Bab 18

Quantum Key Distribution

Quantum key distribution adalah metode untuk *key agreement* yang didasarkan pada fisika kuantum. Metode ini bukan suatu sistem kriptografi yang menggunakan *quantum computer*, melainkan suatu sistem yang didasarkan pada kenyataan bahwa jika pengukuran dilakukan terhadap suatu partikel yang terisolir (contohnya foton), maka pengukuran tersebut mempengaruhi kelakuan dari partikel tersebut. Fisika kuantum tidak akan dibahas panjang lebar disini, hanya sifat dasar polarisasi foton saja dan asumsi bahwa suatu *quantum state* tidak dapat di*clone*. Kita juga tidak akan bahas *no cloning theorem*. Pembahasan disini lebih pada logika dari protokol untuk *quantum key distribution* (dengan asumsi *quantum state* tidak dapat di*clone*), jadi bukan pada aspek fisika kuantum dari *quantum key distribution*. Bahkan kita akan lebih fokus lagi pada jenis protokol berbasis pengukuran, bukan pada protokol berbasis *quantum entanglement*. Sebagai contoh akan kita bahas protokol Bennett-Brassard. Penggunaan *Heisenberg uncertainty principle* di buku ini adalah sebagai limitasi teknik pengukuran, bukan sebagai suatu limitasi dari apa yang dapat kita ketahui, jadi bukan penggunaan yang kontroversial.

Sinar dapat dipolarisir misalnya dengan filter Polaroid atau dengan kristal *calcite*. Foton yang terpolarisir bisa diambil dari sinar yang telah dipolarisir dengan cara yang serupa dengan yang dilakukan dalam eksperimen oleh Aspect, Grangier dan Roger (lihat [asp82]). Karena *Heisenberg uncertainty principle*, pengukuran hanya dapat memberikan informasi 1 bit mengenai polarisasi foton. Jika sinar dipolarisir dengan orientasi α dan ditujukan ke filter B yang mempunyai orientasi β, maka setiap foton dalam sinar berperilaku dikotomis dan probabilistik saat bertemu filter B yaitu:

- foton ditransmisi oleh B dengan probabilitas $\cos^2(\alpha - \beta)$, atau
- foton diabsorbsi oleh B dengan probabilitas $\sin^2(\alpha - \beta)$.

Jadi foton bersifat deterministik hanya jika α dan β paralel (foton dipastikan ditransmisi oleh B) atau α dan β tegak lurus (foton dipastikan diabsorbsi oleh B). Jika α dan β tidak tegak lurus, tidak ada informasi tambahan yang bisa didapatkan jika foton ditransmisi karena foton ditransmisi dengan polarisasi β, jadi orientasi α sudah "dilupakan" oleh foton.

Dalam ilmu fisika kuantum, konsep probabilitas yang digunakan adalah *probability amplitude*, yang harus dikuadratkan untuk mendapatkan probabilitas. Itulah sebabnya probabilitas untuk foton ditransmisi adalah $\cos^2(\alpha - \beta)$, dimana $\cos(\alpha-\beta)$ adalah *probability amplitude*. *Internal state* dari sistem kuantum (contohnya polarisasi foton) direpresentasikan menggunakan vektor yang panjangnya 1 dalam ruang linear menggunakan *complex field* (ruang Hilbert). Untuk polarisasi foton, ruang Hilbert yang digunakan adalah ruang Hilbert dua dimensi, jadi *state* dari foton dapat direpresentasikan menggunakan kombinasi linear dari dua vektor yang *linearly independent*, contohnya

$$r_1 = \begin{bmatrix} 1 \\ 0 \end{bmatrix}, \qquad r_2 = \begin{bmatrix} 0 \\ 1 \end{bmatrix},$$

dimana r_1 merepresentasikan polarisasi horisontal dan r_2 merepresentasikan polarisasi vertikal. Jadi suatu foton yang terpolarisir dengan orientasi α direpresentasikan oleh vektor $(\cos\alpha, \sin\alpha)$. Jika foton tersebut diukur polarisasi horisontal dan vertikalnya, maka foton tersebut "memilih" untuk menjadi horisontal dengan probabilitas $\cos^2\alpha$, atau menjadi vertikal dengan probabilitas $\sin^2\alpha$. Basis $\{r_1, r_2\}$ disebut basis *rectilinear*. Sebagai alternatif, kita dapat menggunakan

