Simulasi Pemanfaatan Quantum Key Distribution Dalam Pengiriman Kunci Kriptografi Simetris

Aufa Fadhlurohman - 13518009
Program Studi Teknik Informatika
Sekolah Teknik Elektro dan Informatika
Institut Teknologi Bandung, Jalan Ganesha 10 Bandung
E-mail : aufafadhlurohman@gmail.com

***Abstrak*—Saat ini, perkembangan komputasi kuantum menunjukkan potensi yang luar biasa. Potensi ini dapat dilihat dari berbagai konsep yang diperkenalkan. Fenomena supremasi kuantum atau titik di mana komputer kuantum dapat memecahkan masalah yang tidak dapat diselesaikan komputer klasik semakin jelas dirasakan. Salah satu bidang yang merasakan dampak dari perkembangan ini adalah bidang kriptografi. Berbagai algoritma dan protokol kriptografi diprediksi dapat dipecahkan tanpa memerlukan waktu yang panjang jika komputer kuantum dengan daya yang cukup berhasil dibangun. Fenomena ini akan menghasilkan kondisi ketidakpastian pada sistem keamanan data yang saat ini digunakan. Potensi ketidakamanan yang besar ini membuat bidang kriptografi harus senantiasa beradaptasi dan mempersiapkan apabila keadaan tersebut terjadi. Salah satu konsep komputasi kuantum yang berkaitan dengan keamanan adalah quantum key distribution. Konsep ini menghadirkan standar baru dalam komunikasi yang aman. Dalam kriptografi kunci simetris, diperlukan saluran komunikasi yang aman dari penyadapan untuk melakukan pengiriman kunci. Konsep distribusi kunci yang menggunakan kanal dan konsep kuantum menjadi salah satu alternatif untuk mengatasi permasalahan pengiriman ini.**

Kata Kunci—Quantum Key Distribution. Post-Quantum Cryptography, Distribusi Kunci, Anti Penyadapan

I. PENDAHULUAN

Di era disrupsi, teknologi berkembang dengan sangat cepat. Perkembangan yang begitu cepat ini membuat setiap bidang harus selalu siap beradaptasi untuk dapat mempertahankan nilainya. Salah satu ancaman disrupsi teknologi terbesar pada beberapa tahun ke depan setelah era kecerdasan buatan adalah komputasi kuantum.

Komputasi kuantum adalah kombinasi dari fisika kuantum, ilmu komputer, dan teori informasi [1]. Berbagai publikasi mengenai konsep pemanfaatan fenomena kuantum untuk komputasi ini menunjukkan hasil yang luar biasa. Hal ini menyebabkan komputer kuantum disebut sebagai *super computer* yang banyak digunakan di masa depan. Teknologi ini dikembangkan dengan memanfaatkan kondisi elemen kuantum seperti superposisi, interferensi, dan keadaan berbelit dalam melangsungkan perhitungannya. Konsep mekanika kuantum dan teori informasi yang digabungkan ini berhasil menghadirkan sudut pandang baru dalam komputasi. Berbagai algoritma dan protokol yang dapat memanfaatkan fenomena ini terus dikembangkan seiring dengan pengembangan komputer kuantum yang memiliki daya besar. Berbagai perusahaan teknologi besar seperti Google, Microsoft, hingga IBM sedang mengembangkan perangkat keras komputer kuantum ini diiringi dengan mempersiapkan algoritma dan protokol untuk memanfaatkannya. Pada tahun 2019, perusahaan Google mengeluarkan hasil risetnya berupa konsep supremasi kuantum. Supremasi kuantum berbicara tentang kemampuan komputer kuantum yang dapat melakukan pekerjaan yang komputer klasik tercanggih yang saat ini ada di dunia tidak dapat lakukan. Konsep ini memberikan gambaran awal mengenai dampak disrupsi besar dari penemuan teknologi kuantum. Oleh karena itu, antisipasi terhadap dampak yang mungkin terjadi dengan kehadiran komputer kuantum harus menjadi hal yang diperhatikan.

Saat ini, keamanan komunikasi dibangun oleh berbagai konsep kriptografi. Hal ini membuat kriptografi harus dikembangkan demi menjaga sistem keamanan dengan kehadiran komputer kuantum berdaya besar di masa depan. Saat ini, kebanyakan dari sistem kriptografi dibangun dengan dasar matematis. Keamanan diciptakan dengan membuat suatu perhitungan yang sulit dipecahkan oleh komputer klasik dengan waktu yang efisien. Salah satu contohnya adalah skema kriptografi asimetrik yang banyak digunakan untuk membentuk keamanan internet. Skema ini menjadi salah satu sasaran nyata dengan kehadiran komputer kuantum. Menurut Arslan dan Ulker (2018), kekuatan matematis skema kriptografi asimetris tidak mampu menyediakan tingkat keamanan yang cukup untuk menghindari serangan yang memanfaatkan komputer kuantum[2]. Algoritma Shor yang diciptakan Peter Shor dapat melakukan faktorisasi bilangan yang sangat besar dengan menggunakan komputer kuantum. Proses ini dapat digunakan untuk memecahkan algoritma kriptografi kunci publik seperti RSA dengan cepat.

