\psi\rangle$, maka tidak ada operator unitari U yang bisa melakukan:

$$U(|\psi\rangle \otimes |e\rangle) = |\psi\rangle \otimes |\psi\rangle$$

untuk semua $|\psi\rangle$.

Karena sifat kuantum yang linear, proses penyalinan universal akan menghasilkan konflik ketika superposisi hadir.

Teorema ini dapat digunakan pada:

- Perlindungan alami terhadap pencurian informasi. Hal ini karena *qubit* tidak bisa digandakan yang menyebabkan data kuantum sulit untuk disadap tanpa diketahui.
- Dasar keamanan komunikasi kuantum. Hal ini digunakan dalam implementasi protokol QKD.
- Membatasi bagaimana informasi kuantum diproses, dikirim, dan diamankan.

Berikut adalah prinsip ketidakpastian Heisenberg yang mendasari QKD:

- a. Dalam QKD, foton (partikel cahaya) digunakan sebagai *Qubit*. Polarisasi foton (arah getaran medan listrik) dapat mewakili $|0\rangle$ atau $|1\rangle$.
- b. Ketika foton dikirimkan, polarisasinya berada dalam superposisi hingga diukur oleh penerima. Proses pengukuran akan menyebabkan superposisi runtuh ke salah satu keadaan yang mungkin.
- c. Meskipun tidak secara langsung digunakan dalam Protokol QKD BB84, konsep *entanglement* memiliki implikasi penting dalam pengembangan protokol QKD lainnya.
- d. Setiap upaya untuk mengukur sifat kuantum dari foton yang membawa informasi kunci akan mengganggu keadaan foton tersebut, sehingga gangguan ini dapat terdeteksi oleh pengirim dan penerima.

Contoh penerapan prinsip ketidakpastian dalam QKD yaitu:

- a. Alice (pengirim) mengirimkan foton dengan polarisasi yang dipilih secara acak (horizontal atau vertikal).
- b. Bob (penerima) juga memilih basis pengukuran secara acak. Jika Bob memilih basis yang sama dengan Alice, ia akan mendapatkan hasil pengukuran yang benar. Namun, jika basis yang dipilih berbeda, hasil pengukuran Bob tidak pakai.

Jika ada penyadap yang mencoba mengukur foton sebelum mencapai Bob, ia akan mengubah polarisasi foton tersebut, sehingga ketika Bob melakukan pengukuran, hasilnya akan berbeda dengan yang diharapkan. Hal ini akan terdeteksi oleh Alice dan Bob ketika mereka membandingkan hasil pengukuran mereka.

Keunikan mekanika kuantum berpotensi meningkatkan berbagai aplikasi inovatif di berbagai bidang. Selain QKD, berikut ini adalah beberapa aplikasi lain dari mekanika kuantum:

1. Komputasi Kuantum (*Quantum Computing*)

Komputer kuantum memiliki potensi untuk menyelesaikan masalah tertentu jauh lebih cepat daripada komputer klasik. Algoritma seperti Shor dan Grover, masing-masing, memungkinkan pemecahan masalah faktorisasi bilangan prima dan pencarian data dalam *database* besar secara efisien. Komputer kuantum juga dapat digunakan untuk menyimulasikan sistem molekuler dengan akurasi tinggi, yang berpotensi merevolusi pengembangan obat dan bahan baru. Google memiliki komputer kuantum yang dapat menyelesaikan tugas tertentu dalam waktu yang jauh lebih singkat daripada superkomputer klasik.

2. Sensor Kuantum (*Quantum Sensing*)

Sensor kuantum dapat mendeteksi sinyal yang sangat lemah, seperti medan magnet yang sangat kecil atau perubahan gravitasi yang sangat halus. Aplikasi sensor kuantum adalah navigasi presisi tinggi, pencitraan medis, dan deteksi materi gelap (*dark matter*).

3. Kriptografi Pasca-kuantum (*Post Quantum Cryptography*)

Algoritma kriptografi pasca-kuantum didasarkan pada prinsip-prinsip mekanika kuantum dan dirancang untuk tahan terhadap serangan dari komputer kuantum. *National Institute of Standards and Technology* (NIST) sedang mengembangkan standar baru untuk kriptografi pasca-kuantum.

4. *Mikroskop Elektron Transmisi* (TEM)

TEM memanfaatkan sifat gelombang dari elektron untuk menghasilkan gambar dengan resolusi sangat tinggi, memungkinkan kita melihat struktur atom dan molekul. TEM digunakan secara luas

dalam penelitian material untuk mempelajari struktur kristal, cacat, dan sifat elektronik material.

5. Laser

Prinsip dasar laser didasarkan pada konsep transisi elektronik dalam atom. Laser digunakan dalam berbagai bidang, mulai dari komunikasi optik hingga pembedahan.

6. Semikonduktor

Pemahaman tentang sifat kuantum elektron dalam semikonduktor memungkinkan pengembangan transistor dan sirkuit terpadu yang menjadi dasar dari semua perangkat elektronik modern. Diode, transistor, dan cip komputer semuanya memanfaatkan prinsip-prinsip mekanika kuantum.

7. Jam Atom

Jam atom memanfaatkan transisi energi dalam atom untuk mencapai akurasi waktu yang sangat tinggi. Jam atom digunakan sebagai standar waktu internasional.

Mekanika kuantum memiliki potensi besar untuk merevolusi berbagai bidang teknologi dan ilmu pengetahuan di masa depan. Berikut adalah beberapa area potensial mekanika kuantum:

1. Komunikasi Kuantum

Komunikasi kuantum menggunakan prinsip-prinsip kuantum seperti *entanglement* untuk menciptakan saluran komunikasi yang aman dan hampir tidak mungkin untuk disadap sebagai contoh adalah kuantum Internet yaitu jaringan global yang memungkinkan komunikasi dan komputasi kuantum di seluruh dunia. kuantum internet dapat membuka peluang untuk komunikasi aman dan berbagi sumber daya kuantum jarak jauh. Penelitian terkini telah menunjukkan kemampuan untuk mendistribusikan kunci enkripsi rahasia melalui satelit dengan jarak ribuan kilometer, serta

membangun jaringan prototipe yang menghubungkan berbagai kota. Kemajuan signifikan juga telah dicapai dalam pengembangan *repeater* kuantum untuk memperluas jangkauan jaringan. Meskipun masih menghadapi berbagai tantangan teknis, internet kuantum diproyeksikan akan merevolusi dunia digital dan mentransformasi berbagai aspek kehidupan manusia.

2. Material dan Kimia Kuantum

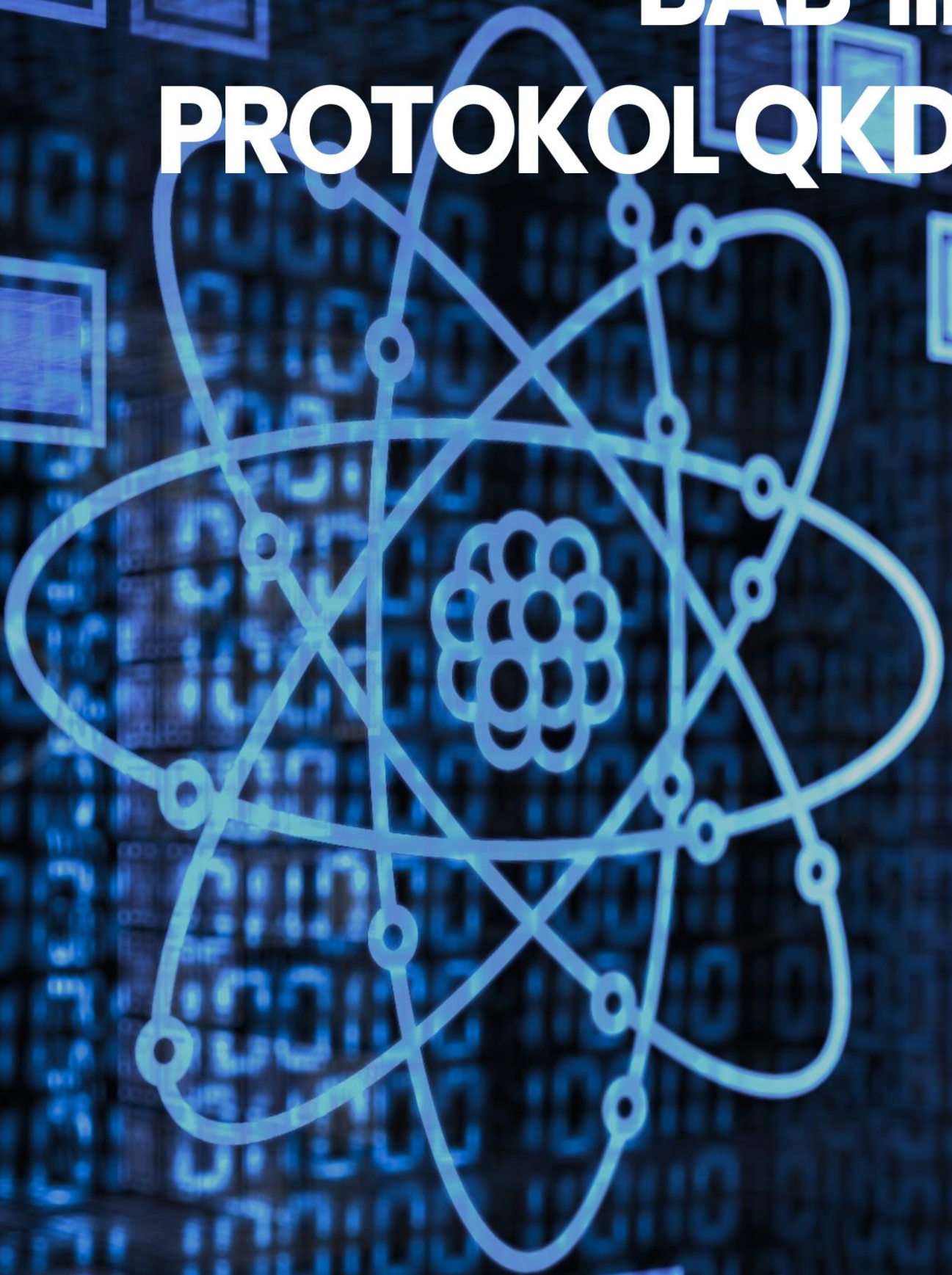
Material dan kimia kuantum adalah bidang yang berkembang pesat dengan potensi luar biasa untuk merevolusi teknologi di masa depan. Saat ini, para ilmuwan telah berhasil menciptakan material kuantum dengan sifat-sifat unik seperti superkonduktivitas pada suhu tinggi dan kemampuan untuk memanipulasi cahaya dengan presisi yang belum pernah terjadi sebelumnya. Di bidang kimia kuantum, simulasi molekul yang canggih memungkinkan prediksi reaksi kimia dan desain obat yang lebih akurat dan efisien. Di masa depan, material dan kimia kuantum diprediksi akan membawa inovasi revolusioner seperti :

- a. Baterai dengan kapasitas dan daya tahan jauh lebih tinggi: Bayangkan ponsel yang dapat diisi daya dalam hitungan detik dan bertahan selama berminggu-minggu.
- b. Panel surya dengan efisiensi energi yang luar biasa: Memanfaatkan energi matahari secara maksimal untuk sumber energi bersih dan berkelanjutan.
- c. Obat-obatan yang dirancang khusus untuk setiap individu: Pengobatan yang lebih tepat sasaran dan efektif untuk berbagai penyakit.

Material baru yang lebih kuat, ringan, dan tahan lama: Membuka kemungkinan baru dalam konstruksi, transportasi, dan berbagai industri lainnya.

