UNIVERSIDAD SIMÓN BOLÍVAR

DPTO. DE ELECTRÓNICA Y CIRCUITOS

DISTRIBUCIÓN DE LLAVES CUÁNTICAS

Presentación 1:

BB92 Protocol

Autor:

Ángel Álvarez

16-10031

Febrero, 2022

1. Preliminares

Entendamos que Alice y Bob son dos entes que desean establecer una llave aleatoria entre ellos. Si utilizan un canal clásico no tienen forma de saber si existe algún ente extraño que les este robando la información. Por suerte, en un canal cuántico es imposible copiar los qubits desconocidos o medirlos sin dejar rastro.

Este protocolo es una versión más libre de su primera y popular versión de 1984, llamado protocolo BB84. En esencia, la idea es igual. Ambos hacen uso del hecho que medir un estado cuántico cambia el estado irremediablemente como herramienta para proteger la información.

El proceso tiene dos versiones: una donde Alice y Bob comparten pares EPR previamente entrelazados y otra donde Alice prepara estados individuales y luego los envía a Bob. Ambos casos serán tratados, pero primero hay que entender el protocolo original; BB84.

2. BB84 Protocol

2.1. Bases

1a. En la versión EPR, con pares EPR previamente entrelazados y distribuidos entre Alice y Bob. Alice escoge bases ortogonales de manera aleatoria para medir un miembro de cada par EPR luego de que sean distribuidos. Generalmente son las bases:

$$\begin{aligned} X &: |+\rangle \ , \ |-\rangle \, , \\ Z &: |0\rangle \ , \ |1\rangle \, . \end{aligned} \tag{1}$$

Debido a la medida de Alice en su miembro del par EPR, esto hará colapsar el otro par de Bob. El esquema de codificación que utilizarán es conocido entre ambos previa la comunicación.

1b. En la versión no-EPR, Alice prepara una secuencia aleatoria de bits codificándolos en una secuencia de qubits. Luego, Alice genera una secuencia de bases

ortogonales, generalmente X y Z. Mide uno a uno los qubits con su respectivo proyector y se los envía a Bob.

2. Bob decide medir aleatoriamente en una secuencia de las bases X y Z los estados que el posee. Mantiene los resultados de sus medidas en privado.

3. Alice y Bob comparan públicamente las bases que usaron, dejando únicamente aquella información donde coincidan entre los dos las bases usadas.

4. Alice y Bob proceden a revisar sus datos. Deciden sacrificar aleatoriamente parte de los bits de la llave para asegurar que coinciden perfectamente. De existir discrepancia es muy probable que exista un ente externo interviniendo en la distribución y abortan esa llave. Este proceso lo repiten varias veces hasta asegurar.

2.2. Ejemplo numérico

Supongamos que el esquema de codificación es:

$$\begin{aligned} |0\rangle &\to 0, \\ |1\rangle &\to 1, \\ |+\rangle &\to 0, \\ |-\rangle &\to 1. \end{aligned} \tag{2}$$

La llave generada por Alice es:

$$1001010110, \tag{3}$$

que codificado en qubits sería:

$$|1001010110\rangle\,. \tag{4}$$

Y que las bases que generó son:

$$XXZZXZXZXZ. \tag{5}$$

Si hacemos pasar la llave por dichas bases, lo que recibe Bob sera:

$$|- + 01 + 1 + 1 - 0\rangle\,. \tag{6}$$

Ahora, Bob genera sus bases para medir:

$$XZXZZZXXZZ \tag{7}$$

Bob realiza la medida obteniendo:

$$\begin{aligned}
|-\rangle &\xrightarrow{X} 1\\
|+\rangle &\xrightarrow{Z} ?\\
|0\rangle &\xrightarrow{X} ?\\
|1\rangle &\xrightarrow{Z} 1\\
|+\rangle &\xrightarrow{Z} ?\\
|1\rangle &\xrightarrow{Z} 1\\
|+\rangle &\xrightarrow{X} 0\\
|1\rangle &\xrightarrow{X} ?\\
|-\rangle &\xrightarrow{Z} ?\\
|0\rangle &\xrightarrow{Z} 0
\end{aligned} \tag{8}$$

Dejando la cadena de bits: 1??1?10??0.