$$d_1 = \begin{bmatrix} \frac{1}{\sqrt{2}} \\ \frac{1}{\sqrt{2}} \end{bmatrix}, \qquad d_2 = \begin{bmatrix} \frac{1}{\sqrt{2}} \\ -\frac{1}{\sqrt{2}} \end{bmatrix},$$

dimana d_1 merepresentasikan polarisasi 45 derajat dan d_2 merepresentasikan polarisasi 135 derajat. Basis $\{d_1, d_2\}$ disebut basis *diagonal*. Dua basis (contohnya *rectilinear* dan *diagonal*) disebut *conjugate* jika setiap vektor dalam satu basis mempunyai proyeksi yang sama panjang ke dua vektor dalam basis pasangannya. Sebagai contoh, d_1 jika diproyeksikan ke r_1 dan r_2 menjadi

$$d_1 = \begin{bmatrix} \frac{1}{\sqrt{2}} \\ \frac{1}{\sqrt{2}} \end{bmatrix} = \frac{1}{\sqrt{2}} \begin{bmatrix} 1 \\ 0 \end{bmatrix} + \frac{1}{\sqrt{2}} \begin{bmatrix} 0 \\ 1 \end{bmatrix} = \frac{1}{\sqrt{2}} r_1 + \frac{1}{\sqrt{2}} r_2,$$

dimana $\frac{1}{\sqrt{2}}$ merupakan *probability amplitude* d_1 akan memilih r_1 atau r_2 jika diukur menggunakan basis *rectilinear*, jadi probabilitas untuk memilih r_1 atau r_2 sama yaitu $(\frac{1}{\sqrt{2}})^2 = \frac{1}{2}$. Ini berarti suatu foton yang berada pada *state* tertentu dalam suatu basis (d_1 atau d_2 dalam basis *diagonal*, r_1 atau r_2 dalam basis *rectilinear*) akan berperilaku acak (semua informasi hilang) jika diukur

menggunakan basis *conjugate*. Sebetulnya masih ada satu lagi basis yang *conjugate* dengan basis *rectilinear* dan basis *diagonal* dalam ruang Hilbert dua dimensi yaitu basis *circular*, akan tetapi basis tersebut tidak diperlukan disini.

Secara garis besar, dalam *quantum key distribution*, saluran kuantum tidak digunakan untuk transmisi naskah, baik naskah asli maupun naskah yang telah dienkripsi, melainkan digunakan untuk transmisi bit secara acak antara dua pengguna yang pada awalnya tidak memiliki rahasia bersama. Dengan probabilitas yang sangat tinggi, keduanya dapat mendeteksi apabila ada pihak ketiga yang telah menyadap transmisi bit melalui saluran kuantum, karena pihak ketiga harus melakukan pengukuran yang menyebabkan transmisi kemungkinan besar terganggu (karena pengukuran bisa merubah polarisasi foton). Jika kedua pengguna berpendapat bahwa transmisi tidak terganggu, maka deretan bit yang telah ditransmisi dapat digunakan untuk membuat kunci rahasia bersama. Jika tidak, maka hasil tranmisi dibuang, dan transmisi dicoba lagi (dengan urutan bit acak yang lain).

Secara lebih rinci, pengguna pertama (sebut saja Alice) membuat deretan bit acak dan deretan basis acak. Untuk setiap bit, Alice mentransmisi bit tersebut kepada pengguna kedua (sebut saja Bob) melalui saluran kuantum, menggunakan basis untuk bit tersebut (yang telah dibuat secara acak *rectilinear* atau *diagonal*). Bob "membaca" transmisi dari Alice dengan mengukur deretan bit menggunakan deretan basis yang ia buat acak, independen dari deretan basis yang digunakan Alice. Secara rerata, Bob akan menggunakan basis yang benar untuk setengah dari semua bit yang ditransmisi. Alice dan Bob mencocokkan basis yang mereka pergunakan, dengan menggunakan jalur umum untuk komunikasi. Dari semua pengukuran yang cocok, Bob memilih kira-kira sepertiga bit secara acak, lalu Alice dan Bob mencocokkan bit-bit yang terpilih melalui jalur umum. Jika semua bit cocok, maka Alice dan Bob dapat cukup yakin bahwa transmisi telah berlangsung secara benar tanpa penyadapan. Alice dan Bob dapat mengambil sisa dua pertiga dari bit yang diukur secara benar, dan menggunakannya untuk membuat kunci rahasia bersama. Tentunya banyaknya bit yang digunakan tergantung pada apa yang diperlukan untuk membuat kunci rahasia bersama. Jika kunci rahasia merupakan *one-time pad* (biasanya sistem *quantum key distribution* digunakan untuk membuat *one-time pad*), maka diperlukan deretan bit yang panjang. Gambar 18.1 memperlihatkan contoh suatu sesi protokol Bennett-Brassard dimana hasil yang dapat digunakan untuk membuat kunci rahasia bersama adalah $1, 0, 1, 1$.

