Quantum Digital Signature

Gisca Tamara / 13507003
Program Studi Teknik Informatika ITB, Bandung
email: if17003@students.if.itb.ac.id

Abstrak

Kriptografi adalah salah satu cara untuk melindungi data-data kita terhadap penyadapan atau penyerangan dari pihak yang tidak kita inginkan. Banyak sekali aplikasi dari kriptografi yang telah digunakan oleh masyarakat kita, salah satunya digital signature. Seiring dengan perkembangan jaman, teknologi dari digital signature pun semakin maju, hal ini ditujukan agar pengiriman dan penerimaan data dapat terjamin keasliannya. Salah satu perkembangan digital signature adalah dengan menggunakan metode quantum dengan berdasarkan ketidakpastian Heisenberg, sehingga disebut dengan Quantum Digital Signatrue. Tingkat keamanan dari metode quantum ini lebih tinggi dari metode yang digunakan sebelumnya, yaitu dengan menggunakan kunci publik yang mendasarkannya pada perhitungan matematis. Lain halnya dengan metode quantum yang mendasarkan perhitungannya pada prinsip fisika yang lebih kompleks.

Kata kunci: Kriptografi, Quantum Digital Signature, Kunci Publik.

1. Pendahuluan

Ilmu Kriptografi sebenarnya sudah mulai dipelajari manusia sejak tahun 400 SM, yaitu pada zaman Yunani kuno. Dari catatan bahwa "Penyandian Transposisi" merupakan sistem kriptografi pertama yang digunakan atau dimanfaatkan. Bidang ilmu ini terus berkembang seiring dengan kemajuan peradaban manusia, dan memegang peranan penting dalam strategi peperangan yang terjadi dalam sejarah manusia, mulai dari sistem kriptografi "Caesar Chiper" ang terkenal pada zaman Romawi kuno, "Playfair Cipher" yang digunakan Inggris dan "ADFVGX Cipher" yang digunakan Jerman pada Perang Dunia I, hingga algoritma-algoritma kriptografi rotor yang populer pada Perang Dunia II, seperti Sigaba / M-134 (Amerika Serikat), Typex (Inggris), Purple (Jepang), dan mesin kriptografi legendaris Enigma (Jerman).

Induk dari keilmuan dari kriptografi sebenarnya adalah matematika, khususnya teori aljabar yang mendasar ilmu bilangan . Oleh karena itu kriptografi semakin berkembang ketika komputer ditemukan. Sebab dengan penemuan komputer memungkinkan dilakukanya perhitungan yang rumit dan komplekdalam waktu yang relatif sangat singkat, suatu hal yang sebelumnya tidak dapat dilakukan. Dari hal tersebut lahirlah banyak teori dan algotitma penyandian data yang semakin kompleks dan sulit dipecahkan. Dewasa ini bidang ilmu kriptografi memiliki kemungkinan aplikasi yang sangat luas, mulai dari bidang militer, telekomunikasi, jaringan komputer, keuangan dan perbakan, pendidikan dan singkatnya dimana suatu kerahasiaan data amatdiperlukan disitulah kriptografi memegang peranan pentingh. Produk-produk yamg menggunakan kriptografi sebagai dasarnyapun cukup beragam, mulai dari kartu ATM, E-Commerce, secure e-mail dan lain-lain.

Kemajuan di bidang telekomunikasi dan komputer ini telah memungkinkan seseorang untuk melakukan transaksi bisnis secara cashless, selain itu ia juga dapat mengirimkan informasi kepada temannya secara on-line. Kegiatan-kegiatan tersebut tentu saja akan menimbulkan resiko bilamana informasi yang sensitif dan berharga tersebut diakses oleh orang-orang yang tidak berhak (*unauthorized persons*). Misalnya, informasi mengenai nomor kartu kredit anda, bila informasi ini jatuh kepada orang-orang yang jahat maka anda harus bersiap-siap terhadap melonjaknya tagihan kartu kredit anda.

