Penerapan Kriptografi Kuantum untuk Kriptanalisis

Pradipta Yuwono – NIM : 13506103
Program Studi Teknik Informatika, Institut Teknologi Bandung
Jl. Ganesha 10, Bandung
E-mail : if16103@students.if.itb.ac.id

Abstract *– Sebuah algoritma kriptografi yang ideal adalah algoritma yang tidak dapat dipecahkan oleh orang lain selama orang tersebut tidak mempunyai kunci untuk mendekripsinya (unbreakable cipher). Sampai saat ini satu-satunya unbreakable cipher yang diketahui hanyalah one time pad, namun algoritma ini tidak begitu populer karena kurang efisien.*
Beberapa dekade lalu, beberapa matematikawan memperkenalkan algoritma kriptografi baru berupa fungsi satu arah yang disebut kriptografi kunci publik yang sangat aman dan efisien. Salah satu algoritma kriptografi kunci publik yang tergolong aman adalah algoritma RSA. Pada saat itu matematikawan memperkirakan akan membutuhkan waktu beberapa ribu tahun untuk memecahkan algorima RSA ini menggunakan teknik brute force.
Seiring dengan perkembangan kemajuan teknologi informasi, kriptanalis menunjukkan bahwa dengan kemampuan komputer modern saat ini kita mampu memecahkan algoritma kunci publik tersebut hanya dalam tempo beberapa bulan saja. Pada masa yang akan datang, kecepatan proses kriptanalisis dapat meningkat jauh lebih cepat berkat perkembangan komputasi kuantum. Komputasi kuantum dapat diaplikasikan pada proses kriptanalisis yang dinamakan sebagai kriptanalisis kuantum. Dengan kriptanalisis kuantum, algoritma yang sebelumnya sangat sulit dipecahkan seperti RSA dapat dipecahkan dalam waktu yang jauh lebih singkat.
Pada makalah ini penulis mencoba membuat rumus matematis bagaimana langkah-langkah penerapan kriptografi kuantum untuk menyelesaikan permasalahan kriptanalisis yang rumit, seperti pada algoritma RSA.

Kata Kunci*: kriptografi kuantum, komputasi kuantum, kriptoanalisis, mekanika kuantum*

1. Pendahuluan

Kriptografi adalah seni dan ilmu untuk menjaga kerahasian sebuah pesan dengan cara menyandikannya ke dalam bentuk yang tidak dapat dimengerti maknanya. Tujuan kriptografi adalah untuk mengirimkan sebuah informasi sehingga hanya penerima yang dituju saja yang dapat membaca informasi tersebut.

Kriptografi sudah dikenal sejak zaman romawi kuno. Pada saat itu Julius Caesar menggunakan suatu teknik kriptografi untuk menyamarkan pesan rahasianya, sehingga pihak yang tidak berkepentingan tidak dapat memahami isi pesan yang sesungguhnya. Teknik yang digunakan saat itu adalah substitusi satu karakter pada teks asli dengan karakter lain yang dinamakan Caesar Cipher.

Seiring dengan berjalannya waktu, berkembanglah teknik-teknik kriptografi yang lebih efisien dan lebih aman. Selain ilmu kriptografi, ikut berkembang pula ilmu kriptanalisis 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.

Pesatnya perkembangan teknologi informasi menyebabkan ukuran transistor dalam sebuah prosesor semakin mengecil dan kecepatannya semakin meningkat. Beberapa tahun yang akan datang diramalkan transistor pada sebuah prosesor akan bekerja dalam skala atomik. Pada skala atomik, hukum fisika yang mendasari bekerjanya transistor tersebut akan jauh berbeda dibandingkan pada skala makroskopik. Pada skala atomik, prosesor bekerja berdasarkan prinsip mekanika kuantum, sehingga berkembanglah teknologi komputasi kuantum.

Komputer kuantum adalah perangkat komputasi yang memanfaatkan langsung fenomena mekanika kuantum, seperti quantum superposition dan quantum entanglement untuk menyelesaikan operasi pada data. Pada komputer konvensional, informasi disimpan dalam bit-bit, pada komputer kuantum, informasi disimpan pada qubit (quantum binary digit). Prinsip dasar dari komputasi kuantum adalah properti kuantum dapat digunakan untuk merepresentasikan dan mengkonstruksi data, dan mekanisme kuantum dapat digunakan untuk melakukan operasi pada data. Penggunaan kuantum komputer untuk kriptanalisis me-mungkinkan proses pemecahan kode kriptografi menjadi jauh lebih cepat dibandingkan dengan algoritma konvensional.

