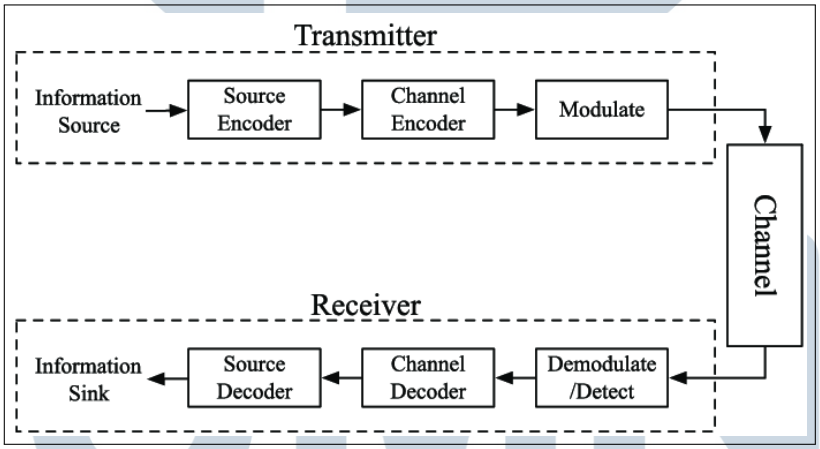
BAB 2
LANDASAN TEORI

2.1 Transmisi Data dan Keamanan Transmisi Data

Transmisi data merupakan proses pengiriman informasi dari suatu entitas ke entitas lain melalui media komunikasi tertentu yang melibatkan komponen utama berupa pengirim (*sender*), kanal transmisi (*channel*), dan penerima (*receiver*). Menurut kajian sistem komunikasi digital modern, struktur komunikasi tersebut menjadi kerangka fundamental dalam memahami bagaimana sinyal diproses dari sumber hingga tujuan [23]. Dalam sistem komunikasi digital, data yang dikirimkan mengalami proses pengkodean, modulasi, propagasi melalui kanal, hingga proses demodulasi dan dekode pada sisi penerima. Model dasar ini menjadi fondasi dalam menganalisis potensi gangguan yang dapat muncul selama proses transmisi berlangsung.



Gambar 2.1. Model Dasar Sistem Transmisi Data

Setiap kanal komunikasi memiliki karakteristik fisik yang berbeda tergantung pada media yang digunakan, seperti kabel tembaga, serat optik, maupun sistem nirkabel. Kanal dapat mengalami redaman sinyal, interferensi, distorsi, serta noise yang berdampak pada meningkatnya bit error rate (BER). Analisis kanal komunikasi modern menunjukkan bahwa karakteristik kanal secara langsung mempengaruhi reliabilitas sistem transmisi digital, terutama pada jaringan berkecepatan tinggi [24]. Oleh karena itu, pemodelan kanal dan penerapan teknik pengendalian error menjadi aspek penting dalam menjaga keandalan komunikasi jarak jauh.

Selain gangguan fisik, kanal komunikasi publik juga menghadapi ancaman keamanan dari pihak tidak berwenang. Ancaman tersebut dapat berupa penyadapan pasif terhadap lalu lintas data maupun manipulasi aktif terhadap pesan yang dikirimkan. Studi keamanan jaringan terkini mengidentifikasi bahwa serangan eavesdropping dan man-in-the-middle masih menjadi ancaman dominan dalam komunikasi berbasis jaringan publik [25]. Serangan semacam ini dapat menyebabkan kebocoran informasi serta pelanggaran integritas data tanpa terdeteksi oleh sistem komunikasi konvensional.

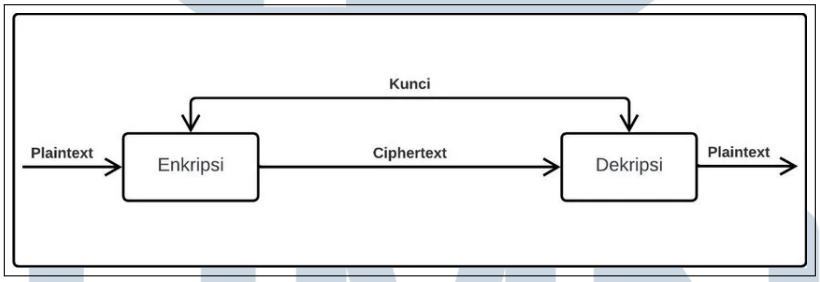
Untuk menjamin keamanan komunikasi, konsep secure data transmission dikembangkan dengan mengacu pada prinsip confidentiality, integrity, and availability (CIA triad). Pendekatan ini tidak hanya mencakup penggunaan algoritma kriptografi, tetapi juga integrasi mekanisme autentikasi, manajemen kunci, serta kontrol akses guna mencegah akses tidak sah terhadap informasi. Implementasi keamanan berbasis CIA triad masih menjadi fondasi arsitektur keamanan sistem informasi modern sebagaimana dibahas dalam literatur keamanan siber kontemporer [26]. Dengan demikian, pengamanan komunikasi harus dilakukan secara menyeluruh pada berbagai lapisan sistem.

Enkripsi merupakan mekanisme utama dalam melindungi data selama transmisi dengan mengubah pesan asli (plaintext) menjadi bentuk tersandi (ciphertext). Algoritma kriptografi modern seperti Advanced Encryption Standard (AES) banyak digunakan karena menawarkan tingkat keamanan yang tinggi dengan efisiensi komputasi yang baik. Keamanan sistem enkripsi simetris sangat bergantung pada kerahasiaan kunci yang digunakan [27]. Oleh sebab itu, distribusi dan pengelolaan kunci menjadi faktor kritis dalam mendukung keamanan transmisi data terenkripsi.

