Perbandingan Public Key Cryptography dengan Quantum Cryptograpy

Marianti Putri Wulandari – 13503093

Program Studi Teknik Informatika, Institut Teknologi Bandung
Jl Ganesha No 10, Bandung
Email : if13093@students.if.itb.ac.id

Abstraksi :

Public key cryptography atau kriptografi kunci publik merupakan salah satu bentuk kriptografi yang saat ini sering digunakan dalam kehidupan sehari-hari. Jenis kriptografi ini menggunakan pasangan kunci publik dan kunci privat yang dibangkitkan dengan teknik-teknik tertentu. Kedua kunci tersebut memiliki hubungan asimetrik sedemikian sehingga file yang telah dienkripsi oleh salah satu kunci hanya dapat didekripsi dengan pasangan kuncinya. Hubungan asimetrik tersebut murni didasari oleh perhitungan secara matematis.

Quantum cryptography merupakan jenis kriptografi lain yang muncul di tahun 1980-an. Tidak seperti *public key cryptography* yang didasari perhitungan matematis, *quantum cryptography* didasari oleh perhitungan fisika terutama oleh teori fisika kuantum yang berhubungan dengan photon-photon dan *Heisenberg uncertainty principle* atau prinsip ketidakpastian Heisenberg.

Dengan teknik pendekatan yang berbeda, *public key cryptography* dan *quantum cryptography* tetap memiliki tujuan yang sama, yaitu untuk menjaga kerahasiaan suatu dokumen dari pihak-pihak yang tidak berhak. Dalam makalah ini, akan dilakukan perbandingan dari kedua jenis kriptografi tersebut dari segi prinsip dasar, kelebihan, kelemahan dan karakteristik masing-masing jenis kriptografi.

Kata Kunci :
Public Key Cryptography, Quantum Cryptography, photon, Heisenberg

---

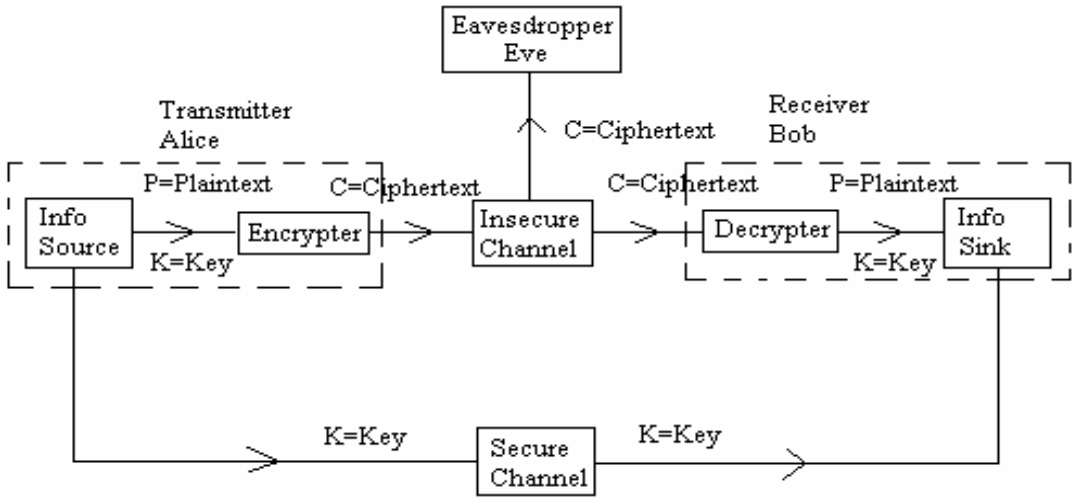
I. Public Key Cryptography

1. Sejarah dan Latar Belakang

Public key cryptography atau *asymmetric cryptography* pertama kali dicetuskan oleh Whitfield Diffie dan Martin dari Standford University pada tahun 1976. Prinsip mereka kemudian dikembangkan oleh Ronald Rivest, Adi Shamir dan Leonard Adleman dari Massachusetts Institute of Technology pada tahun 1978 menjadi algoritma RSA yaitu salah satu algoritma kunci public yang saat ini banyak digunakan dalam kehidupan sehari-hari. *Public key cryptography* merupakan jenis kriptografi yang dianggap dapat mengatasi masalah yang muncul dari *symmetric cryptography*.

Symmetric cryptography merupakan jenis kriptografi pertama yang pertama kali digunakan. Berikut ini adalah skema umum dari *symmetric cryptography*.

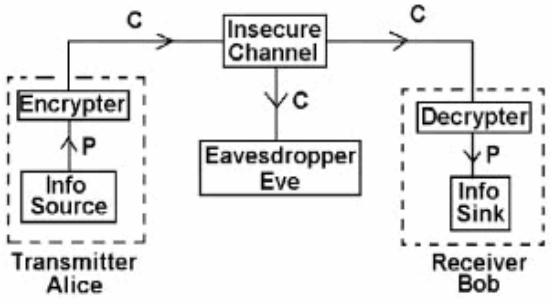
Misalkan Alice akan mengirim sebuah pesan rahasia ke Bob menggunakan *symmetric cryptography*. Pesan rahasia yang disebut dengan *plaintext* P, dienkripsi menggunakan kunci rahasia K menjadi *ciphertext* C. *Ciphertext* C kemudian dikirim ke Bob melalui jalur komunikasi yang mungkin tidak aman. Bob akan dapat mendekripsi *ciphertext* C menggunakan kunci K menjadi *plaintext* P kembali.



Gambar 1. Skema Umum *Symmetric Cryptography*

Masalah yang dihadapi dalam *symmetric cryptography* adalah sebelum Alice dan Bob dapat berkomunikasi secara rahasia mengenai *plaintext* P, mereka harus melakukan komunikasi secara rahasia terlebih dahulu mengenai kunci K. Bahkan jika Alice dan Bob telah berhasil mengkomunikasikan kunci K melalui jalur yang dianggap aman, tidak ada jaminan bahwa kunci K telah dikirim secara aman tanpa adanya penyadapan yang dilakukan oleh Eve.

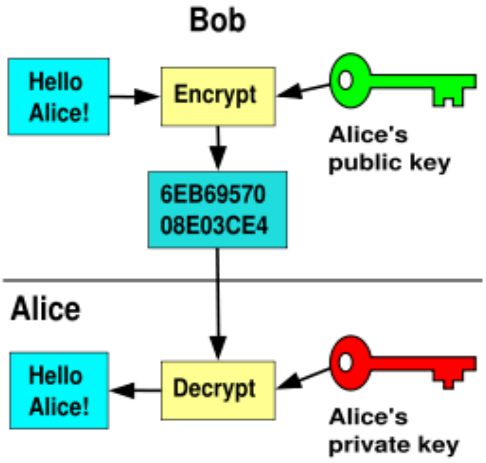
Pada *public key cryptography*, Alice dan Bob tidak lagi harus melakukan komunikasi mengenai kunci K. Kriptografi ini menggunakan sepasang kunci publik dan kunci privat untuk melakukan enkripsi dan dekripsi. Berikut ini adalah skema umum dari *public key cryptography*.

