Imitasi Quantum Key Distribution Menggunakan Komputasi Klasik beserta Aplikasinya dalam Steganografi

R. Purwoko Cahyo Nugroho – 13510014[1]
Program Studi Teknik Informatika
Sekolah Teknik Elektro dan Informatika
Institut Teknologi Bandung, Jl. Ganesha 10 Bandung 40132, Indonesia
[1]13510014@std.stei.itb.ac.id

***Abstract*—Makalah ini membahas Quantum Key Distribution, sebuah mekanisme transmisi kunci untuk pengamanan pesan selanjutnya, beserta usaha untuk melakukan implementasi distribusi kunci tersebut ke dalam komputer konvensional berbasis bit biner. Selain itu, distribusi kunci yang sudah dibuat dalam basis biner akan dilakukan steganografi sebagai media pengirimannya. Ini dilakukan untuk meningkatkan keamanan transmisi.**

***Index Terms*—quantum key distribution, photon polarization, digital steganography.**

I. PENDAHULUAN

A. Latar Belakang

Semenjak fisika Newtonian dipatahkan oleh fisika kuantum, orang-orang mulai melakukan eksplorasi prinsip kuantum dalam berbagai bidang ilmu, termasuk informatika. Bahkan eksplorasi ini sudah sampai ke titik penyusunan komputer kuantum secara hipotesis, mengindikasikan adanya revolusi komputer beberapa tahun ke depan. Di samping itu, pertukaran data dan informasi akan makin cepat dengan adanya metode lebih canggih untuk pengiriman foton (berkas-berkas cahaya).

Sejak komersialisasi komputer dan jaringan internet, dunia ini makin terasa sempit karena mudahnya berhubungan dengan orang lain pada jarak yang jauh sekalipun. Tiga orang di tiga benua yang berbeda kini bisa bercakap-cakap secara langsung dengan penundaan penyampaian informasi yang tidak signifikan. Sejalan dengan kemampuan yang makin tinggi, aliran data dan informasi juga luar biasa meningkat. Dan seperti halnya di dunia nyata, ada saja orang-orang yang serba ingin tahu urusan orang lain, baik itu karena hobi maupun kepentingan tertentu. Dengan demikian, aspek keamanan dari informasi yang ditransmisikan harus terjaga untuk meningkatkan kepercayaan pada penggunaan media ini.

Metode pengamanan pesan bisa bermacam-macam caranya, ada steganografi, penyembunyian pesan sehingga tidak dapat dideteksi, ada pula kriptografi, pengacauan pesan sehingga tidak dapat dibaca oleh orang yang tidak memiliki pengetahuan mengenai cara membacanya. Kedua metode ini merupakan inti dari usaha pengamanan data dan informasi di dunia digital dari orang-orang yang ingin tahu. Makalah ini akan membahas kombinasi dari kedua metode tersebut beserta usaha untuk menggabungkannya dengan teknologi berbasis kuantum yang belum sepenuhnya dapat diimplementasikan (masih berupa ide) dalam rangka mencapai derajat keamanan yang tinggi.

B. Sistematika Makalah

Bagian pertama makalah ini akan membahas prinsip kriptografi, prinsip komputasi kuantum dan steganografi. Kemudian dilanjutkan dengan metode Quantum Key Distribution beserta usaha aplikasinya pada komputer konvensional, juga akan dieksplorasi penggunaan QKD yang dikombinasikan dengan metode steganografi.

II. DASAR TEORI

Ada tiga hal yang secara utama dibahas sebagai teori, yaitu prinsip kriptografi, komputasi kuantum, dan steganografi.

A. Kriptografi

Kriptografi secara etimologis berasal dari bahasa Yunani; kriptos berarti tersembunyi, rahasia, dan graphein berarti tulisan. Secara terminologis, kriptografi adalah teknik mengacaukan pesan dan membuatnya tidak bisa dipahami oleh pihak ketiga.

