Kriptografi Kuantum dengan gagasan Bennet dan Bassard

Anwari Ilman (13506030)
Jurusan Teknik Informatika ITB, Bandung 40132.
Email: if16030@students.if.itb.ac.id

Abstract *– Makalah ini membahas tentang penggunaan mekanika kuantum untuk membangun sebuah sistem kriptografi yang aman. Jika kita perhatikan lebih jauh lagi, mekanika kuantum yang digunakan pada benda-benda sub-atomik sifatnya sangat berbeda jika kita bandingkan dengan aturan mekanika fisika yang lazim terjadi dalam kehidupan sehari-hari. Kelainan tersebut didapatkan dari prinsip ketidak-pastian Heisenberg yang menyatakan bahwa setiap pengukuran sesungguhnya melakukan perlawanan terhadap obyek yang kita ukur.*

Dengan menggunakan gagasan Bennett dan Brassard yang dikemukakan pada tahun 1984, k*elainan pada mekanika kuantum ini dapat dimanfaatkan untuk membangun sistem sandi kriptografi yang aman dari sadapan pihak lain.*

Kata Kunci*: Mekanika kuantum, kriptografi, Heisenberg, Bennett dan Brassard.*

1. PENDAHULUAN

Kriptografi (*cryptography*) berasal dari Bahasa Yunani: "*cryptós*" artinya "*secret*" (rahasia), sedangkan "*gráphein*" artinya "*writing*" (tulisan). Jadi, secara singkat kriptografi berarti "*secret writing*" (tulisan rahasia).

Berdasarkan definisi kriptografi yang dikemukakan dalam [SCH96]: Kriptografi adalah ilmu dan seni untuk menjaga keamanan pesan (*Cryptography is the art and science of keeping messages secure*), terlihat bahwa kriptografi bukan hanya sekedar proses sains untuk menyandikan pesan, tetapi didalamnya terdapat juga seni untuk membuat metode-metode untuk menyandikan pesan. Tentunya hal ini membutuhkan daya kreatifitas manusia untuk membuat sebuah sandi yang sulit dipecahkan. Disinilah letak keunikan kriptografi. Dibutuhkan sebuah kerjasama antara kreatifitas dan akal cerdas untuk mengenkripsi dan mendekripsikan pesan.

Ilmu kriptografi sudah lama digunakan dan sekarang sudah ada mesin canggih yang khusus dibuat untuk maksud tersebut. Meskipun demikian, ada satu kekurangan yang belum terselesaikan. Misalnya si Ana ingin mengirim informasi yang tidak boleh diketahui oleh orang lain kecuali si Joe. Keduanya dapat membeli mesin pengacak untuk dipakai. Si Ana harus memilih kunci (sandi) yang digunakannya untuk mengacak informasi dengan alat tersebut.

Informasi yang sudah diacak tadi dikirim ke si Joe. Tidak perlu khawatir karena orang lain tak akan dapat membaca isinya secara tepat. Agar si Joe dapat membaca informasi yang dikirimkan oleh si Ana tadi, meskipun dia punya mesin pengacak yang sama dengan milik si Ana tetapi dia harus tahu kunci sandinya. Persoalannya, bagaimana cara si Ana memberitahu si Joe tentang kunci sandinya itu. Jika diberitahukan lewat telepon, jangan-jangan ada yang menyadapnya. Kalau dikirim dengan kurir, apakah orangnya dapat dipercaya. Intinya, si Ana harus menggunakan saluran komunikasi tertentu, yang sukar disadap atau dibocorkan kepada orang lain, untuk memberi tahukan kunci sandinya tadi kepada si Joe.

Kriptografi Kuantum ini diperkirakan dapat digunakan untuk mengirim kunci sandi tadi dengan cara yang tidak mungkin diketahui orang lain kecuali si Joe.

2. MEKANIKA KUANTUM

Mekanika Kuantum menggunakan 'bahasa' yang sangat abstrak. Ungkapan-ungkapan gejala alam dilukiskan secara matematika dalam sebuah *Ruang Vektor R,* yang dimensinya kadang-kadang sangat besar, tak berhingga. Artinya, ruang tersebut dibangun oleh sebuah *kumpulan vektor yang ortonormal,* ukuran satuannya sama dan saling 'tegak-lurus' satu sama lain.