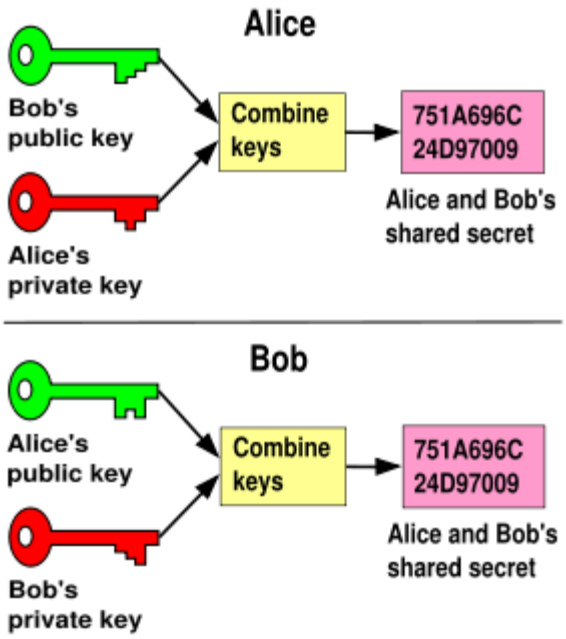


Gambar 2. Skema Umum *Public Key Cryptography*

Jika Alice ingin mengirim pesan rahasia ke Bob, Bob akan membuat sepasang kunci privat dan kunci publik dengan perhitungan matematis tertentu. Kunci privat harus dirahasiakan dari semua orang sedangkan kunci publik dikirimkan ke Alice. Alice akan menggunakan kunci publik tersebut untuk mengenkripsi *plaintext* P menjadi *ciphertext* C kemudian mengirimkan *ciphertext* C tersebut ke Bob. Bob dapat mendekripsi *ciphertext* C menggunakan kunci privat.

Berikut ini adalah gambaran dari hubungan asimetrik dari pasangan kunci privat dan kunci publik yang digunakan dalam melakukan enkripsi dan dekripsi.





Gambar 3. Hubungan Antara Kunci Publik dengan Kunci Privat dalam Melakukan Enkripsi dan Dekripsi

Public key cryptography telah digunakan secara luas selama dua puluh tahun terakhir, salah satu contohnya dalam bidang keamanan jaringan internet. Kriptografi ini dapat dianggap sebagai sebuah kotak surat dimana setiap orang dapat memasukkan surat tetapi hanya pemegang kuncinya saja yang dapat membuka kotak surat tersebut.

Dua cabang utama dari *public key cryptography* adalah enkripsi kunci publik (*public key encryption*) dan pemberian sidik dijital (*digital signature*).

Enkripsi kunci publik digunakan untuk mengenkripsi pesan rahasia. Enkripsi dilakukan dengan kunci publik dan hanya dapat didekripsi dengan kunci privat pasangannya.

Pemberian sidik dijital digunakan untuk memberikan otentikasi isi dan pembuat dari sebuah dokumen. Dokumen dengan sidik dijital tersebut dapat diekstraksi kembali untuk diproses seperti biasa.

Proses yang ada di *public key cryptography* didasari oleh perhitungan matematis, yang disebut dengan fungsi satu arah. Sesuai definisinya, fungsi ini dapat menghitung f(x) jika diberikan variabel x, tetapi terdapat kesulitan untuk menghitung x jika diberikan f(x). Fenomena ini dinamakan *trapdoor function.*

Dalam bidang komputasi, kesulitan yang dimaksud adalah waktu yang dibutuhkan berbanding eksponensial terhadap jumlah bit yang dimasukkan. Tingkat keamanan dari public key cryptography bergantung pada kompleksitas dari perhitungan matematis yang mendasari algoritma enkripsi dan dekripsi dengan menggunakan *trapdoor function*. Kunci untuk melakukan dekripsi tidak mungkin didapat dari perhitungan terhadap kunci untuk melakukan enkripsi.

2. Contoh Perhitungan Matematis dalam *Public Key Cryptography*

Algoritma RSA

Algoritma RSA adalah algoritma kunci publik yang paling popular saat ini. Algoritma ini dibuat oleh tiga orang peneliti dari MIT pada tahun 1976, yaitu Ron (R)ivest, Adi (S)hamir, dan Leonard (A)dleman. Algoritma RSA terdiri dari dua bagian, yaitu proses pembangkitan kunci dan proses enkripsi/dekripsi.

Untuk pembangkitan kunci, prosedur yang harus dilakukan adalah :

1). Pilih dua buah bilangan prima sembarang, p dan q.
2). Hitung $r = p \cdot q$. Sebaiknya $p \neq q$, sebab jika $p = q$ maka $r = p^2$ sehingga p dapat diperoleh dengan menarik akar pangkat dua dari r.
3). Hitung $\phi(r) = (p-1)(q-1)$.
4). Pilih kunci publik, *PK*, yang relatif prima terhadap $\phi(r)$.
5). Bangkitkan kunci rahasia dengan menggunakan persamaan

$$SK = \frac{1 + m\phi(r)}{PK}$$

m adalah suatu bilangan bulat yang dipilih sedemikian sehingga menghasilkan bilangan bulat *SK*.

Sedangkan untuk proses enkripsi/dekripsi, prosedur yang dilakukan adalah sebagai berikut.

1). Plainteks disusun menjadi blok-blok x_1, x_2, …, sedemikian sehingga setiap blok merepresentasikan nilai di dalam rentang 0 sampai $r - 1$.
2). Untuk enkripsi, setiap blok xi dienkripsi menjadi blok yi dengan rumus
yi = xi PK mod r
3). Sedangkan untuk dekripsi, setiap blok cipherteks yi didekripsi kembali menjadi blok xi dengan rumus
xi = yi SK mod r

Berikut ini adalah contoh dalam penggunaan algoritma RSA.

1). Pilih dua bilangan prima.
p = 61 dan q = 53
2). Hitung r = p . q
r = p . q = 61 . 53 = 3233
3). Hitung $\phi(r) = (p - 1)(q - 1)$
$\phi(r) = (61 - 1)(53 - 1) = 3120$
4). Pilih PK yang relatif prima terhadap $\phi(r)$
PK = 17
5). Bangkitkan kunci privat menggunakan persamaan.

$$SK = \frac{1 + m\phi(r)}{PK}$$

SK = 2753

Maka didapat kunci publiknya adalah 17, dengan r = 3233. Dan kunci privatnya adalah 2753 dengan r = 3233.

