KRIPTOGRAFI QUANTUM: SIMULASI PROTOKOL BB84

NURHAYATI ABDUL AZIZ
BAHARI IDRUS
EDDIE SHAHRIL ISMAIL

Fakulti Teknologi & Sains Maklumat, Universiti Kebangsaan Malaysia

ABSTRAK

Masalah pengagihan kunci rahsia yang bebas daripada pengetahuan pihak musuh merupakan kelemahan utama bagi kriptografi moden. Namun, hal ini dapat diselesaikan dengan adanya teknologi kriptografi quantum yang menggunakan ciri-ciri mekanik quantum iaitu prinsip ketidakpastian Heisenberg dan teorem tiada-pengklonan. Melalui ciri-ciri ini, kunci yang lebih selamat dapat dihasilkan kerana kehadiran musuh dapat dikesan sekaligus dapat meningkatkan lagi tahap keselamatan dan kecekapan bagi sesebuah komunikasi. Protokol pertama yang menggunakan konsep kriptografi quantum dikenali sebagai protokol BB84. Projek ini membangunkan sebuah simulasi protokol BB84 mengguna perisian komputer MATLAB versi 7.12. Tujuan dibangunkan adalah bagi melihat tahap ketepatan, keselamatan dan kecekapan protokol BB84. Sistem simulasi yang dibangunkan ini membuat penambahbaikan daripada sistem simulasi sedia ada yang dibangunkan oleh Rednour dalam bahasa JAVA. Berdasarkan keputusan simulasi yang telah dilaksanakan, didapati bahawa ralat dalam menghasilkan kunci yang tepat (bagi situasi ketiadaan musuh) dapat dikurangkan setelah dibandingkan dengan hasil keputusan oleh Rednour. Kunci ini seterusnya boleh digunakan dengan selamat untuk pengkripan dalam kriptografi moden.

PENGENALAN

Kriptografi merupakan satu kajian yang berkaitan dengan penghantaran maklumat secara rahsia. Dengan perkembangan teknologi yang semakin pesat dan perubahan paradigma dalam pembangunan komputer yang akan beralih dari fenomena fizik moden ke mekanik quantum, telah menjadikan kajian ke atas komputer quantum sesuatu yang menarik.

Pada masa kini, kesukaran pemecahan kod rahsia bergantung kepada penyelesaian kekompleksan matematik. Sebagai contoh, penentuan faktor dua nombor perdana. Jika dua nombor ini mempunyai digit yang begitu besar maka pemprosesan yang diperlukan dengan menggunakan komputer semasa akan melibatkan masa yang sangat panjang. Namun, semenjak kejayaan Shor (1997) mencipta teori algorima masa-polinomial, masalah pengiraan kekompleksan matematik ini menjadi mudah untuk diselesaikan dengan adanya penggunaan teknologi komputer quantum. Secara tidak langsung ianya telah mendorong kepada perkembangan bidang kriptografi quantum.

Kriptografi quantum diadaptasi daripada sifat-sifat mekanik quantum iaitu Prinsip Ketidakpastian Heisenberg (Wiesner 1983) dan Teorem Tiada-pengklonan (Wootters & Zurek 1982). Melalui sifat-sifat ini, kriptografi quantum dikatakan mampu menyelesaikan masalah utama dalam pembahagian kunci kerana dapat mengesan kehadiran musuh. Dengan

penggunaan satu lagi saluran komunikasi bersifat quantum, tahap keselamatan komunikasi menjadi lebih terjamin.

Protokol pertama yang mengaplikasikan konsep kriptografi quantum dikenali sebagai protokol BB84 (Bennett & Brassard 1984). Namanya diambil sempena dengan nama pencipta protokol tersebut iaitu Bennett dan Brassard pada tahun 1984. Kajian ini kemudiannya melibatkan pembangunan sistem simulasi bagi protokol ini dengan menggunakan komputer klasik. Satu perisian komputer yang berteraskan matematik digunakan, iaitu MATLAB (2011). Seterusnya, tahap ketepatan, keselamatan dan kecekapan protokol diuji.

PENYATAAN MASALAH

Kriptografi merupakan satu kajian yang berkaitan dengan penghantaran maklumat secara rahsia. Dengan perkembangan teknologi yang semakin pesat dan perubahan paradigma dalam pembangunan komputer yang akan beralih daripada fenomenon fizik moden kepada mekanik quantum, telah menjadikan kajian ke atas komputer quantum sesuatu yang menarik.

Terdapat kelemahan dalam kriptosistem moden yang mendorong kepada perkembangan bidang kriptografi quantum. Antaranya adalah seperti yang dinyatakan oleh Bennett dan Brassard (1984) iaitu pertama, teori maklumat telah menunjukkan bahawa kriptosistem kunci rahsia tidak akan menjadi selamat kecuali apabila kunci hanya digunakan sekali sahaja dan panjangnya mestilah sama dengan panjang mesej tersembunyi. Kedua, teknologi terkini dilihat semakin mampu untuk menyelesaikan pengiraan matematik yang rumit dalam masa yang lebih singkat.

Kriptografi quantum, diadaptasi daripada sifat-sifat mekanik quantum iaitu prinsip ketidakpastian Heisenberg (Wiesner 1983) dan teorem tiada-pengklonan (Wootters & Zurek 1982). Melalui sifat-sifat ini, kriptografi quantum dikatakan mampu menyelesaikan masalah utama dalam pembahagian kunci kerana dapat mengesan kehadiran musuh. Dengan penggunaan satu lagi saluran komunikasi bersifat quantum, tahap keselamatan komunikasi menjadi lebih terjamin.

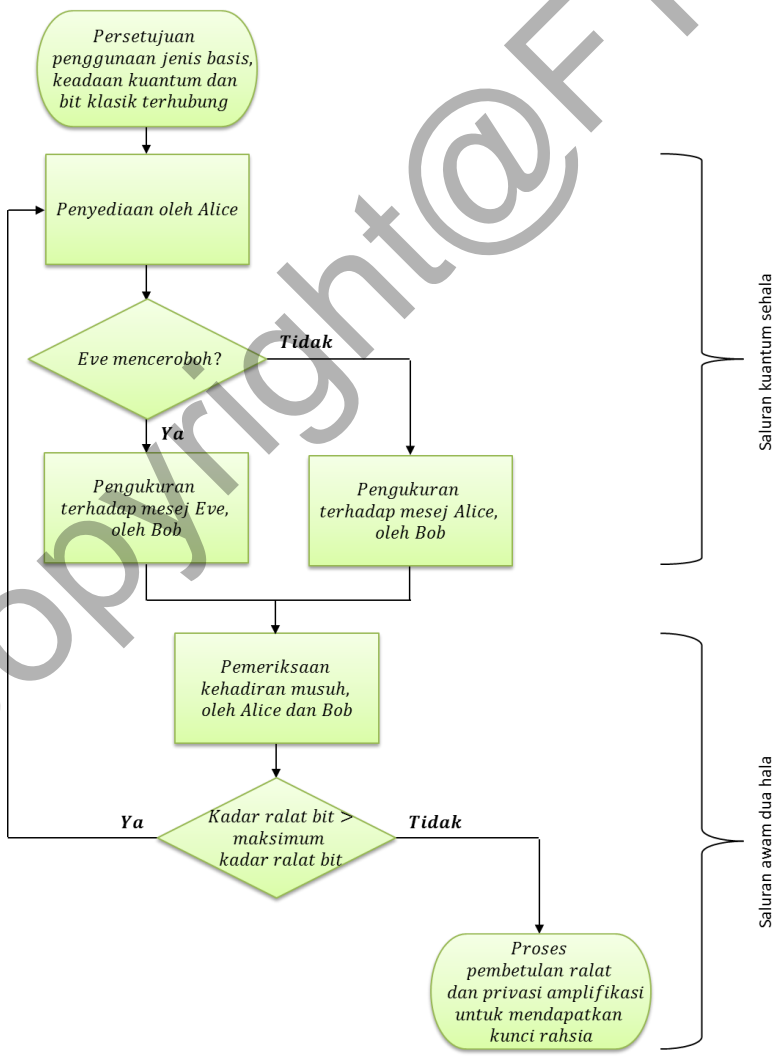
OBJEKTIF KAJIAN

Objektif projek ini ialah:

a) Membangunkan sebuah sistem simulasi protokol BB84 dengan menggunakan perisian MATLAB versi 7.12.
b) Menguji aspek ketepatan, keselamatan dan kecekapan simulasi protokol BB84 yang dibina.

METOD PEMBANGUNAN PROTOKOL BB84

Senario bagi simulasi protokol BB84 yang dibangunkan ini mengandaikan bahawa pengirim dan penerima mesej dikenali sebagai Alice dan Bob, manakala musuh yang mencerobohi komunikasi pula dikenali sebagai Eve. Proses pembinaan protokol ini terdiri daripada empat fasa utama, iaitu Penyediaan, Pencerobohan, Pengukuran dan Saluran Awam. Rujuk Rajah 1 bagi melihat carta alir fasa-fasa yang terlibat dalam protokol BB84 ini. Terdapat dua saluran komunikasi yang terlibat iaitu saluran komunikasi quantum dan saluran komunikasi awam.



Rajah 1 Carta alir fasa kajian protokol BB84

Fasa Penyediaan

Terlebih dahulu, diandaikan bahawa Alice dan Bob telah membuat persetujuan melalui komunikasi klasik berkenaan dengan hubungan di antara jenis basis, keadaaan-keadaan foton dan bit klasik bagi setiap satu basis yang akan digunakan dalam protokol BB84. Rujuk Jadual 1 bagi melihat contoh hubungan tersebut.

Jadual 1 Hubungan di antara basis, keadaan foton dan juga bit klasik

Basis	Keadaan foton	Bit klasik
+	$\|-\rangle$	0
	$\|\|\rangle$	1
×	$\|\backslash\rangle$	0
	$\|/\rangle$	1

Fasa penyediaan ini hanya melibatkan pengirim mesej iaitu Alice dengan menggunakan saluran komunikasi quantum sehala. Matlamat Alice adalah untuk menghantar mesej dalam bentuk foton yang diwakilkan sebagai qubit kepada Bob $\{|-\rangle, |\backslash\rangle, ||\rangle$ atau $|/\rangle\}$. Berikut merupakan langkah-langkah (pseudokod) yang diambil oleh Alice dalam penyediaan mesej kunci tersebut:

Langkah 1: Pilih bilangan bit n untuk dihantar sebagai mesej. Bilangan bit mestilah nombor genap. Contohnya,

$$n = 8.$$

Langkah 2: Pilih nilai maksimum kadar ralat bit $maxBER$. Nilai tersebut mestilah berada di antara 0 hingga 1. Contohnya,

$$maxBER = 0.2.$$

Langkah 3: Sediakan satu siri bit klasik secara rawak $bitA$, yang panjangnya adalah n. Contohnya,

$$bitA = 0\ 1\ 0\ 0\ 0\ 1\ 0\ 0$$

Langkah 4: Sediakan satu siri polarisasi basis secara rawak $basisA$, yang panjangnya adalah n. Contohnya,

$$basisA = \times\times\times\times + \times\times\times$$

Langkah 5: Menghasilkan satu siri polarisasi keadaan quantum, $qstateA$, berdasarkan setiap satu bit klasik dan basis yang disediakan. Rujuk Jadual 1 bagi mendapatkan hasil keadaan quantum. Contohnya, jika dilihat pada kedudukan pertama bit klasik dan basis yang disediakannya iaitu 0 dan '×'. Berdasarkan Jadual 1, keadaan quantum yang sepadan adalah '\'. Bagi keseluruhan keadaan quantum yang terhasil adalah,

$$qstateA = \backslash\ /\ \backslash\ \backslash - /\ \backslash\ \backslash$$

Langkah 6: Simpan $qstateA$ ke dalam fail untuk dihantar kepada Bob.

Secara keseluruhannya, langkah-langkah dalam fasa ini adalah hampir sama seperti yang dilakukan oleh Rednour, iaitu dalam fasa Alice. Walaubagaimanapun terdapat beberapa pertambahan langkah yang perlu diambil kira bagi memudahkan lagi proses dalam kajian ini. Langkah 1 adalah penting bagi memastikan bahawa panjang bilangan bit adalah sama untuk setiap kali siri bit klasik, polarisasi basis dan polarisasi keadaan quantum dihasilkan. Manakala Langkah 2 pula adalah penting bagi melakukan proses pembetulan ralat dalam fasa Saluran Awam nanti.

Fasa Pencerobohan

Fasa ini pula hanya melibatkan musuh, iaitu Eve, juga dengan menggunakan saluran komunikasi quantum sehala. Matlamat Eve adalah untuk mendapatkan seberapa banyak maklumat mengenai kunci. Berikut merupakan langkah-langkah yang diambil oleh Eve:

Langkah 1: Memilih sama ada ingin mencerobohi komunikasi ataupun tidak. Contohnya, ingin menceroboh.

Langkah 2: Membaca satu-persatu mesej yang sedang dihantar oleh Alice kepada Bob, iaitu $qstateA$.

Langkah 3: Menyediakan satu siri polarisasi basis secara rawak $basisE$, bagi setiap satu mesej yang dibaca dalam Langkah 2. Perlu diingatkan bahawa hanya Alice yang mengetahui jenis basis yang digunakannya. Contohnya,

$$basisE = + \times\times + \times + \times +$$

Langkah 4: Menghasilkan satu siri polarisasi keadaan quantum $qstateE$. Jika pemilihan basisnya tepat iaitu sama seperti Alice, maka keadaan quantum yang terhasil

akan sama seperti Alice. Namun jika sebaliknya, maka keadaan quantum yang terhasil menjadi rawak. Ini bermaksud terdapat dua jenis keadaan quantum yang mungkin terhasil bagi setiap satu basis yang dipilih salah dan kebarangkaliannya pula adalah 0.5 bagi setiap satu keadaan. Hal ini merujuk kepada sifat unik foton dalam mekanik quantum.

Sebagai contoh, lihat perbandingan pada kedudukan pertama bagi keadaan quantum Alice dengan basis Eve, iaitu '\' dan '+'. Dengan merujuk Jadual 1, basis yang dipilih oleh Eve '+' tidak mempunyai keadaan quantum yang dipilih oleh Alice '\'. Maka Eve telah membuat pemilihan basis yang salah. Oleh itu, keadaan quantum yang akan terhasil adalah secara rawak. Sama ada '−' ataupun '|' dan masing-masing berkebarangkalian sebanyak 0.5. Katakan dalam kes ini, keadaan quantum yang terhasil ialah'−'.