BAB III

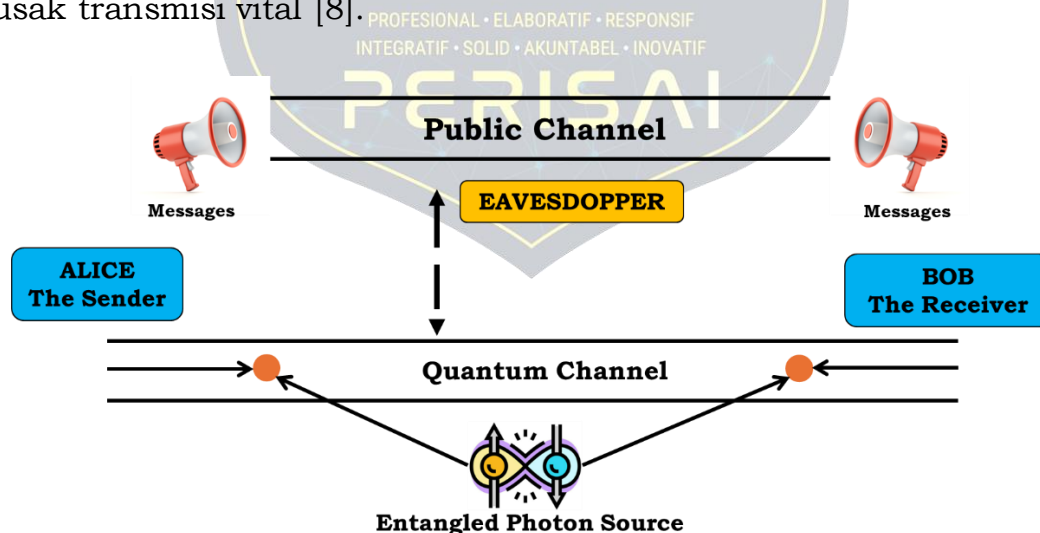
PROTOKOL QKD



BAB III PROTOKOL QKD

Salah satu aplikasi kriptografi kuantum adalah QKD. QKD memanfaatkan hukum-hukum fisika kuantum untuk menjamin transfer informasi yang aman secara mutlak dari pengirim (Alice) ke penerima (Bob). Melalui QKD, Alice dan Bob dapat berbagi kunci rahasia acak yang dapat digunakan untuk keperluan enkripsi dan autentikasi. Berbeda dengan kriptografi klasik yang bergantung pada kompleksitas komputasi, QKD menawarkan tingkat keamanan tanpa syarat (*unconditional security*) terhadap penyadap apa pun, bahkan yang memiliki daya komputasi tak terbatas.

Ide dasar di balik QKD adalah untuk mengkodekan bit kunci kriptografi dalam keadaan kuantum foton dan mengirimkannya melalui saluran optik, seperti kabel serat optik atau tautan ruang bebas. Dengan mempersiapkan dan mengukur foton ini dengan hati-hati dalam keadaan kuantum tertentu, Alice dan Bob dapat menghasilkan kunci acak bersama sekaligus mendeteksi segala upaya oleh penyadap (biasanya disebut Eve) untuk mencegat atau merusak transmisi vital [8].



Gambar 3.1 Konsep dasar protokol QKD berbasis *entanglement* digambar ulang dari [9].

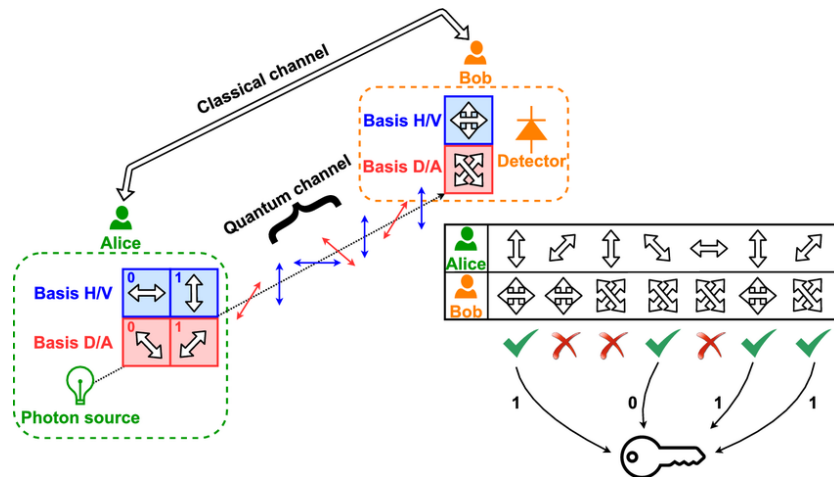
Berikut ini adalah penjelasan singkat beberapa protokol QKD yang terbagi dalam 3 (tiga) kategori [10] yaitu protokol QKD berbasis foton tunggal, protokol QKD berbasis keadaan koheren lemah dan protokol QKD berbasis *entangled photon*. Ilustrasi konsep dasar protokol QKD berbasis *entangled photon* ditunjukkan pada Gambar 3.1.

A. PROTOKOL QKD BERBASIS FOTON TUNGGAL

Berikut ini adalah penjelasan singkat mengenai 2 (dua) buah protokol QKD berbasis foton tunggal yaitu Protokol BB84 dan Protokol B92.

1. Protokol BB84

Protokol BB84 adalah salah satu protokol QKD yang diusulkan dan didemonstrasikan secara eksperimental pada tahun 1984 [11]. Protokol ini diberi nama berdasarkan nama penemunya yaitu Charles H. Bennett dan Gilles Brassard dan merupakan protokol QKD pertama [12] yang paling banyak digunakan karena kesederhanaan dan jaminan keamanannya. Landasan yang digunakan dalam protokol ini adalah prinsip ketidakpastian fisika kuantum. Ketika informasi dikodekan dalam state kuantum non-ortogonal seperti foton tunggal dengan arah polarisasi 0° , 45° , 90° , dan 135° maka penyadap tidak dapat memperoleh informasi parsial tentang informasi tersebut tanpa mengubahnya secara acak dan cara yang tidak dapat dikontrol, sehingga kemungkinan besar akan terdeteksi oleh pengguna yang sah [11]. Gambar 3.2 menunjukkan ilustrasi Protokol BB84.



Gambar 3.2 Protokol BB84
digambar ulang dari [13].

Langkah-langkah dasar Protokol BB84 [8]:

- Alice menghasilkan barisan bit acak dan untuk setiap bit secara acak memilih satu dari dua basis (baik basis komputasional $\{|0\rangle, |1\rangle\}$ atau basis Hadamard $\{|+\rangle, |-\rangle\}$) untuk mengodekannya. Kemudian, Alice menyiapkan foton dalam status kuantum yang sesuai dan mengirimkannya ke Bob melalui saluran kuantum.
- Untuk setiap foton yang diterimanya, Bob secara acak memilih satu dari dua basis untuk mengukurnya dan mencatat hasilnya, yaitu bit 0 atau 1.
- Setelah semua foton dikirim dan diterima, Alice dan Bob secara terbuka membandingkan pilihan basis mereka melalui saluran klasik yang diautentikasi. Mereka membuang bit apa pun yang pilihan basisnya tidak cocok, sehingga menyisakan kunci bersama yang telah tersaring.
- Untuk memeriksa penyadapan, Alice dan Bob secara acak memilih sebagian bit vital yang tersaring dan membandingkan nilai-nilainya. Jika tingkat kesalahan di bawah ambang batas tertentu, mereka dapat yakin bahwa tidak ada penyadapan yang

terjadi dan dapat menggunakan bit kunci tersaring yang tersisa sebagai kunci rahasia untuk mengenkripsi komunikasi mereka.

Keamanan protokol BB84 bergantung pada fakta bahwa setiap upaya Eve untuk mencegat dan mengukur foton tentu akan menimbulkan kesalahan yang dapat dideteksi dalam kunci tersebut karena teorema tanpa kloning (*no-cloning theorem*) dan prinsip ketidakpastian mekanika kuantum.

Secara khusus, jika Eve mencoba mengukur foton pada satu basis dan kemudian mengirimkannya kembali ke Bob, ada peluang 50% Bob akan memilih basis lain untuk mengukurnya, yang menghasilkan hasil acak dan peluang kesalahan sebesar 25%. Demikian pula, jika Eve mencoba membagi foton dan mengukurnya di kedua basis secara bersamaan, keadaan yang dihasilkan akan menjadi campuran dari kedua keadaan basis, yang sekali lagi akan menimbulkan kesalahan.

Dengan menganalisis tingkat kesalahan pada kunci yang tersaring secara cermat, Alice dan Bob dapat mengikat jumlah informasi yang dapat diperoleh Eve tentang kunci tersebut dan, jika perlu, melakukan langkah-langkah amplifikasi privasi tambahan (*additional privacy amplification*) untuk mengurangi informasi Eve ke tingkat yang sangat kecil.

Berikut ini adalah contoh perhitungan protokol BB84:

- a. Alice dan Bob diasumsikan dapat mengirim sinyal cahaya satu sama lain melalui optik luar angkasa atau tautan serat optik.
- b. Keduanya mempunyai sumber photon-tunggal yang dapat memproduksi photon-photon dalam berbagai state polarisasi ($\uparrow, \leftrightarrow, \cup, \cap$ atau $|0\rangle, |1\rangle, |+\rangle, |-\rangle$) dan alat pengukuran foton independen dengan basis X dan Z.

c. Hal-hal yang mungkin dilakukan Alice, berlaku juga untuk Bob. Jadi hanya perlu mempertimbangkan kasus Alice mentransmisikan foton ke Bob.

d. Alice misalnya membangkitkan barisan bit acak 16 bit

1010 0011 1010 0011

e. Selanjutnya Alice menyiapkan barisan 16 photon yang dipolarisasi secara acak dengan pilihan aturan sebagai berikut:

1) untuk bit 1, Alice menggunakan polarisasi acak $\uparrow = |0\rangle$ atau $\cap = |+\rangle$,

2) untuk bit 0, Alice menggunakan polarisasi acak $\leftrightarrow = |1\rangle$ atau $\cup = |-\rangle$.

f. Secara konsisten dengan barisan bit dan aturan peilihan-acak di atas, persiapan yang dilakukan Alice menghasilkan barisan photon-terpolarisasi sebagai berikut:

$\uparrow \leftrightarrow \cap \cup \leftrightarrow \leftrightarrow \cap \uparrow \uparrow \cap \leftrightarrow \cup \cup \cap \uparrow$

g. Bob menerima barisan photon dan membuat 16 pengukuran yang berkaitan berdasarkan pilihan acak basis X dan Z miliknya.

h. Tabel 3.1 menunjukkan basis pilihan Bob dan outcome setiap pengukuran Bob

Tabel 3.1 Basis pilihan Bob dan outcome pengukuran Bob.