Misalkan ingin mengenkripsi pesan dengan x_i = 123. Maka hasil enkripsinya adalah sebagai berikut.

$$y_i = x_i^{PK} \bmod r$$
$$y_i = 123^{17} \bmod 3233 = 855$$

Hasil dekripsi dari *ciphertext* tersebut adalah sebagai berikut.

$$x_i = y_i^{SK} \bmod r$$
$$x_i = 855^{2753} \bmod 3233 = 123$$

II. Quantum Cryptography

1. Sejarah dan Latar belakang

Quantum cryptography pertama kali dicetuskan oleh Stephen Wiesner dari Columbia University pada tahun 1970-an. Ide tersebut kemudian dikembang-kan oleh Charles H. Bennett dan Gilles Brassard dari University of Montreal di tahun 1980-an.

Tidak seperti sistem kriptografi lainnya, yaitu *symmetric cryptography* dan *public key cryptography* yang menggunakan dasar perhitungan matematis dalam menjaga isi pesan dari penyadap, *quantum cryptography* menggunakan dasar perhitungan fisika, terutama teori fisika kuantum yang berhubungan dengan photon-photon dan *Heisenberg uncertainty principle* atau prinsip ketidak-pastian Heisenberg.

Pada dasarnya *quantum cryptography* tidak sepenuhnya mengganti sistem kriptografi yang ada dan bukanlah suatu cara baru dalam melakukan enkripsi dan dekripsi. *Quantum cryptography* dikembangkan secara khusus untuk menangani masalah pertukaran kunci yang muncul di sistem kriptografi yang telah ada, yaitu *symmetric cryptography* dan *public key cryptography*. Masalah ini berupa adanya keharusan untuk secara rahasia mengkomunikasikan kunci yang akan digunakan.

Photon

Dalam bidang fisika modern, *photon* merupakan partikel dasar yang berperan dalam fenomena elektromagnetik karena menjadi media interaksi elektromagnetik dalam bentuk cahaya. *Photon* tidak memiliki massa dan bergerak dengan kecepatan konstan c (3×10^8 m/s), yaitu kecepatan cahaya di ruang hampa. *Photon* dianggap sebagai gabungan dari gelombang dan partikel sehingga memiliki properti dari keduanya.

Konsep *photon* telah membawa perkembangan pesat terhadap teori dan eksperimen fisika, seperti laser, *Bose-Einstein condensation*, teori bidang kuantum, dan interpretasi probabilistik dari mekanika kuantum. Berdasarkan model standar dari suatu partikel, *photon* berperan dalam menghasilkan seluruh bidang elektrik dan magnetik.

Photon diaplikasikan dalam berbagai bidang teknologi, seperti *photochemistry*,

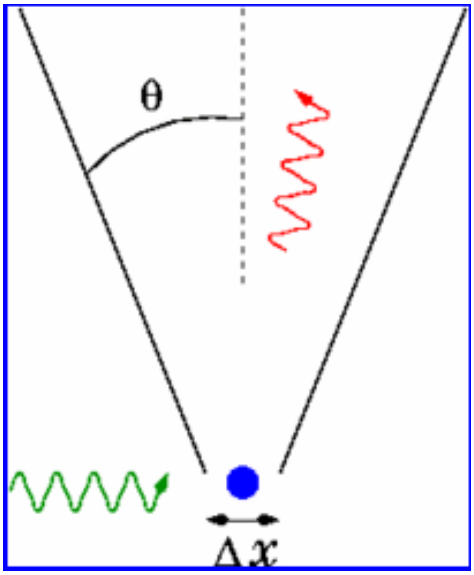
mikroskop resolusi tinggi, perhitungan jarak molekul. Belakangan ini, *photon* telah dipelajari sebagai elemen dari komputer kuantum dan untuk aplikasi lainnya dalam komunikasi optik seperti *quantum cryptography*.

Heisenberg Uncertainty Principle

Gambar 4. Heisenberg di Tahun 1927

Prinsip fisika yang mendasari *quantum cryptography* adalah *Heisenberg uncertainty principle*, yang mengatakan bahwa mustahil untuk mengetahui pasangan variabel mengenai sebuah partikel, keduanya secara tepat. Setiap pasangan variabel disebut *conjugate variables*, dan semakin tepat nilai salah satu variabel maka semakin tidak pasti nilai variabel pasangannya.

Pada gambar di bawah, terlihat lokasi suatu elektron (yang berbentuk bulat) menggunakan mikroskop gamma-ray Heisenberg. Gamma-ray yang datang ke arah elektron terpantul oleh elektron dengan sudut θ. Perhitungan yang dilakukan untuk mencari posisi elektron dengan akurat akan mengakibatkan ketidakpastian pada nilai Δx yang bergantung pada nilai θ dan panjang gelombang λ dari cahaya yang datang.



Gambar 5. Keadaan Elektron di Satu Waktu

Contoh lainnya untuk pasangan variabel posisi dan momentum partikel. Semakin tepat nilai posisi partikel, semakin tidak pasti nilai momentum partikel tersebut, dan sebaliknya. Prinsip ini berlaku juga untuk pasangan variabel yang lain, seperti energi dan waktu, polarisasi horizontal dan vertikal.

Lalu pada perkembangan selanjutnya, muncul pendapat baru yang berjudul *entanglement* yang menyatakan bahwa nilai variabel dari partikel-partikel sangat berhubungan satu sama lain. Sekumpulan partikel tidak dapat digambarkan dengan menentukan status dari satu partikel. Partikel-partikel tersebut akan saling mempengaruhi sehingga tidak dapat ditentukan berdasarkan eksperimen yang dilakukan terhadap satu partikel. Hubungan ini berlaku bahkan untuk partikel-partikel yang terpisah jauh dalam satu waktu.

Berdasarkan dua ketentuan tersebut, yaitu *uncertainty* dan *entanglement*, dikembangkan dua tipe pendekatan dalam *quantum cryptography*. Tipe yang pertama, bernama *Polarized Photons*,

menggunakan polarisasi dari photon untuk mengkode bit-bit informasi dan menggunakan kuantum acak (*quantum randomness*) untuk menjaga penyadapan kunci rahasia.