Jika ada pihak ketiga yang menyadap transmisi melalui jalur kuantum, maka besar kemungkinan ada ketidak-cocokan dalam sepertiga bit yang dicocokkan, kecuali jika jumlah bit yang disadap tidak terlalu banyak. Komunikasi melalui jalur publik juga harus diamankan dari penyusupan. Ini dapat dilakukan misalnya menggunakan *tag* Wegman-Carter (lihat [weg81]) untuk *secure hashing* (lihat bab 9). Menggunakan *secure hashing* sebagai *message*

authentication code merupakan sesuatu yang cukup umum untuk mekanisme *authentication*.

Meskipun beberapa produk komersial *quantum key distribution* telah dipasarkan, keamanan dari *quantum key distribution* masih dipertanyakan. Sebagai contoh, Jörgen Cederlöf dan Jan-Åke Larsson membahas kelemahan *tagging* Wegman-Carter sebagai mekanisme *authentication* (lihat [ced08]). Kelemahan pada *detector module* yang digunakan dalam produk komersial *quantum key distribution* juga telah dipublikasi (lihat [mak09]). Dengan menimbang berbagai kelemahan yang telah dipublikasi, dan kenyataan bahwa *quantum key distribution* belum merupakan *proven technology*, maka buku ini belum bisa merekomendasikan penggunaan *quantum key distribution*.

18.1 Ringkasan

Di bab ini telah dibahas secara ringkas cara melakukan *key agreement* menggunakan *quantum key distribution*. Protokol yang telah dibahas adalah protokol Bennett-Brassard. Pembahasan fisika kuantum hanya sebatas sifat dasar polarisasi, sekedar cukup untuk menjelaskan protokol Bennet-Brassard. Karena beberapa kelemahan *quantum key distribution* dan kenyataan bahwa *quantum key distribution* belum merupakan *proven technology*, penggunaan *quantum key distribution* belum bisa direkomendasikan.

Jika *quantum key distribution* kelak menjadi sesuatu yang praktis, maka enkripsi *one-time pad* juga akan menjadi praktis, meskipun aplikasinya terbatas karena sifat *quantum key distribution* yang *point-to-point* secara fisik.

TRANSMISI JALUR KUANTUM															
A	0	1	1	0	1	1	0	0	1	0	1	1	0	0	1
A	D	R	D	R	R	R	R	R	D	D	R	D	D	D	R
A	↗	↑	↘	→	↑	↑	→	→	↘	↗	↑	↘	↗	↗	↑
B	R	D	D	R	R	D	D	R	D	R	D	D	D	D	R
B	1		1		1	0	0	0		1	1	1		0	1
TRANSMISI JALUR PUBLIK															
B	R		D		R	D	D	R		R	D	D		D	R
A			√		√			√				√		√	√
√			1		1			0				1		0	1
B					1									0	
A					√									√	
HASIL															
√			1					0				1			1

Legenda

A	-	Alice
B	-	Bob
R	-	*Rectilinear* (basis)
D	-	*Diagonal* (basis)
→	-	Polarisasi untuk 0 (basis *rectilinear*)
↑	-	Polarisasi untuk 1 (basis *rectilinear*)
↗	-	Polarisasi untuk 0 (basis *diagonal*)
↘	-	Polarisasi untuk 1 (basis *diagonal*)
√	-	ok

Gambar 18.1: Contoh Sesi Protokol Bennett-Brassard