2. Kriptanalisis Klasik

Kriptanalisis adalah seni dan ilmu untuk memecahkan ciphertext atau kunci pada sebuah kriptosistem. Teknik kriptanalisis digunakan baik oleh ilmuwan untuk menguji kekuatan suatu kriptosistem maupun oleh *hacker* untuk memecahkan kriptosistem secara ilegal. Riset kriptanalisis selalu berdasarkan asumsi bahwa penyerang memiliki pengetahuan menyeluruh mengenai sistem kriptografi tersebut dan satu-satunya hal yang tidak ia ketahui hanyalah kuncinya (*key*). Asumsi ini berdasarkan prinsip Kerckhoff. Tujuan dari kriptanalisis adalah untuk menemukan plaintext yang sesuai dengan ciphertext tertentu yang telah diketahui, atau akan lebih baik lagi jika menemukan juga kunci yang digunakan dalam sistem kriptografi tersebut.

2.1. Skenario Serangan

Ada bermacam-macam tipe serangan terhadap kriptosistem yang dapat dikelompokkan berdasarkan tingkat pengetahuan yang tersedia bagi si penyerang. Skenario serangan yang paling umum digunakan dijelaskan dibawah ini.

2.1.1. Ciphertext Only Attack

Pada serangan ini, penyerang memiliki akses pada sejumlah ciphertext yang sudah dienkripsi dengan kunci yang sama namun belum diketahui isi kuncinya, plaintext yang bersesuaian juga belum diketahui oleh penyerang. Penyerang dapat mendeduksi ciphertext untuk mendapatkan plaintext atau key yang sesuai. Serangan ini dianggap berhasil jika plaintext atau key berhasil ditemukan. Kebanyakan cipher yang digunakan saat ini kebal terhadap serangan jenis ini. Cipher yang berhasil dibongkar dengan mudah menggunakan teknik ini umumnya langsung menjadi kadaluarsa.

2.1.2 Known Plaintext Attack

Pada serangan ini, penyerang mengetahui satu atau lebih ciphertext beserta plaintextnya yang sesuai, sahingga penyerang harus mencoba mencari tahu kuncinya dengan informasi yang tersedia tersebut. Serangan ini dianggap berhasil jika kunci berhasil ditemukan atau ciphertext lainnya dengan kunci yang sama dapat dikonversi menjadi plaintext.

2.1.3 Chosen Plaintext Attack

Ini adalah jenis serangan yang tidak realistis, dimana penyerang dapat men-submit plaintext pada beberapa mesin yang kemudian akan menghasilkan output berupa ciphertext hasil enkripsi dengan menggunakan kunci rahasia tertentu. Banyak cipher terbukti tidak kebal terhadap serangan jenis ini.

2.1.4 Side Channel Attacks

Serangan side-channel dapat muncul ketika penyerang mampu menggunakan beberapa tambahan informasi (selain dari informasi yang tersedia lewat prinsip Kerckhoff) yang bocor dari implementasi fungsi kriptografi, yang kemudian dapat dimanfaatkan untuk memecahkan kriptosistem tersebut.

2.2. Metode Kriptanalisis

Ada banyak metode kriptanalisis yang telah dipublikasikan beberapa tahun belakangan ini. Beberapa metode yang paling umum digunakan dijelaskan dibawah ini.

2.2.1 Kriptanalisis Diferensial

Kriptanalisis diferensial diperkenalkan oleh Biham dan Shamir pada CRYPTO'90. Ini adalah serangan bertipe Chosen Plaintext Attack, yang dapat dimodifikasi menjadi Known Plaintext Attack. Metode ini dapat diaplikasikan pada kriptosistem yang menggunakan teknik substitusi dan permutasi pada algoritmanya. Metode ini mempelajari bagaimana diferensiasi pada input dapat mempengaruhi hasil diferensiasi pada output.