Tipe yang kedua, bernama *Entangled Photons*, menggunakan status photon yang rumit dan saling berhubungan untuk mengkode bit-bit dan menentukan kunci hanya dilakukan setelah perhitungan yang dilakukan oleh Alice dan Bob.

a. Polarized Photons
Polarized Photons dikembangkan oleh Charles H. Bennet dan Gilles Brassard pada tahun 1984. Skema kriptografi, yang disebut BB84, menggunakan getaran (pulse) dari cahaya yang terpolarisasi, dengan satu *photon* per *pulse*.

Terdapat dua tipe polarisasi untuk mengkode, yaitu linear dan sirkular. Polarisasi linear berupa vertikal atau horizontal, dan polarisasi sirkular berupa kiri dan kanan. Misalnya polarisasi vertikal untuk "0" dan polarisasi horizontal untuk "1", atau polarisasi kiri untuk "0" dan polarisasi kanan untuk "1". Untuk menghasilkan kunci acak, Alice harus mengirim kedua polarisasi dengan peluang yang sama.

b. Entangled Photons
Entangled Photons dikembangkan oleh Artur Ekert pada tahun 1991. Terdapat tiga hal yang dipertimbangkan dalam skema Ekert.

Pertama, hubungan antar partikel terlihat dari fakta bahwa jika Alice dan Bob menguji arah polarisasi (horizontal atau vertikal) dari partikel-partikel, maka mereka akan mendapatkan jawaban yang berlawanan. Hal ini berlaku juga untuk polarisasi sirkular. Hasil pengujian masing-masing bersifat acak sehingga mustahil bagi Alice untuk memprediksi apakah Alice akan mendapat polarisasi vertikal atau horizontal.

Kedua, jika Alice dan Bob melakukan perhitungan polarisasi, jawaban mereka tidak sepenuhnya berhubungan. Akan tetapi, kemungkinan di atas 50% bahwa perhitungan Alice sama dengan perhitungan Bob, dan sebaliknya.

Ketiga, penyadapan yang dilakukan oleh pihak lain dapat memperlemah hubungan tersebut, yang dapat terdeteksi oleh Alice dan Bob.

2. Contoh Perhitungan Fisika dalam *Quantum Cryptography*

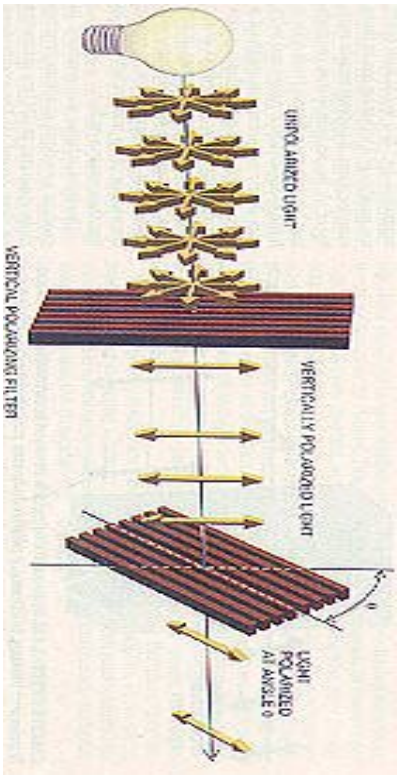
Algoritma BB84

Protokol *quantum cryptography* pertama adalah BB84 yang dikembangkan oleh Bennett dan Bassard di tahun 1984. Protokol ini telah diuji coba untuk bekerja melalui kabel *fiber-optic* sepanjang lebih dari 30 km. Berdasarkan spekulasi, protokol BB84 dapat diimplementasikan untuk jarak lebih dari 100 km, namun hal ini belum diverifikasi.

Protokol BB84 juga menggunakan dua jenis polarisasi, yaitu polarisasi linear (vertikal dan horizontal) dan polarisasi sirkular (kiri dan kanan). Bennett dan Brassard menilai bahwa jika Alice hanya menggunakan satu jenis polarisasi dalam berkomunikasi dengan Bob, maka penyadapan yang dilakukan oleh Eve tidak dapat terdeteksi. Eve dapat menangkap pesan yang Alice kirim dengan keakuratan 100%, dan kemudian meneruskan pesan tersebut ke Bob.

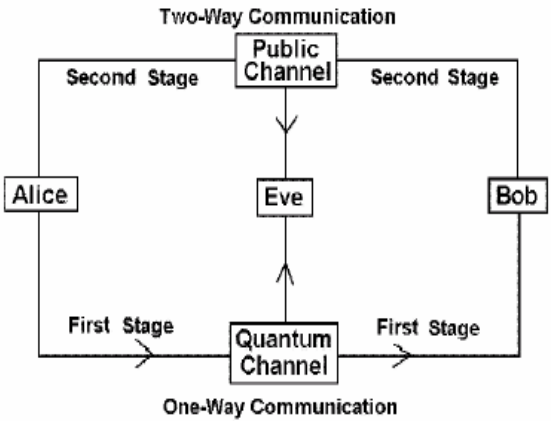
Tindakan penyadapan oleh Eve akan mempengaruhi polarisasi photon yang menyebabkan perubahan jenis polarisasi pada bit yang diterima Bob sehingga bit tidak dapat ketahui karena operator dari kedua polarisasi berbeda. Berikut ini adalah contoh terjadinya perubahan jenis polarisasi.

Pada gambar di bawah ini terlihat bahwa pada awalnya jenis polarisasi photon adalah polarisasi linear (horizontal atau vertikal). Di satu titik, karena ada faktor-faktor tertentu dari luar, seperti tindakan penyadapan atau gangguan teknis atau yang disebut dengan *noise*.



Gambar 6. Contoh Terjadinya Perubahan Jenis Polarisasi

Dalam keadaan yang sebenarnya, transmisi bit akan mengalami *noise* yang tidak bisa dihindari sepenuhnya dan dapat menyebabkan perubahan terhadap bit-bit tersebut. Alice dan Bob tidak dapat membedakan perubahan bit yang disebabkan oleh *noise* dan perubahan bit yang disebabkan oleh penyadapan.



Gambar 7. Skema Umum Protokol BB84

Gambar di atas adalah skema dari protokol BB84. Untuk dapat mendeteksi penyadapan dari pihak ketiga, dilakukan komunikasi antara Alice dan Bob melalui dua tahap. Tahap pertama dilakukan melalui jalur komunikasi kuantum satu arah dari Alice ke Bob. Tahap kedua dilakukan melalui jalur komunikasi publik dua arah.

a. Tahap 1, Komunikasi Melalui Jalur Kuantum
   Di tahap pertama, Alice akan mengkode setiap bit menggunakan polarisasi sirkular atau polarisasi linear dengan peluang yang sama. Karena operator perhitungan untuk polarisasi sirkular tidak sama dengan polarisasi linear, maka berdasarkan prinsip ketidak-pastian Heisenberg, pihak penerima, baik Bob maupun Eve tidak dapat menerima kiriman Alice dengan tingkat keakuratan lebih dari 75%.