2. Kriptografi

Kriptografi berasal dari bahasa yunani yang terdiri dari kata *kryptos* yang berarti tersembunyi dan *grafo* yang berarti tulis. Kriptografi, secara umum adalah ilmu dan seni untuk menjaga kerahasiaan berita. Selain pengertian tersebut kriptografi juga merupakan ilmu yang mempelajari teknik-teknik matematika yang berhubungan dengan aspek keamanan informasi seperti kerahasiaan data, keabsahan data, integritas data, serta autentikasi data.

Ada empat tujuan mendasar dari ilmu kriptografi yang merupakan aspek keamanan informasi yaitu :

1. Kerahasiaan

   Merupakan layanan yang digunakan untuk menjaga isi dari informasi dari siapapun kecuali yang memiliki otoritas atau kunci rahasia untuk membuka atau mengupas informasi yang telah disandi.

2. Integritas data

   Berhubungan dengan penjagaan dari perubahan data secara tidak sah. Untuk menjaga integritas

data, sistem harus memiliki kemampuan untuk mendeteksi manipulasi data oleh pihak-pihak yang tidak berhak, antara lain penyisipan, penghapusan, dan pensubsitusian data lain kedalam data yang sebenarnya.

3. Autentikasi

   Berhubungan dengan identifikasi / pengenalan, baik secara kesatuan sistem maupun informasi itu sendiri. Dua pihak yang saling berkomunikasi harus saling memperkenalkan diri. Informasi yang dikirimkan melalui kanal harus diautentikasi keaslian, isi datanya, waktu pengiriman, dan lain-lain.

4. Non-repudiasi

   Usaha untuk mencegah terjadinya penyangkalan terhadap pengiriman atau terciptanya suatu informasi oleh yang mengirimkan/membuat.[1]

Namun, di dalam dunia ini ada pihak-pihak yang menginginkan suatu informasi rahasia yang tidak ia berhak miliki, sehingga melakukan berbagai cara untuk menyadap atau menyerang informasi tersebut, yang lebih dikenal dengan cryptanalytic attacks yaitu usaha-usaha yang dilakukan seseorang untuk memperoleh informasi ataupun data yang telah dienkripsi. Secara ringkas terdapat tujuh macam *basic cryptanalytic attacks* berdasarkan tingkat kesulitannya bagi penyerang, dimulai dari yang paling sulit adalah :

- *Ciphertext-only attack.*

Dalam penyerangan ini, seorang cryptanalyst memiliki ciphertext dari sejumlah pesan yang seluruhnya telah dienkripsi menggunakan algoritma yang sama.

- *Known-plaintext attack*

Dalam tipe penyerangan ini, cryptanalyst memiliki akses tidak hanya ke ciphertext sejumlah pesan, namun ia juga memiliki plaintext pesan-pesan tersebut.

- *Chosen-plaintext attack*

Pada penyerangan ini, cryptanalyst tidak hanya memiliki akses atas ciphertext dan plaintext untuk beberapa pesan, tetapi ia juga dapat memilih plaintext yang dienkripsi.

- *Adaptive-chosen-plaintext attack*

Penyerangan tipe ini merupakan suatu kasus khusus chosen-plaintext attack. Cryptanalyst tidak hanya dapat memilih plaintext yang dienkripsi, ia pun memiliki kemampuan untuk memodifikasi pilihan berdasarkan hasil enkripsi sebelumnya. Dalam chosen-plaintext attack, cryptanalyst mungkin hanya dapat memiliki plaintext dalam suatu blok besar untuk dienkripsi; dalam adaptive-chosen-plaintext attack ini ia dapat memilih blok plaintext yang lebih kecil dan kemudian memilih yang lain berdasarkan hasil yang pertama, proses ini dapat dilakukannya terus menerus hingga ia dapat memperoleh seluruh informasi.

- *Chosen-ciphertext attack*

Pada tipe ini, cryptanalyst dapat memilih ciphertext yang berbeda untuk didekripsi dan memiliki akses atas plaintext yang didekripsi.

- *Chosen-key attack*

Cryptanalyst pada tipe penyerangan ini memiliki pengetahuan tentang hubungan antara kunci-kunci yang berbeda.

- *Rubber-hose cryptanalysis*

Pada tipe penyerangan ini, cryptanalyst mengancam, memeras, atau bahkan memaksa seseorang hingga mereka memberikan kuncinya. [2][3]

3. Quantum Cryptography

Quantum cryptography pertama kali dicetuskan oleh Stephen Wiesner dari Columbia University pada tahun 1970-an. Ide tersebut kemudian dikembangkan 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 ketidakpastian 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.