2.2.2. Kriptanalisis Linear

Kriptanalisis linear diperkenalkan oleh Mitsuru Matsui pada EUROCRYPT'93. Metode ini tergolong sebagai plaintext attack, yang dapat juga diaplikasikan pada ciphertext only attack dalam beberapa situasi. Pendekatan ini berbeda dari kriptanalisis diferensial, namun berkaitan. Kriptanalisis linier terdiri dari dua bagian. Bagian pertama mengonstruksi persamaan linier yang menghubungkan plaintext, ciphertext, dan bit kunci yang memiliki bias yang tinggi. Bagian kedua adalah penggunaan persamaan linier ini bersama dengan pasangan plaintext-ciphertext yang diketahui untuk menurunkan bit kunci.

2.2.3 Simple Power Analysis

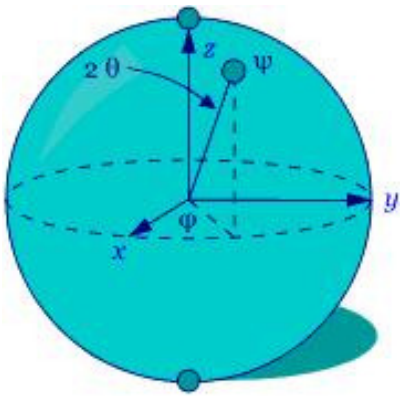
Simple power analysis adalah bentuk side-channel attack, yang memanfaatkan informasi konsumsi daya pada sistem yang mengim-plementasikan algoritma kriptografi tersebut. Teknik ini mengasumsilkan bahwa penyerang mampu melakukan pengukuran pada daya yang dikonsumsi oleh perangkat kriptograf tersebuti. Serangan yang lebih kuat seperti Differential Power Analysis (DPA) dan High-Order Differential Power Analysis (HO-DPA) telah diformulasikan menggunakan variasi dari metode ini

2.2.4 Acoustic Cryptanalysis

Kriptanalisis akustik tergolong dalam kriptanalisis jenis side-channel attack. Teknik ini menggunakan pancaran akustik dari komputer untuk membuat asumsi mengenai implementasi pada sebuah algoritma. Kriptanalisis akustik modern kebanyakan berfokus pada suara yang dihasilkan oleh keyboard komputer atau komponen internal komputer, tapi dalam sejarahnya teknik ini juga diaplikasikan pada gelombang suara pada printer dan mesin cipher elektromekanikal.

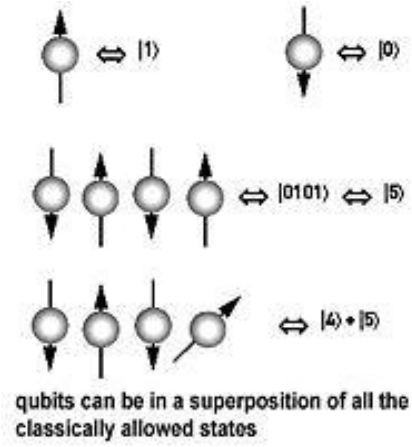
3. Komputasi Kuantum

Komputer kuantum adalah perangkat komputasi yang memanfaatkan fenomena mekanika kuantum seperti superposisi dan *quantum entanglement* untuk melakukan operasi pada data. Pada komputer konvensional, informasi disimpan sebagai bit, pada komputer kuantum informasi disimpan sebagai qubit (quantum bit). Sebuah komputer klasik memiliki memori yang tersusun atas beberapa bit, dimana tiap-tiap bit menyimpan salah satu nilai antara 1 atau 0. Komputer kuantum memiliki memori yang tersusun atas beberapa qubit. Sebuah qubit dapat menyimpan nilai 1, 0, atau superposisi dari keduanya, sehingga komputer jenis ini mengijinkan jumlah state yang tak terhingga. Komputer kuantum bekerja dengan memanipulasi qubit-qubit ini dengan seperangkat *quantum logic gate*. Prinsip dasar dari komputasi kuantum adalah pemanfaatan properti kuantum untuk merepresentasikan dan menyusun data-data, dan mekanisme kuantum untuk melakukan operasi pada data. Bloch sphere dibawah ini merepresentasikan qubit, blok pembangun dasar pada komputer kuantum:



3.1. Bits Vs. Qubits

Bayangkan sebuah komputer konvensional yang beroperasi pada register 3-bit. Pada satu waktu tertentu, bit-bit pada register harus berada pada salah satu state tertentu yang pasti, misalnya 101. Jumlah kemungkinan state pada register tersebut adalah $2^3 = 8$ yaitu 000, 001, 010, 011, 100, 101, 110, dan 111. Berbeda dengan komputer konvensional, komputer kuantum menggunakan qubit-qubit untuk menyimpan informasinya. Qubit-qubit pada komputer kuantum dapat berada dalam superposisi dari seluruh state yang diijinkan. State pada komputer kuantum dengan register 3-qubit dideskripsikan oleh vektor 8 dimensi (a, b, c, d, e, f, g, h) yang disebut *ket*. Total jumlah pangkat dua dari koefisien-koefisien tersebut , $|a|^2 + |b|^2 + ... + |h|^2$ haruslah sama dengan satu. Lebih jauh, nilai dari koefisien-koefisien tersebut adalah bilangan kompleks. Karena state direpresentasikan oleh fungsi gelombang kompleks, dua state yang ditambahkan bersama-sama dapat saling mengalami interferensi.



3.2 Aplikasi Komputasi Kuantum pada Kriptanalisis

Komputer kuantum memiliki potensi besar untuk dimanfaatkan pada proses kriptanalisis. Karena state kuantum dapat berada dalam superposisi, kemungkinan akan muncul paradigma baru pada komputer. Peter Shor dari Bell Labs telah membuktikan kemungkinan tersebut, dan berbagai tim ilmuwan telah mendemonstrasikan satu atau beberapa aspek mengenai rekayasa komputasi kuantum pada beberapa tahun belakangan ini. Sejauh ini, belum ada bukti yang memadai mengenai bagaimana cara mendesain komputer semacam ini. Namun seandainya komputer kuantum dapat diproduksi secara massal, banyak hal yang akan berubah. Komputasi paralel kemungkinan akan menjadi sebuah standar di masa depan. Beberapa aspek kriptografi juga akan berubah. Karena

komputer kuantum dapat mengerjakan pencarian kunci menggunakan teknik brute force dengan sangat cepat, panjang kunci yang saat ini dianggap sudah efektif karena berada di luar jangkauan serangan brute force komputer konvensional, beberapa tahun yang akan datang kemungkinan akan berhasil dipecahkan dengan teknik yang sama menggunakan komputer kuantum. Panjang kunci yang dibutuhkan untuk mengatasi serangan komputer kuantum akan jauh lebih panjang. Beberapa penulis bahkan memperkirakan bahwa tidak ada lagi teknik enkripsi yang aman setelah kemunculan komputer kuantum

Faktorisasi integer saat ini dipercaya tidak dapat dipecahkan dengan mudah oleh komputer konvensional untuk bilangan integer yang besar yang merupakan hasil produk dari beberapa bilangan prima. Komputer kuantum dapat secara efisien memecahkan persoalan ini menggunakan algoritma Shor untuk menemukan faktornya. Sehingga komputer kuantum di-khawatirkan dapat memecahkan banyak sistem keamanan yang umum digunakan saat ini untuk mengenkripsi data pada website, email, dll. Salah satu cara untuk meningkatkan keamanan pada algoritma seperti RSA adalah dengan cara meningkatkan panjang kuncinya dan berharap komputer kuantum tidak memiliki cukup sumber daya untuk memecahkannya. Kemampuan komputer kuantum lainnya yang tidak dimiliki komputer konvensional adalah *quantum database search*, yang dapat dikerjakan menggunakan algoritma Grover pada komputer kuantum.

Anggap ada sebuah permasalahan yang memiliki empat ciri-ciri sebagai berikut:

1. Satu-satunya cara untuk memecahkan permasalahan ini adalah dengan menebak jawabannya berulang-ulang dan kemudian mengeceknya.
2. Ada n kemungkinan jawaban untuk dicek.
3. Setiap kemungkinan jawaban membutuhkan total waktu yang sama untuk pengecekan
4. Tidak ada clue sedikitpun mengenai jawaban mana yang kemungkinan memiliki probabilitas lebih tinggi.

Contoh dari permasalahan ini adalah pada kasus menebak isi password pada file yang terenkripsi.