Meskipun algoritma kriptografi modern mampu memberikan tingkat keamanan yang tinggi, tantangan utama terletak pada mekanisme distribusi kunci melalui kanal publik. Sistem pertukaran kunci klasik umumnya tidak memiliki kemampuan deteksi gangguan secara inheren, sehingga penyadapan terhadap proses distribusi kunci dapat terjadi tanpa diketahui oleh pihak yang berkomunikasi. Perkembangan komputasi berperforma tinggi serta potensi ancaman komputasi kuantum di masa depan semakin meningkatkan urgensi pengembangan metode distribusi kunci yang lebih fundamental secara keamanan [28].

2.2 Enkripsi dan Distribusi Kunci Kriptografi

Enkripsi merupakan mekanisme utama dalam menjaga kerahasiaan informasi selama proses transmisi data. Dalam sistem komunikasi modern, enkripsi data umumnya dilakukan menggunakan algoritma kriptografi simetris seperti Advanced Encryption Standard (AES) karena efisiensinya dalam memproses data berukuran besar dengan kompleksitas komputasi yang relatif rendah [29]. AES bekerja menggunakan blok data 128-bit dengan variasi panjang kunci 128, 192, dan 256 bit, serta dirancang untuk tahan terhadap berbagai bentuk serangan kriptanalisis klasik. Implementasi AES dalam pengamanan file digital menunjukkan bahwa algoritma ini mampu mengenkripsi dan mendekripsi data secara efektif tanpa perubahan signifikan terhadap ukuran file, dengan waktu eksekusi yang meningkat seiring bertambahnya ukuran data dan panjang kunci yang digunakan [30]. Meskipun demikian, keamanan enkripsi simetris sepenuhnya bergantung pada kerahasiaan kunci yang dibagikan antara pengirim dan penerima, sehingga pengamanan kunci menjadi faktor yang sangat krusial.

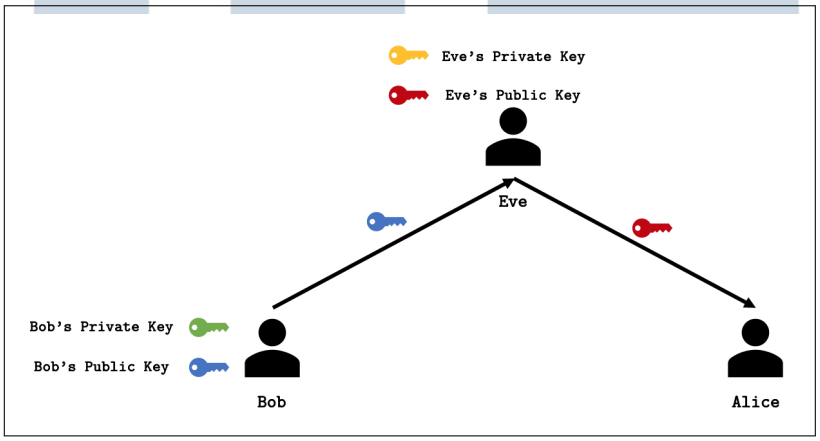


Gambar 2.2. Model sistem enkripsi simetris

Dalam sistem komunikasi terdistribusi dan jaringan nirkabel, manajemen kunci (key management) mencakup proses pembangkitan, distribusi, penyimpanan, penggunaan, hingga pencabutan kunci. Kelemahan pada salah satu tahapan siklus hidup kunci dapat menyebabkan kompromi terhadap seluruh sistem keamanan komunikasi. Studi mengenai skema manajemen kunci pada jaringan wireless menunjukkan bahwa tantangan utama terletak pada efisiensi distribusi, skalabilitas, serta ketahanan terhadap serangan pada kanal komunikasi publik [31]. Oleh karena itu, meskipun algoritma enkripsi simetris seperti AES memiliki tingkat keamanan yang tinggi, sistem transmisi data tetap sangat bergantung pada mekanisme distribusi kunci yang aman dan andal.

Distribusi kunci klasik umumnya dilakukan menggunakan kriptografi asimetris seperti RSA atau Diffie–Hellman, yang memungkinkan pertukaran kunci

melalui kanal publik tanpa harus membagikan kunci rahasia secara langsung. Namun, pendekatan ini memiliki keterbatasan, terutama dalam lingkungan komunikasi nirkabel yang rentan terhadap penyadapan. Analisis terhadap mekanisme pembangkitan dan pertukaran kunci pada lapisan komunikasi wireless menunjukkan adanya risiko interception serta keterbatasan dalam hal efisiensi dan skalabilitas sistem [32]. Selain itu, mekanisme distribusi kunci klasik tidak memiliki kemampuan deteksi gangguan secara inheren, sehingga penyadapan terhadap proses pertukaran kunci dapat terjadi tanpa diketahui oleh pihak yang berkomunikasi.



