Perbandingan Antara Kriptografi Modern dengan Kriptografi Kuantum

Shinta Marino[1]
1) Jurusan Teknik Informatika ITB, Bandung 40132, email: if14130@if.itb.ac.id

Abstract *– Algoritma kriptografi ideal adalah algoritma tidak dapat dipecahkan kecuali orang tersebut mempunyai kunci untuk mendekripsinya (unbreakable cipher). Sampai saat ini satu-satunya unbreakable cipher yang diketahui adalah one time pad yang tidak efisien untuk diimplementasikan.*
Sementara itu, sejumlah algoritma kriptografi yang dianggap paling aman menggantungkan derajat keamanannya kepada kompleksitas kunci. Algoritma kriptografi yang sangat jelas menggunakan prinsip ini adalah kriptografi kunci publik.
Sampai sekarang masih banyak yang menganggap metode ini sudah cukup aman, akan tetapi ternyata ada cara yang diperkirakan dapat melakukan komputasi tersebut lebih cepat sehingga private key dapat ditemukan dalam waktu yang jauh lebih singkat, yaitu dengan quantum cryptanalysis. Quantum cryptanalysis menggunakan quantum computer yang dapat melakukan perhitungan dengan lebih cepat.
Adanya kriptanalisis kuantum memberi kesempatan baru bagi para kriptanalis dalam memecahkan cipherteks. Tapi di sisi lain menurunkan derajat keamanan algoritma-algoritma kriptografi yang keamanannya bergantung pada kompleksitas kunci.

Kata Kunci*: algoritma, kriptografi kuantum, kriptografi kunci publik*

1. PENDAHULUAN

Ilmu kriptografi telah dikenal sejak lama. Mulai dari algoritma paling sederhana seperti Caesar Cipher sampai dengan algoritma kriptografi modern yang banyak digunakan saat ini. Seiring dengan berkembangnya ilmu kriptografi ikut pula berkembang ilmu kriptoanalisis yaitu ilmu untuk memecahkan cipherteks yang telah di enkripsi dengan suatu algoritma kriptografi. Bersama-sama kriptografi dan kriptoanalisis tergabung dalam suatu bidang yang disebut kriptologi.

Kriptografi dan kriptoanalisis terus berkembang beririrngan. Para ahli kriptologi akan berlomba-lomba menemukan cara untuk memecahkan sebuah algoritma kriptografi yang baru muncul. Sebagai ilmu yang terus berkembang, selalu muncul inovasi baru dalam dunia kriptologi. Saat ini perkembangan kriptoanalisis sedikit terhambat oleh keterbatasan kemampuan komputasi computer saat ini. Sejumlah algoritma kriptografi modern memanfaatkan hambatan ini. Sejumlah algoritma kriptografi modern saat ini akan dengan mudah dapat dipecahkan jika kunci yang digunakan tergolong pendek. Akan tetapi, jika kunci yang digunakan cukup panjang (biasanya mencapai 100 angka) dibutuhkan waktu yang sangat lama untuk menemukan kunci untuk memecahkan cipherteks tersebut.

Para ahli kriptologi terus menerus mencari kemungkinan baru untuk diterapkan dalam dunia kriptologi. Salah satu ide yang muncul belakangan ini, walaupun baru sebatas pembahasan teori adalah kuantum kriptologi.

2. KRIPTOGRAFI MODERN

Algoritma kriptografi modern berbasis bit. Setiap operasi enkripsi dilakukan pada bit-bit data. Dengan demikian, seluruh data yang sifatnya digital dapat di enkripsi dengan menggunakan algoritma kriptografi ini.

Algoritma kriptografi modern terbagi menjadi dua bagian utama berdasarkan kunci yang digunakan untuk melakukan enkripsi dan dekripsi. Kedua bagian itu adalah algoritma kunci asimetri dan algoritma kunci simetri

2.1. Kriptografi Kunci Asimetri (Kunci Publik)

Algoritma kunci asimetri adalah algoritma kriptografi yang mempunyai sepasang kunci berbeda untuk melakukan enkripsi dan dekripsi. Algortima jenis ini lebih dikenal dengan nama algoritma kunci publik (*public key algorithm*). Prinsip kunci asimetri ini pertama kali muncul dari usul Whitfield Diffie dan Martin Hellman pada tahun 1976 yang saat itu bekerja di *Stanford University*. Sementara itu implementasi algoritma jenis ini pertama kali dikembangkan oleh Ronald Rivest, Adi Shamir, dan Leonard Adleman dari Massachusetts Institute of Technology pada tahun 1978.