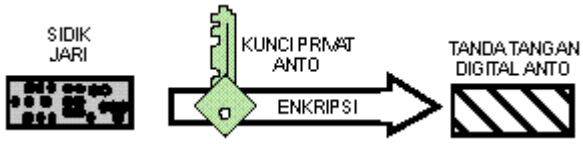
3.1 Quantum Digital Signature

Pada saat ini marak terjadinya suatu pemalsuan baik secara langsung maupun virtual. Akan tetapi pemalsuan secara virtual sepertinya menjadi salah satu hal yang sangat sering terjadi. Maka untuk mencegahnya kita membubuhkan tanda tangan kita pada pesan tersebut. Dalam dunia elektronik, pengirim pesan membubuhkan tanda tangan digitalnya pada pesan yang akan dikirimkan sehingga penerima pesan dapat merasa yakin bahwa pesan itu memang dikirim oleh pengirim yang asli.

Sifat yang diinginkan dari tanda tangan digital diantaranya adalah:

1. Tanda tangan itu asli (otentik), tidak mudah ditulis/ditiru oleh orang lain. Pesan dan tanda tangan pesan tersebut juga dapat menjadi barang bukti, sehingga penandatangan tak bisa menyangkal bahwa dulu ia tidak pernah menandatanganinya.
2. Tanda tangan itu hanya sah untuk dokumen (pesan) itu saja. Tanda tangan itu tidak bisa dipindahkan dari suatu dokumen ke dokumen lainnya. Ini juga berarti bahwa jika dokumen itu diubah, maka tanda tangan digital dari pesan tersebut tidak lagi sah.
3. Tanda tangan itu dapat diperiksa dengan mudah.
4. Tanda tangan itu dapat diperiksa oleh pihak-pihak yang belum pernah bertemu dengan penandatangan.
5. Tanda tangan itu juga sah untuk kopi dari dokumen yang sama persis.

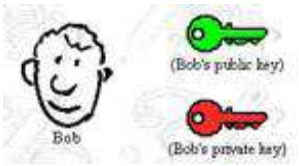
Meskipun ada banyak skenario, ada baiknya kita perhatikan salah satu skenario yang cukup umum dalam penggunaan tanda tangan digital. Tanda tangan digital memanfaatkan fungsi *hash* satu arah untuk menjamin bahwa tanda tangan itu hanya berlaku untuk dokumen yang bersangkutan saja. Bukan dokumen tersebut secara keseluruhan yang ditandatangani, namun biasanya yang ditandatangani adalah sidik jari dari dokumen itu beserta *timestamp*-nya dengan menggunakan kunci privat. *Timestamp* berguna untuk menentukan waktu pengesahan dokumen. [4]



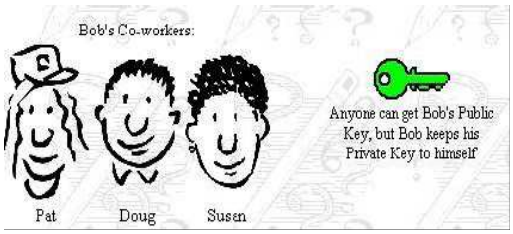
Gambar 1. Pembuatan tanda tangan digital

Keabsahan tanda tangan digital itu dapat diperiksa oleh penerima pesan. Pertama-tama penerima pesan membuat lagi sidik jari dari pesan yang diterimanya. Lalu penerima pesan mendekripsi tanda tangan digital pengirim untuk mendapatkan sidik jari yang asli. Penerima pesan lantas membandingkan kedua sidik jari tersebut. Jka kedua sidik jari tersebut sama, maka dapat diyakini bahwa pesan tersebut ditandatangani oleh pengirim pesan.

Berikut ini merupakan gambaran lain dari digital signature. Misalnya saja, Bob telah diberi 2 kunci, salah satunya disebut public key dan yang satu disebut private key.