Kriptografi memiliki empat tujuan:

- rahasia: hanya orang dimaksud yang boleh membaca pesan
- integritas: hanya orang dimaksud yang boleh mengubah isi pesan
- otentikasi: benar-benar orang dimaksud yang mengirimkan / menerima pesan
- nirpenyangkalan: pesan yang diterima / dikirim benar-benar dari / untuk orang yang dimaksud

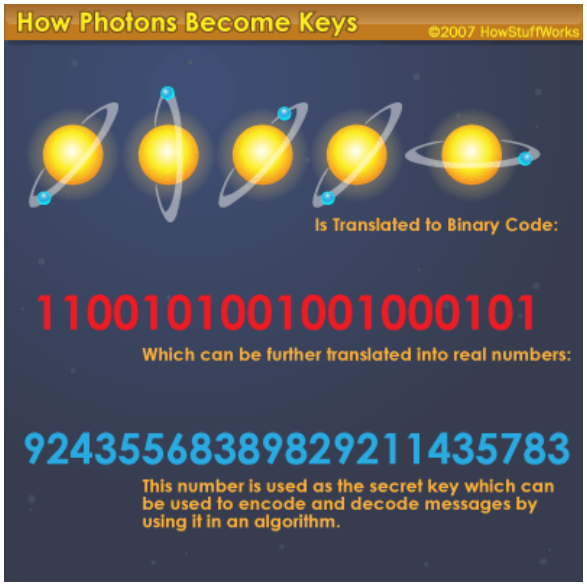
Metode kriptografi ada dua berdasarkan publisitas kunci, kunci publik dan kunci privat. Kriptografi kunci publik berarti sebagian kunci aman untuk dipublikasikan dan menjadi cara untuk membuat pesan teracak, sedangkan kriptografi kunci privat berarti seluruh bagian kunci harus tersembunyi dari jangkauan pihak luar karena cara untuk mengacak dan mengembalikan pesan hanya melalui kunci tersebut.

Kedua jenis kriptografi berdasarkan publisitas kunci tersebut memiliki satu kesamaan: berkunci. Dan karena kunci sukar untuk dipertukarkan dengan aman, hal itu membuat kriptografi secara keseluruhan tidak aman. Satu-satunya algoritma kriptografi yang aman adalah one-time-pad, algoritma kriptografi yang bisa menggunakan algoritma apapun (secara klasik hanya digunakan algoritma translasi biasa). One-time-pad bisa menggunakan algoritma apapun karena fokus keamanannya bukan pada algoritma, melainkan pada kunci yang digunakan. Secara klasik, pengguna one-time-pad menggunakan sebuah buku kunci yang setiap kuncinya hanya digunakan sekali, memiliki panjang berapapun, dan tidak berulang. Inti dari penggunaan one-time-pad adalah kerancuan. Para kriptanalis akan berusaha memecahkan cipher yang ditransmisikan, namun karena setiap transmisi menggunakan kunci yang selalu berbeda, maka cipher yang lewat hanya akan tampak seperti karakter random yang tidak bermakna. Kriptanalis tahu bahwa ini adalah sebuah teks cipher, tetapi mereka tidak akan berhasil memecahkannya karena kunci yang digunakan bisa berupa string apapun.

B. Quantum Cryptography (Quantum Key Distribution)

Kriptografi kuantum bermula dari perkembangan fisika kuantum, dan secara umum menggunakan sifat-sifat mekanika kuantum (seperti spin elektron) untuk mengamankan informasi yang ada, alih-alih menggunakan berbagai persamaan matematika (yang membuat keamanan data dari kerumitan persamaan sehingga sukar untuk menurunkan nilai sebenarnya dari ciphertext). Dalam makalah ini, digunakan aplikasi kriptografi kuantum, distribusi kunci kuantum (Quantum Key Distribution), varian BB84.