Skema kriptografi simetris dan fungsi hash juga terdampak dari kehadiran komputasi kuantum. Namun, dampak yang dirasakan tidak sebesar yang akan dialami pada sistem kriptografi kunci asimetris. Kedua skema ini hanya perlu pengembangan untuk membuat semakin kuat. Untuk fungsi hash, peningkatan jumlah kunci minimal dua kali lipat sudah cukup untuk menekan kemampuan komputer kuantum untuk menyerang sistem keamanan yang memanfaatkan skema ini[3].

Potensi celah keamanan yang timbul akibat kehadiran komputer kuantum membuat usaha menemukan solusi kriptografi post-quantum menjadi salah satu isu yang sangat penting. Pengembangan ini harus dilakukan selama jumlah daya qubit (quantum bit) pada komputer kuantum yang dapat diimplementasikan masih dalam jumlah kecil. Keamanan yang lebih dijamin dari skema kriptografi simetris mungkin membuat skema ini menjadi salah satu yang akan kembali dikembangkan ke depannya. Skema kriptografi simetris memerlukan saluran komunikasi yang aman untuk melakukan pengiriman kunci. Salah satu pemanfaatan teknologi kuantum yang berkembang adalah konsep distribusi kunci kuantum. Konsep ini menggunakan saluran dan komputer kuantum untuk menciptakan sistem komunikasi yang aman dari penyadap.

II. Landasan Teori

A. *Komputer Klasik*

Komputer klasik merupakan perangkat komputasi yang bekerja menggunakan sistem digital berbasiskan digit biner (0 dan 1). Perangkat ini dapat melakukan komputasi suatu permasalahan dengan memanfaatkan operasi dari digit-digit biner yang dimiliki. Perkembangan kecepatan komputer klasik berjalan bersamaan dengan semakin efisien dan kecilnya transistor. Transistor merupakan elemen yang dapat menyimpan state listrik untuk merepresentasikan dan melakukan komputasi digital. Penemuan dan perkembangan komputer klasik menyebabkan percepatan inovasi teknologi pada beberapa waktu ke belakang. Salah satu produk dari komputer klasik yang paling berpengaruh dalam perkembangan dunia adalah internet. Internet memudahkan pertukaran informasi dengan konektivitas yang tinggi. Kriptografi modern hadir beriringan dengan munculnya perangkat komputasi ini. Hal ini didorong oleh kebutuhan akan sistem keamanan yang lebih tangguh dengan munculnya komputer.

B. *Komputer Kuantum*

Komputer kuantum merupakan perangkat komputer yang dirancang berdasarkan aturan fisika kuantum. Komputer kuantum melakukan komputasi dengan menggunakan entitas pemrosesan yang disebut *quantum bit* atau qubit. Perangkat ini memiliki kapasitas dan daya pemrosesan yang lebih tinggi dibandingkan dengan komputer klasik [4]. Saat ini, komputer kuantum masih dalam tahap pengembangan. Beberapa perusahaan dan lembaga riset ternama di dunia ikut serta dalam pengembangan ini hingga perangkat komputer ini beberapa kali sudah digunakan walau dalam daya yang rendah. Walaupun dengan daya yang rendah, perangkat tersebut menunjukkan hasil yang sangat memuaskan. Salah satu contoh nyata kemampuan komputer ini dapat dilihat dari hasil publikasi Google AI yang dipimpin oleh ahli fisika John Martinis pada tahun 2019. Publikasi tersebut menyebutkan uji coba mereka dalam menghitung bilangan acak yang sangat rumit dapat diselesaikan dalam waktu 3 menit 20 detik dengan komputer kuantum berdaya 54 qubit. Jika pekerjaan ini dilakukan komputer klasik tercanggih saat itu, diperlukan waktu hingga 10.000 tahun [5].

C. *Qubit*

Qubit merupakan unit pemrosesan terkecil dalam konsep komputasi kuantum. Qubit merupakan partikel berukuran nano yang memiliki sifat mekanika kuantum[6]. Pada dasarnya, sebuah qubit juga dapat memiliki keadaan 0 dan 1 seperti pada konsep bit, namun qubit juga dapat berada pada keadaan superposisi. Superposisi merupakan keadaan di mana pada suatu saat yang bersamaan dapat berada di keadaan 0 dan 1. Sifat dasar ini yang memberikan kemampuan lebih pada komputer kuantum.

Qubit dapat dibuat oleh berbagai elemen fisika yang memenuhi konsep mekanika kuantum. Contohnya adalah spin elektron yang dapat berada pada putaran atas dan putaran bawah atau polarisasi foton yang dapat merepresentasikan keadaan polarisasi vertikal dan polarisasi horizontal.

Qubit direpresentasikan dalam notasi *dirac*. Berikut adalah beberapa representasi matriks dan notasi dari qubit yang sering digunakan dalam kuantum sederhana:

$$\begin{bmatrix}1\\0\end{bmatrix} = |0\rangle, \qquad \begin{bmatrix}0\\1\end{bmatrix} = |1\rangle.$$

$$|+\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle),$$

$$|-\rangle = \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle).$$

D. *Prinsip dalam Komputasi Kuantum*

Salah satu konsep besar dalam komputer kuantum adalah pemanfaatan keadaan superposisi. Keadaan ini didefinsikan sebagai keadaan atom memiliki kondisi 1 (*spin up*) dan 0 (*spin down*) secara bersamaan. Atom akan berada pada kondisi ini sampai dilakukan pengukuran. Proses pengukuran membuat atom harus menentukan pilihan salah satu dari dua kondisi yang dapat terjadi. Pengukuran membuat kondisi atom menjadi tetap[8].