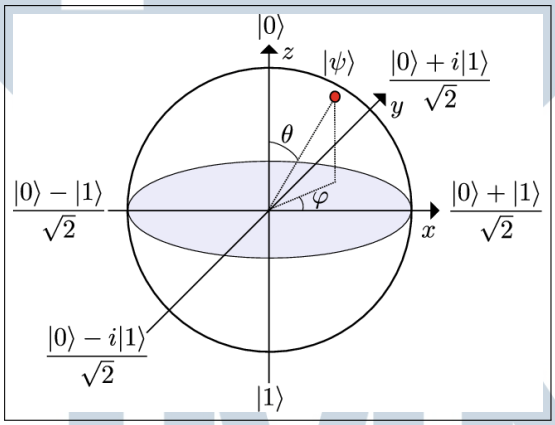
Gambar 2.3. Key exchange dengan keberadaan *intercept-resend attack*

Ancaman terhadap distribusi kunci dan transmisi data dalam jaringan publik tidak hanya bersifat pasif seperti eavesdropping, tetapi juga aktif seperti man-in-the-middle attack. Evaluasi keamanan komunikasi klasik dalam konteks perkembangan komputasi modern menunjukkan bahwa skema kriptografi berbasis asumsi kesulitan komputasi menghadapi tantangan serius, terutama dalam menghadapi potensi komputasi kuantum skala besar [33]. Kerentanan ini meningkatkan urgensi pengembangan mekanisme distribusi kunci yang tidak hanya bergantung pada kompleksitas komputasi matematis, melainkan mampu menjamin keamanan secara lebih fundamental. Kondisi tersebut menjadi dasar munculnya pendekatan distribusi kunci berbasis prinsip mekanika kuantum.

2.3 Konsep Dasar Komputasi dan Kriptografi Kuantum

Perkembangan kriptografi kuantum tidak terlepas dari konsep dasar komputasi kuantum yang memanfaatkan fenomena mekanika kuantum dalam

pemrosesan informasi. Berbeda dengan sistem komputasi klasik yang menggunakan bit dengan nilai diskrit 0 atau 1, sistem komputasi kuantum menggunakan unit informasi yang disebut quantum bit (qubit). Menurut penelitian mengenai perkembangan teknologi kriptografi kuantum, qubit memiliki kemampuan untuk berada pada kombinasi linear dari dua keadaan dasar secara simultan, suatu fenomena yang dikenal sebagai superposisi kuantum [34]. Secara matematis, keadaan qubit dapat direpresentasikan sebagai kombinasi dari state basis ortonormal $|0\rangle$ dan $|1\rangle$, sehingga memungkinkan satu qubit merepresentasikan lebih banyak kemungkinan state dibandingkan bit klasik. Untuk mempermudah pemahaman terhadap berbagai kemungkinan state kuantum tersebut, keadaan qubit sering divisualisasikan menggunakan Bloch sphere, yang menggambarkan seluruh kemungkinan state kuantum dalam ruang tiga dimensi dan membantu menjelaskan bagaimana operasi kuantum memodifikasi state qubit.



Gambar 2.4. Diagram Bloch Sphere

Selain konsep qubit, sistem komunikasi kuantum juga bergantung pada basis pengukuran yang digunakan dalam proses *encoding* dan *decoding* informasi. Dalam banyak protokol kriptografi kuantum, terutama pada skema distribusi kunci kuantum, dua basis yang paling umum digunakan adalah basis komputasi (basis Z) dan basis diagonal (basis X). Penelitian mengenai implementasi *quantum key distribution* dalam jaringan komunikasi modern menunjukkan bahwa basis Z terdiri dari state $|0\rangle$ dan $|1\rangle$, sedangkan basis X terdiri dari state $|+\rangle$ dan $|-\rangle$, yang merupakan superposisi dari state pada basis Z [35]. Karena kedua basis tersebut saling tidak ortogonal, pengukuran pada basis yang berbeda dari basis persiapan state akan menghasilkan hasil yang bersifat probabilistik. Karakteristik ini menjadi komponen penting dalam mekanisme keamanan protokol distribusi kunci kuantum

karena setiap perbedaan basis antara pengirim dan penerima dapat menghasilkan bit yang tidak konsisten, yang selanjutnya dapat digunakan untuk mendeteksi adanya gangguan atau penyadapan pada kanal komunikasi.

Tabel 2.1. Representasi Basis Z dan Basis X pada Qubit

Basis	**State (Dirac)**	**Representasi Vektor**	**Bit**
Z Basis	$\|0\rangle$	$\begin{pmatrix}1\\0\end{pmatrix}$	0
Z Basis	$\|1\rangle$	$\begin{pmatrix}0\\1\end{pmatrix}$	1
X Basis	$\|+\rangle = \frac{\|0\rangle+\|1\rangle}{\sqrt{2}}$	$\frac{1}{\sqrt{2}}\begin{pmatrix}1\\1\end{pmatrix}$	0
X Basis	$\|-\rangle = \frac{\|0\rangle-\|1\rangle}{\sqrt{2}}$	$\frac{1}{\sqrt{2}}\begin{pmatrix}1\\-1\end{pmatrix}$	1

Karakteristik penting lain dalam sistem kuantum adalah proses pengukuran kuantum (quantum measurement) yang memiliki sifat probabilistik dan tidak deterministik seperti pada sistem klasik. Ketika sebuah qubit berada dalam keadaan superposisi dan dilakukan pengukuran pada basis tertentu, state kuantum tersebut akan mengalami fenomena yang dikenal sebagai collapse of the wavefunction, yaitu perubahan dari keadaan superposisi menjadi salah satu state basis yang mungkin. Penelitian mengenai pengembangan simulasi jaringan QKD menjelaskan bahwa probabilitas hasil pengukuran bergantung pada amplitudo kompleks dari state kuantum sebelum proses pengukuran dilakukan [36]. Hal ini menyebabkan proses pengukuran tidak hanya berfungsi sebagai proses observasi, tetapi juga mempengaruhi keadaan sistem kuantum itu sendiri. Konsekuensinya, setiap upaya pengukuran oleh pihak yang tidak berwenang pada kanal komunikasi kuantum dapat menyebabkan perubahan pada state qubit yang dikirimkan, sehingga aktivitas tersebut berpotensi terdeteksi oleh pihak yang berkomunikasi.