Distribusi kunci secara kuantum merupakan salah satu mekanisme yang memanfaatkan prinsip kemampuan kuantum, "Aku diamati, maka aku ada". Prinsip ini melibatkan pengiriman photon yang telah dilakukan polarisasi, sebagaimana foton tidak akan bisa diketahui status polarisasinya melainkan jika diamati, dan jika diamati dengan cara yang salah, maka foton yang hendak diamati itu juga akan berubah sesuai cara mengamatinya. Kondisi sifat kuantum ini amat menyulitkan bagi para pencuri-dengar (eavesdropper) karena jika mereka berusaha mencuri data menggunakan basis yang berbeda dari yang digunakan dalam pengiriman, bukan saja mereka tidak berhasil mendapatkan data yang diinginkan, melainkan juga para komunikan akan menyadari keberadaannya sehingga mungkin akan menutup diri atau setidaknya menjadi lebih waspada akan pesan yang mereka komunikasikan.



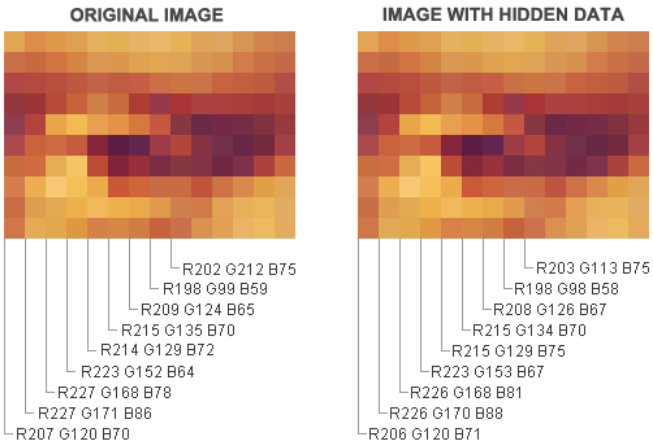
Gambar 1 Spin foton[2]

C. Steganografi

Secara etimologis, steganografi berasal dari *steganos* "tersembunyi" dan *graphein* "citra / tulisan". Steganografi adalah seni dan ilmu untuk menyembunyikan pesan sedemikian hingga tidak ada seorangpun akan mampu mempersepsikan keberadaan pesan. Tidak seperti kriptografi yang terang-terangan mengacaukan isi pesan, membuat semua orang yang membaca langsung tahu bahwa ada pesan yang dikodekan di dalamnya, steganografi berkutat pada usaha menghilangkan jejak bahwa pesan itu pernah ada.

Berdasarkan medianya, steganografi terdiri atas steganografi fisik dan digital. Steganografi fisik mengandalkan media yang bisa diindera manusia, biasanya dibuat pada masa kuno. Jenis ini di antaranya tato pada kepala budak, cetak tebal-tipis tulisan, penyisipan gambar tertentu di dalam gambar yang lain, pesan yang dituliskan di kayu kemudian melapisi kayu tersebut dengan lilin dan dikirimkan sebagai furnitur biasa, dan lain-lain. Sedangkan steganografi digital melibatkan komputasi komputer, terutama manipulasi bit-bit data untuk menyembunyikan sebuah informasi di dalam data yang lain. Contoh paling umum adalah penyembunyian gambar di dalam gambar yang lain. Berbeda dengan steganografi fisik yang semua jenis data sebaiknya bisa diinderakan, steganografi digital tidak memedulikan jenis data, semua data bisa ia serap dan sembunyikan dengan cara yang sama karena semua data yang ada selalu dikodekan menggunakan representasi bit

biner.