   Misalkan simbol untuk jenis polarisasi sirkular adalah O, dan merepresentasikan bit dengan simbol sebagai berikut.

Nilai Bit	Simbol
0	→
1	←

   Lalu untuk simbol untuk jenis polarisasi linear adalah +, dan merepresentasikan bit dengan simbol sebagai berikut.

Nilai Bit	Simbol
0	↕
1	↔

   Alice ingin mengirimkan kunci dengan pilihan jenis polarisasi sebagai berikut.

Nilai Bit	Jenis Polarisasi	Simbol Bit
1	O	←
0	+	↕
0	+	↕
1	+	↔

1	O	←
1	+	↔
0	O	→
1	O	←
0	+	↔
0	O	→
1	+	↔
1	+	↔
1	O	←
0	O	→
0	+	↕
1	O	←
1	O	→
0	O	→
1	O	←
0	+	↕
0	O	→
1	+	↔
1	+	↔
1	O	←
0	O	→
1	O	←
0	O	→
0	+	↕
1	O	←
1	O	→
0	+	↕
1	+	↔
1	O	←
0	+	↕
0	+	↕
1	+	↔
1	O	←
1	+	↔
0	O	→
1	O	←
0	+	↔
0	O	→
1	O	←
0	+	↕
1	+	↔
1	O	←
1	+	↔
0	O	→
1	O	←

0	+	↔
0	O	→
1	O	←
1	+	↔
1	+	↔

b. Tahap 2. Komunikasi Melalui Jalur Publik

Di tahap ini, Alice dan Bob melakukan komunikasi melalui jalur publik dalam empat fase untuk melihat adanya penyadapan atau tidak.

1). Fase 1, Ekstraksi Kunci

Dalam fase ini, Bob melakukan pemilihan secara acak terhadap jenis polarisasi yang digunakan untuk setiap bit yang diterima. Kemudian Bob mencocokan pilihannya dengan Alice melalui jalur publik. Alice akan menjawab pilihan-pilihan mana yang benar. Alice dan Bob juga melakukan pencocokan terhadap kelengkapan bit karena terdapat kemungkinan Bob tidak menerima bit-bit tertentu yang dikirim oleh Alice. Hal ini disebabkan adanya penyadapan atau gangguan pada alat pendeteksi di pihak Bob.

Berikut ini adalah bit-bit yang diterima dan pilihan jenis polarisasi Bob.

Simbol Bit di Alice	Jenis Polarisasi Alice	Simbol Bit di Bob	Jenis Polarisasi Bob	Nilai Bit
←	O	←	O	1
↕	+	↕	+	0
↕	+	←	O	Hapus
↔	+	↔	+	1
←	O	←	O	1
↔	+	↔	+	1
→	O	↕	O	Hapus
←	O	←	O	1
↔	+	↔	+	1
→	O	↕	+	Hapus
↔	+	↔	+	1
↔	+	←	+	Hapus

←	O	←	O	1
→	O	→	O	0
↕	+	↕	O	Hapus
←	O	←	+	Hapus
→	O	→	O	0
→	O	→	O	0
←	O	←	O	1
↕	+	↕	+	0
→	O	↕	+	Hapus
↔	+	↔	+	1
↔	+	←	+	Hapus
←	O	←	O	1
→	O	→	O	0
←	O	←	O	1
→	O	→	O	0
↕	+	↕	O	Hapus
←	O	←	+	Hapus
→	O	→	O	0
↕	+	←	O	Hapus
↔	+	↔	+	1
←	O	←	O	1
↕	+	↕	+	0
↕	+	←	O	Hapus
↔	+	↔	+	1
←	O	←	O	1
↔	+	↔	+	1
→	O	↕	O	Hapus
←	O	←	O	1
↔	+	↔	+	1
→	O	↕	+	Hapus
←	O	←	O	1
↕	+	←	O	Hapus
↔	+	↔	+	1
←	O	←	O	1
↔	+	↔	+	1
→	O	↕	O	Hapus
←	O	←	O	1
↔	+	↔	+	1
→	O	↕	+	Hapus
←	O	←	O	1
↔	+	→	O	Hapus
↔	+	→	O	Hapus

Setelah semua bit dicocokkan, bit-bit dengan pilihan jenis polarisasi yang salah dan bit-bit yang hilang akan dihapus. Bit-bit dengan pilihan yang benar akan dikode kembali dari kode dengan polarisasi menjadi bit (0 atau 1). Misalkan batas *error* Barisan bit tersebut akan menjadi kunci sementara bagi Alice dan Bob, yaitu 1011111110001011010 0110111111111111.

2). Fase 2, Mendeteksi Kesalahan (*error*) di Kunci Sementara
Di fase ini, Alice dan Bob saling mencocokkan sebagian bit secara acak dari kunci sementara Alice dan Bob melalui jalur publik untuk mendeteksi tingkat *error* (R) di kedua kunci tersebut. Bit-bit yang salah kemudian dihapus dari kunci sementara. Jika nilai R melebihi batas nilai kesalahan (R_{maks}), maka kedua kunci tidak dapat digunakan. Oleh karena itu, Alice dan Bob harus kembali ke tahap 1 dan mulai lagi dari awal.

3). Fase 3, Ekstraksi Kunci Sementara
Tujuan dari fase ini adalah untuk menghilangkan seluruh *error* dari kunci sementara yang tersisa. Hasil dari fase ini adalah kunci bebas *error* yang disebut dengan *reconciled key*. Fase ini terdiri dari dua langkah.

Langkah pertama adalah Alice dan Bob memilih permutasi acak dari kunci sementara. Kemudian Alice dan Bob membagi kunci sementara ke dalam blok-blok dengan panjang L, sedemikian sehingga setiap blok tidak memiliki *error* lebih dari satu.

Untuk setiap blok, Alice dan Bob saling mencocokkan bit *parity*-nya tanpa memperhitungkan bit paling kanan dari blok. Jika blok Alice dan Bob memiliki bit *parity* yang berbeda, maka dilakukan *binary search* untuk mencari *error*. Yaitu dengan cara membagi blok menjadi dua

subblok, mencocokkan bit *parity*-nya tanpa memperhatikan bit paling kanan dari subblok. Hal ini dilakukan secara rekursif hingga bit yang *error* ditemukan dan kemudian dihapus. Setelah itu, dilanjutkan ke blok selanjut-nya hingga seluruh blok telah selesai diproses.