Keadaan obyek kita dilukiskan oleh sebuah *'state vector'* $|\varphi\rangle$. dalam Ruang Vektor *R* tadi. Setiap vektor dalam *R* selalu dapat dituliskan sebagai kombinasi linier dari vektor-vektor ortonormal pembangun *R*, dengan koefisien yang nilainya bilangan kompleks. Jadi, kalau kumpulan vektor ortonormal pembangun *R* tadi kita tuliskan sebagai $|0\rangle$, $|1\rangle$, $|2\rangle$, …dst, maka kita boleh menuliskan $|\varphi\rangle$ sebagai

$$|\varphi\rangle = \sum_i c_i |i\rangle$$

c1, c2, …bilangan kompleks.

'*Observable*' , yaitu besaran fisika yang biasa kita amati atau kita ukur, dalam 'bahasa' ini dilukiskan oleh sebuah operator A dalam *R* dengan sifat *self-*

adjoint. Artinya kalau diungkapkan dalam representasi matriks, transpos dari *complex-conjugate*-nya mempunyai nilai sama dengan matriksnya sendiri.

$$A_{ji}^{*} = A_{ij}$$

Sifat ini menjamin bahwa nilai eigen dari operator tersebut selalu berupa bilangan riil, meskipun elemen matriksnya sendiri boleh berupa bilangan kompleks. Fungsi-fungsi eigen dari sebuah operator yang melukiskan *observable* tadi, jika di normalisasikan besarnya, dapat berfungsi sebagai basis ortonormal dari Ruang Vektor *R*. Karena itu setiap status vektor seperti $|\varphi\rangle$ juga dapat dituliskan sebagai kombinasi linier dari basis ortonormalnya operator A.

Berbeda dengan aturan mekanika klasik, bila kita melakukan pengukuran besaran yang dilukiskan oleh operator A tadi, maka nilai yang muncul sebagai hasil pengukuran tersebut hanyalah nilai eigen dari operator A tadi. Jadi seandainya |0>, |1>, |2>, …dst itu kebetulan set ortonormal dari vektor eigen operator A, maka tentunya kita dapat menuliskan :

$$Aij = \langle i \mid A \mid j \rangle = \delta_{ij}\, a_j$$

dengan a_1, a_2, ….adalah nilai eigen dari operator A. Pada kebanyakan kasus nilai a_1, a_2, .. untuk besaran momentum sudut misalnya, berupa bilangan diskrit. Itulah sebabnya penyajian seperti ini dinamakan kuantum, tidak seperti yang lazim kita temukan sehari-hari bahwa momentum sudut sebuah benda yang bergerak nilainya boleh berapa saja.

Jika obyek yang kita garap itu ada pada "state" $|\varphi\rangle$ yang boleh ditulis sebagai

$$|\varphi\rangle = \sum_i c_i |i\rangle$$

maka pengukuran kita akan menghasilkan nilai a_1 dengan peluang $|c_1 c_1^{*}|$, atau menghasilkan nilai a_2 dengan peluang $|c_2 c_2^{*}|$, …dst.

'Kelainan' yang lebih jauh lagi dalam Mekanika Kuantum adalah bahwa bila pengukuran besaran A tadi ternyata menghasilkan nilai a_2 misalnya, maka "state" obyek kita langsung berubah menjadi |2>. Jadi kita kehilangan informasi tentang kondisi obyek kita sebelum pengukuran.

Tentu saja aturan atau teori semacam ini tidak mudah diterima orang banyak. Tetapi rupanya perangai alam ini memang begitu, dan kita tidak bisa merubahnya. Kalau itu memang yang 'benar' ya harus diterima, bahkan barangkali justru kita berupaya mencari cara bagaimana dapat memanfaatkannya.

Kenyataan yang 'aneh' itulah yang akan dimanfaatkan dalam teknik kriptografi kuantum. Bahkan diperkirakan kriptografi cara kuantum ini justru manjadi sistem sandi yang bisa dijamin tak dapat disadap orang lain yang tidak berhak mengetahuinya.

2.1 Proses Komputasi Secara Mekanika Kuantum

Ilmu dan teknologi komputer telah berkembang dengan pesat. Semua aturan yang dipakai adalah aturan yang lazim dikenal dalam ilmu fisika klasik. Salah satu basis dasar yang membangun komputasi saat ini adalah penggunaan 'bahasa' yang hanya punya dua kemungkinan, "nyala" atau "padam" karena beroperasi dengan listrik. Yang lebih sering digunakan adalah istilah bahasa aljabar Boolean : "benar" (*true*) dan "salah" (*false*). Atau juga kalau dikaitkan dengan perwujudan bilangan dipakai "sistim bilangan biner", hanya mengenal angka 0 dan angka 1 saja.