Keamanan algoritma kriptografi kunci asimetri berbasis pada kompleksitas komputasi. Hal ini dilakukan dengan menggunakan sebuah fungsi satu arah (*one way function)* yaitu fungsi *f(x)* dimana melakukan perhitungan *f(x)* akan jauh lebih mudah dibanding mencari nilai *x* dari fungsi *f(x)* yang diketahui. Dengan kata lain, perhitungan untuk mencari nilai *x* dari fungsi *f(x)* sangat kompleks sehingga membutuhkan waktu sangat lama untuk memecahkannya. Kompleksitas komputasi yang harus dilewati akan meningkat secara eksponensial seiring

bertambahnya panjang key *x*.

Seluruh algoritma kunci public mendasarkan keamanannya pada kompleksitas komputasi dengan asumsi perkembangan terknologi tidak mampu menandingi kompleksitas yang telah dibangun sehingga bahkan dengan kemampuan komputer tercepat saat ini pun dibutuhkan waktu sangat lama untuk memecahkan algoritma tersebut. Asumsi tersebut masih belum terbukti. Jika suatu saat ditemukan cara baru dalam dunia matematika untuk melakukan perhitungan dengan lebih mudah, maka seluruh algoritma kriptografi kunci public yang dikenal saat ini menjadi tidak berharga dan data-data yang telah di enkripsi dengan algoritma tersebut dapat dipecahkan dengan mudah.

2.1. Kriptografi Kunci Simetri

Algoritma kunci simetri merupakan algoritma yang hanya membutuhkan kunci yang sama untuk melakukan enkripsi dan dekripsi. Algoritma kriptografi jenis ini relative lebih aman dibanding algoritma kunci public, karena tidak seperti algoritma kunci public yang keamanannya didasarkan pada kompleksitas komputasi, algoritma kunci simetri mendasarkan keamanannya pada kerahasiaan kunci.

Akan tetapi ternyata algoritma jenis ini juga mempunyai kelemahan yang terletak pada masalah distribusi kunci. Kunci pada algoritma ini idealnya harus mempunyai panjang minimal sama dengan panjang pesan yang akan di enkripsi. Hal ini menuntut kedua pihak untuk mempunyai dua set kunci yang identik. Masalah utama saat ini adalah bagaimana caranya kedua pihak yang saling berkirim pesan tersebut untuk saling memberikan kunci. Di samping itu untuk meningkatkan keamanan, sebuah kunci yang sudah pernah digunakan tidak boleh digunakan lagi untuk menghindari pihak luar yang melakukan *eavesdropping* untuk mendapatkan dua cipherteks berbeda yang di enkripsi dengan kunci yang sama. Karena melalui dua cipherteks tersebut, kunci dapat diperoleh dengan teknik tertentu. Dengan pergantian kunci untuk setiap pesan yang di enkripsi, masalah distribusi kunci antar kedua belah pihak yang berkomunikasi menjadi makin kompleks.

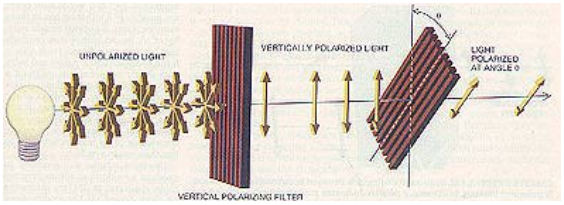
Karena masalah distribusi kunci ini, saat ini algoritma kunci simetri seperti *one-time pad* hanya digunakan pada aplikasi yang bersifat kritis.