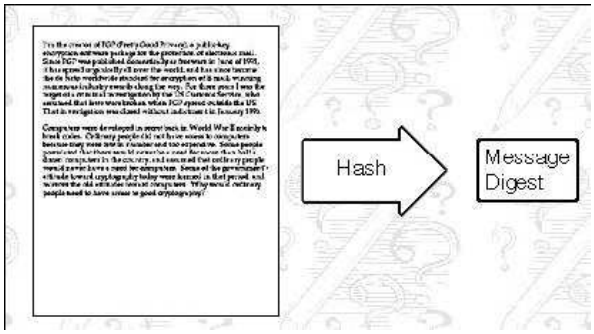
Gambar 2. Dua Kunci Pada Bob



Gambar 3. Kunci Publik Bob

Kunci publik Bob tersedia untuk siapa saja yang membutuhkannya, tetapi kunci private nya disimpan untuk dirinya sendiri. Dimana kunci tersebut digunakan untuk mengenkripsi data.
Susan dapat mengenkripsi pesan menggunakan kunci publik Bob dan Bob menggunakan kunci privatenya untuk mendekripsi pesan tersebut (seperti gambar dibawah ini). Siapapun dari Teman sekerja bob mungkin mempunyai akses terhadap pesan Susan yang dienkripsi, tetapi tanpa Kunci private Bob, data tersebut tidak berharga.

Gambar 4. Enkripsi dan dekripsi message

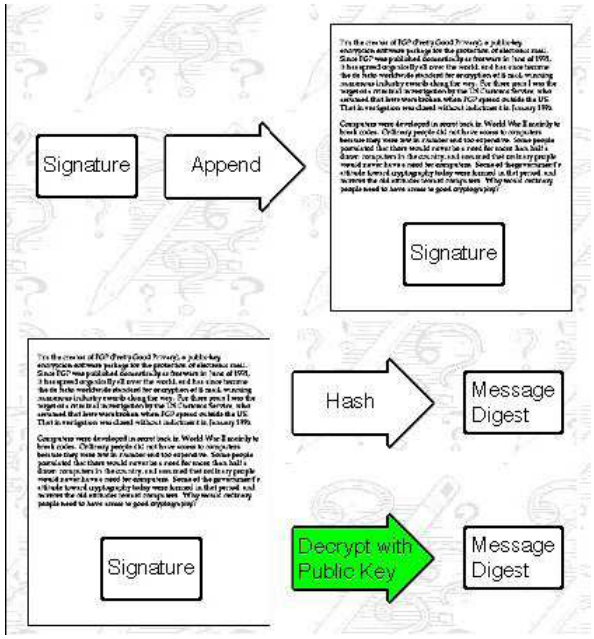


Gambar 5. Hashing

Untuk menandai dokumen, dokumen tersebut akan dihash dengan menggunakan suatu software dan disebut sebagai "Message digest". Kemudian Message Digest tersebut akan dienkripsi dengan kunci publik dan menghasilkan digital signature. Dan digital signature ini akan ditambahkan pada dokumen, sehingga semua data yang telah dihash telah ditandatangani.

Gambar 6. Enkripsi Message Digest

Dengan Kunci private nya dan menggunakan software yang benar, Bob dapat menambahkan digital signature pada dokumen atau data lainnya, dimana suatu digital signature adalah sebuah tanda dari Bob yang ditempatkan pada data secara unik.



Gambar 7. Digital signature pada dokumen

Dengan teknologi yang ada sekarang ini, ditemukan tandatangan digital yang menggunakan teorema quantum cryptography, yang dikenal dengan *quantum digital signature*. *Quantum digital signature* dalam praktiknya mengacu kepada mekanika quantum, dengan berdasar pada teorema ketidakpastian Heisenberg. Sesungguhnya *quantum digital* signature ini hampira sama dengan *classical digital signature* atau yang lebih umum dikenal dengan tanda tangan pada dokumen, hanya saja untuk mendapatkan tandatangan ini harus menggunakan serangkaian perhitungan dan proses yang lebih kompleks. Di dalam digital signature modern keamanan ditingkatkan berdasarkan pada tingkat kesulitan untuk memecahkan permasalahan matematis, yaitu seperti mencari faktor persekutuan terbesar dari suatu bilangan seperti yang digunakan pada algoritma RSA. [5]