Langkah kedua adalah Alice dan Bob memilih secara acak bagian dari kunci sementara dan membandingkan bit *parity*-nya. Jika terdapat bit *parity* yang berbeda, maka Alice dan Bob harus melakukan *binary search* seperti di langkah pertama untuk menemukan dan menghapus *error* tersebut.

Apabila setelah dilakukan N kali langkah kedua dan tidak ditemukan adanya *error*, maka Alice dan Bob dapat mengasumsikan bahwa kunci sementara yang tersisa sudah bebas dari *error*. Kemudian Alice dan Bob menjadikan kunci tersebut sebagai *reconciled key*.

4). Fase 4, Ekstrasi *Final Secret Key*
Alice dan Bob telah mendapatkan *reconciled key* yang tidak dapat diketahui oleh Eve. Kemudian Alice dan Bob akan melakukan proses yang disebut dengan *privacy amplification,* yaitu mengekstrasi *final secret key* dari *reconciled key*.

Terdapat tiga variabel bernilai bilangan asli yang diperhi-tungkan, yaitu k, n, dan s. k adalah batas maksimal jumlah bit yang dapat diketahui Eve berdasarkan tingkat *error* R. n adalah jumlah bit dari *reconciled key*. s adalah nilai parameter keamanan yang ditentukan oleh Alice dan Bob.

Kemudian Alice dan Bob akan memilih sebanyak n-k-s himpunan bagian dari *reconciled key* secara acak. Bit *parity* dari himpunan bagian tersebut akan menjadi *final secret key.*

III. Kelebihan dan Kelemahan Kedua Jenis Kriptografi

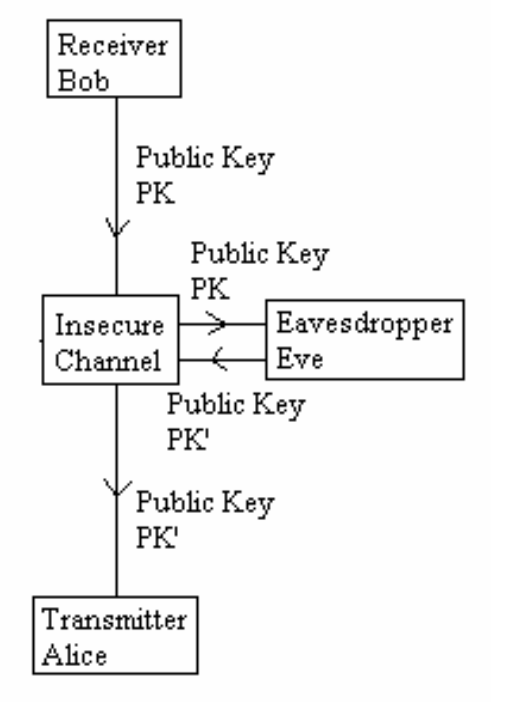
1. Kelebihan *Public Key Cryptography*
   a. *Public Key Cryptography* telah dianggap aman dalam mengenkripsi pesan rahasia dan juga pemberian sidik dijital. Sangat sulit untuk menganalisis *ciphertext* hasil dari enkripsi menggunakan *public key cryptography* tanpa mengetahui kunci yang digunakan. Oleh karena itu, selama pertukaran kunci tidak diganggu oleh pihak ketiga, maka *public key cryptography* menjadi sistem kriptografi yang kuat dan aman.

2. Kelemahan *Public Key Cryptography*
   a. Hingga saat ini *public key cryptography* merupakan sistem kriptografi yang kuat dalam menjamin keamanan pengiriman pesan rahasia. Masalah utama yang dihadapi adalah pertukaran kunci publik antara Alice dan Bob.

      Salah satu strategi penyadapan yang dilakukan adalah Eve menyadap kunci publik asli dari Bob. Kemudian Eve mengirim kunci publik palsu yang dibuat Eve ke Alice. Alice akan mengenkripsi pesan rahasia menggunakan kunci publik palsu tersebut. Saat Alice mengirimkan hasil enkripsi ke Bob, Eve akan menyadap hasil enkripsi tersebut. Kemudian Eve dapat mendekripsi menggunakan pasangan kunci privat palsu yang dimilikinya.

      Berbagai cara dilakukan untuk menghindari terjadinya penyadapan. Salah satu contohnya Alice dan Bob dapat melakukan pertemuan terlebih dahulu untuk menentukan kunci yang akan digunakan. Cara lain juga telah digunakan untuk melakukan per-tukaran kunci publik, namun pada kenyataannya, hingga saat ini cara-

cara tersebut tidak sepenuhnya dianggap aman. Pihak lain masih dapat melakukan penyadapan terhadap pertukaran kunci publik.



Gambar 8. Contoh Strategi Penyadapan

b. *Public key cryptography* tidak memiliki teknik untuk mengetahui apakah telah terjadi penyadapan selama pengiriman kunci publik atau tidak. Oleh karena itu, akan sangat sulit bagi Alice dan Bob untuk menghindari penyadapan karena deteksi terhadap penyadapan tidak dapat dilakukan.

3. Kelebihan *Quantum Cryptography*

a. Quantum cryptography memiliki tingkat keamanan yang sangat tinggi dalam melakukan pertukaran kunci. Kegiatan penyadapan akan menyebabkan perubahan bit dan dapat dengan mudah terdeteksi dari tingkat *error* yang didapat saat melakukan perbandingan antara kunci yang dikirim Alice dengan kunci yang diterima Bob. Oleh karena itu, kunci yang dihasilkan dapat dikatakan bebas penyadapan.

4. Kelemahan *Quantum Cryptography*

a. *Quantum cryptography* memiliki keterbatasan dalam media transmisi bit yang mungkin akan dapat diatasi di masa depan. Keterbatasan ini didasari oleh sifat *photon* yang hanya dapat berpindah antar komputer melalui kabel *fiber-optic* dan sifat *photon* yang akan degenerasi setelah bergerak dalam jarak yang jauh.

Dengan adanya keterbatasan tersebut, quantum cryptography hanya dapat digunakan untuk mengirim kunci antar komputer yang dihubungkan kabel *fiber-optic* dan dengan jarak yang terbatas.

Penelitian telah dilakukan untuk mengatasi keterbatasan sifat *photon* tersebut. Beberapa perusahaan teknologi telah meneliti bahwa transmisi *photon* dapat diperkuat dengan *quantum repeater* sehingga degenerasi *photon* dapat dihindari, bahkan jarak yang dapat dilalui *photon* dapat ditambah.