Barisan bit Alice	1010	0011	1010	0011
Barisan state photon Alice	$\uparrow \leftrightarrow \cap \cup$	$\leftrightarrow \leftrightarrow \cap \uparrow$	$\uparrow \cup \cap \leftrightarrow$	$\cup \cup \cap \uparrow$
Outcome pengukuran Bob (nilai eigen)	+1+1-1-1	+1-1+1+1	-1-1+1+1	-1-1-1+1
Outcome pengukuran Bob (bit)	1100	1011	0011	0001

- i. Pengukuran nilai eigen $+1$ dinamakan informasi bit 1. Pengukuran -1 dinamakan informasi bit 0. Nilai Eigen didapatkan dengan " $\langle \psi|Z|\psi \rangle$ " atau " $\langle \psi|X|\psi \rangle$ ". Gerbang X dinyatakan dengan $X = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}$, sedangkan gerbang Z dengan $Z = \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}$.
- j. Tabel 3.1 menunjukkan pilihan acak Bob dari pengukuran basis X dan Z dapat “benar” atau “salah”. Pilihan basis yang benar berhubungan dengan pengukuran $\uparrow, \leftrightarrow$ dengan Z dan $\cup, \cap$ dengan X.
- k. Lakukan perbandingan antara baris paling atas dengan baris paling bawah, terlihat bahwa pilihan benar memberikan Bob bit-bit informasi yang selalu benar dengan barisan awal Alice.
- l. Pada kasus pilihan basis salah, bit informasi bon secara inheren acak dan tidak berkorelasi dengan barisan Alice.
- m. Langkah Bob selanjutnya adalah mengkomunikasikan dengan Alice menggunakan jaringan publik seperti telepon atau email tentang barisan basis-pengukuran
- ZXZX XZZX XZXX XXZZ
- n. Alice kemudian menggunakan jaringan publik sama untuk memberi Bob jawabannya dalam bentuk:
- Yes No No. Yes No Yes No oNo No Yes No YesYesNoYes
- o. Jawaban ini menginformasikan Bob untuk mengetahui mana pengukurannya yang bisa dipakai atau tidak bisa. Bit-bit invalid harus dibuang sebagai:

$$1--0/-0--/--1-/00-1 \equiv 1001001$$

- p. Ini merupakan kunci rahasia untuk mengenkripsi dan mendekripsi pesan melalui jaringan publik yang digunakan oleh Alice dan Bob.

Berikut contoh kode program Python menggunakan Pustaka Qiskit untuk mensimulasikan Protokol BB84.

```
#Bagian ini menginstal Pustaka Qiskit yang diperlukan dan
mengimpor modul-modul yang dibutuhkan untuk membuat dan
mensimulasikan sirkuit kuantum.
!pip install qiskit=="0.45.1" matplotlib pylatexenc qiskit-
aer=="0.14.0.1"
from qiskit import QuantumCircuit , Aer, execute
from qiskit.visualization import plot_histogram
import numpy as np

# Alice membangkitkan barisan acak 16 bit.
n =16
alice_bits = np.random.randint(2 , size=n)

# Alice mempersiapkan barisan 16 photon dengan polarisasi acak
# Alice memilih basis acak untuk masing-masing bit (0 untuk
basis Z dan 1 untuk basis X)
alice_bases = np.random.randint (2 , size=n)

# Membuat sirkuit kuantum
qc = QuantumCircuit(n, n)

# Circuit dengan n qubit dan n bit klasik
for i in range(n):
    # Mengatur keadaan awal sesuai dengan bit acak Alice
    if alice_bits[i] == '1':
        qc.x(i)
    # Terapkan gerbang Hadamard jika basis yang dipilih adalah
    X
```

```

    if alice_bases[i] == 1:
        qc.h(i)

#Bob secara acak memilih basis pengukurannya (0 untuk basis Z,
1 untuk basis X)
bob_bases= np.random.randint(2, size=n)

#Bob mengukur qubit dengan basis pilihannya
for i in range (n):
    if bob_bases [i] == 1:
        # Terapkan gerbang Hadamard jika basis Bob adalah X
        qc.h(i)
        # Mengukur qubit
        qc.measure(i, i)

#Ekseskusi sirkuit menggunakan simulator kuantum
backend = Aer.get_backend('qasm_simulator')
result = execute (qc, backend, shots=1).result()
counts = result.get_counts (qc)
# Dapatkan bitstring yang diukur dari Bob
measured_bits= list(counts.keys())[0]
#Bandingkan basis Alice dan Bob untuk menentukan kunci bersama
shared_key= []
for i in range (n):
    # Simpan bit ketika basisnya cocok
    if alice_bases [i] == bob_bases [i]:
        shared_key.append (int(measured_bits[i]))

#Menampilkan hasil
print (f"Alice's bits: {''.join(str (b) for b in alice_bits)}")
print (f"Alice's bases: {''.join(str (b) for b in
alice_bases)}")
print (f"Bob's bases: {''.join(str (b) for b in bob_bases)}")
print (f"Bob's measured bits: {measured_bits}")

```

```
print (f"Sharedkey: {''.join(str (b) for b in shared_key)}")
```

2. Protokol B92

Penjelasan mengenai Protokol B92 diambil dari makalah yang disusun oleh Maria E. Sabani, dkk [14]. Pada tahun 1992 Charles Bennett memperkenalkan protokol distribusi kunci kuantum baru, yang dinamai berdasarkan nama belakangnya dan tahun penerbitannya [15]. Protokol ini pada dasarnya merupakan varian dari Protokol BB84, dengan perbedaan utama bahwa B92 menggunakan dua state polarisasi, bukan empat state seperti yang digunakan dalam Protokol BB84. Protokol ini merupakan protokol dengan dua state kuantum non-ortogonal yang dengan arsitekturnya, penyadap dapat dideteksi.

B92 adalah skema QKD yang menggunakan foton terpolarisasi untuk komunikasi dua pihak, Alice dan Bob, melalui dua saluran. Satu saluran publik klasik, tempat pengguna yang curang dapat memiliki akses dan satu saluran kuantum. Seperti BB84, protokol B92 memiliki dua fase, transmisi kuantum yang terjadi ke dalam saluran kuantum, dan fase kedua yang terjadi ke dalam saluran klasik.

Langkah-langkah protokol B92 dijelaskan di bawah ini.

- Alice memilih *string* bit $a = (a_1, \dots, a_n)$ dan mengkodekan setiap nilai bit $a_i, i \in \{1, \dots, n\}$, 0 sebagai $|0\rangle$ dan 1 sebagai $|+\rangle = \frac{|0\rangle + |1\rangle}{\sqrt{2}}$.
- Alice mengirimkan *qubit*-nya ke Bob. Bob menghasilkan string bit $b = (b_1, \dots, b_n)$ dan memilih basis $\oplus$ untuk $b_i = 0$ dan basis $\otimes$ untuk $b_i = 1$.
- Bob mengukur hasilnya dan hasil ini membentuk bit string lain s . Jika Bob memperoleh hasil -1 maka bit s adalah $s_i = 0$, dan jika Bob memperoleh hasil +1 maka $s_i = 1$.

- d. Melalui saluran publik Bob menginformasikan s dan menjaga b tetap rahasia.
- e. Alice dan Bob hanya memilihi pasangan bit $[a_i, b_i]$ untuk $s_i = 1$.

Berikut adalah contoh cara kerja Protokol B92:

Tabel 3.2 Cara kerja Protokol B92.

Bit yang dikirim Alice a_i	0	0	0	0	1	1	1	1
Polarisasi basis Alice	$ 0\rangle$	$ 0\rangle$	$ 0\rangle$	$ 0\rangle$	$ 1\rangle$	$ 1\rangle$	$ 1\rangle$	$ 1\rangle$
Bit yang dipilih oleh Bob b_i	0	0	1	1	0	0	1	1
Basis Bob	$\oplus$	$\oplus$	$\otimes$	$\otimes$	$\oplus$	$\oplus$	$\otimes$	$\otimes$
Hasil pengukuran Bob	$ 0\rangle$	$ 1\rangle$	$ +\rangle$	$ -\rangle$	$ 0\rangle$	$ 1\rangle$	$ +\rangle$	$ -\rangle$
Nilai s	0	-	0	1	0	1	0	-

B. PROTOKOL QKD BERBASIS KEADAAN KOHEREN LEMAH

1. Protokol SARG04 [10]

Protokol SARG04 [Scarani, V., Acín, A., Ribordy, G., & Gisin, N. (2004). Quantum cryptography protocols robust against photon number splitting attacks for weak laser pulse implementations. *Physical Review Letters*, 92, 057901], yang diberi nama berdasarkan nama para penemunya yaitu Scarani, Acín, Ribordy dan Gisin, dirancang untuk lebih tahan terhadap serangan *photon-number-splitting* (PNS). Protokol ini didasarkan pada pengamatan bahwa protokol BB84 menjadi tidak aman terhadap serangan PNS ketika penyadap (Eve) dapat menyimpan satu foton. Dalam kasus tersebut, Eve hanya perlu membedakan antara dua *eigenstate* dari operator Hermitian yang telah diketahui setelah fase penyaringan (*sifting phase*). Untuk mengatasi hal ini, SARG04 bekerja dengan mengodekan bit klasik ke dalam pasangan keadaan yang tidak ortogonal, yang tidak dapat dibedakan secara deterministik. Hal ini mirip dengan pendekatan dalam protokol B92. Contoh cara kerja protokol SARG04 ditunjukkan pada Tabel 3.3.

Tabel 3.3 Cara kerja protokol SARG04

Langkah	Alice	Transmisi	Bob
1	Barisan bit x_A	1 1 0 0 1 0 1 0 1	
	Barisan bit y_A untuk basis	1 0 0 0 0 1 1 1 1	
2	Basis persiapan	✕++++✕✕✕✕	
	Barisan Qubit		
4		1 1 0 1 0 0 1 1 0	Barisan bit y_B untuk basis
		✕✕+✕+++✕✕+	Basis pengukuran
		1 1 0 1 1 1 1 0 1	Nilai bit yang diukur
6	Pencocokan hasil ($x_A = x_B?$)	✓✓✓✕✓✓✓✓	Pencocokan hasil ($x_A = x_B?$)
7	<i>Sifted key</i> y'_A	- - - 0 - 1 - - -	<i>Sifted key</i> $y'_A = y'_B$

Dalam implementasinya, SARG04 memodifikasi BB84 dengan mengodekan setiap bit ke dalam basis, bukan ke dalam keadaan. Pada langkah ke-5 dari BB84, alih-alih mengungkapkan basis yang digunakan Alice, Bob justru mengungkapkan hasil pengukurannya x_B . Jika basis yang digunakan Alice sama dengan basis pengukuran Bob, maka Bob akan memperoleh nilai bit yang benar. Namun, jika basisnya berbeda, terdapat kemungkinan 50% bahwa hasil pengukuran Bob salah. Oleh karena itu, pada langkah ke-6, Alice

memeriksa bit hasil pengukuran Bob x_B yang berbeda dengan data bit miliknya x_A , dan memberi tahu Bob untuk hanya menyimpan data tersebut. Data tersebut merepresentasikan anti-korelasi antara urutan bit yang mengodekan basis persiapan Alice y_A dan basis pengukuran Bob y_B . Bob hanya perlu melakukan negasi pada urutan bit y_B . Langkah-langkah lainnya dalam protokol ini tetap sama seperti BB84.

Protokol SARG04 pada dasarnya menggabungkan konsep dari BB84 dan B92, dan meningkatkan keamanan terhadap serangan PNS dengan memanfaatkan fakta bahwa Eve hanya dapat memperoleh informasi penuh dari pulsa yang mengandung lebih dari dua foton. Ambang atenuasi kritis (*critical attenuation*) δ_c kini ditentukan oleh probabilitas tiga foton p_3 , bukan dua foton p_2 seperti dalam BB84. Dengan demikian, SARG04 terbukti lebih tangguh terhadap serangan PNS dan dapat memperpanjang jarak aman transmisi dari sekitar 50 km (BB84) menjadi sekitar 100 km dalam kondisi tanpa kesalahan. Selain itu, penggunaan *decoy states* (keadaan umpan) juga dapat ditambahkan untuk memperoleh informasi tambahan mengenai potensi serangan dari Eve.

2. Protokol *Coherent One Way* (COW) [10]

Protokol *Coherent One-Way* (COW) memanfaatkan koherensi fasa antara pulsa-pulsa berturutan untuk memantau karakteristik saluran kuantum ketika digunakan pulsa koheren lemah. Dalam protokol ini, Alice menghasilkan pulsa dengan rata-rata jumlah foton μ yang dipisahkan oleh interval waktu tetap τ . Dengan menggunakan modulator intensitas, Alice dapat menciptakan pulsa kosong (sebagai sinyal berhenti) atau pulsa berisi (sebagai sinyal jalan).

