Bab 27

Masa Depan Kriptografi

Masa depan kriptografi akan dipengaruhi oleh perkembangan ilmu dan teknologi terkait. Ilmu dan teknologi yang perkembangannya akan sangat berpengaruh pada masa depan kriptografi termasuk:

- matematika,
- *hardware*, dan
- *quantum computing*.

Ketiga hal tersebut akan dibahas di bab ini.

27.1 Perkembangan Matematika

Tahun 1976, Martin Gardner menulis dalam Scientific American bahwa kunci RSA sebesar 129 digit akan aman untuk sekitar 40 *quadrillion* tahun. Kurang dari 20 tahun kemudian, tepatnya tahun 1994, kunci tersebut dapat diuraikan menggunakan metode *quadratic sieve*. Ini adalah contoh bagaimana terobosan di bidang matematika dan algoritma dapat mempengaruhi kriptografi secara signifikan. Dewasa ini metode *number field sieve* bahkan lebih efisien dibandingkan metode *quadratic sieve* dalam menguraikan bilangan yang sangat besar (lebih dari 100 digit).

Perkembangan lain di bidang matematika yang telah mempengaruhi kriptografi adalah penggunaan *elliptic curves over finite field*. Di masa yang akan datang, kriptografi *public key* yang berdasarkan pada penggunaan *elliptic curve* berpotensi mengambil alih posisi RSA sebagai algoritma yang dominan. Ini karena dengan kemajuan di bidang *hardware*, besarnya kunci yang dperlukan akan meningkat. Keunggulan kriptografi *public key* versi *elliptic curve* adalah keperluan peningkatan besar kunci tidak sedrastis untuk RSA, seperti terlihat

di tabel berikut yang menunjukkan perbandingan besar kunci dalam bit untuk kekuatan yang sama.

RSA	ECDSA/ECES
1024	160
2048	224
3072	256
7680	384
15360	512

RSA menggunakan kunci 1024 bit kekuatannya ekuivalen dengan kriptografi versi *elliptic curve* (ECDSA/ECES) menggunakan kunci 160 bit. RSA menggunakan kunci 15360 bit kekuatannya ekuivalen dengan ECDSA/ECES menggunakan kunci 512 bit. Dimana kunci RSA besarnya naik menjadi 15 kali lipat, untuk ECDSA/ECES kunci hanya diperlukan naik menjadi sekitar 3 kali lipat. Ini jelas menunjukkan keunggulan kriptografi *public key* versi *elliptic curve*.

Perkembangan dimasa depan dalam matematika dan algoritma, terutama dalam:

- penguraian bilangan bulat,
- komputasi logaritma diskrit, dan
- aljabar abstrak,

akan terus mempengaruhi kriptografi.

27.2 Perkembangan Hardware

DES sudah tidak digunakan lagi bukan karena algoritmanya lemah, melainkan besar kunci terlalu kecil. Saat ini kunci sebesar 56 bit dapat dicari secara *brute force* menggunakan *hardware* kini, dalam waktu yang tidak terlalu lama, dengan ongkos yang relatif murah.

Dengan perkembangan *hardware* di masa depan yang akan semakin cepat dan semakin murah, besar kunci untuk enkripsi mungkin perlu ditingkatkan. Saat ini enkripsi simetris dengan kunci 256 bit masih memiliki ruang cukup besar. Akan tetapi bisa saja terjadi terobosan di bidang *hardware* yang akan mengancam keamanan enkripsi simetris dengan kunci 256 bit.

Perkembangan *hardware* di masa depan tidak akan hanya berfokus pada peningkatan *clock speed*, namun juga pada peningkatan *parallelism*. Peningkatan *parallelism* akan terjadi di berbagai bagian, mulai dari bagian terkecil *processor* yang dapat dibuat *parallel*, sampai dengan *multi-processor* yang mempunyai interkoneksi dengan *bandwidth* yang sangat tinggi. Jenis *parallelism* juga akan

ada yang bersifat simetris dan akan ada yang bersifat asimetris misalnya menggunakan *co-processor*. Tentunya peningkatan *parallelism* di *hardware* juga akan diiringi dengan peningkatan penggunaan *parallelism* di *software*, baik yang secara otomatis dilakukan oleh *compiler*, maupun yang dilakukan secara *manual* oleh *programmer* misalnya menggunakan *threads*.