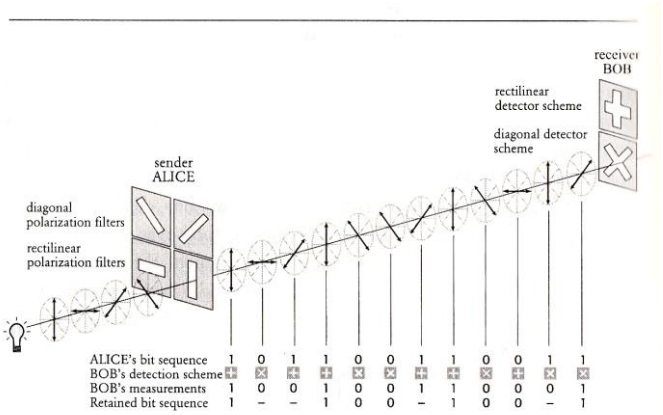


Gambar 2 Steganografi
[http://www.steganographypro.com/img/stega-per-pics.png]

Steganografi digital pun terdiri atas bermacam-macam jenis, sesuai jenis data yang membawanya. Yang paling umum digunakan adalah audio dan visual karena itu juga merupakan media yang paling sering dipertukarkan sehingga akan mengurangi kecurigaan ketika mempertukarkan berkas suara, gambar, maupun video.

III. IMITASI QUANTUM KEY DISTRIBUTION PADA KOMPUTER KONVENSIONAL

QKD-BB84 protocol pertama kali diusulkan oleh Charles Bennett and Gilles Brassard pada 1984. Idenya adalah pembangkitan dan pengiriman foton terpolarisasi. Setiap foton memiliki pilihan basis (0° dan 90°) dan penyimpangan (rectilinear = 0°, diagonal = +45°) sehingga total ada 4 polarisasi yang diizinkan (Tabel 1). Jika ada sebuah foton terpolarisasi 0° dan dibaca menggunakan filter 135°, maka pembacaan akan gagal dan foton sekarang terpolarisasi pada 135°. Polarisasi foton tidak bisa diamati tanpa mengubahnya menjadi kepolaran filter pengamat. Pengirim (Alice) akan membangkitkan basis dan penyimpangan secara random dan terpisah, mempolarisasi foton sesuai basis + penyimpangan, kemudian mengirimkan foton tersebut melalui jalur komunikasi umum. Bob, yang menerima foton-foton tersebut, kemudian membangkitkan filter-filter random untuk membaca foton yang ia terima. Setelah semua foton diterima, Bob memberitahu Alice indeks-indeks foton yang berhasil ia tangkap, kemudian Alice mengirimkan sebuah ciphertext "challenge" untuk didekripsi oleh Bob. Bob menjawab dengan plaintext, kemudian Alice menentukan berapa foton yang benar-benar didekripsi oleh Bob. Setelahnya, mereka menyepakati bagian kunci mana saja yang akan digunakan menjadi kunci pertukaran pesan sesi tersebut dan bisa langsung berkirim pesan dengan kunci yang telah disepakati tadi. Apa yang membuat mekanisme ini menjadi spesial adalah kemampuannya untuk membuat setiap sesi pengiriman pesan menjadi seolah-olah dienkripsi menggunakan one-time pad, membuat setiap sesi menjadi hampir tidak mungkin dipecahkan dengan kriptanalisis.



Gambar 3 Ilustrasi pengiriman foton
[http://1.bp.blogspot.com/-CItzMpljuqk/TWGU7ADNb1I/AAAAAAAABCQ/4JGzxpEhbV4/s1600/quantum_crypto.jpg]

Mekanisme pertukaran kunci ini lebih canggih dalam menangani pencuri-dengar, karena setiap usaha mencuri-dengar yang gagal akan direkam oleh foton tersebut dan kemudian secara tidak langsung dilaporkan kepada penerima foton, yang otomatis akan membandingkan nilai kunci yang dimiliki penerima terhadap pengirim (Alice). Challenge yang dijawab Bob akan rusak sehingga Alice dapat mendeteksi keberadaan pencuri-dengar.