Untuk permasalahan dengan empat ciri-ciri diatas, waktu yang dibutuhkan komputer kuantum untuk memecahkan nya sama dengan akar pangkat dua dari n, sedangkan rata-rata waktu yang dibutuhkan oleh komputer konvensional adalah (n+1)/2. Ini adalah peningkatan kecepatan yang sangat signifikan, yang dapat mengurangi waktu penyelesaian dari beberapa tahun menjadi beberapa detik. Sehingga komputer kuantum ini kemungkinan dapat digunakan untuk menyerang cipher-cipher simetris seperti Triple DES dan AES dengan mencoba menebak-nebak kunci rahasianya

4. Langkah -Langkah Kriptanalisis Kuantum

Pada bagian ini penulis mencoba menjelaskan menurut perhitungan matematika yang penulis coba kembangkan sendiri mengenai bagaimana algoritma kriptografi kuantum bekerja untuk memecahkan persoalan kriptanalisis yang rumit seperti misalnya memecahkan cipher RSA atau algoritma cipher handal lainnya. Algoritma yang digunakan adalah algoritma Shor, yang digunakan pada komputer kuantum. Penulis memberikan contoh cara memecahkan cipher RSA, meskipun algoritma ini juga dapat digunakan untuk memecahkan cipher lainnya. Penulis tidak akan membahas banyak mengenai RSA karena berada di luar spesifikasi makalah.

RSA, teknik enkripsi kunci publik yang paling umum digunakan, bekerja berdasarkan fakta bahwa bilangan yang sangat besar sangat sulit untuk difaktorkan. Sebagai contoh, kunci enkripsi X adalah produk hasil perkalian dua angka prima Y dan Z (X=YZ), dan dengan memecahkan kunci tersebut diturunkan untuk mencari nilai Y dan Z, dengan nilai X sudah diketahui. Persoalan ini sulit dipecahkan dalam waktu singkat untuk nilai X yang sangat besar. Misalnya, jika X adalah 639551091939800586960985 62723, maka berapa nilai Y dan Z? Dengan komputer yang sangat cepat sekalipun, persoalan ini membutuhkan waktu lama untuk memecahkannya.

Salah satu metode untuk menyelesaikannya adalah menggunakan aritmatika modular. Pada matematika modular anda ambil sebuah bilangan, misal M, dan setiap kali anda berurusan dengan bilangan yang lebih besar dari M, anda kurangi sebesar M hingga anda menangani bilangan yang lebih kecil dari M. Jam adalah contoh umum untuk aritmatika "mod 12". Misalnya, pukul 31 sama dengan pukul 19 dan juga sama dengan pukul 7. Kita dapat menulisnya sebagai berikut:

$$[31]_{12} = [19]_{12} = [7]_{12}$$

Sekarang coba kita perhatikan persamaan berikut:

$$[2^0]_{15} = [1]_{15}$$
$$[2^1]_{15} = [2]_{15}$$
$$[2^2]_{15} = [4]_{15}$$
$$[2^3]_{15} = [8]_{15}$$
$$[2^4]_{15} = [1]_{15} \quad ([16]_{15} = [1]_{15})$$
$$[2^5]_{15} = [2]_{15} \quad ([32]_{15} = [2]_{15})$$
$$\ldots$$

Pola ini: 1, 2, 4, 8, 1, 2, 4, 8, 1,... akan berulang terus selamanya. Inilah alasan mengapa persamaan ini begitu berguna. Untuk setiap nilai A (tidak peduli berapapun nilai A), jika kita dapat menemukan nilai terkecil r dimana $[A^r]_M = [1]_M$ maka, jika r bernilai genap, kita dapat merumuskannya menjadi seperti berikut:

$$[A^r]_M = [1]_M$$
$$\Rightarrow [A^r - 1]_M = [0]_M$$
$$\Rightarrow [A^{2\frac{r}{2}} - 1^2]_M = [0]_M$$
$$\Rightarrow [(A^{\frac{r}{2}} - 1)(A^{\frac{r}{2}} + 1)]_M = [0]_M$$