Metode Kunci Pubilk

Pubilk 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. Pada intinya, akan lebih mudah untuk menentukan nilai hasil jika nilai masukan diberikan daripada menentukan nilai masukan dengan diketahui nilai hasil. Contoh klasik adalah perkalian dari dua buah bilangan prima yang sangat besar. Mungkin perkalian adalah hal yang mudah, akan tetapi pencarian faktor dari suatu bilangan tanpa diketahui nilai primanya adalah hal tidak mungkin dapat dikerjakan dengan mudah dan dalam waktu yang singkat.

$$x \mapsto f(x) \text{ mudah} \quad (1)$$

$$f(x) \mapsto x \text{ sulit} \quad (2)$$

seperti halnya digital signature klasik, digital signature quantum juga menggunakan kunci asimetris. Maka, seseorang yang ingin menggunakan metode ini harus membuat satu atau lebih pasangan kunci. Pada umunya, kita dapat membagi kelompok dalam digital signature quantum menjadi dua, yaitu:

1. Kelompok/seseorang yang membuat kunci publik pesan dari string private metode klasik

$$k \mapsto |f_k\rangle \quad (3)$$

2. Kelompok/seseorang yang membuat kunci publik pesan dari kunci string private metode quantum.

$$|k\rangle \mapsto |f_k\rangle \quad (4)$$

Pada kedua kasus, f adalah suatu fungsi quantum satu arah yang mempunyai kesamaan dengan fungsi satu arah dari metode klasik. Maka, hasil yang didapat sangat mudah untuk dikomputasi, di lain pihak, dengan menggunakan metode klasik, fungsi ini tidak mungkin untuk dibalikkan (invert) meskipun seseorang menggunakan berbagai macam strategi untuk berbuat kecurangan sekalipun dengan menggunakan metode quantum.

Syarat Untuk Tandatangan yang Baik dan Berguna

Kebanyakan dari syarat-syarat untuk digital signature klasik juga digunakan pula untuk susunan *quantum digital signature*, antara lain:

1. Rencana yang menyediakan keamanan untuk menangkal campur tangan oleh
   a. pengirim setelah mengenkripsi pesan
   b. penerima pesan
   c. orang ketiga
2. Membuat pesan yang tersandi menjadi mudah
3. Setiap penerima pesan mempunyai jawaban yang sama, untuk memeriksa sahnya suatu algoritma

Fungsi Satu Arah

Teorema Holevo menyebutkan bahwa sesuatu yang diberikan dari n-qubits (quantum bit) tidak dapat diekstraksi lebih dari n informasi bit klasik. Satu kemungkinan yang dapat meyakinkan bahwa susunan yang dipergunakan kurang dari qubits untuk panjang string yang telah ditentukan adalah dengan pendekatan ortogonal,

$$|\langle f_k | f'_k \rangle| < \delta \qquad \text{for } k \neq k' \wedge 0 \leq \delta \leq 1 \quad (5)$$

Persamaan ini memberikan kita kemungkinan untuk menimbulkan basis yang lebih dari dua. Maka, untuk menjelaskan informasi yang terdiri dari 2^n bit, kita dapat menggunakan kurang dari n qubits.

Contoh: basis 3 qubits

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

Hanya m qubits yang diperlukan untuk menjelaskan n bit klasik dimana $3^m = 2^n$.

Dari Teorema Holevo dan fakta yang ada, bahwa m dapat lebih kecil dari n, maka kita dapat mengambil hanya m bit saja dari n bit pada pesan. Lebih umum, jika seseorang mendapatkan T salinan dari kunci publik, dia dapat mengekstraksi paling banyak Tm bit dari kunci private. Jika δ adalah bilangan yang besar, n-Tm menjadi sangat besar pula, yang membuat hal ini tidak mungkin untuk seseorang menerka kunci yang asli. Sebagai catatan, anda tidak dapat membedakan antara dua kondisi non-ortogonal, jika anda hanya mempunyai kondisi yang petunjuk yang sedikit. Ini adalah salah satu cara bagaimana fungsi satu arah dengan metode quantum bekerja.