Tabel 1 Ilustrasi Polarisasi Foton

Basis	0	1
+	↑	→
X	↗	↘

Pembahasan mengenai imitasi QKD dalam komputer klasik akan dibagi ke dalam dua bagian: tantangan dan perancangan.

A. Tantangan

Pada prinsipnya, quantum key distribution tidak mungkin diimplementasikan pada komputer

konvensional karena tidak adanya sifat-sifat kuantum pada komputer konvensional: ketidakmampuan komputer konvensional menangani qubits, bit kuantum (Φ^+, Φ^-, Ψ^+, Ψ^-) yang berbeda dari bit pada komputasi konvensional (0 dan 1). Oleh karena itu, perlu dilakukan penyesuaian agar quantum key distribution nantinya akan bisa diimplementasikan di atas komputer konvensional.

Kedua, jaringan komputer komersial masa kini belum bisa mengakomodasi pengiriman foton terpolarisasi tertentu tanpa harus mengekspos frekuensi dan polarisasi berkas cahaya tersebut secara eksplisit. Harus diadakan metode lain yang bisa membuat polarisasi tersembunyi sehingga usaha menyembunyikan pesan (kunci yang didistribusikan) tidak menjadi kepalsuan.

Ketiga, karena kunci yang didistribusikan juga harus aman, metode pengamanan pesan tertentu juga harus diimplementasikan sebagai sebuah kesatuan dengan metode pengiriman kunci ini. Metode pengamanan pesan harus lebih kuat atau lebih tersamar sehingga penyadap akan lebih kesulitan dalam mencoba memecahkan pengaman pesan.

B. Perancangan

Setelah masalah-masalah yang membuat QKD tidak bisa diimplementasikan di komputer konvensional berhasil dipahami, diusulkan sebuah rancangan implementasi yang membuat imitasi kemampuan-kemampuan QKD akan bisa digunakan juga oleh komputer konvensional. Namun solusi tersebut harus tetap menjaga keamanan sebagaimana QKD yang sebenarnya.

Solusi ini berpusat pada konversi polarisasi foton menjadi bilangan bit biasa, dengan penyesuaian supaya satu domain qubit bisa muat dalam representasi bit.

Pertama, translasi basis. Kedua basis (0 dan 1) bisa dimasukkan ke dalam basis biner. Selanjutnya, translasi penyimpangan. Basis rectilinear(+) dan diagonal(X) diubah menjadi penjumlahan dan perkalian yang sesungguhnya dalam biner, menjadi +1 (mod 2) dan X1 (mod 2). Sehingga hasil imitasinya adalah sebagaimana tabel 2.

Tabel 2 Hasil Translasi ke Biner

Pada komputer kuantum:

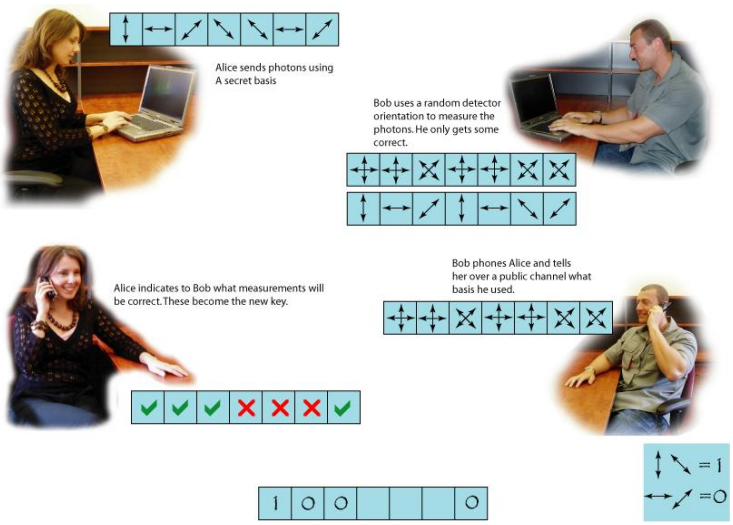
Basis	0	1
+	↑	→
X	↗	↘

Pada komputer klasik:

Basis	0	1
+ 1 (mod 2)	1	0
X 1 (mod 2)	0	1

Tampak pada tabel 2 di atas bahwa nilai akhir ‘foton’ berupa nilai awal yang ditambah atau dikali satu. Kemudian hasil inilah yang ditransmisikan melalui jaringan transmisi konvensional. Imitasi ini diharapkan bisa menyamai keamanan QKD yang sebenarnya.