Bit logika ke- k dikodekan ke dalam urutan dua pulsa, yang terdiri dari kombinasi antara pulsa kosong dan berisi dengan menggunakan persamaan berikut:

$$|0_A\rangle = |\sqrt{\mu}\rangle_{2k-1} |0\rangle_{2k}$$

$$|1_A\rangle = |0\rangle_{2k} |\sqrt{\mu}\rangle_{2k-1}$$

dengan $|\sqrt{\mu}\rangle$ adalah state koheren dengan amplitudo $\sqrt{\mu}$ dan $|0\rangle$ adalah state vakum tanpa foton. Catat bahwa $|0_A\rangle$ dan $|1_A\rangle$ tidak ortogonal.

Meskipun keadaan kuantum yang digunakan untuk mewakili bit 0 dan bit 1 tidak ortogonal, keduanya tetap dapat dibedakan secara optimal dengan mengukur waktu kedatangan pulsa.

Untuk memantau kondisi saluran, Alice juga menyisipkan sejumlah kecil urutan *decoy* (umpan) di antara dua bit logika. Karena laser dalam protokol ini menggunakan mode yang terkunci, terdapat koherensi fasa antara setiap dua pulsa tak kosong, yang penting untuk deteksi upaya penyadapan. Jika penyadap (Eve) mencoba membaca saluran, koherensi fasa ini akan terganggu dan dapat dideteksi oleh penerima (Bob).

Pada Gambar 3.3 terlihat di sisi Bob, pulsa-pulsa dibagi menjadi dua jalur: (1) dikirim ke detektor D_B (jalur data) dan (2) dipantulkan ke dalam interferometer yang terdiri dari detektor D_{M1} dan D_{M2} (jalur pemantauan). Pada jalur data, D_B mengukur intensitas pulsa dan dapat membedakan antara bit logika dan *decoy*. Pada jalur pemantauan, ketika kedua pulsa pada waktu k dan $k+1$ tidak kosong, hanya D_{M1} yang akan aktif pada waktu $k+1$. Jika Eve mengganggu koherensi dengan membaca saluran, dia dapat terdeteksi melalui pemicuannya pada D_{M2} untuk kejadian tersebut.

Dengan mempertimbangkan tiga pulsa paling kanan pada Gambar 2.3, deteksi upaya Eve dapat dijelaskan sebagai berikut: jika Eve menyerang secara koheren di antara pemisahan bit (pulsanya 2 dan 3), maka dia akan merusak koherensi urutan *decoy* (pulsanya 1 dan 2); jika dia menyerang secara koheren dalam setiap bit (pulsanya 1 dan 2), maka koherensi akan rusak di pemisahan (pulsanya 2 dan

3). Eve dapat melakukan serangan koheren pada lebih banyak pulsa, namun dalam hal ini dia merusak koherensi pada lebih sedikit posisi dan mendapatkan informasi yang lebih sedikit.

Langkah-langkah dalam Protokol COW adalah sebagai berikut:

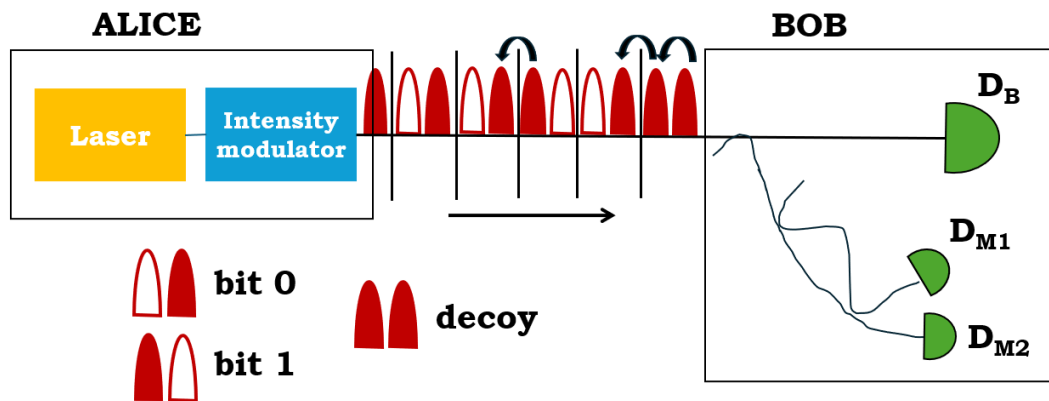
- a. Alice mengirimkan sejumlah besar pulsa. Sebagian besar pulsa ini mewakili bit logika 0 dan 1, sementara sebagian kecil mewakili *decoy*.
- b. Bob mengumumkan bahwa dia telah menerima *qubit* melalui saluran klasik publik. Selanjutnya, Alice mengungkapkan slot waktu $\{k_d\}$ yang sesuai dengan urutan *decoy*. Bob menghapus semua deteksi pada waktu $2k_d - 1$ dan $2k_d$, serta memeriksa apakah detektor D_{M2} pernah aktif pada waktu $2k_d$. Kemudian, Alice dan Bob dapat memperkirakan gangguan koherensi pada pulsa *decoy* dengan menghitung visibilitas

$$V = \frac{p(D_{M1}) - p(D_{M2})}{p(D_{M1}) + p(D_{M2})}$$

dengan $p(D_{Mj})$ adalah probabilitas deteksi di D_{Mj} pada saat hanya D_{M1} yang seharusnya menembak. Visibilitasnya harus satu jika Eve tidak menyerang.

- c. Untuk bit-bit yang tidak sesuai dengan urutan *decoy*, Bob mengungkapkan waktu $2k + 1$ yang mendeteksi sinyal pada D_{M2} . Alice memeriksa apakah salah satu dari deteksi tersebut sesuai dengan kejadian bit logika 0, yaitu urutan $|1\rangle_k |0\rangle_{k+1}$. Selanjutnya, Alice dan Bob dapat memperkirakan gangguan koherensi di sepanjang pemisahan bit.
- d. Berdasarkan langkah-langkah b dan c, Alice dan Bob dapat menghitung informasi yang mungkin telah bocor ke pihak Eve.
- e. Alice dan Bob melakukan koreksi kesalahan dan penguatan privasi untuk menghasilkan kunci rahasia akhir.

Visibilitas digunakan untuk menghitung informasi yang bocor ke Eve berdasarkan visibilitas dan tingkat kesalahan bit. Skematik Skematik Protokol COW ditunjukkan pada Gambar 3.3, dengan panah di atas pulsa pada gambar tersebut menunjukkan koherensi.



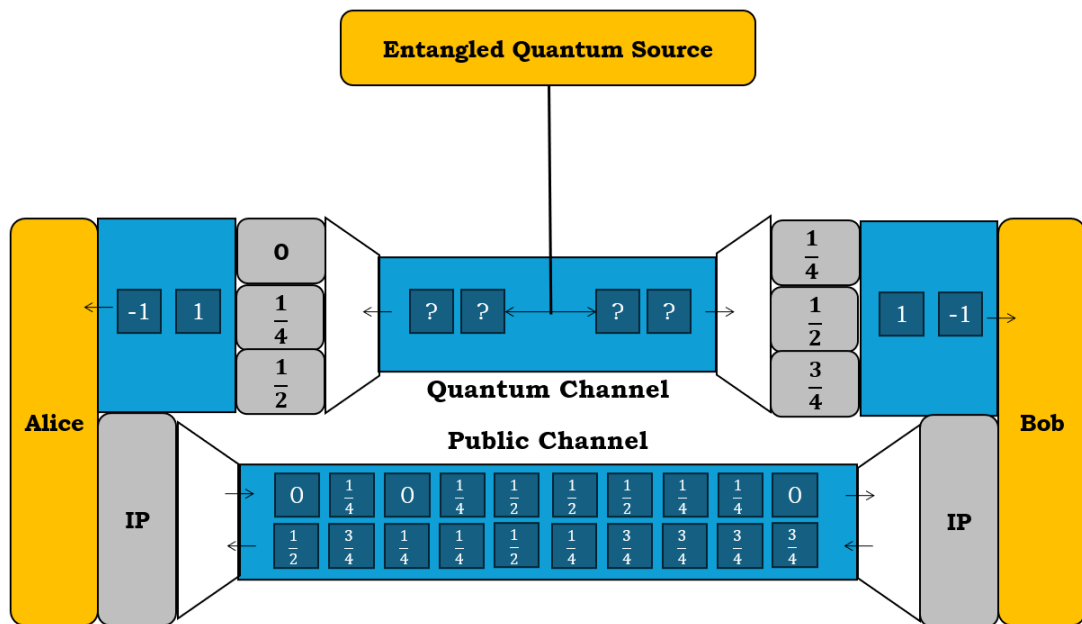
Gambar 3.3 Skematik Protokol COW digambar ulang dari [10].

C. PROTOKOL QKD BERBASIS FOTON YANG SALING TERJERAT

Protokol Ekert 91 (E91) yang diusulkan oleh Artur Ekert pada tahun 1991 adalah salah satu protokol QKD yang memanfaatkan fenomena kuantum yang dikenal sebagai *entanglement* atau keterjeratan kuantum.

1. Prinsip Dasar

Protokol E91 menggunakan pasangan foton yang *entangled* untuk membentuk dasar dari distribusi kunci kuantum. Dalam keadaan *entanglement*, dua foton yang dihasilkan memiliki keadaan kuantum yang saling terkait, sedemikian rupa sehingga pengukuran pada satu foton langsung mempengaruhi keadaan foton yang lain, bahkan jika mereka dipisahkan oleh jarak yang jauh. Prinsip dasar dari protokol E91 adalah bahwa dua partisipan (biasanya disebut Alice dan Bob) dapat menggunakan foton *entangled* untuk menghasilkan kunci kriptografi yang benar-benar acak dan identik, dengan keamanan yang dijamin oleh hukum mekanika kuantum. Ilustrasi Protokol E91 ditunjukkan pada Gambar 3.4.



Gambar 3.4 Protokol E91
digambar ulang dari [16].

2. Langkah – langkah Protokol E91

Berikut adalah langkah-langkah kerja Protokol E91 dalam distribusi kunci kuantum:

a. Persiapan Sumber *Entangled*

- 1) Sebuah sumber *entangled* (misalnya, kristal *nonlinier* yang memfasilitasi proses *down-conversion* para metrik spontan) menghasilkan pasangan foton yang terikat (*entangled*) dalam keadaan kuantum yang saling berlawanan. Sumber ini bisa berada di tempat netral atau di salah satu pihak, misalnya Alice.
- 2) Sumber foton *entangled* mengirimkan satu foton dari setiap pasangan kepada Alice dan foton pasangannya kepada Bob melalui kanal komunikasi yang aman (misalnya, serat optik).

b. Pemilihan Basis Pengukuran

1) Pemilihan Basis Acak

Alice dan Bob masing-masing memilih salah satu basis pengukuran mereka secara acak dari set basis pengukuran yang telah ditentukan sebelumnya untuk setiap foton yang mereka terima. Pada Protokol E91, basis pengukuran untuk setiap foton adalah sudut tertentu pada sumbu Bloch (misalnya, basis Z, X, dan Y). Alice memilih salah satu dari tiga basis pengukuran (A1, A2, A3). Bob memilih salah satu dari tiga basis pengukuran (B1, B2, B3).

2) Pengukuran Foton: Setelah memilih basis, Alice dan Bob mengukur polaritas foton yang mereka terima. Hasil pengukuran ini adalah bilangan biner (0 atau 1), tergantung pada keadaan polaritas foton.