Tentunya jika *quantum computing* menjadi realitas, jenis kriptografi yang dapat digunakan secara efektif akan berbeda dari yang digunakan sekarang. Kita akan bahas *quantum computing* di bagian berikut.

27.3 Quantum Computing

Sekitar tahun 1982, Richard Feynman sedang mencoba melakukan simulasi interaksi beberapa partikel dalam fisika kuantum. Yang ia temukan adalah, jika menggunakan cara komputasi klasik (ekuivalen dengan penggunaan Turing *machine*), maka secara umum simulasi memerlukan sumber daya yang bersifat *exponential*. Untuk interaksi n partikel, simulasi menggunakan komputasi klasik membutuhkan sumber daya yang *exponential* dalam n, sedangkan alam dapat melakukannya hanya menggunakan n partikel dalam *real time*. Ini mengindikasikan bahwa komputasi klasik bukanlah cara paling efisien untuk melakukan komputasi, dan menjadi inspirasi untuk konsep *quantum computing* (komputasi kuantum). Ada komputasi yang mempunyai kompleksitas *exponential* dalam komputasi klasik tetapi mempunyai kompleksitas linear dalam komputasi kuantum. Persoalannya adalah bagaimana ini dapat dimanfaatkan.

Ada dua konsep fisika kuantum yang menjadi dasar dari komputasi kuantum:

- *superposition* dari *quantum states*, dan
- *quantum entanglement*.

Menurut fisika kuantum, suatu partikel bisa berada dalam suatu *quantum state* yang merupakan *superposition* dari dua *quantum state* murni sekaligus, dimana suatu *quantum state* murni adalah *quantum state* yang dapat diobservasi secara klasik. Sebagai contoh kita gunakan *spin* (perputaran) dari suatu partikel relatif terhadap suatu arah. Jika tidak nol, perputaran relatif terhadap suatu arah dapat diobservasi secara klasik sebagai *down* (0) atau *up* (1), yang masing-masing adalah *quantum state* murni. Menggunakan notasi fisika kuantum, kedua *quantum state* murni tersebut adalah

$$|0\rangle \text{ dan } |1\rangle.$$

Superposition ψ dari kedua *quantum state* murni adalah kombinasi linear

$$\psi = \alpha|0\rangle + \beta|1\rangle$$

dimana secara umum α dan β masing-masing bisa berupa bilangan kompleks, tetapi untuk keperluan kita cukup merupakan bilangan nyata. α adalah apa yang disebut *probability amplitude* untuk $|0\rangle$, sedangkan β adalah *probability amplitude* untuk $|1\rangle$. Jika observasi dilakukan terhadap partikel yang berada dalam *superposition* seperti diatas, maka kemungkinan bahwa partikel berada pada *state* $|0\rangle$ adalah α^2, kemungkinan bahwa partikel berada pada *state* $|1\rangle$ adalah β^2, sedangkan kemungkinan lain tidak ada. Jadi

$$\alpha^2 + \beta^2 = 1.$$

Yang menarik adalah setiap *probability amplitude*, yang merupakan bagian internal dari *superposition state*, bisa berupa bilangan negatif. Jika $|0\rangle$ dan $|1\rangle$ kita anggap sebagai basis, maka *state* dari partikel dapat direpresentasikan sebagai vektor

$$\begin{bmatrix} \alpha \\ \beta \end{bmatrix}.$$

Dalam fisika kuantum, jika sepasang partikel telah berinteraksi maka terjadi *quantum entanglement* dimana apa yang terjadi pada satu partikel secara instan mempengaruhi partikel pasangannya. Masing-masing partikel bisa berada dalam suatu *superposition state*, tetapi pada saat observasi secara klasik dilakukan pada satu diantaranya (yang membuatnya "memilih" suatu *state* murni), maka partikel pasangannya langsung memasuki *state* murni yang sesuai. Contohnya, jika pasangan bersifat komplementer dan observasi membuat satu partikel memasuki *state* $|0\rangle$, maka partikel pasangannya langsung memasuki *state* $|1\rangle$.