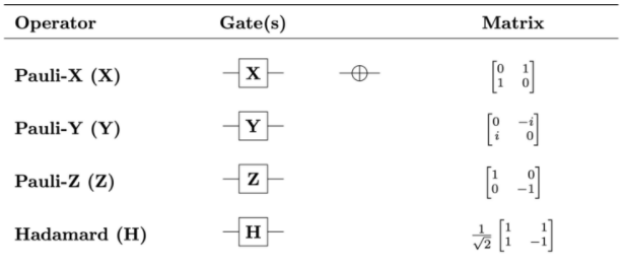
Komputer kuantum dapat bekerja lebih cepat dari komputer klasik karena perhitungan yang dapat dilakukan secara simultan. Kemungkinan hasil dari perhitungan ini akhirnya bervariasi. Pengukuran adalah tindakan yang menyebabkan berhentinya proses perhitungan qubit dan memaksa sistem menentukan *state*. Sistem paralel ini menjadi dasar dari cepatnya proses komputasi pada komputer kuantum [8].

Salah satu fenomena menarik lain dalam komputer kuantum adalah keadaan berbelit (*entanglement*). Konsep ini menghadirkan suatu penemuan baru yaitu telepati kuantum. Jika dua atom mendapatkan gaya tertentu, kedua atom tersebut dapat masuk ke keadaan berbelit dan menjadi saling terhubung walau memiliki jarak yang jauh. Perlakukan terhadap satu

atom akan menyebabkan atom lainnya mengalami hal yang sama. Sifat ini membuat komunikasi menggunakan komputer kuantum dapat mencapai kecepatan yang sangat tinggi karena terjadi secara instan [8].

E. Gerbang Kuantum

Gerbang kuantum digunakan dalam melakukan operasi kuantum. Gerbang ini dapat membangun rangkaian kuantum yang melakukan proses tertentu. Terdapat beberapa jenis gerbang kuantum yang banyak digunakan. Gambar 1 menunjukkan beberapa gerbang logika kuantum berserta matriks representasinya.



Gambar 1. Gerbang Logika Kuantum

Sumber: Rxtreme, diakses melalui *https://en.wikipedia.org/*

F. Quantum Key Distribution

Distribusi kunci kuantum atau *quantum key distribution* (QKD) merupakan protokol distribusi yang memanfaatkan hukum alami dasar untuk melakukan pengamanannya. Sistem ini berbeda dengan pengamanan klasik yang mengedepankan perhitungan matematis yang kompleks untuk membuat aman. Salah satu prinsip dasar yang dimanfaatkan adalah teori bahwa kondisi kuantum (*quantum states*) tidak dapat disalin atau didapatkan tanpa melalui pengukuran yang mengubah *state* tersebut. Penyadap yang ingin membaca pesan yang dikirim akan mengubah kondisi qubit yang dikirim dan dapat dilakukan verifikasi dengan melakukan perbandingan nilai yang didapatkan.

Distribusi kunci kuantum bekerja dengan memanfaatkan kanal kuantum dan melakukan transmisi menggunakan elemem kuantum seperti partikel cahaya atau foton. Partikel ini bertransmisi menggunakan kabel fiber optik, sehingga dapat dilihat bahwa implementasi QKD membutuhkan infrastruktur baru yang melibatkan kanal dan komputer kuantum. Mekanisme QKD pada umumnya juga masih memanfaatkan kanal klasik untuk dapat mengirimkan informasi yang sifatnya terbuka.

G. Kriptografi Kunci Simetris

Kriptografi kunci simetris adalah sistem kriptografi yang proses enkripsi dan dekripsinya dilakukan dengan kunci yang sama. Terdapat berbagai algoritma yang memiliki prinsip demikian. Konsep ini memiliki kelebihan karena kecepatannya yang tergolong lebih cepat dibandingkan mayoritas kriptografi kunci asimetris. Namun, konsep kriptografi kunci simetris memiliki masalah terkait dengan distribusi kunci. Kunci privat harus dikirim melalui saluran yang benar-benar aman. Saluran yang aman ini umumnya lambat dan mahal[9].

Komputer kuantum memiliki algoritma yang memiliki kemampuan tinggi dalam memecahkan masalah faktorisasi. Hal ini menyebabkan beberapa algoritma kunci asimetris yang memanfaatkan sulitnya proses faktorisasi seperti RSA dapat dengan cepat diserang oleh algoritma kuantum shor. Kekuatan algoritma kunci publik dan hash ternyata lebih tinggi dalam menghadapi kehadiran komputer kuantum. Dua konsep ini lebih tahan dari serangan kuantum, hanya diperlukan peningkatan jumlah kunci dan berbagai optimasi untuk membuatnya semakin tahan. Oleh karena itu, diperlukan saluran yang dapat mengirimkan informasi kunci secara aman. Dan salah satu konsep komputer kuantum yaitu distribusi kunci kuantum menawarkan kemampuan tersebut.