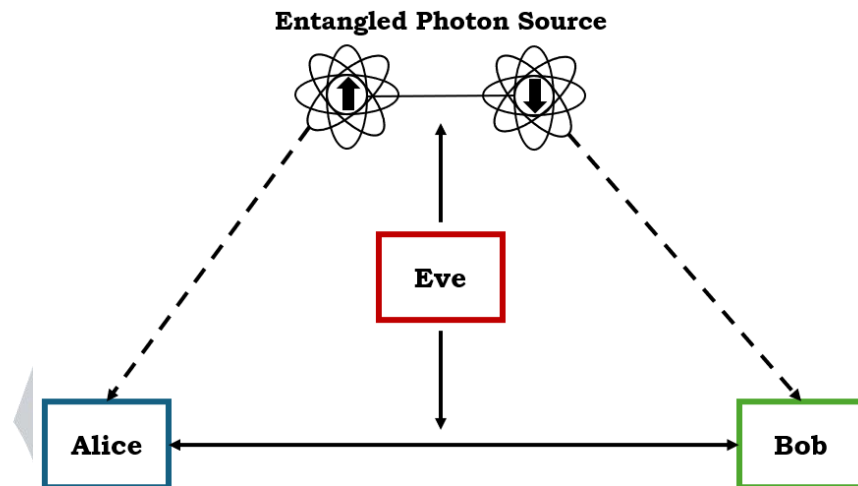
c. Pertukaran Informasi Klasik dan Pembentukan Kunci

1) Pertukaran Basis Pengukuran: Setelah pengukuran selesai, Alice dan Bob saling bertukar informasi melalui kanal klasik (seperti internet) mengenai basis yang mereka gunakan untuk setiap pengukuran, tetapi tidak mengungkapkan hasil pengukurannya.

2) Pembuangan Data yang Tidak Sesuai: Alice dan Bob kemudian membuang hasil pengukuran yang menggunakan basis yang berbeda, hanya menyimpan hasil pengukuran dengan basis pengukuran mereka cocok.

3) Pemeriksaan *Eavesdropping* (Penyadapan): Alice dan Bob menggunakan sebagian dari hasil pengukuran yang cocok untuk memeriksa keberadaan *eavesdropper* (penyadap) yang mungkin mengganggu kanal kuantum. Jika ada *eavesdropper* (misalnya, Eve) yang mencoba menyadap kanal, maka hukum mekanika kuantum akan menyebabkan ketidakcocokan dalam korelasi hasil pengukuran. Dengan

membandingkan sebagian dari data yang disimpan, Alice dan Bob dapat menghitung parameter Bell (*Bell inequality*). Jika hasil ini tidak sesuai dengan nilai yang diharapkan dari pasangan foton yang benar-benar *entangled*, maka mereka dapat mendeteksi adanya *eavesdropping* (Gambar 3.5).



Gambar 3.5 Konsep *eavesdropping*.

- 4) Pembentukan Kunci Akhir: Jika hasil pemeriksaan menunjukkan bahwa tidak ada penyadap yang mengganggu, Alice dan Bob menggunakan sisa data dari hasil pengukuran yang cocok untuk membentuk kunci kriptografi yang aman.

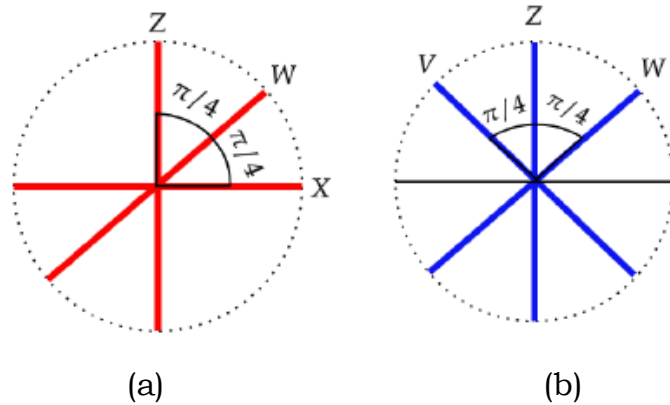
Berikut adalah contoh perhitungan protokol E91:

- 1) Alice memilih 9 basis pengukuran secara acak dari himpunan $\{A_i\}$ dimana dilakukan dengan cara mengukur sudut $\phi_a^i = \{0, \frac{1}{4}\pi, \frac{1}{2}\pi\}$ sebagaimana ditunjukkan pada Gambar 3.6 (a)

ZZWXZWXXW

- 2) Bob memilih 9 basis pengukuran secara acak dari himpunan $\{B_i\}$ dimana dilakukan dengan cara mengukur sudut $\phi_a^j = \{\frac{1}{4}\pi, \frac{1}{2}\pi, \frac{3}{4}\pi\}$ sebagaimana ditunjukkan pada Gambar 3.6 (b)

ZVWWWVZWV



Gambar 3.6 Contoh perhitungan Protokol E91.

- 3) Alice mengukur *qubit* pertama dan Bob mengukur dengan basis tersebut

$$P_{AB} = \langle \phi^+ | Z \otimes Z | \phi^+ \rangle = 1$$

$$\langle \phi^+ | Z \otimes Z | \phi^+ \rangle = 0,7071$$

$$|\phi\rangle_{AB} = \frac{Z \otimes Z |\phi^+\rangle}{\sqrt{P}} = \frac{1}{\sqrt{2}} (|00\rangle + |11\rangle)$$

$$|\phi\rangle_{AB} = \frac{Z \otimes V |\phi^+\rangle}{\sqrt{P}} = \begin{pmatrix} 0,5946 \\ 0,5946 \\ -0,5946 \\ 0,5946 \end{pmatrix}$$

- 4) Alice mengukur *qubit* pertama dan Bob mengukur dengan basis tersebut

$$E_{AB} = \langle \phi^+ | W \otimes W | \phi^+ \rangle = 0,9999$$

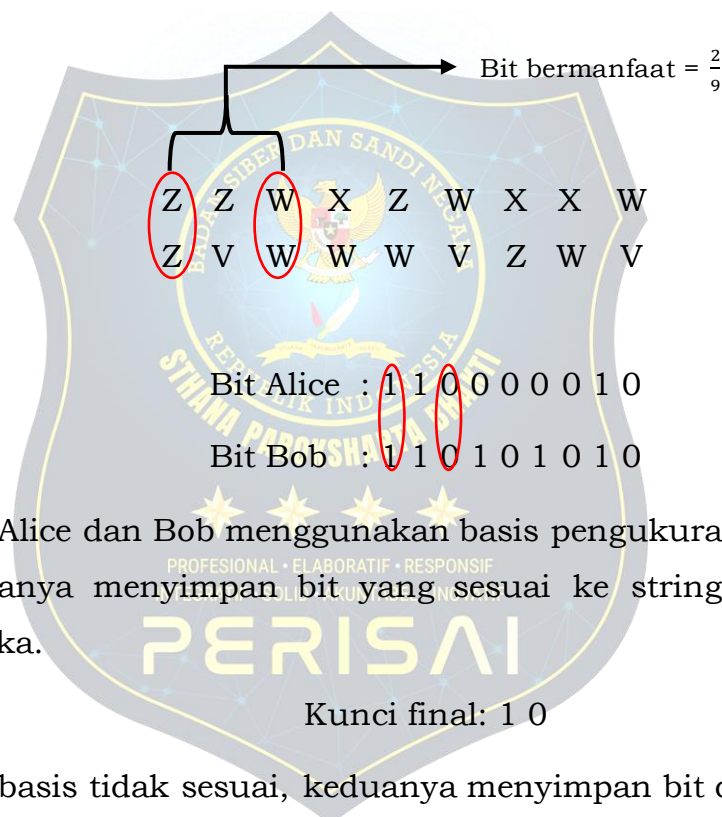
$$\langle \phi^+ | X \otimes W | \phi^+ \rangle = 0,3535$$

$$|\phi\rangle_{AB} = \frac{W \otimes W |\phi^+\rangle}{\sqrt{P}} = \frac{1}{\sqrt{2}} (|00\rangle + |11\rangle)$$

$$(|\phi\rangle_{AB})^2 = \frac{1}{2} (|00\rangle + |11\rangle)$$

$$|\phi\rangle_{AB} = \frac{X \otimes W |\phi^+\rangle}{\sqrt{P}} = \begin{pmatrix} 0,5946 \\ -0,5946 \\ 0,5946 \\ 0,5946 \end{pmatrix}$$

- 5) Alice dan Bob menyimpan informasi tentang dasar pengukuran yang Alice gunakan untuk setiap *qubit*.
- 6) Alice dan Bob mengumumkan arah yang mereka pilih untuk setiap pengukuran.
- 7) Untuk pasangan dengan arah yang sejajar, yaitu, pasangan (A1, B1) dan (A3, B3), mereka menghasilkan hasil yang sepenuhnya berkorelasi terbalik.
- 8) Alice dan Bob membandingkan basis pengukuran.



- 9) Jika Alice dan Bob menggunakan basis pengukuran yang sama, keduanya menyimpan bit yang sesuai ke string kunci akhir mereka.

Kunci final: 1 0

- 10) Jika basis tidak sesuai, keduanya menyimpan bit dan informasi yang sesuai tentang basis yang mereka gunakan dalam register terpisah.

Z X Z W X X W

V W W V Z W V

- 11) Untuk mendeteksi penyadapan, Alice dan Bob dapat menghitung uji statistik ketidaksetaraan CHSH, S , menggunakan nilai ekspektasi antara basis Alice dan Bob:

$$S = \langle Z \otimes W \rangle + \langle X \otimes W \rangle + \langle Z \otimes V \rangle - \langle X \otimes V \rangle$$

$$\langle A \otimes B \rangle = P(1,1) + P(0,0) - P(1,0) - P(0,1)$$

$$\rho_{AB} = \langle \phi^+ | Z \otimes W | \phi^+ \rangle = \frac{1}{\sqrt{2}}$$

$$\rho_{AB} = \langle \phi^+ | X \otimes W | \phi^+ \rangle = \frac{1}{\sqrt{2}}$$

$$\rho_{AB} = \langle \phi^+ | Z \otimes V | \phi^+ \rangle = \frac{1}{\sqrt{2}}$$

$$\rho_{AB} = \langle \phi^+ | X \otimes V | \phi^+ \rangle = \frac{1}{\sqrt{2}}$$

12) Dari perhitungan sebelumnya diperoleh $S = \frac{1}{\sqrt{2}} + \frac{1}{\sqrt{2}} + \frac{1}{\sqrt{2}} - \frac{1}{\sqrt{2}} = 2\sqrt{2}$

13) Dengan menggunakan ketidaksetaraan CSH $|S| \leq 2$. Karena $S \geq 2$ maka perhitungan melanggar ketidaksetaraan CSH.

14) Jika tidak melanggar ketidaksetaraan CSH, kunci final tidak digunakan untuk enkripsi dan dekripsi.

15) Jika melanggar ketidaksetaraan CSH, kunci final digunakan untuk enkripsi dan dekripsi melalui jaringan publik yang digunakan oleh Alice dan Bob. Kunci final tersebut 1 0.

Berikut adalah struktur pesan protokol E91

Sumber yang dapat dipercaya menghasilkan, misalnya, 9 pasangan partikel spin-1/2 dalam keadaan *singlet* atau terjerat dan mengirimkannya ke Alice dan Bob.