Meskipun belum ada penjelasan yang memuaskan mengenai apa yang sebenarnya terjadi dengan *superposition* dan *entanglement* (masalah ini dijuluki *quantum interpretation problem*), dari segi matematika tidak ada masalah. Kita tidak akan bahas masalah *quantum interpretation* dan akan fokus pada matematika yang digunakan.

Jika unit informasi terkecil dalam komputasi klasik adalah bit, maka unit informasi terkecil dalam komputasi kuantum adalah qubit. Berbeda dengan bit yang hanya bisa mempunyai nilai 0 atau 1, qubit bisa mempunyai nilai yang merupakan *superposition* dengan representasi $\alpha|0\rangle + \beta|1\rangle$. Komputasi kuantum dilakukan menggunakan 3 macam *gate* dengan input 1 qubit, dan 1 macam *gate* dengan input 2 qubit. *Gate* pertama adalah *not gate* N yang dapat direpresentasikan menggunakan matrik transformasi sebagai berikut:

$$\begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}.$$

Efek dari transformasi *not* terhadap qubit $\alpha|0\rangle + \beta|1\rangle$ adalah

$$\begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} \begin{bmatrix} \alpha \\ \beta \end{bmatrix} = \begin{bmatrix} \beta \\ \alpha \end{bmatrix},$$

jadi menghasilkan qubit $\beta|0\rangle+\alpha|1\rangle$. *Gate* kedua adalah Hadamard *gate* H yang dapat direpresentasikan menggunakan matrik transformasi sebagai berikut:

$$\begin{bmatrix} 1/\sqrt{2} & 1/\sqrt{2} \\ 1/\sqrt{2} & -1/\sqrt{2} \end{bmatrix}.$$

Efek dari transformasi Hadamard terhadap qubit $\alpha|0\rangle + \beta|1\rangle$ adalah

$$\begin{bmatrix} 1/\sqrt{2} & 1/\sqrt{2} \\ 1/\sqrt{2} & -1/\sqrt{2} \end{bmatrix} \begin{bmatrix} \alpha \\ \beta \end{bmatrix} = \begin{bmatrix} \frac{1}{\sqrt{2}}(\alpha+\beta) \\ \frac{1}{\sqrt{2}}(\alpha-\beta) \end{bmatrix},$$

jadi menghasilkan qubit $\frac{1}{\sqrt{2}}(\alpha+\beta)|0\rangle + \frac{1}{\sqrt{2}}(\alpha-\beta)|1\rangle$. Perhatikan bahwa jika transformasi Hadamard *gate* dilakukan terhadap $|0\rangle$ maka kita akan dapatkan $\frac{1}{\sqrt{2}}|0\rangle + \frac{1}{\sqrt{2}}|1\rangle$, yang merupakan nilai *superposition* dengan probabilitas yang sama untuk menghasilkan $|0\rangle$ atau $|1\rangle$ jika observasi secara klasik dilakukan. Jika transformasi Hadamard *gate* dilakukan terhadap $|1\rangle$ maka kita akan dapatkan $\frac{1}{\sqrt{2}}|0\rangle - \frac{1}{\sqrt{2}}|1\rangle$, yang juga mempunyai probabilitas yang sama untuk menghasilkan $|0\rangle$ atau $|1\rangle$ jika observasi secara klasik dilakukan. *Gate* ketiga adalah *gate* Z yang dapat direpresentasikan menggunakan matrik transformasi sebagai berikut:

$$\begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}.$$

Efek dari transformasi *gate* Z terhadap qubit $\alpha|0\rangle + \beta|1\rangle$ adalah

$$\begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix} \begin{bmatrix} \alpha \\ \beta \end{bmatrix} = \begin{bmatrix} \alpha \\ -\beta \end{bmatrix},$$

jadi menghasilkan qubit $\alpha|0\rangle - \beta|1\rangle$. Jadi *gate* Z melakukan negasi terhadap *probability amplitude* untuk $|1\rangle$.