Lihat pula pada kedudukan kedua. Keadaan quantum Alice ialah '/' dan basis Eve ialah '×'. Diketahui bahawa basis Eve, '×' mempunyai keadaan quantum '/' seperti yang dihantar oleh Alice. Maka Eve telah memilih basis yang tepat. Hasilnya, keadaan quantum Eve menjadi sama seperti Alice. Berikut merupakan keseluruhan keadaan quantum Eve yang terhasil.

$$qstateE = - \; / \; \backslash \; - \; \backslash \; - \; \backslash \; |$$

Langkah 5: Menghasilkan satu siri bit klasik $bitE$, berdasarkan kepada keadaan quantum Eve yang terhasil tadi. Contohnya,

$$bitE = 0\;1\;0\;0\;0\;0\;0\;1$$

Langkah 6: Simpan $qstateE$ ke dalam fail untuk dibaca oleh Bob.

Dalam fasa kedua ini, langkah-langkah yang diambil adalah sama seperti yang dilakukan oleh Rednour dalam fasa *Eve*. Tiada sebarang perubahan yang dilakukan. Cuma pengguna boleh memilih sama ada ingin mencerobohi komunikasi dalam fasa ini ataupun tidak.

Fasa Pengukuran

Merupakan fasa terakhir dalam saluran quantum sehala. Langkah-langkah yang diambil dilakukan oleh penerima mesej, iaitu Bob. Matlamat Bob adalah untuk membaca mesej dari Alice dan membuat pengukuran terhadapnya {'×' atau '+'}.

Langkah 1: Baca satu-persatu mesej keadaan quantum yang sedang dihantar oleh Alice (atau Eve jika wujud).

Langkah 2: Sediakan satu siri polarisasi basis secara rawak, $basisB$, bagi setiap satu mesej yang dibaca dalam Langkah 1. Sama seperti Eve, Bob juga tidak mengetahui jenis basis yang digunakan oleh Alice. Contohnya,

$$basisB = \times\times + \times\times\times + +$$

Langkah 3: Menghasilkan satu siri polarisasi keadaan quantum $qstateB$ dengan cara membuat perbandingan di antara basis Bob dengan keadaan quantum yang diterimanya, sama ada daripada Alice ataupun Eve.

Katakan Eve tidak wujud. Maka proses yang dilakukan adalah sama seperti yang dilakukan oleh Eve dalam Langkah 4 fasa Pencerobohan.

Namun sekiranya Eve wujud, maka perbandingan yang dibuat adalah dengan keadaan quantum Eve. Ini bermaksud hasil keadaan quantum Bob bergantung kepada keadaan quantum Eve, bukannya Alice. Walaupun Bob telah membuat pilihan basis yang sama seperti Alice, namun setelah Eve membuat pemilihan basis yang salah, ia akan menjejaskan nilai foton tersebut. Kesannya, kebarangkalian penghasilan keadaan quantum dikurangkan kepada 0.25 bagi setiap satu keadaan.

Contoh keadaan quantum Bob yang terhasil adalah seperti berikut:

$$qstateB = / \; / \; - \; \backslash \; \backslash \; / \; | \; |$$

Langkah 4: Menghasilkan satu siri bit klasik $bitB$, berdasarkan kepada keadaan quantum Bob yang terhasil tadi.

$$bitB = 1\;1\;0\;0\;0\;1\;1\;1$$

Terdapat perbezaan yang diambil dalam fasa ini jika dibandingkan dengan fasa *Bob* yang dilakukan oleh Rednour. Perbezaan tersebut adalah pengasingan langkah seterusnya ke dalam fasa Saluran Awam. Ini bagi memudahkan proses komunikasi saluran awam dua hala.

Fasa Saluran Awam

Dalam fasa ini pula, komunikasi dijalankan melalui saluran awam dua hala. Fasa ini melibatkan komunikasi di antara Alice dan Bob. Matlamat mereka adalah untuk mengesan kehadiran Eve.

Langkah 1: Proses saringan kunci dijalankan. Bob membaca basis yang digunakan oleh Alice bagi setiap qubit.

Langkah 2: Sekiranya Alice dan Bob mendapati terdapatnya perbezaan basis yang mereka gunakan, maka bit klasik bagi basis tersebut akan dibuang. Sekiranya basis sama, maka bit tersebut akan dikekalkan. Bit-bit yang tinggal dipanggil sebagai kunci saringan.

Langkah 3: Alice memilih subset bagi kunci saringan secara rawak untuk diuji.

Langkah 4: Berdasarkan subset tersebut, perbandingan bit klasik kepunyaan Alice dan Bob dilakukan. Sekiranya didapati kesemua bit-bit tersebut adalah sama, maka kesimpulan yang boleh dibuat adalah Eve tidak mencerobohi komunikasi. Namun sekiranya terdapat perbezaan, maka Eve dikatakan mencerobohi komunikasi.

Sebagai contoh, rujuk Jadual 2 di bawah untuk melihat hasil daripada Langkah 1 hingga 4 ini.

Jadual 2 Hasil komunikasi dalam fasa Saluran Awam

bitA	0	1	0	0	0	1	0	0
basisA	×	×	×	×	+	×	×	×
basisB	×	×	+	×	×	×	+	+
bitB	1	1	0	0	0	1	1	1
basisA = basisB (Y/T)	Y	Y	T	Y	T	Y	T	T
Kunci saringan (Bob)	1	1		0		1		
Kunci saringan (Alice)	0	1		0		1		
Uji (Y/T)	Y	T		T		Y		

Lihat pada kedudukan pertama bit yang diuji, kunci saringan Bob didapati tidak sama dengan kunci saringan Alice. Maka kesimpulan yang boleh dinyatakan adalah Eve telah mencerobohi komunikasi.

Langkah 5: Alice dan Bob mengira kadar ralat bit masing-masing. Sekiranya didapati nilai tersebut melebihi nilai maksimum kadar ralat bit yang telah ditetapkan oleh Alice, maka mereka dinasihatkan untuk memberhentikan komunikasi ini dan memulakan semula protokol. Namun sekiranya kadar ralat bit berada di bawah tahap maksimum, maka mereka bolehlah meneruskan ke langkah seterusnya. Contohnya,

$$Kadar\ ralat\ bit = \frac{Jumlah\ bilangan\ bit\ diuji - Bilangan\ bit\ diuji\ tepat}{Jumlah\ bilangan\ bit\ diuji}$$

$$= \frac{1}{4} = 0.25$$

$$Kadar\ ralat\ bit = 0.25$$
$$maxBER = 0.2$$
$$\therefore Kadar\ ralat\ bit > maxBER$$

Komunikasi ditamatkan. Protokol dimulakan semula.

Langkah 6: Untuk nilai kadar ralat bit yang kurang daripada tahap maksimum, Alice dan Bob boleh mendapatkan kunci rahsia bersama dengan melakukan pembetulan ralat dan amplifikasi privasi. Langkah ini diabaikan dalam contoh ini.