Peralatan mesin komputer yang ada saat ini menggunakan basis rangkaian listrik dalam bentuk yang sangat kecil yang berfungsi sebagai satuan "nyala-padam" yang dinamakan bit**.** Agar memungkinkan bekerja dalam jumlah yang sangat banyak, ukuran wujudnya diperkecil. Proses memperkecil atau sering disebut 'miniaturisasi' semacam itu tentu ada batasnya. Jika sudah dekat dengan orde 10 nanometer, yaitu kira-kira ukuran molekul atau atom, maka harus berhenti. Dalam wilayah ini perangai alamnya dikendalikan oleh mekanika kuantum yang berbeda dengan mekanika klasik. Karena itu diselidikilah cara-cara baru melakukan komputasi berdasar pada mekanika kuantum.

Agar upaya pemanfaatan mekanika kuantum ini dapat berkembang cepat perlu dimanfaatkan 'bahasa' yang sudah lazim dipakai selama ini, yaitu dipilih Ruang Vektor R yang dimensinya-2, sebagai langkah awalnya. Vektor basisnya boleh dinamakan |0> dan |1>. Kalau dalam ilmu komputer pasangan bilangan 0 dan 1 itu disebut bit, dalam mekanika kuantum akan disebut *qubit*, singkatan dari '*quantum bit'*.

Wujud fisik yang diperkirakan mirip dengan itu adalah *spin elektron* atau *nukleon*, yang hanya memiliki dua status kuantum. Mekanika kuantum untuk *spin elektron* atau *nukleon* pembahasannya lebih sulit karena harus menggunakan cara yang sesuai dengan cirinya, yaitu *spinor*.

Pilihan lain yang matematikanya lebih sederhana adalah status polarisasi dari foton. Seperti kita kenal gelombang elektromagnetik (foton), pada bidang yang tegaklurus arah penjalarannya boleh mempunyai status polarisasi dalam ruang dimensi dua. Sebagai vektor basisnya bisa dipilih status polarisasi datar (horisontal), dan status polarisasi tegak (vertikal).

Tentunya itu dapat kita nyatakan sebagai status |0> dan status |1>.

Status pada umumnya |φ> selalu dapat kita nyatakan sebagai kombinasi linier dari |0> dan |1>. Jadi sebuah foton umumnya dalam kondisi

$$| \varphi > = a | 0 > + b | 1 >$$

dengan a, b adalah konstanta.

Pada keadaan seperti itu, jika kita melakukan pengukuran polarisasinya, yang akan kita peroleh adalah : datar dengan peluang $|a|^2$ atau tegak dengan peluang $|b|^2$. Aturan mekanika kuantum juga menyatakan bahwa jika hasil pengukuran adalah datar maka foton tadi berubah status dari |φ> menjadi |0>. Begitu pula halnya, jika pengukurannya menghasilkan nilai tegak, maka foton akan berubah dari status |φ> menjadi |1>. Untuk maksud pembahasan selanjutnya, kita akan memilih dua vektor khusus, yaitu

$$| + \rangle = (1/\sqrt{2})(| 0 \rangle + | 1 \rangle) \text{ dan}$$
$$| - \rangle = (1/\sqrt{2})(| 0 \rangle - | 1 \rangle)$$

Keduanya, jika diukur memberi peluang (1/2) untuk menghasilkan |0> dan peluang (1/2) untuk menghasilkan |1>.

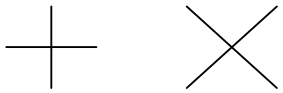
Vektor basis BS1 = {|0>,|1>} tentunya bukan satu satunya basis yang boleh digunakan. Kita boleh memilih basis lain misalnya BS2 = {|0'>, |1'>} yang dapat disusun dari {|0>,|1>} melalui sebuah transformasi 'Unitary'. Basis BS2 tetap ortonormal seperti halnya dengan basis BS1, dan dapat digunakan sebagai acuan pengukuran. Akan kita pilih basis BS2 = {| + >, | - >}.

Dalam bentuk diagram, kalau kita artikan |0> sebagai polarisasi horisontal dan |1> sebagai polarisasi vertikal, kita dapat melukiskannya sebagai berikut :

| 0 > | 1 > | + > | - >

Jika pengukuran kita lakukan dengan basis BS2, maka ungkapan |+> menjadi status polarisasi horisontal, jadi ungkapannya menjadi |0>. Begitu pula dengan |-> dalam pengukuran acuan BS2 nilainya menjadi |1>.