Disamping masalah distribusi kunci, ternyata algoritma ini relative lebih lambat dibanding algoritma kunci publik. Oleh karena itu, pada prakteknya algortima ini tidak banyak digunakan untuk enkripsi data, tetapi lebih banyak digunakan untuk distribusi *session keys* untuk algoritma kriptografi simetri seperti DES yang belum terbukti keamanannya.

2. KRIPTOGRAFI KUANTUM

Ide mengenai kriptografi kuantum berkembang dari ilmu fisika kuantum. Menurut ilmu kuantum, gelombang cahaya terdiri dari partikel-partikel diskrit yang disebut foton (*photon*). Foton adalah partikel tak bermassa yang membawa energy, momentum dan momentum angular. Sementara gelombang elektromagnetik, termasuk gelombang cahaya, dapat dikenai polarisasi. Untuk gelombang cahaya, polarisasi terjadi sesuai dengan arah momentum angular atau perputaran foton. Sebuah foton yang dilewatkan pada filter polarisasi bisa lolos ataupun tidak lolos dari filter tersebut. Tetapi jika foton tersebut lolos, maka polarisasinya akan menjadi sama dengan arah filter yang dilewatinya tanpa mempehitungkan polarisasi awal foton tersebut. Polarisasi foton tersebut dapat diketahui melalui detektor foton untuk mengetahui apakah sebuah foton lolos dari filter yang ada atau tidak.

Dasar dari kriptografi kuantum adalah prinsip ketidakpastian Heisenberg yang menyatakan bahwa suatu pasangan properti fisik saling terhubung sedemikian sehingga pengukuran terhadap salah satu properti akan menghambat pengukuran untuk properti lainnya



Gambar 1 Polarisasi melalui filter

Seperti pada tampak pada gambar 1, sejumlah foton yang dilewatkan pada filter vertikal mampu menembus filter tersebut dan polarisasinya juga berubah menjadi vertikal. Selanjutnya foton-foton tersebut dilewatkan kembali pada sebuah filter yang mempunyai sudut θ terhadap garis vertikal. Kembali sebagian dari foton tersebut mampu menembus filter kedua dan arah polarisasinya pun berubah menjadi θ˚ dari garis vertikal. Berdasarkan penelitian yang dilakukan, sudut θ yang berbeda memberikan probabilitas yang berbeda pula untuk foton mampu menembus filter kedua. Semakin besar nilai θ, probabilitas foton untuk mampu menembus filter kedua semakin kecil sampai akhirnya mencapai nilai 0 pada θ = 90˚. Pada saat θ = 45˚, kemungkinan foton untuk melewati filter kedua tepat mempunyai nilai ½. Ini adalah hasil yang sama dengan sebuah aliran foton yang secara acak dilewatkan pada filter kedua. Dengan demikian, filter pertama dikatakan melakukan randomisasi pengukuran pada filter kedua.

Dalam kuantum kriptografi, jika Alice menggunakan filter 0˚ atau 90˚ untuk memberi foton-foton polarisasi awal, Bob yang menerima pesan dapat mengetahui polarisasi awal foton dengan menggunakan filter dengan ukuran sudut yang sama. Tetapi jika Bob

menggunakan filter yang salah, ia tidak akan mendapatkan informasi apapun mengenai polarisasi awal foton-foton tersebut. Dengan demikian, jika seseorang berusaha melakukan intersepsi pada pesan yang dikirim Alice pada Bob, sebut saja Eve, dengan menggunakan filter yang sesuai dengan filter yang digunakan Alice, ia bisa mendapatkan polarisasi asli dari foton tersebut, tetapi jika ia menggnakan filter yang salah ia tidak akan bisa memperoleh informasi yang diinginkan, disamping itu ia tidak akan mampu meneruskan pesan asli kepada Bob. Dengan demikian Bob akan menerima pesan yang rusak atau bahkan tidak menerima pesan apapun sehingga keberadaan Eve dapat diketahui.

Pada prinsipnya, pengiriman pesan dengan menggunakan foton cukup sederhana karena properti polarisasi dapat digunakan untuk merepresentasikan 0 dan 1. Setiap foton menyimpan satu bit informasi kuantum yang disebut qubit. Untuk menerima qubit, penerima harus mengetahui polarisasi foton tersebut.