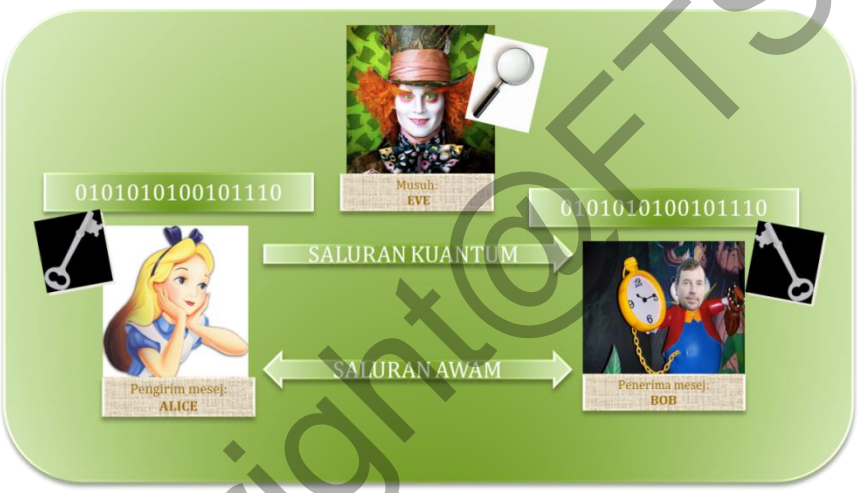
Namun dalam kajian ini, langkah terakhir (pembetulan ralat dan amplifikasi privasi) tidak dilakukan secara mendalam. Ini kerana terdapat pelbagai kaedah lain yang mungkin lebih stabil untuk diaplikasikan.

Secara kesimpulannya, terdapat beberapa perbezaan langkah yang diambil jika dibandingkan dengan fasa *Bob* yang dilakukan oleh Rednour. Rednour membuat keputusan setelah sampai pada Langkah 4. Namun bagi kajian ini, adalah penting untuk melakukan Langkah 5 dan Langkah 6. Maklumat kadar ralat bit perlu dipertimbangkan untuk ke proses menetapkan kunci rahsi yang bebas sepenuhnya daripada pengetahuan Eve.

PELAKSANAAN SISTEM SIMULASI PROTOKOL BB84

Bahagian ini membincangkan hasil kajian iaitu satu simulasi dengan memberikan dua contoh situasi. Situasi pertama adalah dengan ketiadaan musuh, manakala kedua adalah dengan kehadiran musuh. Simulasi dibangunkan menggunakan MATLAB.

Untuk memudahkan lagi pemahaman mengenai protokol ini, adalah penting sekiranya watak-watak yang terlibat diperkenalkan. Secara umumnya, pengirim dan penerima mesej, masing-masing dikenali sebagai Alice dan Bob. Manakala musuh yang cuba mencerobohi komunikasi pula dikenali sebagai Eve. Komunikasi di antara Alice dan Bob melibatkan dua saluran, iaitu dimulai dengan saluran komunikasi kuantum sehala, dan kemudiannya saluran komunikasi awam dua-hala. Rajah 2 menunjukkan komunikasi bagi protokol BB84.

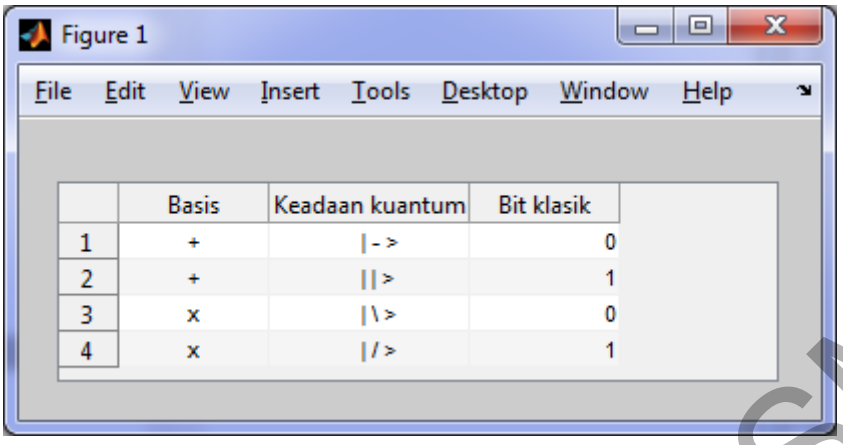


Rajah 2 Senario komunikasi protokol BB84

Pelaksanaan Protokol BB84 Tanpa Kehadiran Musuh

Fasa Penyediaan

Setelah membuat persetujuan mengenai jenis basis, keadaan kuantum dan bit klasik yang terhubung, maka Rajah 3 dihasilkan sebagai maklumat.



Rajah 3 Hubungan di antara basis, keadaan kuantum dan juga bit klasik

Seterusnya, langkah-langkah berikut diambil oleh Alice.

Langkah 1: Pilih bilangan bit, n untuk dihantar sebagai mesej. Bilangan bit mestilah nombor genap. Sekiranya nombor yang dipilih adalah nombor ganjil, maka mesej ralat akan dipaparkan.

Langkah 2: Pilih nilai maksimum bagi kadar ralat bit, $maxBER$. Nilai tersebut mestilah berada di antara 0 hingga 1. Sekiranya nilai berada di luar kadar, maka mesej ralat akan dipaparkan.

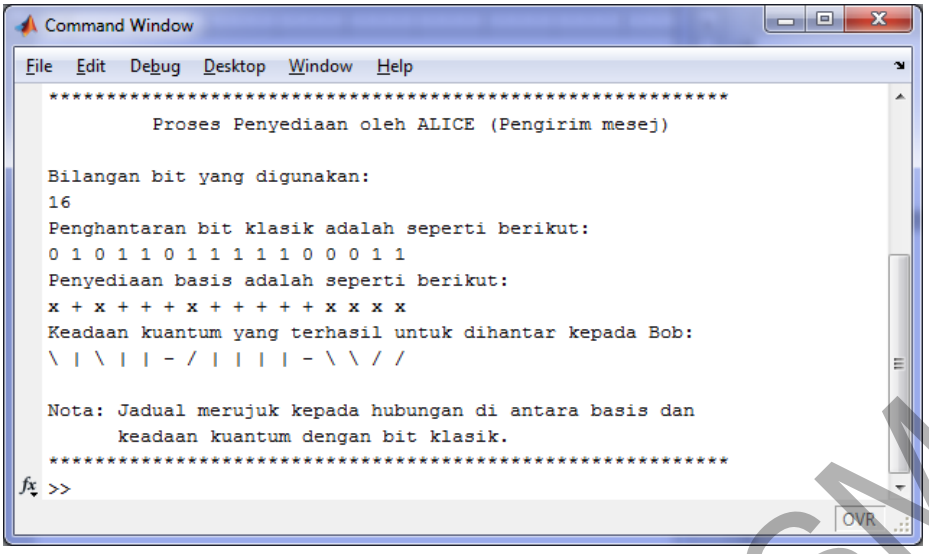
Langkah 3: Sediakan satu siri bit klasik secara rawak $bitA$, yang panjangnya adalah n.

Langkah 4: Sediakan satu siri polarisasi basis secara rawak $basisA$, yang panjangnya adalah n.

Langkah 5: Menghasilkan satu siri polarisasi keadaan kuantum $qstateA$, berdasarkan setiap satu bit klasik dan basis yang disediakan. Rujuk Jadual 2 bagi mendapatkan hasil keadaan kuantum.

Output bagi Langkah 3 hingga 5 adalah seperti dalam Rajah 4.

Langkah 6: Simpan $qstateA$ ke dalam fail bernama qstateA.mat untuk dihantarkan kepada Bob.