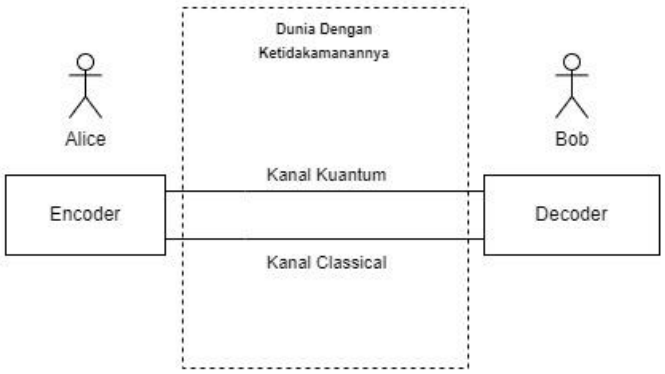
III. RANCANGAN DAN IMPLEMENTASI

A. Skema Distribusi

Konsep distribusi kunci kuantum pada implementasinya memerlukan kanal kuantum. Saat ini kanal kuantum diimplementasikan menggunakan kabel fiber optik. Kanal ini memiliki kemampuan untuk menghantarkan informasi kuantum dengan kemampuan fisikanya. Dalam penelitian ini, akan digunakan perangkat simulasi untuk melakukan percobaan pengiriman kunci dengan sistem distribusi kunci kuantum ini.

Proses proses pengiriman data rahasia memanfaatkan algoritma kriptografi kunci simetris dan distribusi kunci kuantum menggunakan dua buat kanal yang berbeda. Kanal kuantum digunakan untuk pengiriman kunci agar tetap aman dan memiliki kemampuan prediksi akan penyadapan. Kanal klasik akan digunakan untuk pengiriman pesan terenkripsi sehingga keamanannya berada pada pesan yang tidak lagi bermakna.

Skema distribusi pesan dan kunci dapat dilihat pada gambar 2. Alice merepresentasikan pengirim pesan sedangkan bob sebagai penerima. Pesan terenkripsi dikirim melalui kanal klasik, proses enkripsi dapat dilakukan dengan memanfaatkan berbagai algoritma kunci simetris seperti DES, Stream Cipher, Vigenere Cipher, Enigma Cipher, RC4, RC5, dan banyak lainnya. Pada percobaan kali ini, digunakan algoritma RC4 modified untuk mengenkripsi yang melalui tahap *key-scheduling algorithm* dan *pseudo-random generation algorithm* untuk proses enkripsi dan dekripsinya. Pada implementasi riil mungkin dapat memanfaatkan algoritma yang lebih kuat dan sulit untuk diserang, khususnya yang tahan akan serangan kuantum. Alice akan melakukan enkripsi pesan dan mengirimkannya melalui kanal klasik dan Bob menerima pesan terenkripsi tersebut. Untuk membaca pesan bermakna, Bob membutuhkan kunci dekripsi yang hanya dimiliki Alice. Alice akan mengirimkan kunci ini melalui kanal kuantum yang menggunakan konsep distribusi kunci kuantum.



Gambar 2. Ilustrasi Skema Pemanfaatan Distribusi Kunci Kuantum

Sumber: Dokumentasi Penulis

Simulasi implementasi dilakukan dengan memanfaatkan kakas Qiskit. Kakas ini menyediakan lingkungan riset dan pengembangan pemrograman kuantum. Kakas ini sudah menyediakan metode visualisasi yang memudahkan dalam memahami program yang dibangun. Program dijalankan dalam layanan IBM Quantum Lab yang disediakan perusahaan besar IBM untuk mendapatkan visualisasi yang lebih baik dalam representasi qubitnya.

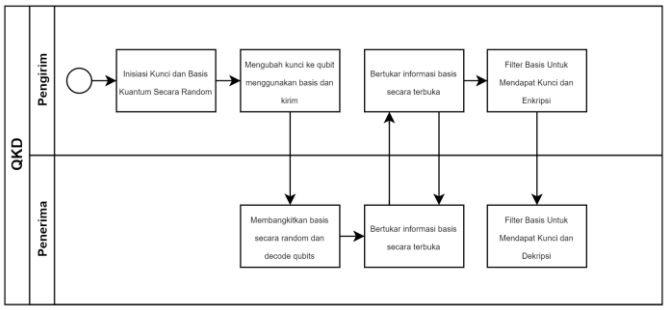
B. Simulasi Implementasi

Konsep keamanan distribusi kunci kuantum diciptakan lewat pemanfaatan sifat kondisi kuantum yang berubah setelah terjadinya pengukuran. Ketika Alice ingin mengirimkan qubit ke Bob, jika terdapat penyadap yang mencoba mengukur data yang sedang dalan pengiriman, kondisi state kuantum akan berubah sehingga Bob tidak akan mendapatkan state yang dikirimkan Alice.