Untuk memudahkan ilustrasi berikutnya, kita akan menggunakan diagram acuan BS1 dan BS2 dalam bentuk berikut ini :



BS1 BS2

3. HASIL DAN PEMBAHASAN

Kriptografi Kuantum Sederhana

Misalkan si Ana dan si Joe (yang tidak berada di tempat yang sama) ingin berkomunikasi dengan cara yang tidak boleh diketahui oleh orang lain. Keduanya memiliki alat pengacak canggih yang sama. Pada suatu saat si Ana ingin mengirimkan informasi rahasia itu kepada Joe. Persolannya, bagaimana cara mengirim "kunci" sandinya agar hanya Joe yang mengetahuinya. Berikut adalah gagasan Bennett dan Brassard di tahun 1984.

Langkah 1 : si Ana mengirimkan sejumlah foton satu persatu dengan status polarisasi acak antara |0>, |1>, |+>, dan |-> kepada si Joe.

Langkah 2 : si Joe mengatur pengamatan terhadap foton-foton kiriman si Ana, dengan menggunakan detektor lewat basis BS1 dan BS2 secara acak juga. Tentunya sebanyak foton yang dikirimkan oleh si Ana.

Langkah 3: Hasil pengukuran si Joe dicatat tetapi dirahasiakannya. Sedangkan urutan pilihan acak cara pengukuran, BS1 dan BS2 dikomunikasikan kepada si Ana (boleh lewat telepon kalau mau).

Langkah 4: si Ana yang memiliki data tentang kiriman status-status polarisasi foton yang tadi di lepaskan, memberitahukan kepada si Joe, mana diantara deretan pengukuran yang 'benar' . Maksud kata 'benar' adalah : jika yang dikirim itu |0> atau |1> maka pengukuran dilakukan lewat BS1; kalau yang dikirim itu |+> atau |-> pengukuran dilakukan lewat BS2.

Langkah 5 : si Joe yang menyimpan hasil pengukurannya itu kemudian membuang data-data pengukuran yang menurut informasi dari si Ana dinyatakan salah. Nilai biner sisanya (yang benar) 01100101… itulah yang menjadi kesepakatan "kunci" sandi antara Ana dengan Joe.

Dalam bentuk diagram (hanya enam foton berturut-turut yang diungkapkan dalam gambar) skema komunikasi itu dilukiskan sebagai berikut:

Diagram Model Sederhana Kriptografi Kuantum (BB84)

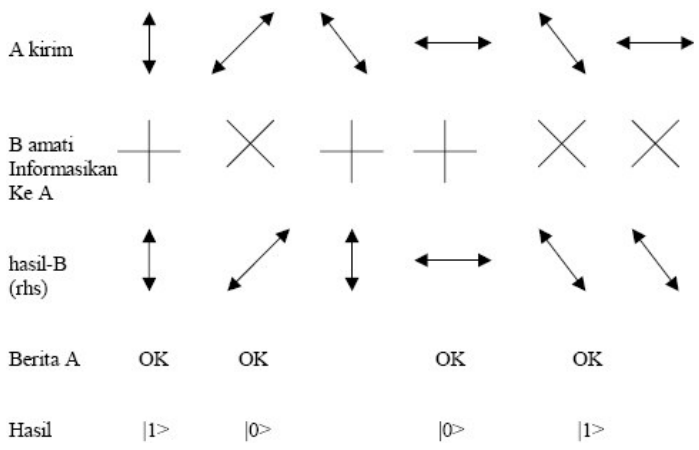


diagram 1

Hasil ini dengan sendirinya diketahui oleh Ana dan diketahui oleh Joe. Ana membuat kiriman informasi dengan menggunakan sandi ini yang diperintahkan kepada Alat Pengacak yang dimilikinya. Joe membaca dengan menggunakan sandi yang sama pada Alat Pengacak yang dimilikinya. Mestinya isinya jelas.

Bagaimana jika seandainya ada orang lain yang menyadap informasi tadi. Artinya, kiriman foton-foton oleh Ana ditangkap orang lain, namakanlah si Erwin. Tentunya si Erwin tidak dapat menyampaikan informasi kepada Ana tentang urutan cara mengamatinya, sebab sebagai penyadap Erwin tak ingin diketahui kegiatannya.

Agar sadapannya tidak disadari oleh yang berhak, tentunya dia harus tetap mengirimkan foton-foton untuk ditangkap oleh si Joe. Tetapi yang seperti apa status polarisasinya? Kemungkinannya dia dapat mengirimkan foton-foton dalam status seperti yang ditangkapnya.