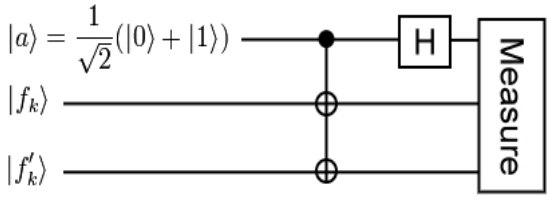
Menyalin kunci publik

Pada kasus klasik, kita membuat kunci publik klasik lain dari kunci private, oleh karena itu, hal ini dengan mudah disediakan untuk setiap penerima menyalin kunci publik. Dalam hal ini, kunci publik dapat dengan mudah didistribusikan secara bebas. Akan tetapi, hal ini menjadi sangat sulit pada kasus dengan metode quantum karena menyalin kondisi dari metode quantum adalah tidak mungkin terjadi dengan tidak adanya teorema yang mendukung penyalinan kunci selama kondisinya sendiri tidak diketahui. Jadi kunci publik hanya dapat dibuat dan didistribusikan oleh seseorang yang mengetahui secara pasti kondisi quantum yang dia ingin buat.

Kunci publik harus sama untuk semua penerima

Untuk lebih yakin bahwa setiap penerima pesan menerima pesan yang sama ketika tes otentikasi pesan, kunci publik harus disebarkan dengan kondisi yang sama pada setiap orang. Hal ini mungkin mudah untuk dilakukan pada metode klasik, karena setiap orang dapat dengan mudah membandingkan dua kumpulan bit dan memastikannya identik satu sama lain. Akan tetapi, hal ini sangatlah membingungkan dan kompleks. Untuk memverifikasinya, jika dua kondisi quantum publik adalah sama, maka untuk membandingkannya harus menggunakan fungsi berikut,

$$|f'_k\rangle = |f_k\rangle \quad (6)$$



Tes Pengecekan untuk Qubits

Tes pengecekan qubits ini dapat dilakukan dengan sirkuit quantum yang menggunakan satu gerbang Fredkin F, satu gerbang Hadamard H dan simpangan qubits a. pertama-tama, simpangan qubits diset menjadi kondisi asimetris

$$|a\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle) \tag{7}$$

Selanjutnya, simpangan qubits ini dijadikan sebagai kontrol dari target $|f_k\rangle$ dan $|f'_k\rangle$ pada gerbang Fredkin. Lalu, gerbang Hadamard digunakan oleh simpangan qubits dan pada akhirnya qubits pertama telah terproses. Jika kedua kondisi menghasilkan bilangan yang identik sama, maka akan memberikan hasil $|0\rangle$. Jika kedua kondisi adalah mendekati ortogonal, maka akan memberikan hasil $|0\rangle$ atau $|1\rangle$.

Hasil perhitungan dari tes pengecekan ini dapat dilihat dengan lebih detail pada penjelasan di bawah ini,

Kondisi secara keseluruhan,

$$|\psi_0\rangle = |a\rangle|f_k\rangle|f'_k\rangle \tag{8}$$

$$|\psi_0\rangle = \frac{1}{\sqrt{2}}\Big(|0\rangle + |1\rangle\Big)|f_k\rangle|f'_k\rangle \tag{9}$$

$$|\psi_0\rangle = \frac{1}{\sqrt{2}}\Big(|0\rangle|f_k\rangle|f'_k\rangle + |1\rangle|f_k\rangle|f'_k\rangle\Big) \tag{10}$$

Setelah gerbang Fredkin diaplikasikan,

$$\Rightarrow \frac{1}{\sqrt{2}}\Big(|0\rangle|f_k\rangle|f'_k\rangle + |1\rangle|\mathbf{f'_k}\rangle|\mathbf{f_k}\rangle\Big) \tag{11}$$

Setelah gerbang Hadamard diaplikasikan pada qubits pertama,

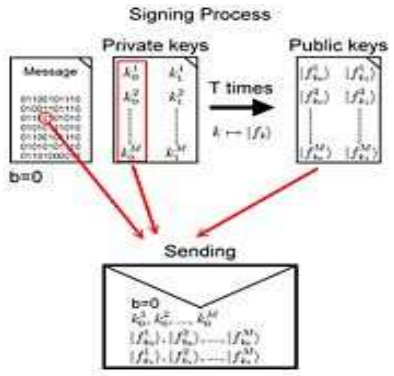
$$\Rightarrow \frac{1}{2}\Big[\Big(|0\rangle + |1\rangle\Big)|f_k\rangle|f'_k\rangle + \Big(|0\rangle - |1\rangle\Big)|f'_k\rangle|f_k\rangle\Big] \tag{12}$$