Protokol distribusi kunci kuantum dapat dirangkum dalam beberapa tahap berikut ini[7]:

1. Pengirim menyiapkan string yang berisikan bilangan biner acak dan sebuah list yang merepresentasikan basis dari setiap bit (panjangnya sama).
2. Pengirim melakukan encoding setiap bit menjadi list qubit yang berdasarkan basis yang dipilih tadi. Qubit ini akan dikirim ke penerima melalui kanal kuantum.
3. Penerima akan menghitung bit yang diterima melalui transfotmasi qubit dengan basis random yang ia bangkitkan.
4. Pengirim dan penerima membagikan yang masing-masing gunakan untuk setiap qubit. Jika penerima mengukur qubit dengan basis yang sama dengan yang pengirim, mereka akan menggunakan basis ini untuk membentuk bagian dari kunci rahasia bersama, kalau berbeda informasi basis tersebut diabaikan.
5. Pengirim dan penerima mendapatkan kunci yang sama, pengirim kunci dapat melakukan enkripsi dengan kunci tersebut sedangkan penerima kunci dapat menunggu kiriman pesan terenkripsi untuk nantinya melakukan dekripsi menggunakan kunci yang ia dapat.

Prosedur diatas dapat diilustrasikan dalam gambar di bawah ini (gambar 3).



Gambar 3. Ilustrasi Skema Distribusi Kunci Kuantum

Sumber: Dokumentasi Penulis

Dalam implementasinya, kunci yang akan diambil adalah N buah bit pertama, dengan N merupakan bilangan terbesar yang masih lebih kecil daripada jumlah bit yang ditemukan dalam distribusi kunci.

IV. EKSPERIMEN DAN HASIL

Eksperimen dilakukan dengan melakukan pengiriman suatu pesan. Tersapat dua buah kasus yang dianalisis, pertama pengiriman nornal dan kedua pengiriman dengan keberadaan penyadap yang mencoba membaca pesan.

A. Pengiriman Tanpa Penyadap

Proses distribusi kunci diawali dengan melakukan inisiasi kandidat kunci dan basis yang akan digunakan untuk membuat qubit dari sisi pengirim. Untuk basis, angka 0 merepresentasikan basis Z sedangkan angka 1 merepresentasikan basis X. berikut adalah tabel transformasi basis yang digunakan:

Tabel 1. Transformasi Bit ke Qubit

Basis	Bit	Qubit
Z	0	$\|1\rangle$
	1	$\|0\rangle$
X	0	$\|+\rangle$
	1	$\|-\rangle$

Kunci Random **Pengirim** :

```
11011110110010010101000101110110011010001101100101101110001011110111010110000011100111010010000001111010010000011001010100000111001000111000011111100010110011110011110101110000000001111011100011001100
```

Basis Random **Pengirim** :

```
00110011101110011100110011110011101011000001000010001111110110111001110110011001
```

```
01001100011101000110011111000111010101011
10110101111000001110101001110101011100110
00111100010101111010000011100101101111100
```

Selanjutnya akan dilakukan pengkodean atau transformasi bit ke qubit berdasarkan bit dan basis yang sudah di-*generate* sebelumnya. Proses encoding dilakukan dengan meaplikasikan transformasi yang ditunjukkan pada tabel 1.

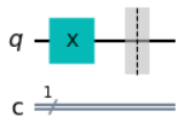
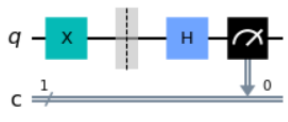
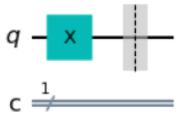
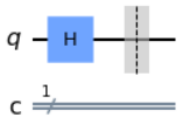
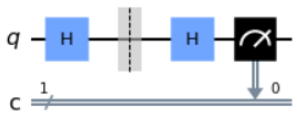
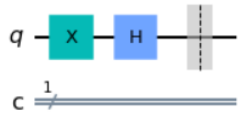
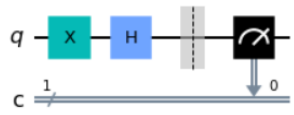
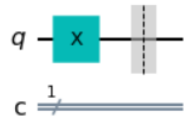
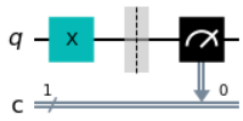
Basis Random **Penerima** :
```
11011110110010010101000101110110011010000
11011011011010111000101111011101011000000
11100111010010000001111010010000110010100
10000011100100011100001111110001011001110
10011110010111000000000111101110001100110
```

Basis acak yang dibangkitkan penerima akan menjadi basis transformasi balik dari qubit menjadi bit. Proses ini menghasilkan list bit berikut:

Pesan Yang **Diterima** :
```
01011110111101010111110111110001110000000
11010001011000000001000001010101110100000
10101011010000000000111001110011000010000
00110001101100011100111110010101000001111
10010011110001111000000110101010001101111
```

Sesuai dengan konsep kuantum yang mengatakan bahwa pesan akan berubah setelah dilakukan pengukuran, maka setelah penerima melakukan pengukuran untuk membaca pesan, qubit pesan akan berubah. Berikut adalah beberapa representasi qubit yang diamati sebelum dan sesudah melakukan pengukuran (5 qubit pertama):

Tabel 2. Perbandingan Qubit Sebelum dan Sesudah Pengukuran

No	Qubit Sebelum Pengukuran	Qubit Sesudah Pengukuran
0		
1		
2		
3		
4		

Setelah pengukuran dilakukan penerima, pengirim dan penerima akan bertukar informasi mengenai basis mereka secara terbuka. Lima basis pertama yang dibangkitkan penerima adalah XXXZZ (11100), sedangkan lima basis pertama pengirim adalah ZZXXZ (00110). Basis yanh sama terjadi pada qubit ke-2 dan qubit ke-4. Pada qubit ke-2, basis yang sama membuat dapat dipastikan pesan hasil decoding dari sisi penerima mendapatkan nilai 0, begitu pula pada hasil qubit ke-4. Sedangkan qubit lainnya memiliki peluang 0,5 sehingga tidak dapat dipastikan memiliki nilai tertentu. Prinsip ini dilakukan untuk 200 qubit yang diproses.