Basis pengukuran Alice	Z	Z	W	X	Z	W	X	X	W
Basis pengukuran Bob	Z	V	W	W	W	V	Z	W	V
Hasil pengukuran Alice	1	1	0	0	0	0	0	1	0
Hasil pengukuran Bob	1	1	0	1	0	1	0	1	0
Alice dan Bob bertukar basis									
Kunci final	1	0							

3. Kode Program Protokol E91

Berikut contoh kode program Python menggunakan Pustaka Qiskit yang menyimulasikan protokol E91 dan menguji ketidaksamaan CHSH (sebuah varian dari ketidaksamaan Bell).

```
#Bagian ini menginstal Pustaka Qiskit yang diperlukan
dan mengimpor modul-modul yang dibutuhkan untuk membuat
dan menyimulasikan sirkuit kuantum.
!pip install qiskit=="0.45.1" matplotlib pylatexenc
qiskit-aer=="0.14.0.1"
from qiskit import QuantumRegister, ClassicalRegister,
QuantumCircuit, execute, Aer
from random import randrange

# Persiapan dan Pengukuran : menyimulasikan 9 kali
proses pembuatan pasangan EPR (Einstein-Podolsky-Rosen)
dan pengukurannya.
basesAlice, keyAlice = [], []
basesBob, keyBob = [], []
# Alice menyiapkan 200 pasang EPR
for i in range(9):
    qreg = QuantumRegister(2)
    creg = ClassicalRegister(2)
    mycircuit = QuantumCircuit(qreg, creg)

    #membuat entanglement
    mycircuit.h(qreg[0])
    mycircuit.cx(qreg[0], qreg[1])

    #Alice memilih basis pengukuran
    choiceAlice=randrange(3)
    #pengukuran pada basis Z
    if choiceAlice==0:
        basesAlice.append('Z')
```

```

#pengukuran pada basis X
if choiceAlice==1:
    mycircuit.h(qreg[0])
    basesAlice.append('X')
#pengukuran pada basis W
if choiceAlice==2:
    mycircuit.s(qreg[0])
    mycircuit.h(qreg[0])
    mycircuit.t(qreg[0])
    mycircuit.h(qreg[0])
    basesAlice.append('W')

#Bob memilih basis pengukuran
choiceBob=randrange(3)
#pengukuran pada basis Z
if choiceBob==0:
    basesBob.append('Z')
#pengukuran pada basis W
if choiceBob==1:
    mycircuit.s(qreg[1])
    mycircuit.h(qreg[1])
    mycircuit.t(qreg[1])
    mycircuit.h(qreg[1])
    basesBob.append('W')
#pengukuran pada basis V
if choiceBob==2:
    mycircuit.s(qreg[1])
    mycircuit.h(qreg[1])
    mycircuit.tdg(qreg[1])
    mycircuit.h(qreg[1])
    basesBob.append('V')

#pengukuran final
mycircuit.measure(qreg, creg)

```

```

job
execute(mycircuit,Aer.get_backend('qasm_simulator'),shots=1)
counts = job.result().get_counts(mycircuit)

#menyimpan hasil
result=list(counts.keys())[0]
keyAlice.append(int(result[0]))
keyBob.append(int(result[1]))

#Kode ini membandingkan basis pengukuran Alice dan Bob.
Jika sama, bit kunci disimpan di finalKeyAlice dan finalKeyBob.
#Jika basis berbeda, data disimpan untuk perhitungan ketidaksamaan CHSH.
#Nilai S dihitung berdasarkan korelasi hasil pengukuran pada berbagai kombinasi basis.
#Jika abs(S) >= 2, ini mengindikasikan pelanggaran ketidaksamaan CHSH, yang menunjukkan adanya korelasi kuantum non-lokal.
finalKeyAlice, finalKeyBob = [], []
diffAlice, diffBob = [], []
diffBasesA, diffBasesB = [], []
for i in range(0, len(basesAlice)):
    if basesAlice[i] == basesBob[i]:
        finalKeyAlice.append(keyAlice[i])
        finalKeyBob.append(keyBob[i])
    else:
        diffAlice.append(keyAlice[i])
        diffBob.append(keyBob[i])
        diffBasesA.append(basesAlice[i])
        diffBasesB.append(basesBob[i])
#kode untuk menghitung nilai S dari ketidaksamaan CHSH
#ZW

```

```

sameZW = 0
diffZW = 0
for i, (bA, bB) in enumerate(zip(diffBasesA,
diffBasesB)):
    if (bA == 'Z' and bB == 'W'):
        if diffAlice[i]==diffBob[i]:
            sameZW=sameZW+1
        else:
            diffZW=diffZW+1
totalZW=sameZW+diffZW
if totalZW!=0:
    ZW=(sameZW-diffZW)/totalZW
else:
    ZW=0

#XW
sameXW = 0
diffXW = 0
for i, (bA, bB) in enumerate(zip(diffBasesA,
diffBasesB)):
    if (bA == 'X' and bB == 'W'):
        if diffAlice[i]==diffBob[i]:
            sameXW=sameXW+1
        else:
            diffXW=diffXW+1
totalXW=sameXW+diffXW
if totalXW!=0:
    XW=(sameXW-diffXW)/totalXW
else:
    XW=0

#XV
sameXV = 0
diffXV = 0

```

```

for i, (bA, bB) in enumerate(zip(diffBasesA,
diffBasesB)):
    if (bA == 'X' and bB == 'V'):
        if diffAlice[i]==diffBob[i]:
            sameXV=sameXV+1
        else:
            diffXV=diffXV+1
totalXV=sameXV+diffXV
if totalXV!=0:
    XV=(sameXV-diffXV)/totalXV
else:
    XV=0
#ZV
sameZV = 0
diffZV = 0
for i, (bA, bB) in enumerate(zip(diffBasesA,
diffBasesB)):
    if (bA == 'Z' and bB == 'V'):
        if diffAlice[i]==diffBob[i]:
            sameZV=sameZV+1
        else:
            diffZV=diffZV+1
totalZV=sameZV+diffZV
if totalZV!=0:
    ZV=(sameZV-diffZV)/totalZV
else:
    ZV=0
S=XW+XW-XV+ZV
print("CHSH inequality value is", S)
print(finalKeyAlice)
print(finalKeyBob)
if abs(S) < 2:
    print("Final Key is 'NOT' use to encrypt and decrypt")
else:

```

```

print("Final Key is use to encrypt and decrypt over a
public channel used by Alice and Bob.")

#Kode ini menghitung secret key rate dengan
membandingkan bit-bit kunci akhir Alice dan Bob dan
jumlah kesalahan
secret_key_rate = 0
for i in range(len(finalKeyAlice)):
if finalKeyAlice[i] == finalKeyBob[i]:
secret_key_rate= secret_key_rate + 1
error = len(finalKeyAlice)-secret_key_rate
print("Total Key di Terima: ",len(finalKeyAlice))
print("Key:", finalKeyAlice)
print("K : ", secret_key_rate)
print("Error: ", error)

```

4. Keamanan Protokol E91

Keamanan protokol E91 dijamin oleh hukum mekanika kuantum melalui fenomena *entanglement*. Berikut adalah beberapa aspek penting dari keamanan protokol ini:

- a. *Non-Clonability*: Dalam mekanika kuantum, tidak mungkin bagi pihak ketiga untuk membuat salinan sempurna dari keadaan kuantum (*no-cloning theorem*). Hal ini membuat penyadapan menjadi sulit karena upaya mengukur atau menyalin keadaan kuantum akan mengganggu sistem dan dapat terdeteksi.
- b. Deteksi *Eavesdropping*: Setiap intervensi oleh pihak ketiga (Eve) yang mencoba mengukur atau mengubah keadaan foton akan menyebabkan gangguan pada korelasi *entangled*, yang dapat dideteksi oleh Alice dan Bob melalui pengujian Bell *inequality*.
- c. Koreksi Kesalahan dan Privasi: Setelah tahap deteksi penyadapan, Alice dan Bob dapat menggunakan teknik koreksi kesalahan dan penguatan privasi untuk memperbaiki dan

memperkuat kunci mereka jika ada kesalahan atau upaya penyadapan terdeteksi.

5. Kelebihan dan Keterbatasan Protokol E91

Kelebihan protokol E91 adalah sebagai berikut:

- a. Keamanan yang sangat tinggi berdasarkan prinsip dasar mekanika kuantum.
- b. Dapat mendeteksi penyadapan secara langsung melalui pengujian ketidaksamaan Bell.
- c. Kunci kriptografi yang dihasilkan benar-benar acak dan tidak dapat diprediksi.

Sementara keterbatasan protokol ini adalah :

- a. Membutuhkan infrastruktur kuantum khusus seperti sumber foton *entangled* dan detektor yang sangat sensitif.
- b. Rentan terhadap hilangnya foton dan gangguan dalam saluran komunikasi kuantum, yang dapat mempengaruhi efisiensi protokol.
- c. Teknologi QKD secara umum masih dalam tahap pengembangan dan belum siap untuk diadopsi secara luas di semua aplikasi komunikasi.



BAB IV

TREN MODERN DALAM JARINGAN QKD

BAB IV

TREN MODERN DALAM JARINGAN QKD

Bab ini akan membahas terkait 2 (dua) tren modern dalam jaringan QKD berdasarkan buku berjudul *Quantum Key Distribution Networks A Quality of Service Perspective* [17]. Tren modern tersebut membahas tentang contoh implementasi QKD di dalam jaringan 5G dan implementasi di dalam kuantum *repeater*.

A. QKD DALAM JARINGAN 5G

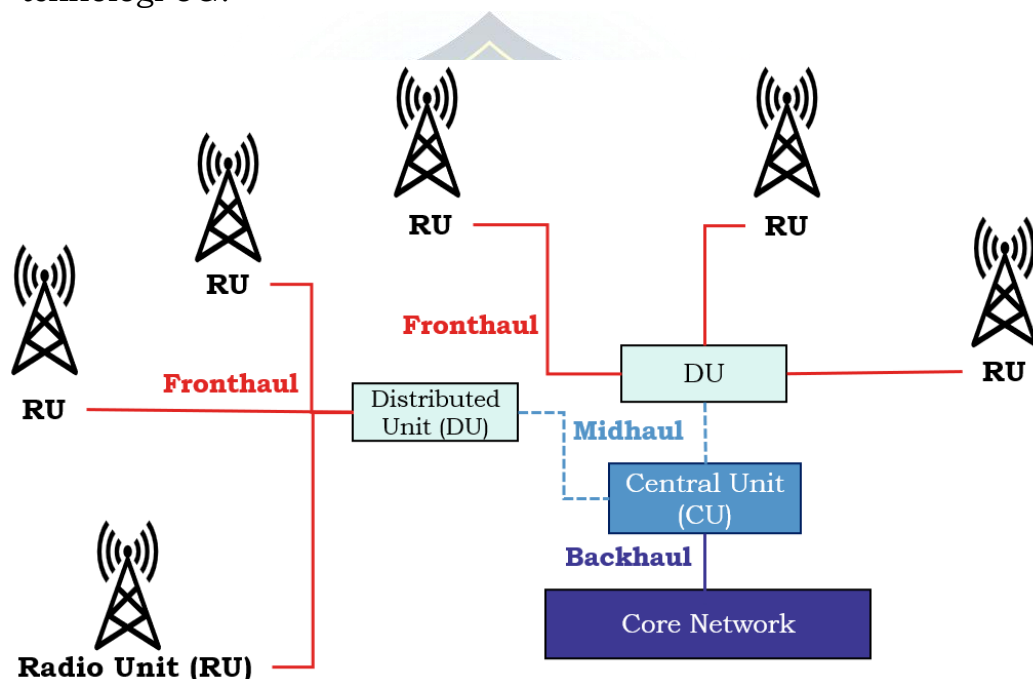
Dengan semakin cepatnya penerapan sistem telekomunikasi 5G, keamanan dan privasi pengguna menjadi aspek yang semakin krusial. Jaringan 5G dirancang untuk mendukung kinerja tinggi dan berbagai aplikasi penting seperti kendaraan otonom, bedah jarak jauh, fungsi autopilot, pengelolaan kendaraan secara remot, sistem *smart-grid*, dan aplikasi lainnya yang berkaitan dengan keselamatan jiwa. Oleh karena itu, jaringan ini sangat bergantung pada koneksi jaringan yang aman dari ujung ke ujung (*end-to-end secure network*). Visi utama dari 5G adalah menyediakan kecepatan data yang sangat tinggi dengan latensi yang sangat rendah, peningkatan kapasitas stasiun basis secara signifikan, serta kepadatan jaringan untuk meningkatkan kualitas layanan (*Quality of Service/QoS*) bagi aplikasi-aplikasi masa depan.