Kuantum kriptografi juga mampu memecahkan masalah distribusi kunci. Salah satu pihak yang berkomunikasi akan mengusulkan kunci dengan mengirim sejumlah foton dengan polarisasi acak. Foton-foton tersebut kemudian digunakan untuk menghasilkan sederetan angka. Jika key tersebut sempat diambil oleh pihak lain, foton yang sampai akan mengalami perubahan, sehingga keberadaan *eavesdropper* dapat terdeteksi. Pengirim kemudian dapat mengirim lagi kunci lain. Jika kunci telah diterima dengan aman, kunci tersebut digunakan untuk me-enkripsi pesan yang kemudian bisa dikirim dengan sarana komunikasi biasa.

Ide untuk menggunakan protokol di atas pertama kali di publikasikan oleh Charles Bennett dan Gilles Brassard pada tahun 1984. Sistem ini kemudian disebut sistem BB84. Sistem BB84 berjalan sebagai berikut : Alice dan Bob masing-masing mempunyai dua alat polarisasi foton. Salah satu alat tersebut mempunyai polarisasi 0˚/90˚ dan yang lainnya dengan polarisasi 45˚/135˚. Alice dan Bob berkomunikasi melalui sebuah saluran kuantum dimana Alice dapat mengirimkan foton kepada Bob dan sebuah saluran umum dimana mereka dapat melakukan diskusi. Seorang *eavesdropper*, Eve diasumsikan mempunyai tenaga komputasi yang tidak terbatas dan akses terhadap kedua saluran yang digunakan Alice dan Bob.

Pertama-tama, Alice menentukan sederetan kunci kemudian mengirimkannya dalam bentuk foton kepada Bob dimana setiap foton dipolarisasi secara acak dalam salah satu arah polarisasi yang dimilikinya yaitu :0˚, 45˚, 90˚, dan 135˚.

Gambar 2 Kunci yang dibuat oleh Alice

Gambar 3 Kunci Alice setelah dipolarisasi acak

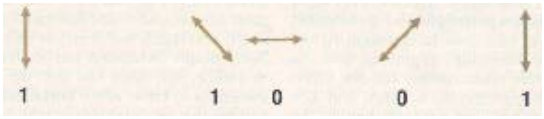
Ketika Bob menerima foton tersebut, ia menggunakan salah satu alat polarisasinya yang dipilih secara acak. Pilihan acak ini memungkinkan pilihan Bob tidak sama dengan Alice. Jika alat polarisasi yang digunakan Bob tidak sesuai dengan Alice, maka akan dihasilkan sesuatu yang acak.

Gambar 4 Hasil Polarisasi acak dari Bob

Untuk menghilangkan kesalahan yang terjadi akibat perbedaan polarisasi Alice dan Bob melakukan diskusi melalui saluran umumsetelah seluruh foton terkirim. Bob memberi tahu Alice basis yang ia gunakan untuk setiap foton dan Alice memberi tahu Bob apakah basis tersebut benar atau salah. Alice dan Bob tidak menyebutkan hasil yang sebenarnya, hanya basis dari polarisasi yang dilakukan.

Gambar 5 Hasil pencocokan kunci Alice dan hasil polarisasi acak dari Bob

Seluruh data yang tidak cocok hasil polarisasinya dibuang menyisakan dua string yang identik masing-masing dimiliki oleh Alice dan Bob.



Gambar 4 String kunci identik yang dihasilkan Alice dan Bob

Dengan demikian Alice dan Bob berhasil berbagi kunci tanpa secara langsung menyebutkan kunci tersebut sehingga Eve tidak bisa mendapatkan kunci yang sebenarnya. Walaupun Eve mampu menangkap Foton yang dikirim Alice, melakukan polarisasi terhadap foton tersebut kemudian meneruskannya kepada Bob, Eve akan merusak 25% bit yang dikirim. Jika suatu saat Alice dan Bob bertemu secara langsung dan membandingkan foton yang mereka punya, akan segera diketahui bahwa pengiriman kunci tersebut telah diganggu oleh orang lain.