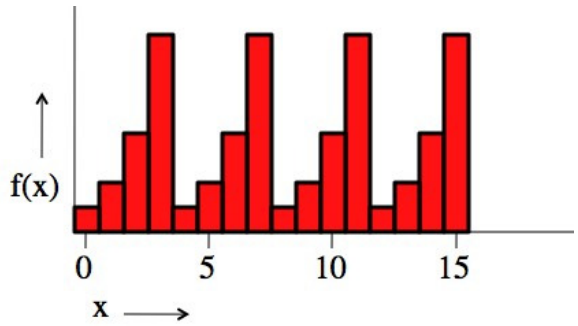
Jika r tidak bernilai genap maka kita ubah nilai A dan kita coba lagi perhitungan tersebut seterusnya hingga didapatkan hasil yang kita inginkan. Ketika kita menyebut sebuah persamaan sama dengan $[0]_M$, artinya adalah persamaan tersebut merupakan kelipatan dari M. Jadi $(A^{\frac{r}{2}} - 1)$ dan $(A^{\frac{r}{2}} + 1)$ memiliki faktor yang sama dengan M. Jadi untuk contoh "mod 15", A=2, M=15, dan r=4:

$$[2^4]_{15} = [1]_{15}$$
$$\Rightarrow [2^4 - 1]_{15} = [0]_{15}$$
$$\Rightarrow [(2^2 - 1)(2^2 + 1)]_{15} = [0]_{15}$$
$$\Rightarrow [(3)(5)]_{15} = [0]_{15}$$

Didapatkan faktor dari 15, yaitu 3 and 5. Untuk nilai M yang sangat besar, kita tidak dapat memangkatkan nilai A menjadi sangat tinggi dan menunggu hingga ditemukannya $[A^r]_M = [1]_M$. Karena tidak ada cukup waktu bagi komputer untuk melakukakan komputasi pada nilai A dengan pangkat yang sangat besar.

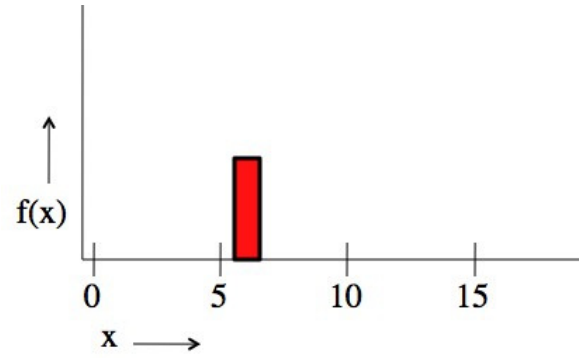
Oleh sebab itulah komputasi kuantum digunakan. Komputer kuantum tidak memiliki masalah untuk meningkatkan nilai A hingga berpangkat-pangkat yang sangat tinggi.

Solusinya adalah menggunakan algoritma Shor. Jadi, intinya adalah kita mencari nilai r yang memiliki dua sifat yaitu: nilainya merupakan bilangan terkecil sehingga $[A^r]_M = [1]_M$, dan setiap kali kita memangkatkan A menjadi lebih tinggi, r sama dengan total jumlah persamaan yang dibutuhkan agar pola tersebut berulang. Pada contoh "mod 15" diatas kita akan mendapatkan grafik dengan pola sebagai berikut:



Singkatnya kita ingin mencari nilai r sehingga nilai fungsi $[A^x]_M$ berulang setiap r, sehingga kita dapat melakukan trik $(A^{r/2} + 1)(A^{r/2} - 1)$. Karena fungsi ini memiliki pola perulangan yang cukup baik, transformasi Fourier dapat digunakan. Transformasi Fourier memecah sinyal ke dalam komponen frekuensi mereka, dan fungsi yang berulang memiliki frekuensi yang jelas. Kita dapat memanfaatkan frekuensi tersebut untuk mendapatkan nilai r. Semakin kecil r semakin cepat fungsi berulang dan semakin tinggi frekuensinya. Semakin besar nilai r, semakin lambat fungsi berulang dan semakin rendah frekuensinya.

Mengapa kita membutuhkan komputer kuantum untuk mengerjakan hal ini? Kita menginginkan fungsi-funsi tersebut untuk berada dalam satu komputer dalam waktu bersamaan. Komputer klasik hanya dapat melihat satu nilai x pada satu waktu, seperti pada gambar di bawah, jadi tidak masuk akal jika kita berbicara mengenai perulangan dan frekuensi pada komputer klasik ini. Kita membutuhkan komputer kuantum untuk mengerjakan beberapa nilai sekaligus dalam satu prosesor yang sama.