Ketiga transformasi diatas merupakan apa yang disebut *unitary transformation*. Matrik U disebut *unitary* jika $UU\dagger = I$, dimana $U\dagger$ didapat dengan men-*transpose* U kemudian melakukan *complex conjugate* terhadap hasilnya. Untuk ketiga transformasi diatas, $U\dagger = U$, jadi U merupakan *inverse* untuk U. Kita dapat periksa bahwa $NN = I$, $HH = I$ dan $ZZ = I$. Jadi setelah transformasi terhadap qubit, transformasi dapat juga digunakan untuk mengembalikan qubit ke *state* semula. Sebagai contoh, jika transformasi Hadamard dilakukan terhadap $\frac{1}{\sqrt{2}}|0\rangle+\frac{1}{\sqrt{2}}|1\rangle$, maka kita akan dapatkan kembali $|0\rangle$. Dalam komputasi kuantum, semua transformasi bersifat *reversible*.

Gate dengan input 2 qubit yang diperlukan adalah apa yang dinamakan *controlled-not* . Dalam komputasi kuantum, 2 qubit merupakan produk tensor,

jadi jika $|\psi_1\rangle = \alpha_1|0\rangle + \beta_1|1\rangle$ dan $|\psi_2\rangle = \alpha_2|0\rangle + \beta_2|1\rangle$, maka

$$|\psi_1, \psi_2\rangle = |\psi_1\rangle|\psi_2\rangle = \begin{bmatrix} \alpha_1\alpha_2 \\ \alpha_1\beta_2 \\ \beta_1\alpha_2 \\ \beta_1\beta_2 \end{bmatrix}.$$

Jika 2 qubit direpresentasikan seperti diatas, maka transformasi *controlled-not* dapat direpresentasikan dengan matrik

$$\begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{bmatrix}.$$

Hasil transformasi *controlled-not* terhadap $|\psi_1, \psi_2\rangle$ adalah

$$\begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{bmatrix} \begin{bmatrix} \alpha_1\alpha_2 \\ \alpha_1\beta_2 \\ \beta_1\alpha_2 \\ \beta_1\beta_2 \end{bmatrix} = \begin{bmatrix} \alpha_1\alpha_2 \\ \alpha_1\beta_2 \\ \beta_1\beta_2 \\ \beta_1\alpha_2 \end{bmatrix}.$$

Tidak terlalu sulit untuk melihat bahwa transformasi *controlled-not* merupakan *unitary transformation*. Mari kita lihat efek transformasi jika $|\psi_1\rangle = \alpha_1|0\rangle + \beta_1|1\rangle = |0\rangle$. Karena $\alpha_1 = 1$ dan $\beta_1 = 0$, maka hasilnya adalah

$$\begin{bmatrix} \alpha_2 \\ \beta_2 \\ 0 \\ 0 \end{bmatrix},$$

yang berarti tidak ada efek karena hasil sama dengan keadaan semula yaitu

$$\begin{bmatrix} \alpha_1\alpha_2 \\ \alpha_1\beta_2 \\ \beta_1\alpha_2 \\ \beta_1\beta_2 \end{bmatrix}.$$

Sebaliknya, jika $|\psi_1\rangle = |1\rangle$, maka hasilnya adalah

$$\begin{bmatrix} 0 \\ 0 \\ \beta_2 \\ \alpha_2 \end{bmatrix},$$

yang berarti terjadi *negation* pada $|\psi_2\rangle$ (transformasi menukar dua baris terahir).