3. KRIPTOGRAFI MODERN (KRIPTOGRAFI KUNCI PUBLIK) VS KRIPTOGRAFI KUANTUM

Dari segi teori, melalui penjelasan diatasdapat disimpulkan bahwa kriptografi kuantum memiliki tingkat keamanan yang jauh lebih baik dibanding algoritma kriptografi modern. Kriptografi kuantum bahkan mampu mendeteksi keberadaan *eavesdropper* dalam pengiriman pesan karena sederetan foton tidak bisa disalin menjadi dua salinan yang sama persis. Selalu terdapat distorsi pada foton yang sudah disalin. Dengan sifat foton yang demikian itu, kebocoran informasi dapat segera diketahui dan ditangani.

Kelebihan lain dari kriptografi kuantum adalah kemampuan ilmu fisika kuantum untuk menawarkan solusi pada masalah klasik kriptografi yaitu distribusi kunci dengan menggunakan sistem BB84. Walaupun sistem yang digunakan cukup rumit, kriptografi kuantum berhasil memecahkan masalah utama tidak berkembangnya algoritma kriptografi kunci simetri. Dengan kemampuan ini, algoritma kunci simetri yang telah ada saat ini dapat digunakan tanpa harus menghadapi kendala pada distribusi kunci.

Akan tetapi pada kenyataannya, penerapan algoritma kunci public jauh lebih mudah dan sederhana. Disamping konsep fisika kuantum yang sangat membigungkan bahkan bagi para ahli sekalipun, kuantum komputer yang merupakan alat utama dalam menjalankan kriptografi kuantum pun sampai saat ini masih sebatas teori. Menurut teori yang ada, prinsip fisika kuantum akan berlaku pada sekumpulan dimensi yang jumlahnya tak terhingga di luar deteksi indera manusia yang disebut *Hillbert Space*.

Pembuatan *Hillbert Space* inilah yang menjadi kendala dalam pembuatan kuantum komputer. Dalam pembangunan *Hillbert Space* ini menemui banyak rintangan yang menghambat para ahli sampai saat ini.

Padahal jika komputer kuantum berhasil diciptakan, algoritma kriptografi kunci public yang digunakan saat ini akan menjadi hampir tidak berharga karena kuantum komputer mampu memecahkan hambatan kompleksitas komputasi yang diandalkan algoritma kunci publik. Hal ini dapat dilakukan komputer kuantum karena qubit dapat melakukan sejumlah besar komputasi secara bersamaan tidak seperti bit yang hanya mampu melakukan satu komputasi pada suatu waktu tertentu.

4. KESIMPULAN

Kriptografi kuantum adalah sebuah ide menarik yang dapat menimbulkan revolusi dalam dunia kriptografi. Jika kriptografi kuantum dapat benar-benar diterapkan, keamanan pesan yang dikirim untuk berkomunikasi satu sama lain melalui saluran umum akan jauh lebih terjaga.

Kriptografi kuantum dapat membuat algoritma kriptografi kunci publik yang saat ini digunakan secara luas menjadi tidak berharga karena kemampuan komputasi dengan menggunakan teori kuantum jauh lebih tinggi dibanding komputer paling canggih yang kita kenal saat ini

Hanya saja sampai saat ini para ahli belum berhasil menciptakan komputer kuantum yang mampu melakukan perhitungan secara kuantum. Oleh karena itu, untuk saat ini masyarakat dunia masih harus bertahan menggunakan algoritma kriptografi modern khususnya algoritma kriptografi kunci publik yang sejauh ini masih aman untuk digunakan dengan syarat tertentu.

DAFTAR REFERENSI

[1] N. Gisin, G. Ribordy, W. Tittel, H. Zbinden, "*Quantum Cryptography*", Switzerland, 2002.

[2] S. Vittorio, "*Quantum Cryptography : Privacy Through Uncertainty*", www.csa.com/hottopics/crypt, 2002.

[3]T. Siegfield, "*Beyond Bits*", www.ecst.csuchico.edu /~atman/Crypto/quantum/quantum-index.html