Rajah 4 Output bagi Langkah 3 hingga 5 dalam fasa Penyediaan protokol BB84 tanpa kehadiran musuh

Fasa Pencerobohan

Langkah-langkah yang diambil oleh Eve adalah seperti berikut:

Langkah 1: Memilih sama ada ingin mencerobohi komunikasi ataupun tidak. Sekiranya perlu, maka masukkan aksara 'Y' atau 'y'. Jika sebaliknya, maka masukkan pula aksara 'T' atau 't'. Jika aksara lain yang dimasukkan, maka mesej ralat akan dipaparkan.

Fasa Pengukuran

Bob pula mengambil langkah-langkah seperti berikut:

Langkah 1: Baca satu-persatu mesej keadaan kuantum yang sedang dihantar oleh Alice (atau Eve jika wujud).

Langkah 2: Sediakan satu siri polarisasi basis secara rawak $basisB$, bagi setiap satu mesej yang dibaca dalam Langkah 1.

Langkah 3: Menghasilkan satu siri polarisasi keadaan kuantum $qstateB$, dengan cara membuat perbandingan di antara basis Bob dengan keadaan kuantum yang diterimanya, sama ada daripada Alice ataupun Eve. Dalam kes ini, perbandingan dibuat dengan keadaan kuantum Alice.

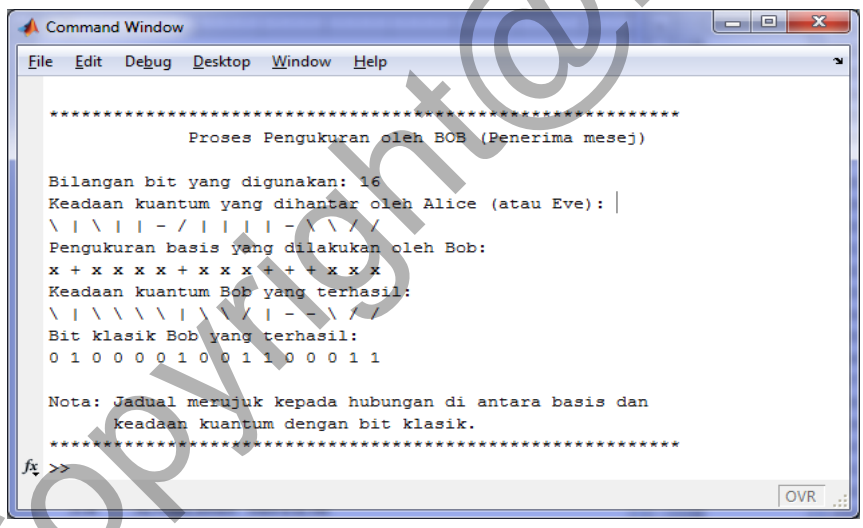
Langkah 4: Menghasilkan satu siri bit klasik $bitB$, berdasarkan kepada keadaan kuantum Bob yang terhasil. Rujuk Rajah 5 bagi melihat output Langkah 1 hingga 4.

Fasa Saluran Awam

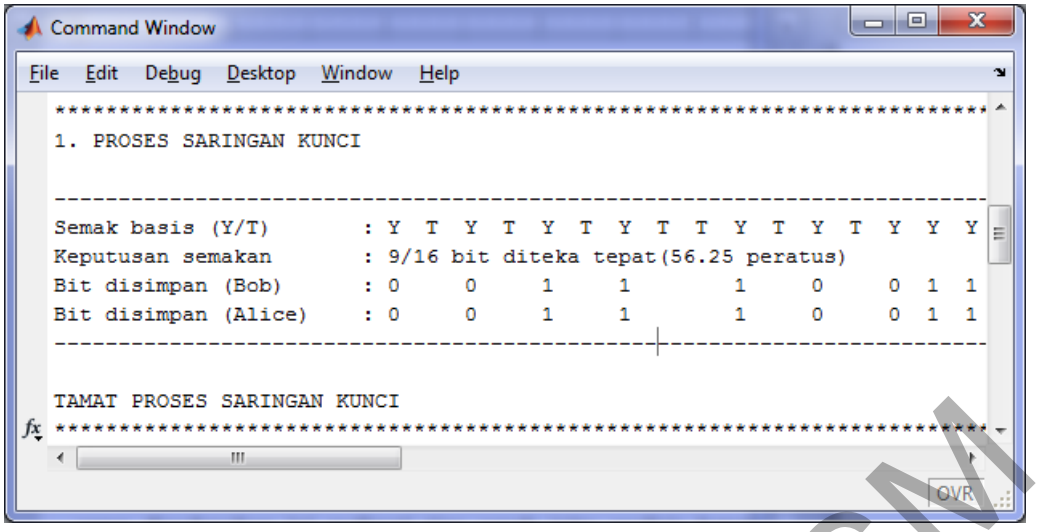
Langkah 1: Proses saringan kunci dijalankan. Bob membaca basis yang digunakan oleh Alice bagi setiap qubit.

Langkah 2: Sekiranya Alice dan Bob mendapati terdapatnya perbezaan basis yang mereka gunakan, maka bit klasik bagi basis tersebut akan dibuang. Sekiranya basis sama, maka bit tersebut akan dikekalkan. Bit-bit yang tinggal dipanggil sebagai kunci saringan. Aksara 'Y' untuk pemilihan basis yang tepat, manakala 'T' adalah sebaliknya.

Output bagi Langkah 1 dan 2 boleh dirujuk dalam Rajah 6.



Rajah 5 Output bagi Langkah 1 hingga 4 dalam fasa Pengukuran protokol BB84 tanpa kehadiran musuh



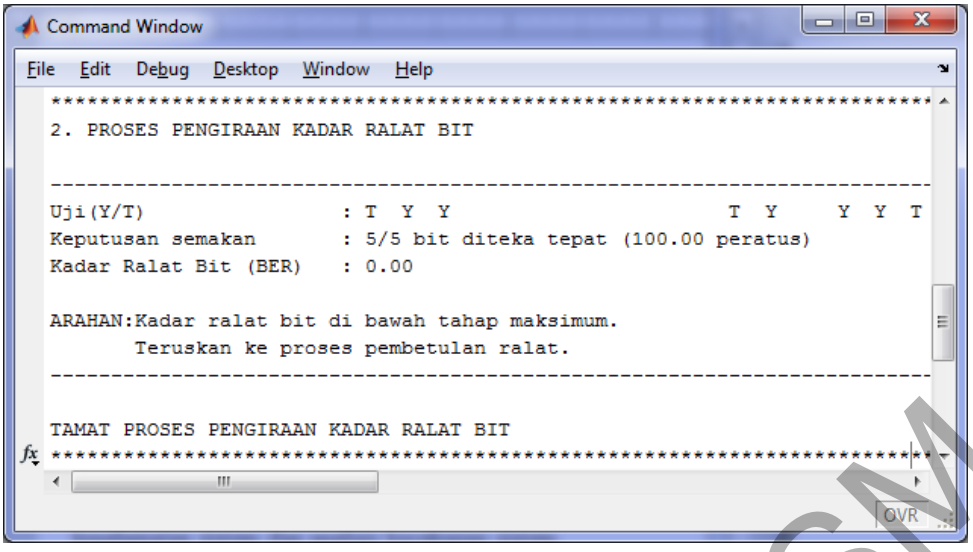
Rajah 6 Output bagi Langkah 1 dan 2 dalam fasa Saluran Awam protokol BB84 tanpa kehadiran musuh

Langkah 3: Alice memilih subset bagi kunci saringan secara rawak untuk diuji. Aksara 'Y' untuk diuji, manakala 'T' untuk diabaikan.