Transformasi *controlled not* mengakibatkan *quantum entanglement* dimana kedua qubit menjadi saling tergantung. Sebagai contoh, kita mulai dengan

$$\alpha_1 = \frac{1}{\sqrt{2}}, \beta_1 = \frac{1}{\sqrt{2}}, \alpha_2 = 1, \beta_2 = 0,$$

jadi qubit pertama berada pada *superposition* dengan probabilitas yang sama untuk menjadi 0 atau 1, sedangkan qubit kedua mempunyai nilai 0. Setelah transformasi *controlled-not*, maka nilai 2 qubit sebagai vektor adalah

$$\begin{bmatrix} \frac{1}{\sqrt{2}} \\ 0 \\ 0 \\ \frac{1}{\sqrt{2}} \end{bmatrix},$$

yang berarti qubit kedua juga berada pada *superposition* dengan probabilitas yang sama untuk menjadi 0 atau 1. Akan tetapi, jika observasi secara klasik dilakukan pada qubit pertama dan sebagai contoh memberi hasil 1 dengan *probability amplitude* 1, maka vektor berubah menjadi

$$\begin{bmatrix} 0 \\ 0 \\ \beta_2 \\ \alpha_2 \end{bmatrix}.$$

Jadi *state* untuk qubit kedua berubah menjadi

$$\begin{aligned} |\psi_2\rangle &= \beta_2|0\rangle + \alpha_2|1\rangle \\ &= |1\rangle, \end{aligned}$$

yang berarti qubit kedua dipaksa mempunyai nilai 1. Perubahan *state* yang disebabkan oleh observasi secara klasik disebut *decoherence*.

Yang sangat menarik dengan komputasi kuantum adalah, jika terdapat n qubit dan setiap qubit berada pada *superposition* dengan kemungkinan yang sama untuk menjadi 0 atau 1, maka komputasi yang dilakukan sekaligus dilakukan pada 2^n *state*. Akan tetapi komputasi yang dilakukan harus bersifat *reversible*, dan kita harus mengharapkan bahwa *decoherence* memberi hasil yang kita inginkan. Oleh sebab itu, biasanya cara kerja komputasi kuantum adalah sebagai berikut:

- Mulai dengan *state space* yang besar.
- Secara bertahap lakukan transformasi yang memperbesar probabilitas *decoherence* akan memberikan hasil yang diinginkan.

- Jika probabilitas sudah cukup besar bahwa *decoherence* akan memberikan hasil yang diinginkan, maka lakukan observasi untuk mendapatkan jawaban.

Pada tahun 1994 Peter Shor (lihat [sho9]) berhasil membuat algoritma untuk menguraikan bilangan bulat yang menggunakan komputasi kuantum sebagai *subroutine*. Untuk menguraikan suatu bilangan ganjil n, pilih secara acak suatu bilangan bulat x dimana $1 < x < n$ dan $\gcd(x, n) = 1$, lalu cari *order* dari x dalam *multiplicative group* modulo n (lihat bagian 10.4), sebut saja r. Setelah r didapat, maka lakukan kalkulasi $\gcd(x^{r/2} - 1, n)$. Karena

$$\begin{aligned}(x^{r/2} - 1)(x^{r/2} + 1) &= x^r - 1 \\ &\equiv 0 \pmod{n},\end{aligned}$$

maka $\gcd(x^{r/2} - 1, n)$ bukan merupakan pembagi yang *non-trivial* dari n hanya jika r ganjil atau $x^{r/2} \equiv -1 \pmod{n}$. Dapat ditunjukkan bahwa probabilitas kegagalan $< 1/2^{k-1}$ dimana k adalah banyaknya bilangan prima ganjil yang membagi n. Dengan menggunakan komputasi kuantum untuk mencari r, kompleksitas dari algoritma ini adalah *polynomial* dalam $\log n$. Jadi jelas jika komputasi kuantum dapat dilakukan dalam skala cukup besar, ini merupakan ancaman terhadap kriptografi yang keamanannya berbasis pada sukarnya penguraian seperti RSA.

27.4 Ringkasan

Di bab ini kita telah bahas perkembangan di masa depan yang dapat mempengaruhi kriptografi secara signifikan, yaitu perkembangan matematika, perkembangan *hardware*, dan *quantum computing*. Terutama jika *quantum computing* menjadi kenyataan, maka jenis kriptografi *public key* yang digunakan harus berubah secara revolusioner.