Secara mudah, jika hasil pengacakan mendapat nilai 0 untuk rectilinear, dan 1 untuk diagonal, maka bit ‘foton’ yang digunakan untuk pembentukan kunci merupakan hasil XNOR basis dan penyimpangan.



Gambar 4 Ilustrasi protokol Quantum Key Distribution BB84

[http://qcvictoria.com/var/qcv/storage/images/media/images/technology/qkd/778-1-eng-AU/qkd.jpg]

IV. STEGANOGRAFI SEBAGAI PENGUAT KEAMANAN TRANSMISI KUNCI

Seperti telah diungkapkan di atas, steganografi adalah ilmu dan seni untuk menyembunyikan informasi sehingga keberadaan informasi tersebut tidak disadari oleh pihak selain yang dimaksud. Steganografi yang akan diimplementasikan dalam makalah ini adalah jenis steganografi digital dengan prinsip visual. Ini juga bisa dikembangkan ke arah audio atau audio-visual jika kebutuhan pesan yang ditransmisikan cukup besar.

Steganografi digital-visual adalah aplikasi steganografi yang memanfaatkan sifat visual sebuah media, biasanya sifat warna yang jika berubah hanya sedikit, tidak akan mampu dipersepsikan oleh mata telanjang manusia. Aplikasi bidang steganografi ini mencakup penyisipan bit-bit pesan ke dalam komponen warna (merah, hijau, biru atau biru muda, magenta, kuning, hitam) di bagian terkecilnya (least significant bit [LSB]) sehingga bit yang dimaksud akan membawa pesan yang diinginkan dengan sedikit mengubah komponen warnanya, namun hanya sedikit sehingga perubahan tersebut tidak mungkin dipersepsikan oleh mata telanjang manusia (Gambar 2). Sebagai contoh

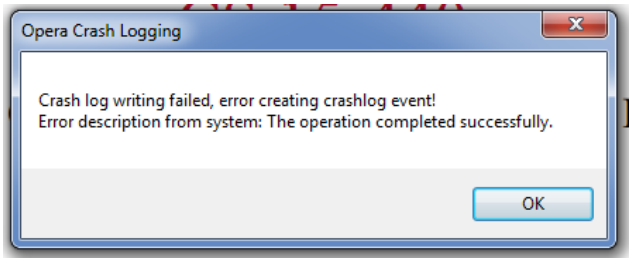
berkas bitmap 24 bit mengandung tiga komponen warna, merah-hijau-biru dan setiap komponen warna direpresentasikan dengan satu byte akan mampu menampung tiga kali lipat LSB, dan jika dalam satu byte akan disisipkan sepasang nilai bit (sepasang LSB tidak akan mengubah warna terlalu jauh hingga mampu dipersepsikan mata telanjang), maka dalam setiap pixel mampu menampung 6 bit informasi.

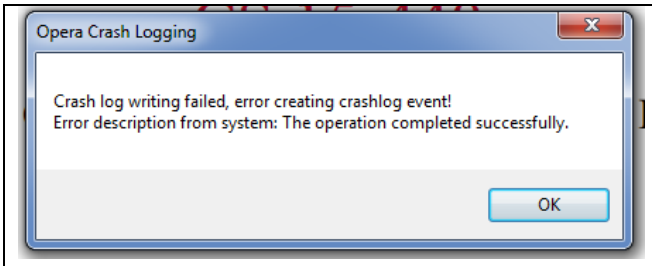
Steganografi yang digunakan di sini adalah tipe visual-digital, dilakukan dengan mengubah 2 bit terkecil dari tiap komponen warna (RGB) pada posisi tertentu dari sebuah gambar bitmap (llihat gambar 2). Metode ini akan mengubah sedikit warna tanpa terlihat dari mata telanjang manusia.