Saat ini juga dilakukan penelitian untuk melakukan transmisi *photon* tanpa kabel. Dengan kemampuan mengirim kunci tanpa melalui kabel, maka *quantum cryptography* dapat digunakan untuk keamanan jaringan internet.

b. *Quantum cryptography* menekankan prosesnya pada pertukaran kunci yang direpresentasikan oleh variabel dari *photon-photon*. Pertukaran kunci tersebut sangat bergantung terhadap transmisi *photon* melalui media kabel *fiber-optic*. Gangguan teknis atau *noise* jelas tidak dapat dihindari selama transmisi *photon* dilakukan. *Noise* tersebut sangat mempengaruhi *photon* dan memungkinkan terjadinya kesalahan-kesalahan pada nilai bit-bit yang diterima. Oleh karena itu, *quantum cryptography* bersifat sangat rentan terhadap *noise* sehingga ada kondisi dimana *quantum cryptography* tidak dapat digunakan.

c. *Quantum cryptography* memiliki dua tahap dalam melakukan pertukaran kunci, yaitu komunikasi satu arah dari Alice ke Bob untuk mengirim kunci dalam representasi kuantum, dan komunikasi publik dua arah antara Alice dan Bob untuk mendapatkan *final secret key* berdasarkan kunci yang dikirim Alice dan kunci yang diterima Bob.

   Kedua tahap ini akan dilakukan hingga mendapatkan *final secret key* yang valid, bebas *error* dan dinyatakan tidak disadap. Proses ini akan memakan waktu yang lama, terlebih lagi jika tingkat *noise* yang muncul sepanjang kabel *fiber-optic* yang dilalui sedang tinggi. Semakin tinggi tingkat *noise*, maka semakin besar kemungkinan *error* yang terjadi sehingga *final secret key* akan semakin sulit didapat.

IV. Perbandingan Public Key Cryptography dengan *Quantum Cryptography*

1. *Public key cryptography* dan *quantum cryptography* memiliki perbedaan utama pada dasar perhitungan yang digunakan. *Public key cryptography* didasari oleh perhitungan matematis pada teknik-teknik yang digunakan dalam menghasilkan kunci privat dan kunci publik. *Random Number Generator* (RNG) sangat berperan dalam proses tersebut untuk menghasilkan kunci privat dan kunci publik yang bersifat acak sehingga dapat mempersulit serangan-serangan dari penyadap.

   Dengan perhitungan secara matematis, kunci privat dan kunci publik yang dihasilkan akan bersifat acak dan pasti, yaitu memiliki struktur yang sama dan melalui proses yang sama sesuai dengan algoritma yang dibuat oleh pemrogram. Oleh karena itu, tingkat keamanan dari kedua kunci ini bergantung dari panjangnya. Semakin panjang kunci, maka semakin banyak kemungkinan kunci yang digunakan dengan perbandingan eksponensial 2 karena satu bit memiliki dua nilai kemungkinan, yaitu 0 atau 1. Misalnya jika panjang kunci yang digunakan adalah 128 bit, maka terdapat 2^{128} kunci yang mungkin digunakan.

   Quantum cryptography didasari oleh perhitungan fisika pada teknik yang digunakan dalam menghasilkan kunci. Kunci didapat berdasarkan nilai-nilai variabel photon yang merepresentasikan bit-bit kunci yang dikirimkan Alice dan yang diterima Bob pada saat itu juga.

   Nilai-nilai variabel tersebut sangat sensitif terhadap jarak yang ditempuh, gangguan teknis atau *noise*, dan tindakan penyadapan. Jika error dari perbandingan antara nilai variabel photon yang dikirimkan Alice dengan nilai variabel photon yang diterima Bob melebihi batas jumlah error yang telah ditentukan sebelumnya, maka kunci tersebut dianggap tidak valid dan harus diulang.

   Dengan perhitungan secara fisika, kunci yang dihasilkan bersifat acak tetapi tidak pasti, yaitu panjang kunci bergantung pada jumlah *error* yang dihasilkan dari proses perbandingan. Karena tidak ada teknik yang dapat membedakan error karena *noise* atau *error* karena penyadapan, maka keputusan diambil berdasarkan probabilitas. Oleh karena itu, penentuan kevalidan suatu kunci sangat bergantung pada probabilitas, bukan pada suatu angka yang pasti.

   Jika dibandingkan, kunci yang dihasilkan oleh *public key cryptography* bersifat lebih stabil karena tidak bergantung pada kondisi fisik selama proses membuat kunci. Sedangkan pada kunci yang dihasilkan oleh *quantum cryptography* tidak terlalu stabil karena dipengaruhi oleh kondisi fisik (jarak yang ditempuh dan *noise*) saat terjadi komunikasi antara Alice dan Bob untuk membandingkan kunci. Sehingga ada saat-saat dimana *quantum cryptography* tidak dapat digunakan berkaitan pada kondisi fisik saat itu.

2. *Quantum cryptography* memiliki keterbatasan dalam media transmisi bit, yaitu hanya dapat menggunakan media kabel *fiber-optic* untuk memungkinkan adanya pengiriman *photon-photon* antara kedua komputer. Hal ini menyebabkan

terbatasnya penggunaan *quantum cryptography* pada kehidupan sehari-hari karena tidak seluruh komputer dihubungkan dengan kabel *fiber-optic*. Terlebih lagi saat ini pengiriman data bit menggunakan jaringan nir-kabel (*wireless*) sudah sangat berkembang.

Public key cryptography tidak memiliki keterbatasan dalam media transmisi bit karena pengiriman bit tidak dilakukan dengan representasi variabel *photon*. Oleh karena itu, *public key cryptography* hingga sekarang dapat digunakan secara luas, baik menggunakan kabel maupun nir-kabel.

3. *Quantum cryptography* memiliki tingkat keamanan yang sangat tinggi terhadap proses pertukaran kunci walaupun dilakukan melalui jalur yang tidak aman. Hal ini disebabkan oleh sifat sensitif dari *photon-photon* terhadap tindakan penyadapan. Selain itu, proses perbandingan dilakukan di saat yang sama karena photon-photon tidak dapat disimpan. Oleh karena itu, Alice dan Bob dapat langsung melakukan deteksi terhadap tindakan penyadapan pada saat itu juga dan kemudian melakukan proses pertukaran kunci hingga didapat kunci yang valid.

   Public key cryptography memiliki kelemahan utama pada masalah pertukaran kunci. Walaupun telah ada sistem kunci publik dan kunci privat, namun perlu ada pertukaran kunci antara pihak penerima dan pihak pengirim yang memungkinkan terjadinya penyadapan.

   Selain itu, kunci-kunci yang dihasilkan sangat rentan terhadap serangan. Salah satu caranya adalah dengan mencoba kemungkinan-kemungkinan kunci. Dengan tingkat kecepatan komputer saat ini, waktu yang digunakan untuk mencoba keseluruhan kemungkinan kunci menjadi semakin pendek. Oleh karena itu, untuk meningkatkan keamanan *public key cryptography* diperlukan bit kunci yang semakin panjang sehingga jumlah kemungkinan akan semakin besar.