Setelah pengurutan untuk $|0\rangle$ dan $|1\rangle$.

$$\Rightarrow |\psi\rangle = \frac{1}{2}\Big[|0\rangle\Big(|f_k\rangle|f'_k\rangle + |f'_k\rangle|f_k\rangle\Big) + |1\rangle\Big(|f_k\rangle|f'_k\rangle - |f'_k\rangle|f_k\rangle\Big)\Big] \tag{13}$$

Jika $|f_k\rangle = |f'_k\rangle$ maka $|\psi\rangle = |0\rangle|f_k\rangle|f_k\rangle$, dimana akan memberikan hasil 0.

Contoh proses validasi dengan menggunakan teorema Gottesman-Chuang



Gambar 8. Proses penginputan

Contoh proses penginputan untuk pesan-bit b=0 menggunakan teorema Gottesman-Chuang.

Misalkan ada seseorang bernama Alice (A) yang ingin mengirimkan pesan kepada Beni (B). Algoritma Hash tidak akan dipergunakan, sehingga Alice harus menginisialkan setiap bit pada pesannya. Pesan-bit **b** $\in \{0, 1\}$.

Alice memilih pasangan M dari kunci private yaitu

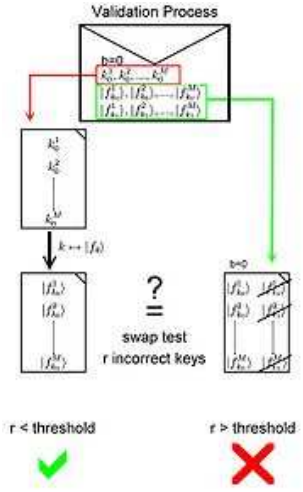
$$\{k_0^i, k_1^i\} \quad 1 \leq i \leq M$$

- Semua kunci k_0 akan digunakan untuk menginsialisasi pesan-bit, jika b = 0.
- Semua kunci k_1 akan digunakan untuk menginisialisasi pesan-bit, jika b = 1.

Fungsi yang memetakan $k \mapsto |f_k\rangle$ dapat diketahui oleh seluruh orang. Sekarang Alice akan mengkomputasi kunci publik yang bersangkutan $\{|f^i_{k0}\rangle, |f^i_{k1}\rangle\}$ dan memberikannya kepada semua penerima pesan. Alice dapat membuat salinan sebanyak dia inginkan, akan tetapi dia harus berhati-

hati untuk membuat salinan agar tidak membahayakan keamanan dari pesan $(n \gg Tm \text{ has to hold })$.

Jika pesan-bit b = 0, maka Alice mengirimkan seluruh kunci private k_0 bersama dengan pesan-bit b kepada Beni. Namun, jika b = 1, maka ia harus mengirimkan seluruh kunci private k_1 bersama dengan pesan-bit b kepada Beni.



Gambar 9. Proses validasi

Saat ini, Beni yang akan bertugas untuk mendekripsi pesan, sehingga ia memerlukan

- Pesan-bit b
- Kunci private yang berkorespondensi yaitu k_0 atau k_1
- Semua kunci publik $\{|f_{k_0}\rangle, |f_{k_1}\rangle\}$

Selanjutnya, Beni akan melakukan perhitungan $|f_{k_b}\rangle$ untuk setiap kunci private yang ia terima, baik k_0 maupun k_1.

Setelah Beni selesai, ia harus melakukan tes pengecekan untuk membandingkan hasil perhitungan yang ia lakukan dengan hasil perhitungan menggunakan kunci publik yang ia terima. Selama tes pengecekan ini menghasilkan hasil yang berbeda, ia harus mencoba untuk menggunakan semua kunci M untuk mendekripsi pesan, dan menghitung berapa banyak kunci yang tidak sesuai dengan yang asli (r). Sudah jelas bahwa M adalah salah satu parameter dari sistem keamanan data, sehingga terasa mustahil untuk melakukan validasi bit yang salah untuk nilai M yang sangat besar.