Langkah 4: Berdasarkan subset tersebut, perbandingan bit klasik kepunyaan Alice dan Bob dilakukan. Sekiranya didapati kesemua bit-bit tersebut adalah sama, maka kesimpulan yang boleh dibuat adalah Eve tidak mencerobohi komunikasi. Namun sekiranya terdapat perbezaan, maka Eve dikatakan mencerobohi komunikasi.

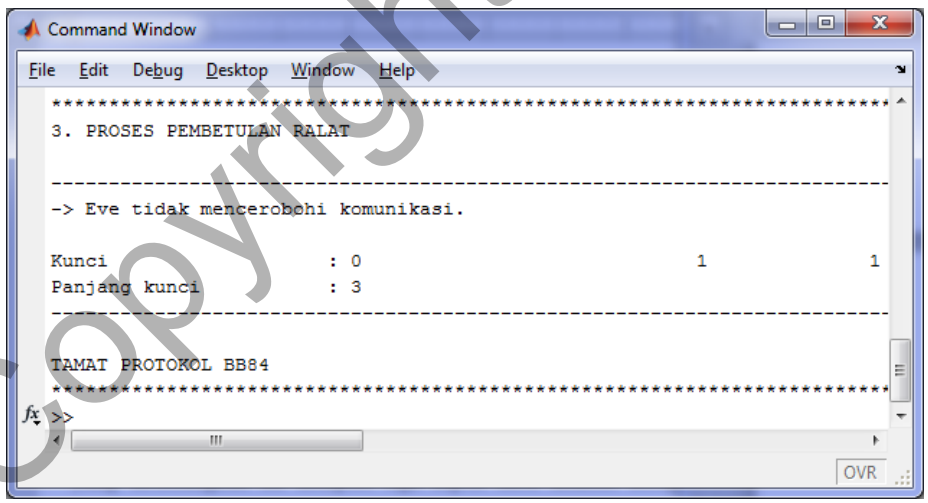
Langkah 5: Alice dan Bob mengira kadar ralat bit masing-masing. Sekiranya didapati nilai tersebut melebihi nilai maksimum kadar ralat bit yang telah ditetapkan oleh Alice, maka mereka dinasihatkan untuk memberhentikan komunikasi ini dan memulakan semula protokol ini. Namun sekiranya kadar ralat bit berada di bawah tahap maksimum, maka mereka bolehlah meneruskan ke langkah seterusnya.

Output bagi Langkah 3 hingga 5 adalah seperti dalam Rajah 7.



Rajah 7 Output bagi Langkah 3 hingga 5 dalam fasa Saluran Awam protokol BB84 tanpa kehadiran musuh

Langkah 6: Bagi nilai kadar ralat bit yang kurang daripada tahap maksimum, Alice dan Bob mendapatkan kunci rahsia bersama dengan melakukan pembetulan ralat dan amplifikasi privasi. Rujuk Rajah 8 bagi melihat output langkah ini.



Rajah 8 Output Langkah 6 dalam fasa Saluran Awam protokol BB84 tanpa kehadiran musuh

Pelaksanaan Protokol BB84 Dengan Kehadiran Musuh

Fasa Penyediaan

Langkah 1: Alice memilih bilangan bit, n untuk dihantar sebagai mesej. Bilangan bit mestilah nombor genap. Sekiranya nombor yang dipilih adalah nombor ganjil, maka mesej ralat akan dipaparkan.

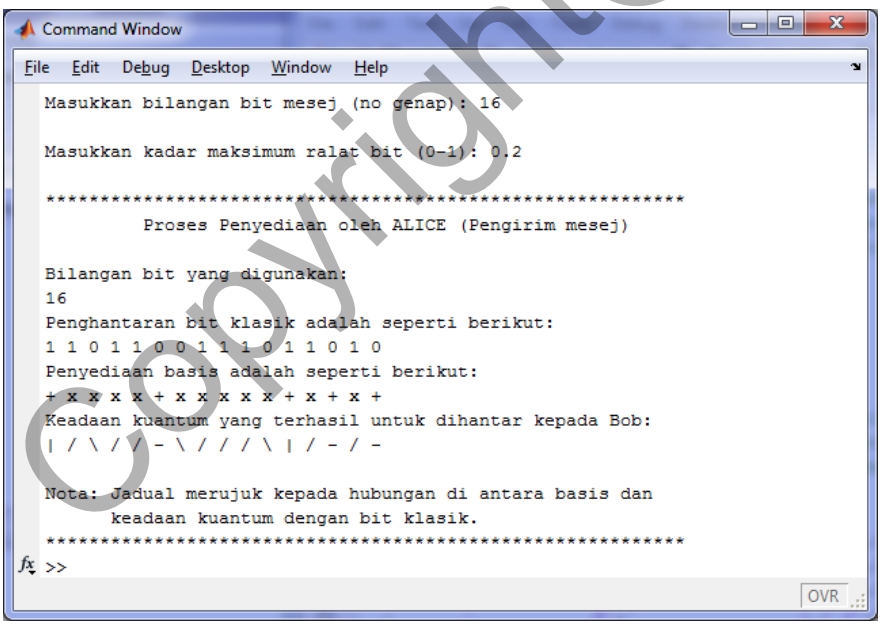
Langkah 2: Alice memilih nilai maksimum kadar ralat bit, $maxBER$. Nilai tersebut mestilah berada di antara 0 hingga 1. Sekiranya nilai berada di luar kadar, maka mesej ralat akan dipaparkan.

Langkah 3: Alice menyediakan bit klasik secara rawak, $bitA$, yang panjangnya adalah n.

Langkah 4: Alice menyediakan polarisasi basis secara rawak, $basisA$, yang panjangnya adalah n.

Langkah 5: Alice menghasilkan polarisasi keadaan kuantum $qstateA$ berdasarkan setiap satu bit klasik dan basis yang disediakan. Rujuk Jadual 2 bagi mendapatkan hasil keadaan kuantum.

Output bagi Langkah 3 hingga 5 adalah seperti dalam Rajah 9.



Rajah 9 Output bagi Langkah 3 hingga 5 dalam fasa Penyediaan protokol BB84 dengan kehadiran musuh

Langkah 6: Alice simpan $qstateA$ ke dalam fail bernama qstateA.mat untuk dihantarkan kepada Bob.

Fasa Pencerobohan

Langkah 1: Eve memilih sama ada ingin mencerobohi komunikasi ataupun tidak. Sekiranya perlu, maka masukkan aksara 'Y' atau 'y'. Jika sebaliknya, maka masukkan pula aksara 'T' atau 't'. Jika aksara lain yang dimasukkan, maka mesej ralat akan dipaparkan. Untuk bahagian ini, katakan bahawa Eve mencerobohi komunikasi ini.