Salah satu model struktural yang sering dijadikan acuan dalam pengorganisasian jaringan telekomunikasi adalah model Cisco, yang terdiri dari tiga lapisan utama, yaitu:

1. lapisan inti (*core layer*) yang menyediakan tulang punggung jaringan dengan konektivitas tanpa gangguan di tingkat nasional dan internasional.
2. lapisan distribusi (*distribution layer*) yang berfungsi sebagai penggabung dan pengarah lalu lintas dari lapisan akses ke lapisan inti, serta menyediakan fungsi transportasi, *multiplexing*, *switching*,

manajemen, dan pengawasan saluran optik untuk transmisi sinyal klien.

3. lapisan akses (*access layer*) yang menghubungkan klien ke jaringan. Lapisan ini ditandai oleh jarak yang pendek karena mempertimbangkan efisiensi biaya. Pada generasi sebelumnya, lapisan akses umumnya menggunakan kabel tembaga, namun kini para operator semakin beralih ke jaringan serat optik guna menyediakan layanan yang lebih cepat sebagaimana dituntut oleh teknologi 5G.



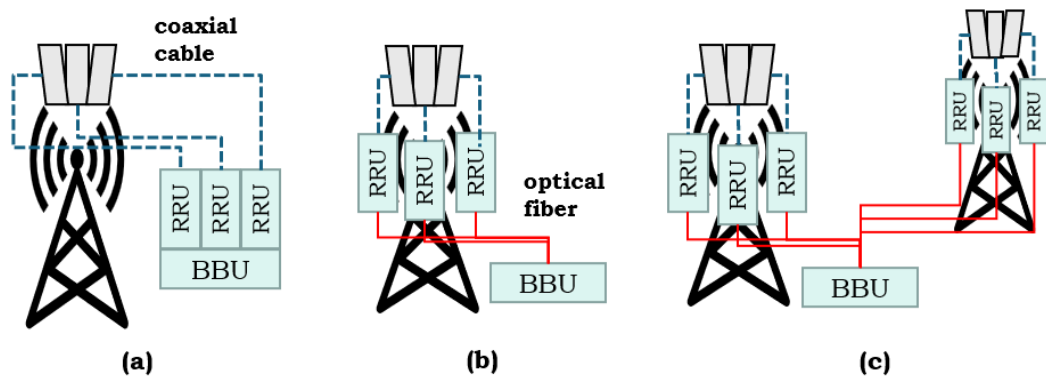
Gambar 4.1 Struktur 5G: bagian fronthaul, midhaul, dan backhaul digambar ulang dari [17].

Gambar 4.1 mengilustrasikan lapisan akses jaringan 5G yang dibagi menjadi tiga bagian sistematis yaitu *fronthaul*, *midhaul*, dan *backhaul*. Pada bagian *fronthaul*, terdapat *Radio Access Network* (RAN) yang menangani komunikasi dengan perangkat pengguna (*User Equipment/UE*). Pada generasi jaringan seluler sebelumnya, stasiun basis (*base station*) terdiri dari satu kotak fisik yang terhubung ke antenna melalui kabel koaksial, namun konfigurasi ini tidak mampu

memenuhi kebutuhan kecepatan tinggi modern karena menyebabkan kehilangan sinyal yang signifikan.

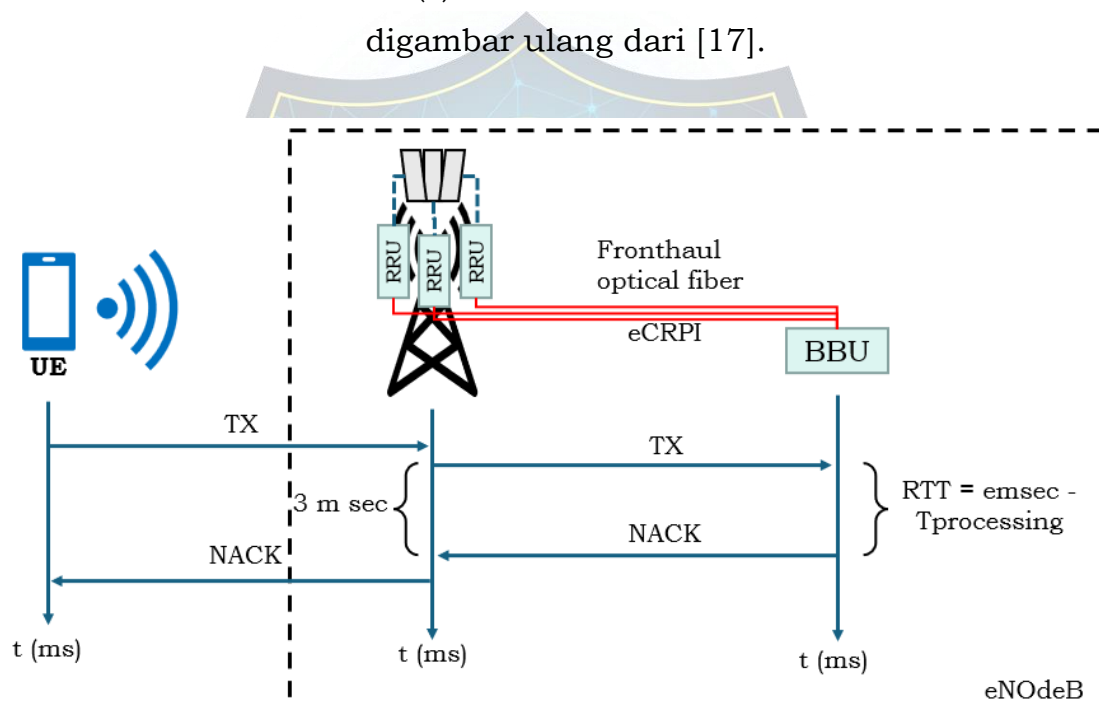
Kemajuan dalam pengembangan komponen elektronik memungkinkan penggabungan beberapa blok komunikasi radio ke dalam satu unit. Hal ini memunculkan arsitektur terpusat atau *Centralized-RAN* (C-RAN) yang ditunjukkan pada Gambar 4.2, dengan stasiun basis terdiri dari unit pengolah sinyal digital bernama *Digital Unit* (DU) atau *Baseband Unit* (BBU), yang melayani beberapa unit radio jarak jauh seperti *Remote Radio Head* (RRH), *Remote Radio Unit* (RRU), atau *Radio Unit* (RU). BBU berfungsi memproses sinyal pita dasar dan terhubung ke jaringan inti, sementara RRU menangani pemrosesan RF dan berisi antenna situs seluler. Koneksi optik diperlukan antara BBU di pusat kendali (*Central Office*) dan RRU untuk menjamin kecepatan komunikasi tinggi, namun dibatasi oleh jarak maksimum sekitar 20 km (ditunjukkan pada Gambar 4.3) agar sesuai dengan persyaratan waktu dari teknologi radio, seperti yang ditentukan oleh protokol HARQ (*Hybrid Automatic Retransmit reQuest*) yang memerlukan latensi kurang dari 3 milidetik.

Jaringan 5G juga ditandai dengan akses heterogen (HetNets), dengan pengguna terhubung ke banyak node jaringan kecil dengan bandwidth tinggi dan latensi rendah. Untuk mendukung hal ini, 3GPP mengembangkan teknologi akses radio baru bernama 5G *New Radio* (NR), yang dirancang agar dapat memberikan kinerja setara dengan kabel serat optik tetapi dengan efisiensi spektral yang lebih tinggi. 5G NR juga ditujukan untuk menghubungkan perangkat *Internet of Things* (IoT) secara efisien, serta mendukung layanan kritikal yang membutuhkan latensi rendah dan tingkat keandalan serta keamanan yang tinggi. 5G NR mencakup dua jenis operasi: *Standalone* (SA) dan *Non-Standalone* (NSA), serta beroperasi dalam dua rentang frekuensi, yaitu Sub-6 GHz (di bawah 6 GHz) dan mmWave (di atas 24 GHz).



Gambar 4.2 Evolusi RAN: (a) RAN terdistribusi; (b) Migrasi ke C-RAN; (c) Struktur C-RAN

digambar ulang dari [17].



Gambar 4.3 Latency link budget RTT lapisan-MAC di C-RAN

digambar ulang dari [17].

Menurut 3GPP, *midhaul* adalah kumpulan jalur yang menghubungkan segmen *fronthaul* dan *backhaul*. Dalam evolusi jaringan 5G melalui pendekatan OPEN RAN, arsitektur BBU dan RRH yang digunakan pada jaringan 4G telah dimodifikasi dengan memisahkan BBU menjadi *Distributed Unit* (DU) dan *Central Unit* (CU). Beberapa fungsi seperti PHY, MAC, dan RLC tetap berada di DU, sementara sisanya dipindahkan ke CU. Dengan demikian, *midhaul*

menghubungkan antara DU dan CU. Selain itu, RRH dan antena kini terintegrasi dalam satu unit yang disebut *Active Antenna Unit* (AAU).

Konfigurasi ini menuntut *fronthaul* untuk mampu mendukung komunikasi berkecepatan tinggi dan memenuhi persyaratan QoS yang ketat. Karena koneksi *fronthaul* menuju RU berada di luar fasilitas fisik operator, aspek keamanannya menjadi penting. Solusi umum untuk pengamanan *fronthaul* adalah penggunaan *Enhanced Common Public Radio Interface* (eCPRI), yang mendukung integrasi dengan MACsec dan IPsec. Karena protokol tersebut menggunakan kunci simetris, maka penerapan QKD sangat relevan.

Walaupun penerapan teknik kriptografi tambahan dapat menambah beban sistem dan menurunkan performa *fronthaul*, keterbatasan jarak *fronthaul* yang hanya beberapa puluh kilometer membuat penerapan QKD menjadi menarik. Karena enkripsi simetris lebih cepat daripada enkripsi asimetris, QKD berpotensi diterapkan selama tersedia kunci kriptografi yang cukup. Oleh karena itu, pengelolaan dan orkestrasi penyimpanan kunci menjadi aspek penting dalam pengembangan QKD.

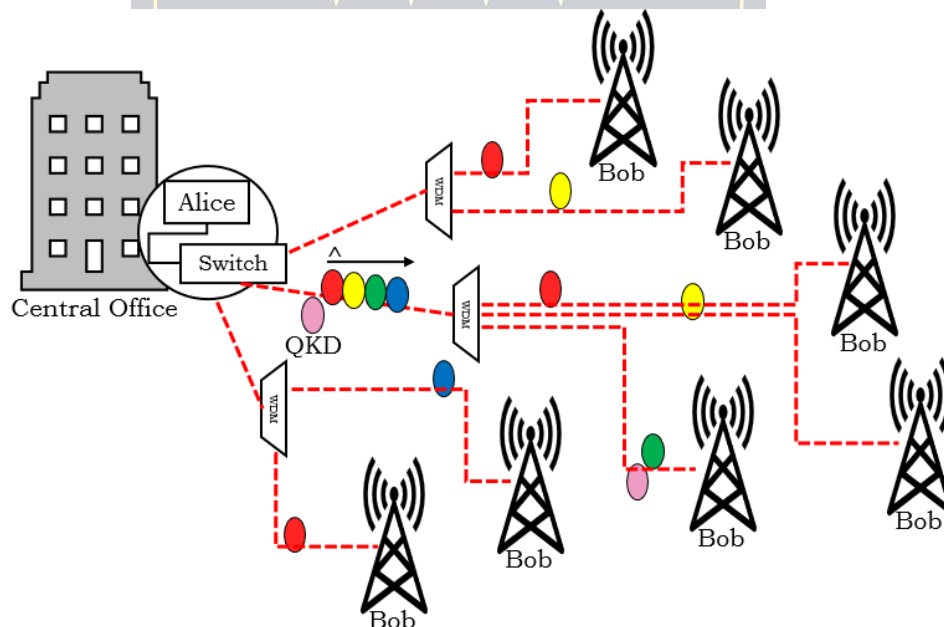
Integrasi QKD pada segmen *fronthaul* jaringan 5G telah menjadi subjek penelitian yang mengevaluasi kinerja sistem QKD dalam batasan jarak dan latensi. Studi juga meneliti penggunaan saluran kuantum dan saluran publik secara bersamaan melalui satu serat optik. Hamburan Raman (*Raman scattering*) terbukti menurunkan performa saluran kuantum, meskipun bisa dikurangi dengan memisahkan kanal atau menggunakan *dark fiber* untuk kanal kuantum.