Selain fenomena pengukuran, keamanan komunikasi kuantum juga didukung oleh prinsip fundamental yang dikenal sebagai no-cloning theorem. Teorema ini menyatakan bahwa tidak mungkin untuk membuat salinan identik dari suatu state kuantum yang tidak diketahui secara sempurna. Berbeda dengan informasi klasik yang dapat direplikasi tanpa batas tanpa mengubah informasi aslinya, state kuantum tidak dapat diduplikasi secara sempurna karena keterbatasan hukum mekanika kuantum. Prinsip ini memiliki implikasi langsung terhadap keamanan komunikasi kuantum karena pihak ketiga tidak dapat menyalin qubit yang dikirimkan tanpa mempengaruhi state aslinya [37]. Dengan demikian, setiap

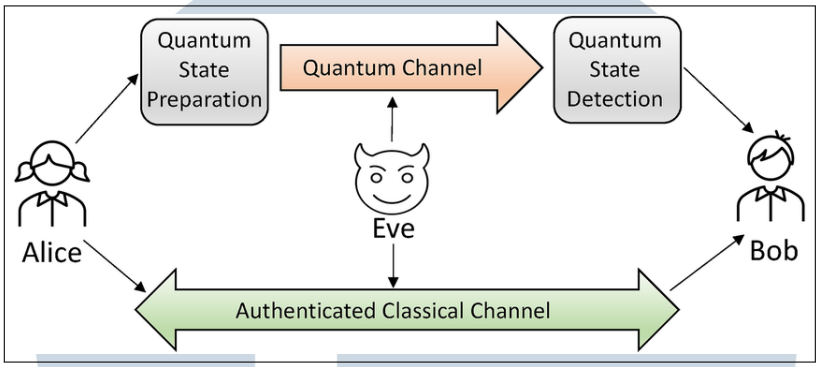
upaya penyadapan terhadap qubit selama proses transmisi berpotensi menimbulkan perubahan yang dapat dideteksi oleh sistem komunikasi. Prinsip no-cloning theorem inilah yang menjadi salah satu dasar teoritis utama dalam pengembangan berbagai protokol Quantum Key Distribution (QKD) yang menjamin keamanan distribusi kunci melalui hukum fisika, bukan hanya melalui asumsi kompleksitas komputasi.

2.4 Quantum Key Distribution (QKD)

Quantum Key Distribution (QKD) merupakan metode distribusi kunci kriptografi yang memanfaatkan prinsip mekanika kuantum untuk memungkinkan dua pihak menghasilkan dan berbagi kunci rahasia secara aman melalui kanal komunikasi kuantum. Berbeda dengan mekanisme distribusi kunci pada kriptografi klasik yang bergantung pada asumsi kesulitan komputasi matematis, QKD memanfaatkan sifat fundamental sistem kuantum dalam menjamin keamanan komunikasi. Konsep ini memungkinkan dua pihak yang umumnya disebut sebagai Alice dan Bob untuk menghasilkan rangkaian bit rahasia bersama melalui pertukaran state kuantum, seperti foton yang membawa informasi kuantum [38]. Informasi kunci tersebut dikodekan dalam state kuantum tertentu sebelum dikirimkan melalui kanal komunikasi kuantum. Jika proses distribusi berlangsung tanpa gangguan, kedua pihak akan memperoleh kunci identik yang kemudian dapat digunakan dalam algoritma kriptografi simetris untuk mengamankan komunikasi data selanjutnya.

Implementasi sistem Quantum Key Distribution umumnya melibatkan dua jenis kanal komunikasi, yaitu quantum channel dan classical channel. Kanal kuantum digunakan untuk mengirimkan state kuantum yang membawa informasi kunci dari pengirim kepada penerima, sedangkan kanal klasik digunakan untuk melakukan pertukaran informasi tambahan yang diperlukan selama proses pembentukan kunci. Keamanan sistem QKD praktis menggunakan komunikasi melalui kanal klasik tetap diperlukan untuk melakukan proses seperti pengumuman basis pengukuran, sinkronisasi data, serta verifikasi hasil pengukuran tanpa mengungkapkan nilai bit sebenarnya [39]. Dalam proses operasionalnya, Alice terlebih dahulu menyiapkan state kuantum yang merepresentasikan bit informasi dan mengirimkannya kepada Bob melalui kanal kuantum. Setelah Bob melakukan pengukuran terhadap state yang diterima, kedua pihak menggunakan kanal klasik untuk melakukan proses seleksi bit yang valid sehingga dihasilkan rangkaian bit

awal yang dikenal sebagai raw key. Struktur komunikasi dua kanal ini merupakan elemen penting dalam implementasi QKD karena memungkinkan proses verifikasi keamanan serta koreksi kesalahan selama pembentukan kunci.