Untuk mendapatkan pesan yang sama, dilakukan penyaringan bit-bit dengan tingkat *confidence* tinggi atau qubit yang diproses dengan basis yang sama. Proses ini dapat dilakukan karena informasi basis telah saling ditukar, baik pengirim dan penerima dapat menyaring berdasarkan informasi yang telah dimiliki. Proses ini menghasilkan bit-bit sebagai berikut:

Pesan **Pengirim** Tersaring :
```
01110111010110100000011100000110111000011
10010000001110101011000001001011100111000
10101110011110100000101001001
```

Pesan **Penerima** Tersaring :
```
01110111010110100000011100000110111000011
10010000001110101011000001001011100111000
10101110011110100000101001001
```

Hasil penyaringan pesan selanjutnya akan dibagi menjadi 2 bagian yaitu sampel dan kunci. Bagian sampel digunakan untuk melakukan verifikasi terkait dengan keamanan kanal kuantum yang digunakan. Pada uji coba kali ini, digunakan 20 bit yang diambil secara acak dari penyaringan untuk menjadi data sampel. Bagian sample ini akan saling dikirimkan secara terbuka dan nilai pengirim dan penerima dibandingkan. Berikut adalah hasil dari pembagian tersebut:

Tabel 3. Pembagian Sampel dan Kunci

Data	Nilai
Posisi Acak	10,20,172,102,13,140,121,3,10, 154,199,91,177,19,132,48,194,11

	2,156,68
Bit Sampel Pengirim	01011101101010001101
Bit Kunci Pengirim	0101110100000011000010111000011 0010000011101011100001010111001 1100101100111010000011000001
Bit Sampel Penerima	01011101101010001101
Bit Kunci Penerima	0101110100000011000010111000011 0010000011101011100001010111001 1100101100111010000011000001

Dari tabel 3, dapat dilihat bahwa bit-bit sampel yang dimiliki pengirim dan penerima memiliki nilai yang sama. Hal ini menunjukkan tidak ada pihak yang berusaha menyadap dalam kanal kuantum, dan qubit yang dikirimkan pengirim diterima dengan baik tanpa adanya pengubahan saat perjalanan pengiriman.

Bilangan biner kunci hasil pemisahan akan menjadi kunci dari proses enkripsi dan dekripsi. Bilangan ini masih bersifat privat dan tidak diketahui siapapun selama bilangan sampel menunjukkan kesamaan. Dikarenakan panjang dari bit-bit kunci tidak merupakan kelipatan 8, maka akan dilakukan pemotongan hingga panjangnya menjadi kelipatan 8 terbesar. Bilangan biner yang didapat terdapat sepanjang 89, untuk itu 1 pesan terakhir dibuang dan bit-bit akan diubah menjadi representasi base64 sebagai kunci. Pengirim akan melakukan enkripsi dan mengirim pesan terenkripsi ke penerima. Penerima akan melakukan dekripsi pesan tersebut dengan kunci yang berhasil didapatkan.

Tabel 4. Pemotongan Bilangan Biner dan Konversi ke Base64

Representasi	Nilai
Biner Kunci	0101110100000011000010111000011 0010000011101011100001010111 0011100101100111010000011000 01
Base64	ugYXDIOuFc5Z0GE=\n

Pesan yang ingin dikirim adalah “Untuk Kita Menaklukan Dunia”. Berikut adalah hasil enkripsi RC4 yang dilakukan pengirim menggunakan kunci yang didapatkan terhadap pesan tersebut:

Tabel 4. Proses Enkripsi Oleh Pengirim

Pesan	Nilai
Plaintext	Untuk Kita Menaklukan Dunia
Ciphertext	<Låª Î!8\x97e®\x9a&\x89ÿü\x11% (\x9a\x86J\xa0\x9e²â\x1cç\x06

Pesan ini dikirimkan melalui kanal klasik. Penerima yang sebelumnya telah memiliki kunci hasil distribusi kunci kuantum dapat melakukan dekripsi terhadap pesan *ciphertext* yang diterima. Dapat dilihat sebelumnya bahwa biner yang didapatkan sama persis, penerima juga melakukan pemotongan dan konversi yang sama pada tabel 3 pada komputernya sendiri. Berikut adalah hasil dekripsi dari penerima:

Tabel 5. Proses Dekripsi Oleh Penerima

Pesan	Nilai
Ciphertext	<Låª Î!8\x97e®\x9a&\x89ÿü\x11% (\x9a\x86J\xa0\x9e²â\x1cç\x06
Plaintext	Untuk Kita Menaklukan Dunia

Tangkapan layar proses dekripsi dapat dilihat pada gambar 4. Skema distribusi kunci kuantum yang diimplementasikan untuk mengirimkan kunci kriptografi simetri berhasil bekerja dengan baik. Pada kasus ini tidak ada pihak yang mencoba membaca nilai yang sedang dikirim sehingga proses berjalan dengan lancar.