Pada diagram berikut dibawah ini Anda dapat menyimak apa yang terjadi seandainya si Erwin melakukan hal seperti itu.

Kalau ada si Erwin yang menyadap:

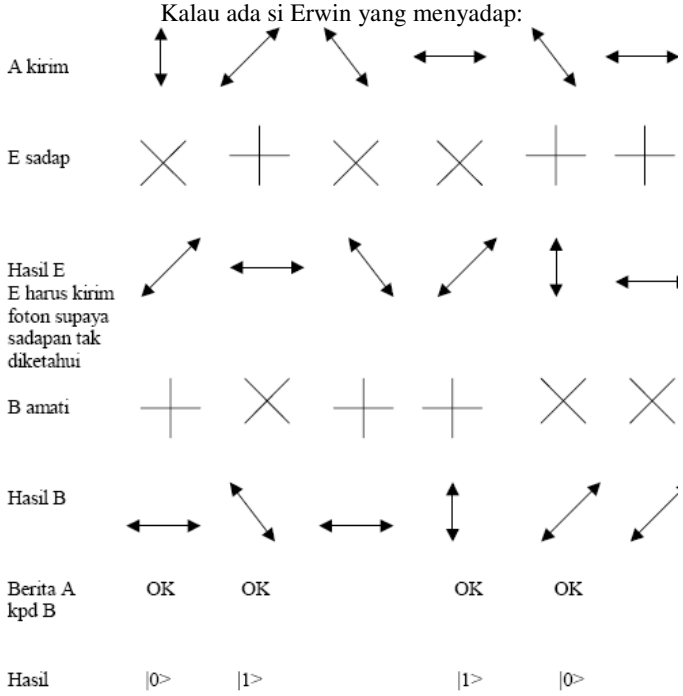


Diagram 2

Ketika dipakai untuk kunci sandi : jelas hasilnya salah (isinya kacau).

Kalau si Erwin kemudian 'membaca' ungkapan si Joe dan menerapkan pada hasilnya sendiri, akan mendapatkan |0>, |0>, |0>, |1> . Jadi juga tidak sesuai dengan kunci sandi yang dipakai oleh si Ana untuk memerintah Alat Pengacak.

Tentu saja jumlah foton yang dikirimkan jumlahnya cukup besar, bukan hanya 6 seperti yang dilukiskan oleh skema ini.

4. KESIMPULAN

Jika saja pengamanan kriptografi itu ternyata sangat sederhana seperti contoh ini, mengapa tidak dilakukan sekarang juga? Bukankah kita punya sinar laser sebagai sumber foton, serat optik sebagai penyalur, serta polarisator sebagai penangkapnya ?

Kita harus ingat bahwa aturan Mekanika Kuantum seperti itu hanya berlaku buat foton tunggal. Berkas sinar laser yang kita pakai itu adalah kumpulan (sering disebut '*ensemble'*) foton. Sifat *ensemble* foton tidak sama dengan perangai foton tunggal. *Ensemble* foton ada dalam keadaan yang dalam mekanika kuantum disebut *mixed state*, sedangkan sebuah foton tunggal ada dalam keadaan yang disebut *pure state.* Hanya *pure state* boleh memiliki status seperti $|\varphi\rangle = a.|0\rangle + b.|1\rangle$ ini. *Mixed state* dalam mekanika kuantum diungkapkan dengan bentuk "*density matrix*".

Jadi, salah satu tantangan untuk mewujudkan kriptografi kuantum ini adalah membuat generator yang memunculkan foton satu demi satu.

DAFTAR REFERENSI

[1] Anton, Howard. (1991). *Aljabar Linear Elementer, Edisi Keempat.* Jakarta: Erlangga.

[2] Munir, Rinaldi. (2003). *Diktat Kuliah IF2153 Matematika Diskrit, Edisi Keempat.* Bandung: Penerbit Informatika.

[3] Quantum Mechanics - Wikipedia, the free encyclopedia, http://en.wikipedia.org/wiki/ Quantum_mechanics. *Diakses pada 30 Desember 2007*

[4] Quantum Cryptography – Quantum Information Technology Group, http://www.quantumlah.org/ tutorial/quantumcrypto. *Diakses pada 30 Desember 2007*

[5] INTEGRAL, Vol. 6 No. 1, April 2001, *Memanfaatkan Mekanika Kuantum Untuk Kriptografi*. oleh Benny S.S.