Gambar 2.5. Model komunikasi quantum

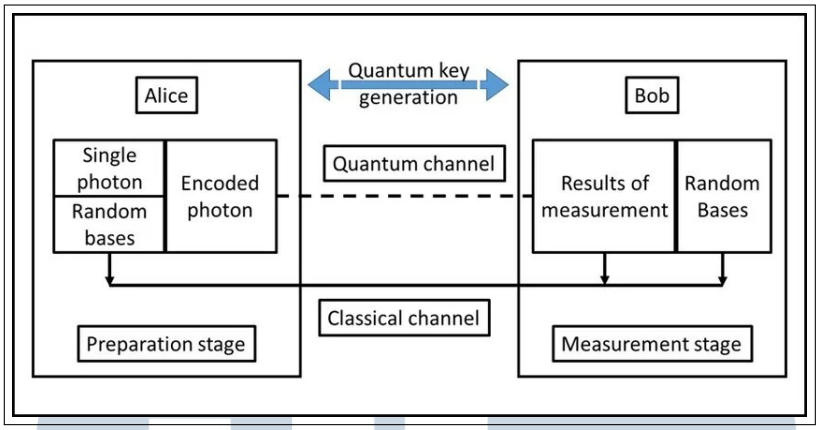
Keamanan Quantum Key Distribution didasarkan pada prinsip fundamental mekanika kuantum yang menyatakan bahwa proses pengukuran terhadap state kuantum dapat menyebabkan perubahan pada state tersebut. Dalam sistem komunikasi kuantum, fenomena ini dikenal sebagai measurement disturbance, di mana setiap upaya pengukuran oleh pihak ketiga dapat mempengaruhi kondisi state kuantum yang dikirimkan. Jaringan QKD modern menunjukkan bahwa sifat ini memungkinkan sistem mendeteksi keberadaan pihak penyadap, yang biasanya disebut sebagai Eve, karena aktivitas pengukuran akan meningkatkan tingkat kesalahan pada hasil pengukuran yang diperoleh oleh penerima [40]. Selain itu, prinsip no-cloning theorem juga menyatakan bahwa state kuantum yang tidak diketahui tidak dapat disalin secara sempurna. Kombinasi kedua prinsip tersebut menjadikan QKD mampu mendeteksi aktivitas penyadapan selama proses distribusi kunci berlangsung, sehingga Alice dan Bob dapat memutuskan apakah kunci yang dihasilkan aman untuk digunakan atau harus dibuang.

Jika dibandingkan dengan metode distribusi kunci klasik, pendekatan yang digunakan dalam QKD memiliki perbedaan mendasar dalam hal mekanisme keamanan. Pada sistem kriptografi klasik, distribusi kunci sering dilakukan menggunakan algoritma berbasis matematika seperti Diffie–Hellman atau RSA, yang mengandalkan kesulitan komputasi terhadap masalah matematis tertentu. Keamanan metode tersebut bergantung pada keterbatasan kemampuan komputasi penyerang dalam memecahkan masalah tersebut dalam waktu yang wajar. Namun, perkembangan teknologi komputasi kuantum berpotensi melemahkan asumsi keamanan tersebut karena algoritma kuantum tertentu dapat menyelesaikan

permasalahan matematika tersebut dengan lebih efisien. Pendekatan distribusi kunci berbasis mekanika kuantum menawarkan paradigma keamanan yang berbeda karena keamanan sistem tidak lagi bergantung pada kompleksitas komputasi, melainkan pada hukum fisika yang mendasari perilaku sistem kuantum itu sendiri [41]. Oleh karena itu, QKD dipandang sebagai salah satu solusi potensial untuk menjamin keamanan distribusi kunci pada sistem komunikasi di era komputasi kuantum.

2.5 Protokol BB84

Protokol BB84 merupakan salah satu protokol Quantum Key Distribution (QKD) pertama yang diperkenalkan untuk memungkinkan dua pihak menghasilkan kunci kriptografi yang aman melalui kanal kuantum. Dalam mekanisme dasar protokol ini, dua entitas komunikasi yang secara konvensional disebut sebagai Alice dan Bob melakukan proses pertukaran informasi kuantum menggunakan partikel seperti foton yang merepresentasikan bit kuantum (qubit). Alice terlebih dahulu menghasilkan deretan bit acak yang kemudian dikodekan ke dalam state kuantum menggunakan dua basis polarisasi yang berbeda. Qubit tersebut kemudian dikirimkan kepada Bob melalui kanal kuantum, sementara Bob melakukan pengukuran terhadap setiap qubit menggunakan basis yang juga dipilih secara acak. Mekanisme ini memungkinkan distribusi kunci yang aman karena setiap percobaan penyadapan akan mempengaruhi state kuantum yang dikirimkan dan menghasilkan kesalahan yang dapat dideteksi pada tahap evaluasi kunci bersama [42]. Dengan demikian, keamanan distribusi kunci dalam protokol BB84 tidak bergantung pada kompleksitas komputasi matematis, tetapi pada prinsip dasar mekanika kuantum yang mengatur perilaku partikel kuantum selama proses transmisi.



Gambar 2.6. Skema model komunikasi BB84

Dalam protokol BB84, informasi kuantum dikodekan menggunakan dua basis ortogonal yang berbeda, yaitu basis komputasi (Z-basis) dan basis diagonal (X-basis). Basis Z terdiri dari dua state dasar $|0\rangle$ dan $|1\rangle$, sedangkan basis X terdiri dari dua state superposisi $|+\rangle$ dan $|-\rangle$. Keempat state tersebut digunakan untuk merepresentasikan nilai bit yang dikirimkan oleh Alice kepada Bob. Ketika Bob melakukan pengukuran menggunakan basis yang sama dengan basis yang digunakan Alice saat proses encoding, maka nilai bit dapat diidentifikasi dengan benar. Sebaliknya, jika Bob menggunakan basis yang berbeda, hasil pengukuran akan bersifat acak karena kedua basis tersebut bersifat tidak kompatibel (mutually unbiased bases). Penggunaan dua basis yang tidak kompatibel ini merupakan komponen penting dalam mendeteksi keberadaan pihak ketiga yang mencoba melakukan penyadapan terhadap kanal komunikasi kuantum [43]. Oleh karena itu, pemilihan basis secara acak oleh kedua pihak menjadi mekanisme fundamental yang mendukung keamanan distribusi kunci dalam sistem QKD.