4. *Quantum cryptography* tidak dapat mendukung kemampuan pemberian sidik dijital (*digital signature*). Saat ini, pemberian sidik dijital yang dilakukan menggunakan quantum cryptography (quantum digital signature) hanya memungkinkan verifikasi sidik dijital oleh sejumlah kecil pihak sehingga tidak dapat digunakan dalam kehidupan sehari-hari. Karena salah satu kemampuan yang harus dimiliki dalam sidik dijital adalah dapat diverifikasi oleh setiap orang, maka *quantum digital signature* masih belum dapat digunakan.

   Hingga saat ini, *public key cryptography* mendukung pemberian sidik dijital dengan baik sehingga dapat digunakan dalam kehidupan sehari-hari. Contohnya dalam pemberian sidik dijital untuk dokumen-dokumen yang tersebar di jaringan internet.

V. Kesimpulan

Dasar perhitungan yang digunakan dalam suatu sistem kriptografi mempengaruhi karakteristik dan penggunaan dari sistem tersebut. *Public key cryptography* yang didasari perhitungan matematis bersifat lebih stabil tanpa dipengaruhi kondisi fisik selama transmisi bit. Hal ini menyebabkan *public key cryptography* dapat digunakan secara luas dalam kehidupan sehari-hari. Namun dengan perhitungan matematis, resiko terjadinya penyadapan tanpa terdeteksi menjadi lebih tinggi.

Quantum cryptography yang didasari perhitungan fisika bersifat lebih labil karena sangat dipengaruhi kondisi fisik selama transmisi bit. Keterbatasan dalam masalah jarak transmisi, *noise*, dan media transmisi menyebabkan terbatasnya penggunaan kriptografi ini. Namun dengan perhitungan fisika melalui nilai-nilai variabel *photon*, penyadapan dapat dengan mudah terdeteksi sehingga kunci dapat dipetukarkan dengan aman.

Kedua jenis kriptografi tersebut memiliki kelebihan dan kelemahan yang saling melengkapi. Untuk perkembangannya, mungkin dapat dilakukan perpaduan antara kedua jenis kriptografi tersebut untuk menghasilkan suatu sistem kriptografi yang memiliki tingkat keamanan dalam enkripsi dan dekripsi pesan, dan juga tingkat

keamanan dalam melakukan pertukaran kunci.

VI. Daftar Pustaka

[1] Bennett, Charles H., dkk. "Experimental Quantum Cryptography", 1991. http://cs.uccs.edu/~cs691/crypto/BBBSS92.pdf Diakses pada tanggal 18 Desember 2006.

[2] Brassard, Gilles. "A Bibligraphy of Quantum Cryptography", 1996. http://www.cs.mcgill.ca/~crepeau/CRYPTO/Biblio-QC.html Diakses pada tanggal 18 Desember 2006.

[3] Gisin, Nicolas, dkk. "Quantum cryptography", 2002. http://ww.gap-ptique.unige.ch/Publications/Pdf/QC.pdf Diakses pada tanggal 18 Desember 2006.

[4] Goldwater, Sharon. "Quantum Cryptography and Privacy Amplification", 1996. http://www.ai.sri.com/~goldwater/quantum.html Diakses pada tanggal 18 Desember 2006.

[5] Hengerer, Roland, Illsley, Martin, dan Black, David. "Quantum cryptography represents the next line of IT security", 2005. http://www.accenture.com/xdoc/en/services/technology/vision/quantum_cryptography.pdf Diakses pada tanggal 18 Desember 2006.

[6] Jennewein, Thomas, dkk. "Quantum Cryptography with Entangled Photons", 1999. http://www.quantum.at/publications/pdffiles/2000-05.pdf Diakses pada tanggal 18 Desember 2006.

[7] Lomonaco, Samuel J. "A Quick Glance at Quantum Cryptography", 1998. http://www.cs.umbc.edu/~lomonaco/lecturenotes/ 9811056.pdf Diakses pada tanggal 18 Desember 2006.

[8] Moses, Tim, Zuccherato, Robert. "Quantum Computing and Quantum Cryptography", 2005. http://www.entrust.com/resources/download/cfm/21190/quantum.pdf Diakses pada tanggal 18 Desember 2006.

[9] Vittorio, Salvatore. "Quantum Cryptography : Privacy Through Uncertainty", 2002. http://www.csa1.co.uk/discoveryguides/crypt/ overview.php Diakses pada tanggal 18 Desember 2006.

[10] Walton, Zachary D., dkk. "One-way entangled-photon autocompensating quantum cryptography", 2003. http://people.bu.edu/alexserg/ oneway.pdf Diakses pada tanggal 18 Desember 2006.

[11] http://www.secoqc.net/downloads/pressrelease/banktransfer_english.pdf Diakses pada tanggal 18 Desember 2006.

[12] http://www.ucci.it/docs/qc-first_glimpse-05.pdf Diakses pada tanggal 18 Desember 2006.

[13] http://en.wikipedia.org/wiki/Heisenberg_uncertainty_principle.htm Diakses pada tanggal 18 Desember 2006.

[14] http://en.wikipedia.org/wiki/Quantum_cryptography.htm Diakses pada tanggal 18 Desember 2006.

[15] http://en.wikipedia.org/wiki/Quantum_entanglement.htm Diakses pada tanggal 18 Desember 2006.

[16] http://en.wikipedia.org/wiki/Quantum_mechanics.htm Diakses pada tanggal 18 Desember 2006.

[17] http://en.wikipedia.org/wiki/Secure_Coummunication_based_on_Quantum_Cryptography.htm Diakses pada tanggal 18 Desember 2006.

[18] http://www.dsi.uniroma1.it/ale/BICI/BiciIndam05/maurer2.pdf Diakses pada tanggal 18 Desember 2006.

[19] http://en.wikipedia.org/wiki/photon.htm Diakses pada tanggal 1 Januari 2007.

[20] http://en.wikipedia.org/wiki/Public-key_cryptography.htm
Diakses pada tanggal 1 Januari 2007.

[21] http://en.wikipedia.org/wiki/Trapdoor_function.htm
Diakses pada tanggal 1 Januari 2007.

[22] http://www.cs.usask.ca/resources/tutorials/csconcepts/1993_3/lessons/L4/PublicKey.html
Diakses pada tanggal 1 Januari 2007.

[23] http://www.rsasecurity.com/rsalabs/node-asp.htm
Diakses pada tanggal 1 Januari 2007.