Upaya penerapan *Continuous Variable QKD* (CV-QKD) tengah dilakukan untuk meningkatkan kecepatan pembangkitan kunci, karena tidak tergantung pada detektor foton tunggal seperti pada *Discrete Variable QKD* (DV-QKD), melainkan menggunakan detektor *balanced homodyne* yang lebih cepat. Untuk mendukung banyak unit RU secara bersamaan, jaringan *fronthaul* 5G juga mengimplementasikan teknologi

W(WDM) untuk meningkatkan kapasitas bandwidth, yang juga dapat dimanfaatkan untuk integrasi CV-QKD dengan kanal klasik.

Gambar 4.4 mengilustrasikan penggunaan satu pemancar QKD yang terhubung dengan beberapa penerima QKD melalui *time-sharing*, *spatial switching*, dan *spectral multiplexing*. Namun, implementasi ini memerlukan sinkronisasi waktu yang ketat dan kemampuan penyimpanan kunci yang besar, terutama bila terjadi kegagalan sinkronisasi atau hambatan lainnya.

Segmen jaringan *backhaul* mencakup komponen-komponen yang menghubungkan stasiun basis dengan inti jaringan. Backhaul dapat diimplementasikan dengan berbagai teknologi komunikasi, seperti nirkabel (tautan satelit atau gelombang mikro) atau pasangan serat optik khusus. Perbedaan teknologi yang digunakan mencerminkan tantangan dalam menjamin keamanan komponen jaringan. Dalam arsitektur C-RAN, BBU ditempatkan di lokasi pusat yang aman, sehingga penggunaan protokol IPsec tambahan yang menambah beban jaringan dapat dianggap tidak diperlukan.



Gambar 4.4 Penerapan QKD dalam jaringan fronthaul seluler 5G digambar ulang dari [17].

Keamanan pada segmen ini lebih tepat dicapai melalui pendekatan *Software-Defined Networking* (SDN) dan *network slicing*, yang memungkinkan penciptaan beberapa jaringan virtual di atas infrastruktur fisik yang sama. Setiap *slice* jaringan dapat memiliki kebutuhan QoS dan keamanan yang berbeda. Misalnya, jaringan untuk kendaraan otonom memerlukan latensi rendah, sementara jaringan untuk *streaming* video berkualitas tinggi membutuhkan bandwidth besar dan latensi rendah.

Arsitektur C-RAN dalam 5G semakin berkembang menuju *cloud-RAN*, dengan komponen jaringan yang dapat divirtualisasikan dan ditempatkan di lingkungan *cloud* yang aman. Pendekatan *Network Function Virtualization* (NFV), seperti vCPE, vEPC, dan vRAN, memungkinkan komponen jaringan dibangun dalam struktur berantai (*service chaining*) dan membutuhkan orkestrasi yang tepat serta manajemen jaringan cepat melalui pengendali SDN.

Komponen virtual ini bisa dipasang di berbagai lokasi fisik dan terhubung ke jalur agregasi kritis yang menentukan fungsi inti jaringan, sehingga keamanannya harus dijamin. Tingkat keamanan yang berbeda dapat diterapkan sesuai kebutuhan. Beberapa *slice* cukup menggunakan algoritma standar seperti AES-256 dengan kunci Diffie-Hellman, sedangkan jalur yang lebih sensitif memerlukan keamanan tingkat tinggi melalui sistem QKD.

Pengendali SDN berperan penting dalam melakukan re-konfigurasi dinamis terhadap sakelar optik untuk mengatur tingkat keamanan jaringan secara efisien. Berdasarkan permintaan dari *orchestrator network slicing* dan pengelola *NFV Management and Orchestration* (MANO), pengendali SDN menyesuaikan konfigurasi jaringan secara dinamis sesuai kebutuhan. Protokol seperti *OpenFlow* dan *NetConf* dapat digunakan untuk tujuan ini.

Pengendali SDN memiliki informasi detail mengenai kondisi jaringan dan dapat menyesuaikan aliran jaringan, mendukung

komunikasi multipath, serta menyediakan redundansi dan keamanan tambahan. Perlu dicatat bahwa pengendali SDN dan node *Key Management System* (KMS) tidak harus berada pada unit fisik yang sama, sehingga memerlukan komunikasi yang jelas dan efektif.

Dalam konteks ini, proyek-proyek seperti *EU H2020 OPENQKD* dan *NATO SPS G5894 Quantum Cybersecurity in 5G Networks* (QUANTUM5) sangat relevan. Kedua proyek tersebut mengeksplorasi penerapan teknologi QKD dalam jaringan 5G melalui studi kasus nyata, dan proyek QUANTUM5 tengah mengembangkan simulator QKD pertama untuk jaringan 5G.

B. QUANTUM REPEATER (REPEATER KUANTUM)

Repeater kuantum adalah teknologi yang dirancang untuk menjembatani komunikasi jarak tak terbatas melalui beberapa titik perantara (hop), seperti halnya *trusted relay*. Namun, berbeda dari *trusted relay* yang bertujuan mengirimkan data secara langsung, *repeater* kuantum berfungsi untuk memperluas proses distilasi kunci kuantum melalui beberapa relai perantara.

Teknologi ini tidak mengikuti prinsip *repeater* konvensional yang memperkuat sinyal, karena penguatan tersebut melanggar *no-cloning theorem* yang menyatakan bahwa keadaan kuantum tidak dapat disalin secara sempurna. Selain itu, redaman pada serat optik membatasi jarak komunikasi langsung secara praktis.

Sebagai gantinya, *repeater* kuantum memanfaatkan keterikatan kuantum untuk mentransfer informasi, serupa dengan konsep teleportasi kuantum. Prosesnya melibatkan sebuah node yang menghasilkan pasangan foton yang saling terikat. Salah satu foton dikirim ke hop pertama dan disimpan dalam memori kuantum. Setelah segmen berikutnya siap, keadaan kuantum dapat dihubungkan dengan hop selanjutnya, dan proses ini berlanjut hingga titik akhir (seperti node

Bob) menerima keadaan yang terikat dengan node awal (seperti Alice), memungkinkan distribusi kunci pada jarak yang sangat jauh.

Tantangan utama dalam teknologi ini adalah menjaga kestabilan dan mengendalikan gangguan (*noise*), karena proses *entanglement swapping* menjadi semakin kompleks dengan bertambahnya jumlah hop. Memori kuantum di setiap titik perantara menjadi komponen penting, dan bisa juga memerlukan asumsi sebagai perangkat tepercaya. Hingga kini, meskipun berbagai aspek dari konsep ini telah berhasil diuji secara eksperimental, *repeater* kuantum yang berfungsi penuh secara praktis masih belum berhasil dikembangkan.



BAB V

PENUTUP



BAB V

PENUTUP

Dokumen ini disusun sebagai pengenalan terhadap kriptografi kuantum, yaitu *Quantum Key Distribution* (QKD). QKD merupakan metode distribusi kunci kriptografi yang didasarkan pada prinsip-prinsip kuantum dan menawarkan keamanan berbasis prinsip fisika kuantum melampaui batas-batas keamanan tradisional yang mengandalkan kompleksitas algoritma matematis. Dengan adanya dokumen ini diharapkan pemangku kepentingan mampu memahami konsep dasar dan implementasi QKD, mekanisme pertukaran kunci di berbagai protokol QKD, serta tren modern implementasi QKD.

Dokumen ini diharapkan dapat menjadi referensi awal dalam penyusunan kebijakan teknis dan strategis nasional, serta mendorong terbentuknya ekosistem kriptografi kuantum yang andal, aman, dan terintegrasi. Hal ini merupakan bagian dari komitmen nasional dalam membangun sistem keamanan informasi yang kuat, adaptif, dan berkelanjutan. Selain itu, dengan pemahaman secara mendalam terhadap teknologi kuantum, diharapkan mampu mengukur kesiapan nasional menghadapi tantangan dan peluang di era perkembangan teknologi kuantum.

REFERENSI

- [1] Lembaga Sandi Negara, *Jelajah Kriptologi*, Jakarta: Lembaga Sandi Negara, 2006.
- [2] A. J. Menezes, P. C. van Oorschot dan S. A. Vanstone, *Handbook of Applied Cryptography*, CRC Press, 1996.
- [3] A. Jones, *Quantum Physics for Beginners: The Easy Guide to Understand how Everything Works*, 2018.
- [4] J. Schneider dan I. Smalley, "What is quantum cryptography," IBM, 01 December 2023. [Online]. Available: <https://www.ibm.com/topics/quantum-cryptography>. [Diakses November 2024].
- [5] ETSI, "Quantum Key Distribution (QKD); Vocabulary," ETSI Industry Specification Group (ISG), Prancis, 2018.
- [6] N. Syahidan dan M. Syahrul, "Otomatisasi Simulasi Quantum Key Distribution Protokol BB84 pada EDU-QCRY1," *Info Kripto*, 2023.
- [7] V. Martin, *Introduction to Quantum Key Distribution*, 2016.
- [8] University of Ottawa, "Phys.Org," Science X Network, 21 Agustus 2023. [Online]. Available: <https://phys.org/news/2023-08-visualizing-mysterious-quantum-entanglement-photons.html>. [Diakses 10 Februari 2025].
- [9] E. F. Climent, *Hacking the hacker My Top 10 Unconventional Cybersecurity Techniques*, 2024.
- [10] A. Nurhadi dan N. Syambas, "Quantum Key Distribution (QKD) Protocols: A Survey," dalam *4th International Conference on Wireless and Telematics (ICWT)*, 2018.

- [11] P. K. Verma, M. El Rifai dan K. W. C. Chan, Multi-photon Quantum Secure Communication, Singapore: Springer Nature Singapore Pte Ltd, 2019.
- [12] C. H. Bennett dan G. Brassard, "Quantum cryptography: Public key distribution and coin tossing," dalam *Proceedings of the International Conference on Computers, Systems & Signal Processing, Bangalore, India. Vol. 1*, New York, 1984.
- [13] C. Branciard, N. Gisin, B. Kraus dan V. Scarani, "Security of two quantum cryptography protocols using the same four qubit states," *Physical Review A*. 72, 2005.
- [14] C. Caputo, M. Simoni, G. A. Cirillo, G. Turvani dan M. Zamboni, "A simulator of optical coherent-state evolution in quantum key distribution systems," dalam *Optical and Quantum Electronics*, 2022.
- [15] M. E. Sabani, I. K. Savvas, D. Poulakis dan G. C. Makris, "Quantum Key Distribution: Basic Protocols and Threats," dalam *PCI '22: Proceedings of the 26th Pan-Hellenic Conference on Informatics*, 2022.
- [16] C. H. Bennett, "Quantum cryptography using any two nonorthogonal states," dalam *Physical Review Letters*, 1992.
- [17] S. Marksteiner, Master Thesis: An approach to securing IPsec with Quantum Key Distribution (QKD) using the AIT QKD software, 2014.
- [18] M. Mehic, S. Rass, P. Fazio dan M. Vozna, Quantum Key Distribution Networks: A Quality of Service Perspective, Cham: Springer Nature Switzerland AG, 2022, p. 223.



**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