- Jika Beni hanya mendapatkan sedikit kunci yang tidak tepat, maka sebagian besar dari bit yang ia terima adalah benar, hal ini dikarenakan kunci yang Beni perhitungkan dan kunci publik hampir sama.
- Jika Beni mendapatkan kunci yang salah, maka dapat dipastikan ada seseorang yang memalsukan pesan yang ia terima

Cara untuk Menghindari Perbedaan Hasil

Salah satu masalah yang muncul khusunya untuk nilai M yang kecil adalah perbedaan banyaknya kunci yang tidak sesuai pada penerima menghasilkan probabilitas yang berbeda. Maka untuk mendekripsi diperlukan lebih dari satu nilai ambang, karena hal ini akan menyebabkan pesan didekripsi secara berbeda, yaitu ketika banyaknya kunci yang tidak sesuai (r) sangat mendekati nilai ambang.

Hal ini dapat dicegah dengan mendefinisikan lebih dari satu nilai ambang, karena banyaknya kesalahan akan meningkat seiring dengan meningkatnya nilai M. adapun nilai ambang yang didefinisikan adalah

- Diterima bila $T_a = c_1M$
- Tidak diterima bila $T_r = c_2M$

Jika banyaknya kunci yang tidak sesuai (r) lebih kecil dari T_a, maka bit dinyatakan valid dengan probabilitas yang tinggi.

Jika banyaknya kunci yang tidak sesuai (r) lebih besar dari T_r, maka bit dinyatakan palsu dengan probabilitas yang tinggi.

Jika banyaknya kunci yang tidak sesuai derada diantara kedua nilai ambang yaitu $T_a <= r <= T_r$, maka penerima tidak dapat memastikan kebenaran dari pesan tersebut, yaitu ketika ada penerima yang lain yang mempunyai hasil yang sama dengan yang anda punya, ketika proses validasi. Maka, pesan yang ia terima pun tidak dapat dipercaya, meskipun ia mengatakan bahwa pesan hasil validasi yang ia lakukan adalah benar.

Jika kita mengasumsikan bahwa jaringan yang digunakan adalah sempurna, dalam hal ini tidak ada gangguan seperti noise, maka bit tidak dapat berubah selama proses pengiriman, sehingga nilai ambang dapat kita set menjadi 0 (nol), karena pada tes pengecekan selalu berhasil, selama hasil yang didapat adalah sama. [6]

4. Kesimpulan

Digital signature dengan menggunakan metode quantum memberikan keamanan yang lebih terjamin daripada memakai kunci publik, karena 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 oleh pengirim pesan dengan kunci yang diterima oleh penerima pesan. Oleh karena itu, kunci yang dihasilkan dapat dikatakan bebas penyadapan. Meskipun terlihat sangat sulit dalam hal perhiutngan akan tetapi seiring dengan perkembangan jaman, masyarakat telah mengembangkan komputer yang mendasarkan perhitungannya dengan metode quantum yang dikenal dengan komputer quantum. Komputer quantum ini dapat menyelesaikan permasalahan dalam perhitungan sehingga menjadi lebih cepat terselesaikan.

Daftar Referensi

[1] http://id.wikipedia.org/wiki/Kriptografi

Diakses pada tanggal 23 Desember 2008

[2] http://www.cryptography.com

Diakses pada tanggal 23 Desember 2008

[3] http://tedi.heriyanto.net/papers/p_kripto.html

Diakses pada tanggal 23 Desember 2008

[4] http://www.geocities.com/amwibowo/resource/komparasi/bab3.html

Diakses pada tanggal 23 Desember 2008

[5] Ramayanti, Desi. "Tugas Akhir Keamanan Sistem Lanjut Aplikasi Digital Signature Sebagai Autentifikasi Pada Kartu Tanda Penduduk. 2007. Teknik Elektro ITB:Bandung

Dikases pada tanggal 23 Desember 2008

[6] http://en.wikipedia.org/wiki/Quantum_digital signature

Diakses pada tanggal 23 Desember 2008