Untuk memahami cara kerjanya, kita mulai dengan sebuah komputer yang memiliki dua register. Notasi "$|1\rangle|2\rangle$" berarti register pertama menyimpan nilai 1 dan register kedua menyimpan nilai 2. Jika beberapa dari nilai ini ditambah bersama-sama berarti komputer tersebut memiliki beberapa state dalam satu waktu. Sebagai contoh: $|1\rangle|2\rangle + |3\rangle|4\rangle$ berarti komputer tersebut menyimpan dua state dalam satu waktu. 1 dan 3 pada register pertama, 2 dan 4 pada register kedua.

Berikut ini adalah langkah-langkah algoritma tersebut hasil analisis secara matematis oleh penulis. Mungkin banyak pembaca yang kurang mengerti penjelasan ini, karena memang penjelasan sesungguhnya jauh lebih panjang, penulis merangkumnya untuk memenuhi standar batas maksimum halaman pada makalah ini. Untuk memahami alur algoritma ini juga memerlukan pemahaman mendalam mengenai fisika kuantum, dan memahami istilah *quantum superposition, quantum entanglement*, dll, yang tidak mungkin dapat dijelaskan disini.

Langkah 1: Inisialisasi register pertama ke superposisi yang sama untuk setiap bilangan yang memungkinkan mulai dari 0 hingga N, dimana N adalah hasil perpangkatan dari angka 2 yang bernilai lebih besar dari M^2. Dan inisialisasi register kedua menjadi nol. N haruslah perpangkatan dari 2 karena sudah ditentukan oleh jumlah qbits pada register pertama. State kuantum dituliskan seperti ini

$$\frac{1}{\sqrt{N}} \sum_{x=0}^{N-1} |x\rangle|0\rangle.$$

Langkah 2: Definisikan $f(x) = [A^x]_M$. Ambil register pertama, jalankan pada fungsi f, dan taruh hasilnya pada register kedua. Sehingga persamaannya menjadi:

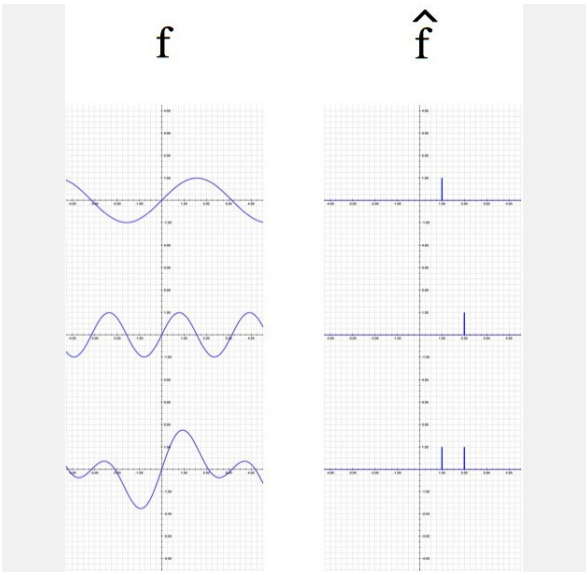
$$\frac{1}{\sqrt{N}} \sum_{x=0}^{N-1} |x\rangle|f(x)\rangle$$

Langkah 3: Perhatikan register kedua. Salah satu kemampuan komputer kuantum yang menakjubkan adalah, kemampuannya melakukan *quantum entangle* antara lingkungan di luar komputer dengan bagian mekanisme internal. Biasa disebut sebagai "wave function collapse", pada kasus ini mayoritas state akan "menghilang", dan sisanya akan terbagi pada interval yang teratur (yang kemungkinan adalah nilai r yang sedang kita cari). Anggaplah nilai f(x) hasil observasi adalah "B". State yang baru akan dituliskan sebagai berikut:

$$\sqrt{\frac{r}{N}} \sum_{j=0}^{N/r} |x_0 + jr\rangle|B\rangle$$

Ini adalah kumpulan input yang dapat menyebabkan hasil f(x)=B, dimulai pada nilai x terendah yang dapat menghasilkan nilai tersebut dan seterusnya setiap r bilangan berikutnya.