Pesan yang akan disisipkan di sini adalah pesan yang berisi kunci kuantum yang hendak ditransmisikan. Pesan tersebut disisipkan secara acak untuk menghindari adanya percobaan pencurian data. Nilai pengumpan dari pengacakan posisi pesan dalam covert message ini bebas ditransmisikan melalui jalur komunikasi umum yang tidak aman hanya jika tidak ada orang lain yang mengetahui bahwa gambar tersebut merupakan covert message yang mengamankan distribusi kunci kuantum. Selanjutnya, Bob menerima kunci stegano dan gambar covert dari Alice dan melakukan ekstraksi kunci yang tersembunyi dalam gambar.

Berikut adalah contoh penggunaan steganografi dalam penyisipan pesan dalam gambar.

Tabel 3 Contoh aplikasi steganografi [http://www.mobilefish.com/services/steganography/steganography.php]

Kunci: “bukusekolah” Pesan:”1100101010010100101010010101001011011101011001010”
 *Gambar 5 Gambar asli sebelum disisipi pesan*



Gambar 6 Gambar setelah disisipi pesan

V. SIMPULAN

Quantum Key Distribution adalah sebuah cara untuk bertukar pesan kunci secara aman sehingga prinsip unbreakable cipher akan dapat dicapai karena penggunaan Quantum Key Distribution pada akhirnya menyerupai algoritma kriptografi one-time-pad, yaitu algoritma kriptografi yang mempertahankan kekuatannya benar-benar kepada kunci. Algoritma kriptografi one-time-pad tidak membutuhkan algoritma yang rumit, karena penggunaan kunci pada one-time-pad yang tidak berulang membuat ciphertext yang dihasilkan sama sekali acak dan tidak bisa ditebak atau dilakukan kriptanalisis. Namun ada satu masalah saat ini, karena belum komersialnya komputer kuantum, QKD belum bisa dikembangkan secara luas.

Makalah ini menjelaskan imitasi quantum key distribution menggunakan komputasi klasik, sehingga diharapkan pengembangan algoritma kriptografi kuantum dapat juga berkembang di atas komputer konvensional dengan perubahan-perubahan seperlunya sehingga komputer konvensional dapat melakukan komputasi atas algoritma distribusi kunci yang dimaksud.

Pengubahan quantum key distribution BB84 protocol yang dilakukan menyebabkan hilangnya polarisasi foton dan digantikan oleh bit biner yang berkorespondensi dengan basis bilangan dan basis penyimpangan.

Di samping melakukan imitasi pada komputer konvensional, hasil kunci yang siap ditransmisikan juga disisipkan ke dalam covert message sehingga kemungkinan pencuri-dengar untuk mengetahui maksud pesan semakin rendah.

REFERENCES

[1] http://www.networkworld.com/weblogs/security/004842.html
[2] http://science.howstuffworks.com/science-vs-myth/everyday-myths/quantum-cryptology.htm
[3] http://www.csa.com/discoveryguides/crypt/overview.php
[4] http://www.cki.au.dk/experiment/qrypto/doc/QuCrypt/bb84coding.html
[5] http://www.quantiki.org/wiki/BB84_and_Ekert91_protocols
P. W. Shor and J. Preskill, “Simple Proof of Security of the BB84 Quantum Key Distribution Protocol”, arXiv:quant-ph/0003004v2.

PERNYATAAN

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

Bandung, 19 Mei 2013

R. Purwoko Cahyo Nugroho – 13510014