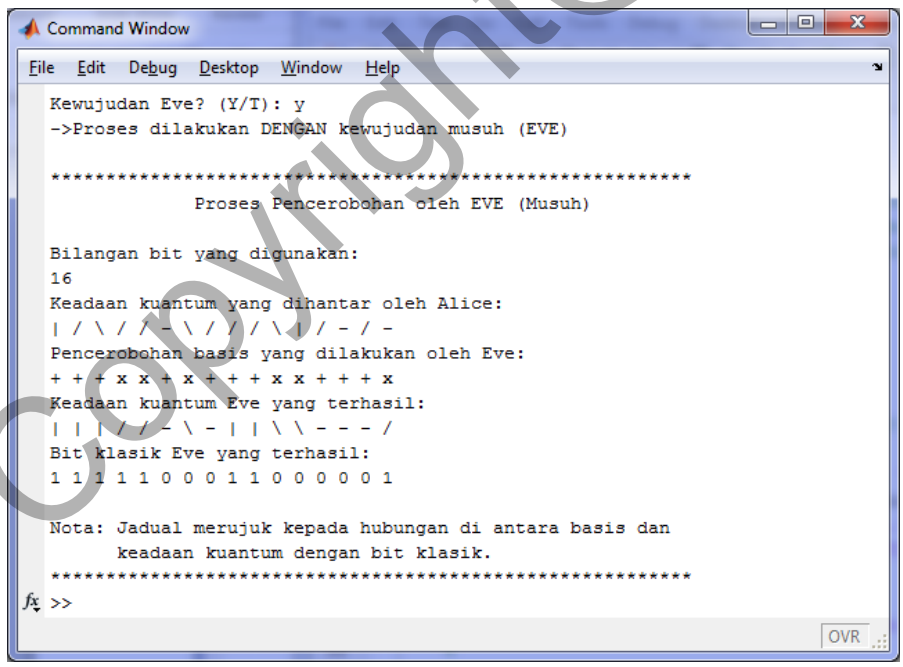
Langkah 2: Membaca satu-persatu mesej yang sedang dihantar oleh Alice kepada Bob, iaitu $qstateA$.

Langkah 3: Menyediakan satu siri polarisasi basis secara rawak $basisE$, bagi setiap satu mesej yang dibaca dalam Langkah 2.

Langkah 4: Menghasilkan satu siri polarisasi keadaan kuantum $qstateE$.

Langkah 5: Menghasilkan satu siri bit klasik $bitE$, berdasarkan kepada keadaan kuantum Eve yang terhasil tadi.

Rujuk Rajah 10 bagi melihat output Langkah 1 hingga 5.



Rajah 10 Output bagi Langkah 1 hingga 5 dalam fasa Pencerobohan protokol BB84 dengan kehadiran musuh

Langkah 6: Simpan $qstateE$ ke dalam fail qsateE.mat untuk dibaca oleh Bob.

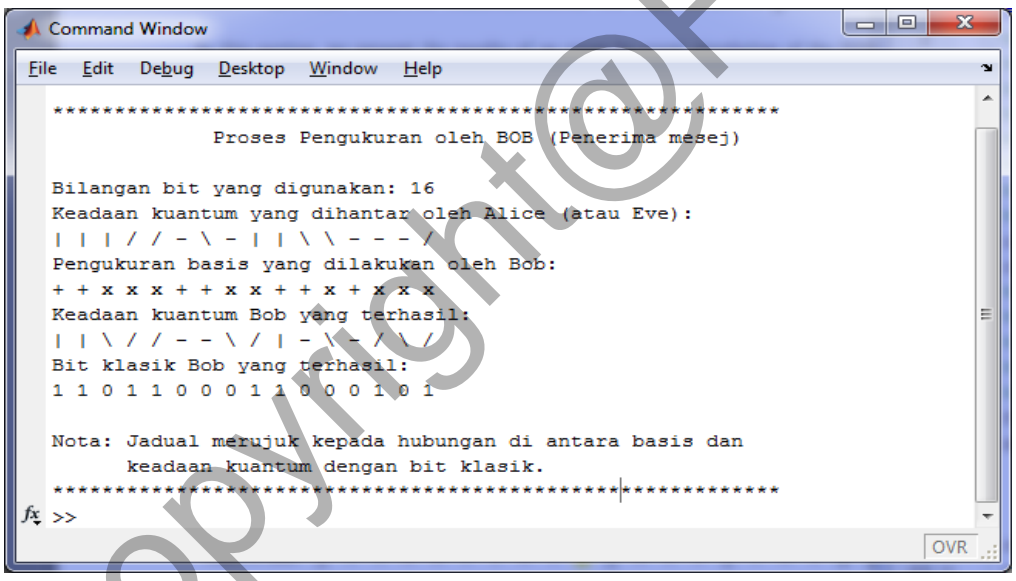
Fasa Pengukuran

Langkah 1: Bob baca satu-persatu mesej keadaan kuantum yang sedang dihantar oleh Alice (atau Eve jika wujud).

Langkah 2: Bob sediakan satu siri polarisasi basis secara rawak $basisB$, bagi setiap satu mesej yang dibaca dalam Langkah 1.

Langkah 3: Menghasilkan satu siri polarisasi keadaan kuantum $qstateB$ dengan cara membuat perbandingan di antara basis Bob dengan keadaan kuantum yang diterimanya, sama ada daripada Alice ataupun Eve. Dalam kes ini, perbandingan dibuat dengan keadaan kuantum Eve.

Langkah 4: Menghasilkan satu siri bit klasik $bitB$, berdasarkan kepada keadaan kuantum Bob yang terhasil tadi. Rujuk Rajah 11 bagi melihat output Langkah 1 hingga 4.



Rajah 11 Output bagi Langkah 1 hingga 4 dalam fasa Pengukuran protokol BB84 dengan kehadiran musuh

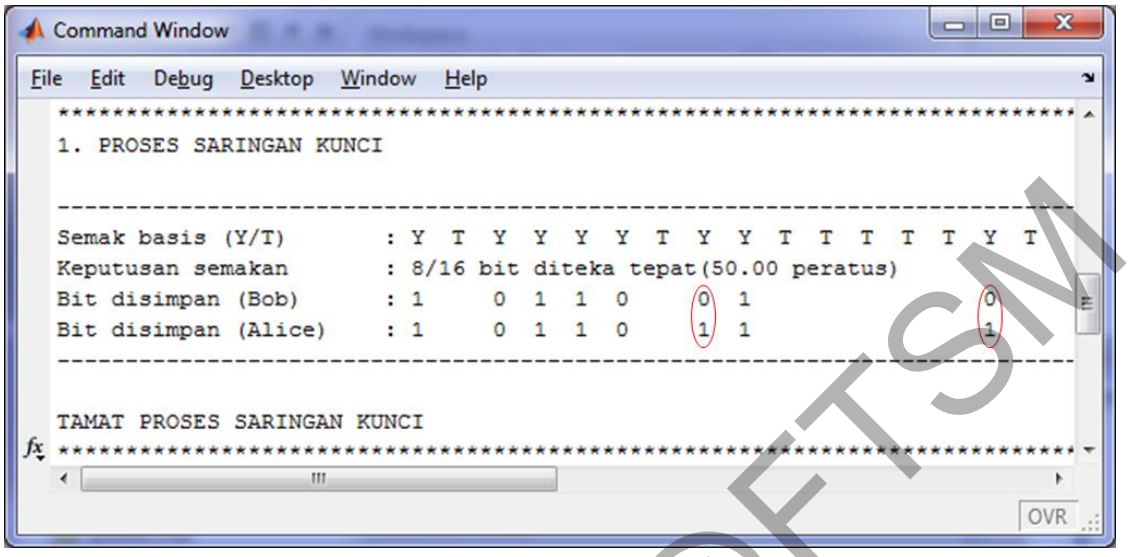
Fasa Saluran Awam

Langkah 1: Proses saringan kunci dijalankan. Bob membaca basis yang digunakan oleh Alice bagi setiap qubit.