Langkah 4: Lakukan transformasi fourier pada register pertama. Jika kita memiliki fungsi f maka hasil transformasi fouriernya ditulis dengan notasi $\hat{f}$ (f hat). Gambar di bawah adalah contoh grafik hasil transformasi fourier pada fungsi Sin(x), Sin(2x), dan fungsi Sin(x)+Sin(2x)



State setelah proses transformasi Fourier adalah:

$$\frac{1}{\sqrt{N}} \sum_{k=0}^{N-1} \left[\sqrt{\frac{r}{N}} \sum_{j=0}^{N/r} e^{-2\pi i \frac{k}{N}(x_0 + jr)} \right] |k\rangle|B\rangle$$

$$= \frac{\sqrt{r}}{N} \sum_{k=0}^{N-1} e^{-2\pi i \frac{k}{N} x_0} \left[\sum_{j=0}^{N/r} e^{-2\pi i \frac{kr}{N} j} \right] |k\rangle|B\rangle$$

Langkah 5: Gambar grafik yang "meruncing" pada langkah sebelumnya menunjukkan ketika kita mengukur nilai dari register pertama, kemungkinan besar kita mengukur nilai k yang menghasilkan $\frac{kr}{N}$ sangat mendekati atau sama dengan nilai integer. Bagian terpenting ada pada bagian $\sum_j e^{-2\pi i \frac{kr}{N} j}$. Ketika $\frac{kr}{N}$ mendekati nilai integer, maka persamaan ini terlihat seperti "1+1+1+1+1…." dan akan menghasilkan nilai sangat besar. Atau justru meniadakan satu sama lain, misal jika $\frac{kr}{N} = \frac{1}{2}$, maka maka persamaan tersebut menjadi "1-1+1-1+1-1…".

Langkah 6: Lakukan beberapa perhitungan matematis. Pada langkah 5 kita mengukur nilai k sehingga $\frac{kr}{N} \approx \ell$, dimana ℓ adalah integer. Kita tahu nilai N berdasarkan hasil pada langkah 1, dan kita tahu nilai k berdasarkan hasil pengukuran, tetapi nilai r dan ℓ tidak diketahui. Jadi yang kita dapat adalah sebuah aproksimasi $\frac{k}{N} \approx \frac{\ell}{r}$. Untuk bilangan M yang kita faktorkan dibutuhkan N> M^2. Dan, karena M>r, N>r^2 juga. Dengan diberikan kondisi seperti ini untuk nilai k yang dihasilkan kita akan mendapatkan nilai unik tertentu untuk ℓ and r. Kita tidak membutuhkan nilai ℓ sehingga dapat diabaikan, yang kita butuhkan hanyalah nilai r. Cara untuk mengetahui berapa nilai $\frac{\ell}{r}$ dari $\frac{k}{N}$ adalah dengan menggunakan teknik yang dinamakan "*Approximation by Continued Fractions*". Setelah ditemukan nilai r, tujuan kita telah tercapai dan algoritma ini berakhir.

5. Kesimpulan

Meskipun komputasi kuantum masih berada dalam tahap perkembangan awal karena baru muncul beberapa tahun belakangan, eksperimen telah dilakukan untuk mengetes operasi komputasi kuantum pada sejumlah kecil qubit. Riset, baik pada area teoritis maupun praktikal, terus berlanjut dengan langkah yang sangat cepat, dan banyak institusi pemerintahan dan militer membantu mendanai riset ini untuk mengembangkan komputer kuantum demi alasan kemanusiaan ataupun alasan militer, seperti kriptanalisis. Jika komputer kuantum skala besar dapat diciptakan, komputer ini dapat memecahkan beberapa persoalan secara eksponensial lebih cepat dibandingkan komputer klasik kita saat ini. Jika memang terbukti kriptanalisis menggunakan komputer kuantum jauh lebih cepat dibandingkan komputer konvensional, maka ilmuwan kemungkinan besar harus mengembangkan algoritma baru yang lebih efisien untuk mengenkripsi pesan-pesan rahasia

DAFTAR PUSTAKA

[1] Munir, Rinaldi, Diktat Kuliah IF5054Kriptografi, Penerbit ITB 2006

[2] Kaku, Michio, Hyperspace - A Scientific Odyssey Through Parallel Universes, Time Warps, and the Tenth Dimension, Doubleday, 1994

[4] http://id.wikipedia.org/wiki/Quantum_Computing

[5] http://id.wikipedia.org/wiki/Quantum_Cryptography