Tabel 2.2. Representasi State Kuantum pada Basis Z dan X dalam Protokol BB84

Basis	**State Kuantum**	**Representasi Polarisasi**	**Bit**
Z	$\|0\rangle$	Horizontal (0°)	0
Z	$\|1\rangle$	Vertical (90°)	1
X	$\|+\rangle$	Diagonal (45°)	0
X	$\|-\rangle$	Anti-diagonal (135°)	1

Setelah proses transmisi dan pengukuran qubit selesai dilakukan, Alice dan Bob melakukan tahap yang dikenal sebagai sifting process melalui kanal komunikasi klasik. Pada tahap ini, kedua pihak saling mengumumkan basis yang digunakan untuk setiap bit tanpa mengungkapkan nilai bit tersebut. Bit

yang diukur menggunakan basis yang berbeda kemudian dibuang, sedangkan bit yang menggunakan basis yang sama dipertahankan sebagai kandidat kunci rahasia. Proses penyaringan ini biasanya menghasilkan sekitar setengah dari jumlah bit awal yang dikirimkan oleh Alice. Tahap sifting memainkan peran penting dalam memastikan bahwa hanya bit yang diukur dengan basis yang konsisten yang digunakan dalam pembentukan kunci bersama. Selain itu, tahap ini juga menjadi bagian awal dari proses evaluasi keamanan sistem QKD karena data yang tersisa akan digunakan untuk menghitung tingkat kesalahan dan mendeteksi kemungkinan adanya gangguan selama proses transmisi kuantum.

Salah satu model serangan yang sering dianalisis dalam protokol BB84 adalah intercept–resend attack, di mana pihak ketiga yang dikenal sebagai Eve mencoba menyadap komunikasi antara Alice dan Bob dengan cara mengukur qubit yang dikirimkan dan kemudian mengirimkan kembali qubit hasil pengukuran kepada Bob. Dalam skenario ini, Eve harus memilih basis pengukuran secara acak karena ia tidak mengetahui basis yang digunakan oleh Alice. Jika basis yang dipilih Eve berbeda dari basis encoding yang digunakan oleh Alice, maka state kuantum yang diukur akan berubah dan menyebabkan gangguan pada sistem. Proses pengukuran oleh pihak ketiga ini akan meningkatkan tingkat kesalahan pada bit yang diterima oleh Bob [44]. Gangguan tersebut kemudian dapat dideteksi oleh Alice dan Bob melalui evaluasi statistik terhadap bit yang dihasilkan, sehingga memungkinkan mereka untuk mengidentifikasi keberadaan penyadapan dan membatalkan proses distribusi kunci jika tingkat kesalahan melebihi ambang batas tertentu.

2.6 *Quantum Bit Error Rate* dan *Key Generation Rate*

Untuk mengevaluasi tingkat keamanan komunikasi dalam sistem QKD, digunakan parameter utama yang dikenal sebagai *Quantum Bit Error Rate* (QBER). QBER didefinisikan sebagai rasio antara jumlah bit yang salah terhadap total bit yang dibandingkan selama proses verifikasi kunci. Nilai QBER dapat meningkat akibat gangguan pada kanal komunikasi, *noise* pada sistem optik, maupun adanya aktivitas penyadapan oleh pihak ketiga. QBER dihitung menggunakan persamaan berikut:

$$QBER = \frac{N_{error}}{N_{total}} \tag{2.1}$$

N_{error} merupakan jumlah bit yang tidak selaras antara kunci Alice dan Bob setelah dibandingkan, sedangkan N_{total} adalah jumlah total bit yang berhasil dipertahankan setelah proses penyaringan (*key sifting*). Dalam konteks protokol BB84, QBER digunakan sebagai indikator utama untuk menentukan apakah kunci yang dihasilkan masih dapat dianggap aman atau harus dibuang. Jika nilai QBER melebihi ambang batas keamanan sekitar 11%, kemungkinan besar telah terjadi interaksi eksternal terhadap *state* kuantum, sehingga *secure key* tidak dapat dihasilkan dan distribusi harus dihentikan [45].

Dalam protokol BB84, serangan *intercept-resend* yang dilakukan oleh penyadap secara penuh akan menghasilkan nilai QBER teoretis sebesar 25% [46]. Oleh karena itu, keberadaan penyadap dapat dideteksi secara deterministik melalui peningkatan nilai QBER.

Selain QBER, efisiensi sistem dalam menghasilkan kunci mentah yang valid diukur menggunakan metrik *Key Generation Rate* (KGR). KGR dirumuskan sebagai berikut:

$$KGR = \frac{N_{sifted}}{N_{initial}} \tag{2.2}$$

N_{sifted} adalah jumlah bit yang tersisa setelah proses *sifting* (memiliki basis yang cocok), dan $N_{initial}$ adalah jumlah qubit awal yang dibangkitkan dan dikirimkan oleh Alice. Secara teoretis, nilai probabilitas KGR akan selalu konvergen di sekitar angka 0.5 (50%) akibat sifat acak dari pemilihan basis yang independen antara pengirim dan penerima.