Gambar 4. Proses Dekripsi Pesan

Sumber: Dokumentasi Penulis

B. Pengiriman Dengan Penyadap

Kasus kedua ini akan mencoba menganalisis kondisi ketika terdapat pihak yang berusaha melakukan penyadapan terhadap proses distribusi kunci. Pada mulanya, dilakukan proses yang sama dengan proses tanpa penyadapan hingga pengirim siap mengirimkan qubit hasil transformasi basis.

Kunci Random **Pengirim** :
1101111011001001010100010111011001101000
1101101101101011100010111101110101100000
1110011101001000000111101001000011001010
1000001110010001110000111111000101100111

1001111001011100000000011110111000110011
Basis Random **Pengirim** : 0011001110111001110011001111001110101100 0001000010001111110110111001110110011001 0100110001110100011001111100011101010101 1011010111100000111010100111010101110011 0011110001010111101000001110010110111100

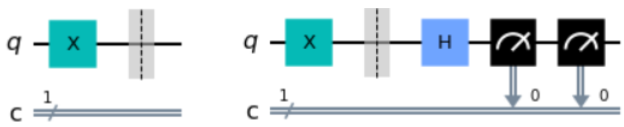
Pada proses pengiriman, ternyata terdapat pihak yang dapat mengakses kanal dan melakukan pengukuran data yang dikirim. Penyadap tersebut melakukan pengukuran dengan basis random seperti yang seharusnya dilakukan penerima.

Basis Random **Penyadap** : 1110001001101110011010101110011001000100 1100101000000100010111000001001100101001 0100100100011110001101110010101011110010 1011011011101100110011101010000001011010 0011110110001111001101100000111010011110
Pesan Yang Didapatkan **Penyadap** : 0000111011011001011100110111001101101000 0101000111101011000011100101111111100000 1110011100101010000111100011000011001111 1000000110011101111001111010000001100110 100111110100110000010011000011010011001

Pesan yang sudah dibaca oleh penyadap akan diteruskan kepada penerima asli. Dikarenakan konsep kuantum yang telah disebutkan sebelumnya, pesan qubit yang terkirimkan berubah kondisi karena proses pengukuran oleh penyadap. Dan pada kasus ini, penerima akan menerima dan melakukan transformasi dengan basis acaknya sendiri. Berikut adalah rangkaian bit yang diterima setelah dilakukan *decoding:*

Basis Random **Penerima** : 0000101100011011000100000000011000001111 0001000101010011111011101101011010000000 1101000110110000101110001010000110000100 1010111111100110100110001010000101010001 1001101010100100111111011010111110011100
Pesan Yang Didapatkan **Penerima** : 0000011111010011111001110111001101010111 0100001001110001001011011100111101100000 1010011111011000010001101101100001001111 1010000100011101111000111010010001110111 1000010001011100010000101010010100010011

Kehadiran penyadap membuat qubit yang diterima penerima mengalami perubahan *state*. Salah satu contohnya dapat dilihat pada gambar 5. Nilai basis pengirim dan penerima sama pada basis qubit ke-1. Seharusnya nilai pada basis ke-1 ini merupakan nilai yang sama, namun penyadapan membuat *state* yang diterima penerima pesan berubah sebelum diterima. Pengubahan ini menyebabkan kemungkinan kemunculan nilai 0 dan 1 masing-masing 50% sehingga tidak ada kepastian pada qubit tersebut. Walaupun kondisi ini tidak bisa dilihat secara langsung, namun hal ini akan berpengaruh saat perbandingan atau verifikasi qubit sampel nantinya.



Gambar 5. Qubit 1 (Terkirim dan Diterima)

Sumber: Dokumentasi Penulis (QisKit)

Seperti sebelumnya, akan dilakukan penyaringan berdasarkan kesamaan basis setelah pertukaran basis dilakukan. Proses ini menghasilkan bit-bit sebagai berikut:

Pesan **Pengirim** Tersaring : 1111010101001110110110111110111011011001 1100100011000101100011001011001100101001 1011011000110100010011
Pesan **Penerima** Tersaring : 0011111001111101010000110100101001011000 1101100011100111101010001111001100001101 1000011001110110010011

Selanjutnya dilakukan pembagian sampel dan kunci. Sampel akan dibagikan secara terbuka dan kunci dijaga tetap privat. Berikut adalah hasil dari pembagian tersebut:

Tabel 6. Pembagian Sampel dan Kunci

Data	Nilai
Posisi Acak	131,68,32,114,109,137,40,89,75, 139,139,4,172,101,149,10,104, 20,111,131
Bit Sampel Pengirim	10100100100011011110
Bit Kunci Pengirim	1111101010111011011101101010011 1000011001110001101011011010100 11010110001100010011
Bit Sampel Penerima	00111100001110011010
Bit Kunci Penerima	0011110011101000010101100010001 1010011101110101001111011000110

	11000110011101010011

Langsung terlihat bahhwa nilai sampel yang didapatkan pengirim dan penerima adalah nilai yang berbeda. Hal ini kemungkinan disebabkan karena adanya penyadap yang melakukan pengukuran terhadap pesan. Pengukuran tersebut menyebabkan berubahnya *state* kuantum yang diterima pihak penerima. Oleh karena itu, kunci yang diterima tidak valid dan harus dilakukan prosedur distribusi ulang sampai ditemukan kondisi yang aman.