Langkah 2: Sekiranya Alice dan Bob mendapati terdapatnya perbezaan basis yang mereka gunakan, maka bit klasik bagi basis tersebut akan dibuang. Sekiranya basis

sama, maka bit tersebut akan dikekalkan. Bit-bit yang tinggal dipanggil sebagai kunci saringan.

Output bagi Langkah 1 dan 2 boleh dirujuk dalam Rajah 12 di bawah.



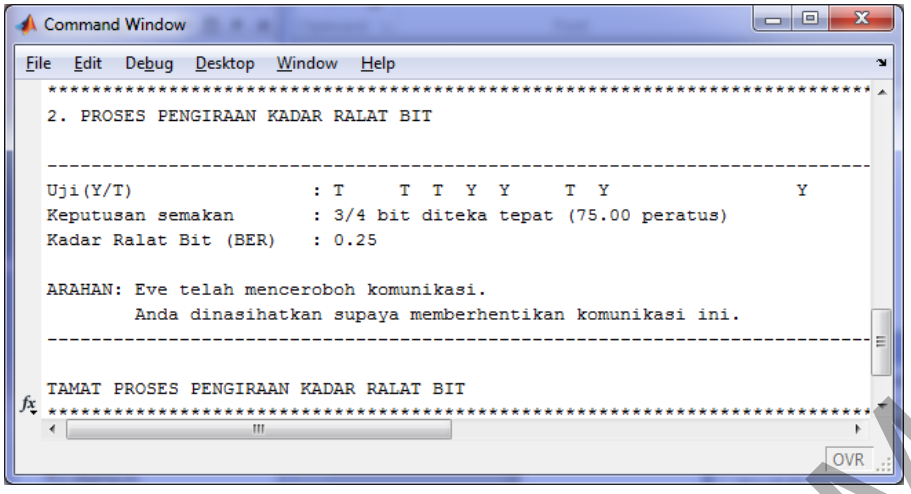
Rajah 12 Output bagi Langkah 1 dan 2 dalam fasa Saluran Awam protokol BB84 dengan kehadiran musuh

Langkah 3: Alice memilih subset bagi kunci saringan secara rawak untuk diuji.

Langkah 4: Berdasarkan subset tersebut, perbandingan bit klasik kepunyaan Alice dan Bob dilakukan. Sekiranya didapati kesemua bit-bit tersebut adalah sama, maka kesimpulan yang boleh dibuat adalah Eve tidak mencerobohi komunikasi. Namun sekiranya terdapat perbezaan, maka Eve dikatakan mencerobohi komunikasi.

Langkah 5: Alice dan Bob mengira kadar ralat bit masing-masing. Sekiranya didapati nilai tersebut melebihi nilai maksimum kadar ralat bit yang telah ditetapkan oleh Alice, maka mereka dinasihatkan untuk memberhentikan komunikasi ini dan memulakan semula protokol ini. Namun sekiranya kadar ralat bit berada di bawah tahap maksimum, maka mereka bolehlah meneruskan ke langkah seterusnya.

Output bagi Langkah 3 hingga 5 adalah seperti dalam Rajah 13 berikut:



Rajah 13 Output bagi Langkah 3 hingga 5 dalam fasa Saluran Awam protokol BB84 dengan kehadiran musuh

Langkah 6: Bagi nilai kadar ralat bit yang kurang daripada tahap maksimum, Alice dan Bob mendapatkan kunci rahsia yang diyakini bersama dengan melakukan pembetulan ralat dan amplifikasi privasi.

KESIMPULAN

Projek penyelidikan ini memfokus kepada pembangunan simulasi protokol BB84 (dengan dan tanpa kehadiran musuh) dengan menggunakan perisian komputer berteraskan matematik, iaitu MATLAB versi 7.12. Sistem simulasi yang dibangunkan ini bertujuan untuk melihat keupayaan sifat mekanik quantum seperti prinsip ketidakpastian Heisenberg dan teorem tiada-pengklonan dalam penghasilan kunci yang bebas daripada serangan musuh.

Antara kelebihan yang terdapat dalam sistem ini adalah seperti berikut:

a) Penambahbaikan dalam penghasilan kunci rahsia yang lebih tepat terutama bagi situasi ketiadaan musuh.

b) Dapat memastikan bahawa kunci yang terhasil selamat daripada gangguan musuh.

c) Capaian sistem yang mudah dan teratur.

RUJUKAN

Benatti, F., Fannes, M., Floreanini, R. & Petritis, D. 2010. *Quantum Information, Computation and Cryptography: An Introductory Survey of Theory, Technology and Experiments, Lecture Notes in Physics, Volume 808.* Berlin: Springer.

Benenti, G., Casati, G. & Strini, G. 2004. *Principles of Quantum Computation and Information, Volume I: Basic Concepts.* Singapura: World Scientific.

Bennett, C.H. & Brassard, G. 1984. Quantum cryptography: Public-key distribution and coin tossing. *In Proceedings of IEEE International Conference on Computers, Systems and Signal Processing, Bangalore, India*, hlm. 175-179.

Bennett, C.H., Bessette, F., Brassard, G., Salvail, L. & Smolin, J. 1991. Experimental quantum cryptography. *Journal of Cryptology* 5(1): 3-28.

Bruss, D., Erd´elyi, G., Meyer, T., Riege, T. & Rothe, J. 2007. Quantum cryptography: A survey. *ACM Comput. Surv.* 39(2): 1-27.

Díaz-Rodríguez, C.A., Olivares-Robles, M.A. & Juárez, A. 2011. An overview of quantum cryptography: Simulation. *IEEE Trans. Inform. Theory* 316-321.

Diffie, W. & Hellman, M. 1976. New directions in cryptography. *IEEE Trans. Inform. Theory* 22(6): 644-654.

Kollmitzer, C. & Pivk, M. 2010. *Applied Quantum Cryptography. Volume 797 of Lecture Notes in Physics*. Berlin: Springer.

MATLAB. 2011. Version 7.12. MathWorks, Inc.

Ouchao, B. & El Kinani, E.H. 2011. Statistical analysis of common qubits between Alice and Bob in BB84 protocol. *Contemporary Engineering Sciences* 4(8): 363-370.

Rednour, S. t.th. An applied simulation of quantum cryptography and an examination of a component of a quantum cryptography apparatus. Laporan projek penyelidikan program sarjana John C. Young. Centre College.

Rivest, R., Shamir, A. & Adleman, L. 1978. A method for obtaining digital signature and public-key. *Communications of the ACM* 21(2): 120-126.

Shuang, Zhao. 2009. Event-based simulation of quantum phenomena. Tesis Ph.D. University of Groningen.

Wiesner, S. 1983. Conjugate Coding. *Sigact News* 15(1): 78-88.

Wootters, W.K. & Zurek, W.H. 1982. A single quantum cannot be cloned. *Nature* 299: 802-803.

Wright, D. 2007. The RSA algorithm. http://imps.mcmaster.ca/courses/SE-4C03-07/wiki/wrighd/rsa_alg.html [15 Jun 2012].