2.7 Entropi Shannon Biner dan *Secret Key Rate* (SKR)

Dalam evaluasi keamanan kriptografi kuantum, ketahanan sebuah kunci tidak hanya diukur berdasarkan jumlah error fisik, tetapi juga melalui kalkulasi batas kebocoran informasi menggunakan Teori Informasi Shannon [47]. Entropi Shannon Biner, yang umumnya dinotasikan sebagai $H(e)$, merupakan landasan matematis untuk mengukur tingkat ketidakpastian atau jumlah informasi yang hilang dalam suatu sistem biner akibat adanya probabilitas kesalahan transmisi. Rumus entropi didefinisikan sebagai berikut:

$$H(e) = -e\log_2(e) - (1-e)\log_2(1-e) \tag{2.3}$$

di mana e merepresentasikan nilai probabilitas kesalahan transmisi atau *Quantum Bit Error Rate* (QBER). Komponen pada rumus ini memiliki makna matematis sebagai berikut:

1. Tanda negatif $(-)$ di awal digunakan karena nilai probabilitas e selalu berada di rentang fraksional antara 0 dan 1. Karena nilai logaritma dari pecahan bernilai negatif, tanda minus berfungsi untuk mengonversinya kembali menjadi besaran informasi yang positif.

2. Bagian pertama $e\log_2(e)$ merepresentasikan porsi informasi yang terkait dengan probabilitas terjadinya *error* (gangguan atau sadapan).

3. Bagian kedua $(1-e)\log_2(1-e)$ merepresentasikan porsi informasi yang terkait dengan probabilitas bit terkirim dengan benar.

Dalam konteks protokol QKD seperti BB84, berdasarkan prinsip *Worst-Case Assumption* dalam keamanan jaringan, seluruh *error* yang terjadi di dalam saluran komunikasi, baik akibat gangguan optik maupun anomali lainnya, harus dianggap sebagai akibat dari aktivitas *eavesdropping* oleh pihak ketiga [48]. Oleh karena itu, fungsi $H(e)$ bertindak sebagai metrik presisi untuk menakar persentase maksimal dari informasi kunci yang secara teoretis telah bocor ke tangan peretas.

Kalkulasi entropi tersebut kemudian menjadi komponen paling krusial dalam menentukan *Secret Key Rate* (SKR), yaitu metrik yang merepresentasikan laju atau rasio pembentukan kunci rahasia final yang dijamin aman secara absolut [49]. Untuk mencapai keamanan tersebut, protokol harus mengaplikasikan fase penguatan privasi (*Privacy Amplification*). Fase ini pada dasarnya adalah proses penyusutan ukuran kunci (*key shrinking*), di mana porsi informasi yang dikalkulasi bocor oleh fungsi $H(e)$ dikurangkan secara paksa dari total kunci yang dimiliki. Rumus teoretis untuk menghitung SKR adalah:

$$R = KGR \times [1-(1+f_e)H(e)] \tag{2.4}$$

Setiap komponen operasional pada rumus di atas memiliki justifikasi spesifik:

1. Angka 1 di dalam kurung siku melambangkan 100% dari kunci tersaring (*sifted key*) yang secara teoretis aman sebelum dikenakan penalti kebocoran.

2. Operasi pengurangan $(-)$ merepresentasikan mekanisme *Privacy Amplification*, di mana sistem membuang (*discarding*) sebagian panjang kunci untuk menutupi informasi yang bocor.

3. Komponen penalti total adalah $(1 + f_e)H(e)$. Angka $1 \times H(e)$ merepresentasikan porsi informasi yang bocor murni ke tangan Eve selama penyadapan transmisi kuantum (sesuai Teorema Shannon). Sedangkan $f_e \times H(e)$ merepresentasikan kebocoran informasi tambahan yang terjadi ketika Alice dan Bob terpaksa berdiskusi di saluran publik tak aman saat menjalankan algoritma *Error Correction*, dengan nilai f_e sebagai faktor tingkat inefisiensinya.

4. Pengali *KGR* di depan tanda kurung digunakan untuk menyelaraskan rasio kunci final tersebut terhadap total qubit orisinal di awal transmisi.

Berdasarkan formulasi tersebut dan batasan teoretis protokol BB84, apabila nilai QBER (e) mencapai atau melampaui 11% ($\sim$0.11), kalkulasi entropi di dalam kurung siku akan membesar secara eksponensial hingga titik di mana kompensasi penyusutan melebihi panjang sisa kunci itu sendiri [50]. Pada titik kritis tersebut, SKR akan jatuh ke angka nol, menandakan bahwa kerahasiaan kunci sudah tidak dapat diselamatkan dan sistem harus membatalkan seluruh sesi transmisi.

2.8 Literature Review

Penelitian mengenai Quantum Key Distribution (QKD) khususnya protokol BB84 telah banyak dilakukan untuk menganalisis keamanan serta performa distribusi kunci pada sistem komunikasi kuantum. Berbagai pendekatan penelitian telah digunakan, mulai dari simulasi protokol BB84, analisis serangan penyadapan, hingga peningkatan keandalan sistem melalui teknik koreksi kesalahan kuantum. Kajian terhadap penelitian terdahulu penting dilakukan untuk memahami perkembangan penelitian pada bidang ini serta mengidentifikasi pendekatan yang telah digunakan dalam menganalisis performa dan keamanan protokol BB84. Tabel 2.3 menyajikan beberapa penelitian terkait yang membahas implementasi, simulasi, serta analisis keamanan pada protokol BB84.