C. Analisis

Dari kedua kasus yang diujikan, dapat terlihat bahwa protokol dan infrastruktur kuantum dapat digunakan untuk melakukan distribusi kunci secara aman. Dalam prosesnya juga dapat dideteksi pengukuran atau penyadapan pesan karena sifatnya yang mengubah *state* dari qubit yang dikirimkan. Namun pada implementasinya, masiuh terdapat peluang penyadapan berhasil jika pembangkitan acak basis pengirim, penyadap, dan penerima serupa atau peluang 50% menghasilkan tebakan yang benar di sisi penerima. Untuk itu, kemampuan dan penelitian untuk hal ini harus terus dikembangkan.

V. KESIMPULAN

Penemuan komputer kuantum membuat terjadinya disrupsi yang besar, khususnya di masa depan. Saat ini, komputer kuantum masih dalam tahap pengembangan, namun konsep yang diperkenalkan sudah cukup membuat berbagai bidang terancam akibat kekuatan "super" yang dimiliki. Bidang kriptografi menjadi salah satu bidang yang mendapatkan pengaruh besar jika komputer kuantum berdaya tinggi berhasil diciptakan. Skema algoritma kriptografi kunci publik atau kriptografi asimetris menjadi salah satu hal yang paling terancam karena terdapat algoritma kuantum yang dapat melakukan faktorisasi secara sangat cepat. Padahal saat ini, skema kriptografi simetris digunakan untuk melakukan pengamanan berbagai informasi penting. Salah satu alternatif penanggulanggannya adalah dengan menggunakan algoritma kriptografi simetris dengan protokol distribusi pesan yang aman dari ancaman quantum. Konsep distribusi kunci kuantum atau quantum key distribution menjadi salah satu konsep yang sedang dikembangkan untuk mendistribusikan kuncu secara aman memanfaatkan komputer dan infrastruktur kuantum.

Protokol distribusi kunci kuantum dapat melakukan pendeteksian penyadapan. Hal ini dilakukan dengan memanfaatkan sifat kuantum yang akan berubah *state* saat dilakukan pengukuran. Namun, masih terdapat celah penyadapan dapat terjadi sehingga protokol ini saat ini masih dikembangkan untuk menciptakan keamanan terbaik yang dapat dilakukan.

UCAPAN TERIMA KASIH

Puji syukur kehadirat Allah SWT, karena atas limpahan rahmat dan karunia-Nya, sehingga penulis dapat menyelesaikan pembuatan makalah ini. Terima kasih penulis ucapkan kepada Bapak Dr. Ir. Rinaldi Munir, M.T. sebagai dosen pengampu dalam mata kuliah IF4020 Kriptografi yang telah memberikan ilmu dan pengalaman yang sangat bermanfaat selama perkuliahan. Terima kasih juga penulis ucapkan kepada kedua Orang Tua penulis yang senantiasa memberikan dukungan moral dalam setiap aktivitas penulis.

REFERENSI

[1] Rieffel, Eleeanor. Polak, Wolfgang. (2011). *Quantum computing: a gentle introduction*. MIT Press 2011.

[2] Arslan, Bilgehan & Ulker, Mehtap & Akleylek, Sedat & Sagiroglu, Seref. (2018). A study on the use of quantum computers, risk assessment and security problems. 1-6. 10.1109/ISDFS.2018.8355318.

[3] Fernández-Caramés, Tiago. (2019). From Pre-Quantum to Post-Quantum IoT Security: A Survey on Quantum-Resistant Cryptosystems for the Internet of Things. IEEE Internet of Things Journal. 7. 10.1109/JIOT.2019.2958788.

[4] J. A. Silva, T. B. Ludermir, W. R. Oliveira. (2016). Quantum perceptron over a field and neural network architecture selection in a quantum computer.

[5] The Conversation. (2019). Klaim Google Terhadap Kemampuan Komputasi Kuantum. Diakses dari *https://theconversation.com/google-klaim-komputer-kuantum-mereka-bisa-selesaikan-komputasi-hanya-3-menit-sementara-komputer-klasik-10-000-tahun-127226*.

[6] Pratama, Andika. (2008). Algoritma Quantum Shor untuk Faktorisasi Bilangan Bulat. Repositori Makalah Matematika Diskrit.

[7] A. Asfaw, dkk. (2021). Learn Quantum Computation Using Qiskit. The Jupyter Notebook Community.

[8] Saputra, Herlambang. (2009). Kajian Tentang Komputer Kuantum Sebagai Pengganti Komputer Konvensional di Masa Depan. Jurnal Generik Vol. 4 No. 2 (Juli 2009).

[9] Munir, Rinaldi. (2021). Slide Perkuliahan IF4020 Kriptografi. Di akses melalui *https://informatika.stei.itb.ac.id/*.

PERNYATAAN

Dengan ini saya menyatakan bahwa makalah yang saya tulis ini adalah tulisan saya sendiri, bukan saduran, atau terjemahan dari makalah orang lain, dan bukan plagiasi.

Depok, 20 Desember 2021

Aufa Fadhlurohman
13518009