Tabel 2.3. Kajian Literatur Penelitian Terkait Protokol BB84

Referensi	**Metode**	**Hasil Penelitian**	**Kontribusi**
[51]	Simulasi Quantum Key Distribution menggunakan protokol BB84 dengan implementasi Python3 untuk memodelkan komunikasi kuantum antara Alice dan Bob serta skenario dengan dan tanpa penyadap (Eve).	Simulasi menunjukkan bahwa keberadaan penyadap dapat dideteksi melalui peningkatan error pada proses distribusi kunci. Sekitar 50% bit awal dieliminasi akibat perbedaan basis dan ambang kesalahan sekitar 0.11%.	Menunjukkan bahwa protokol BB84 dapat dimodelkan dan dianalisis secara efektif melalui simulasi perangkat lunak, serta membuktikan mekanisme deteksi penyadapan berdasarkan prinsip ketidakpastian dan no-cloning.
[52]	Simulasi BB84 menggunakan quantum simulator dengan model sistem yang mempertimbangkan noise serta serangan *intercept-resend*.	Hasil simulasi menunjukkan hubungan antara *Quantum Bit Error Rate (QBER)* dan tingkat intersepsi Eve dengan pendekatan $QBER = 0.25p$. Metode yang diusulkan mampu menghasilkan QBER 0.0189.	Memberikan metode estimasi kepadatan penyadapan pada protokol BB84 dengan mempertimbangkan kondisi kanal kuantum yang tidak ideal dan adanya noise sistem.
			Lanjutan pada halaman berikutnya

Tabel 2.3 Kajian Literatur Penelitian Terkait Protokol BB84 (Lanjutan)

Referensi	**Metode**	**Hasil Penelitian**	**Kontribusi**
[53]	Pendekatan peningkatan keamanan BB84 dengan integrasi *Quantum Error Correction* menggunakan kode stabilizer 5-qubit untuk memperbaiki kesalahan pada komunikasi kuantum.	Eksperimen menunjukkan peningkatan keandalan sistem distribusi kunci dengan nilai fidelitas mencapai 97.98% serta penurunan tingkat kesalahan pada proses pertukaran kunci.	Mengusulkan model peningkatan keamanan dan keandalan QKD melalui integrasi teknik koreksi kesalahan kuantum untuk mengurangi dampak noise dan meningkatkan keamanan komunikasi kuantum.
[54]	Simulasi BB84 menggunakan pendekatan Monte Carlo dengan model depolarizing channel untuk menganalisis pengaruh noise terhadap distribusi kunci kuantum.	Hasil eksperimen menunjukkan hubungan antara probabilitas noise dengan peningkatan QBER serta penurunan secure key rate. Simulasi juga memvalidasi hubungan teoritis antara parameter kanal dan keamanan BB84.	Menyediakan model simulasi yang dapat digunakan untuk menganalisis performa protokol BB84 pada kondisi kanal kuantum yang mengandung noise.

Lanjutan pada halaman berikutnya

Tabel 2.3 Kajian Literatur Penelitian Terkait Protokol BB84 (Lanjutan)

Referensi	Metode	Hasil Penelitian	Kontribusi
[55]	Simulasi protokol BB84 menggunakan platform komputasi kuantum untuk menganalisis pengaruh dinamika kanal komunikasi terhadap distribusi kunci kuantum.	Hasil simulasi menunjukkan bahwa peningkatan jarak transmisi menyebabkan peningkatan Quantum Bit Error Rate (QBER) akibat efek dissipative pada kanal komunikasi kuantum.	Menyediakan model simulasi BB84 untuk menganalisis hubungan antara parameter kanal komunikasi dan tingkat kesalahan bit pada sistem QKD.

Berdasarkan kajian literatur yang ditunjukkan pada Tabel 2.3, dapat diketahui bahwa berbagai penelitian sebelumnya telah mengkaji protokol BB84 dari beberapa perspektif yang berbeda. Penelitian oleh Adu-Kyere, memfokuskan pada implementasi simulasi BB84 menggunakan Python untuk memodelkan komunikasi antara Alice dan Bob serta mendeteksi keberadaan penyadap melalui peningkatan tingkat kesalahan bit. Penelitian lain oleh Fiorini, menganalisis hubungan antara tingkat intersepsi penyadap dengan *Quantum Bit Error Rate* (QBER) menggunakan simulator kuantum dengan mempertimbangkan kondisi kanal yang mengandung *noise*. Sementara itu, Jayachandran. mengusulkan peningkatan keandalan sistem BB84 melalui integrasi mekanisme *Quantum Error Correction* untuk mengurangi kesalahan dalam proses distribusi kunci.

Selain itu, penelitian oleh Kumar. menggunakan pendekatan simulasi Monte Carlo untuk menganalisis pengaruh *depolarizing channel noise* terhadap performa protokol BB84. Penelitian tersebut menunjukkan bahwa peningkatan tingkat *noise* pada kanal komunikasi dapat meningkatkan nilai QBER serta mempengaruhi jumlah kunci yang dapat dihasilkan secara aman. Penelitian lain oleh Salatino. juga mengkaji pengaruh dinamika kanal komunikasi kuantum terhadap proses distribusi kunci melalui simulasi pada platform komputasi kuantum.

Berdasarkan beberapa penelitian tersebut, dapat disimpulkan bahwa sebagian besar penelitian sebelumnya berfokus pada simulasi protokol BB84,

analisis serangan penyadapan, serta pengaruh noise pada kanal komunikasi kuantum. Oleh karena itu, penelitian ini mengimplementasikan simulasi protokol BB84 menggunakan Python dengan mempertimbangkan beberapa parameter sistem, yaitu jumlah bit atau qubit yang dikirimkan, keberadaan penyadap (Eve), serta pengaruh noise pada kanal komunikasi. Evaluasi performa sistem dilakukan menggunakan metrik *Key Generation Rate* (KGR), *Quantum Bit Error Rate* (QBER), *Secret Key Rate* (SKR) untuk menganalisis tingkat keamanan, efisiensi, dan kerahasiaan distribusi kunci pada berbagai kondisi komunikasi kuantum.