Los resultados con ? significan que Bob no puede asegurar que bit obtuvo. Es más fácil ver esto con un ejemplo.

Supongamos que el estado que Alice mandó fue $|+\rangle$, codifico un 1, y Bob escogió la base de Z para medir. Es decir aplico la medida proyectiva P_0 o P_1 a $|+\rangle$, asumamos que usa P_0, ahora la probabilidad de hallar 0 como resultado de dicha medida es:

$$
\begin{aligned}
|c_0|^2 &= \langle +| P_0 |+\rangle = \langle +| \left(|0\rangle \langle 0|\right) |+\rangle , \\
&= \frac{1}{\sqrt{2}}(\langle 0| + \langle 1|)(|0\rangle \langle 0|)\frac{1}{\sqrt{2}}(|0\rangle + |1\rangle), \\
&= \frac{1}{2}(\langle 0|0\rangle + \langle 1|0\rangle)(\langle 0|0\rangle + \langle 0|1\rangle), \\
&= \frac{1}{2}(1+0)(1+0), \\
&= \frac{1}{2}.
\end{aligned} \tag{9}
$$

Es de esperarse que entonces obtengamos 1 tambien con 1/2 de probabilidad. Lo que no le permite a Bob discernir entre si Alice quizo mandar 0 o 1.

Sin embargo, Bob no sabe esto. Bob obtiene un valor con su medida, solamente cuando Alice le hace saber cuales fueron las bases que ella uso que el puede clasificar las sus resultados. Después de hacer pública las bases usas la cadena de bits es: 11100

Luego, ambos deciden seleccionar parte de los datos para confirmar perfectamente que los datos son los correctos. Supongamos que seleccionan dos bits aleatorios de la cadena de bits anteriores, lo que deja la llave compartida entre ambos así: 1100.

Este proceso se repite n veces hasta asegurar que el canal es seguro y confiable. La siguiente tabla resume el proceso:

Bits de Alice	1	0	0	1	0	1	0	1	1	0
Bases de Alice	X	X	Z	Z	X	Z	X	Z	X	Z
Estado de Alice	$\|-\rangle$	$\|+\rangle$	$\|0\rangle$	$\|1\rangle$	$\|+\rangle$	$\|1\rangle$	$\|+\rangle$	$\|1\rangle$	$\|-\rangle$	$\|+\rangle$
Bases de Bob	X	Z	X	Z	Z	Z	X	X	Z	Z
Bits de Bob	1	?	?	1	?	1	0	?	?	0
Comparación	1			1		1	0			0
Verificación				1						
Llave final	1					1	0			0

Cuadro 1: Proceso de Distribución de llave en el protocolo BB84.

2.3. Análisis de seguridad

En la versión de pares EPR compartidos la seguridad es absoluta. Si un intruso intentara interceptar el miembro que se le envía a Bob, Bob al no recibirlo la comunicación no continuaría. Debido a que la codificación ocurre luego de la repartición la información es teleportada a Bob inmediatamente y no existe forma de interceptarla.

En la versión no-EPR requiere un análisis más detallado y es mejor verlo con un ejemplo.

Supongamos que existe un tercer ente llamado Eve cuyo propósito es robar la llave que Alice le quiere enviar a Bob sin ser detectado. Eve se propone interceptar los estados enviados de Alice a Bob por el canal cuántico, medirlos y reenviarlos a Bob. Como Alice anuncia públicamente cuales bases utilizo ella, es sencillo entonces para Eve obtener exactamente el mismo resultado que obtendría Bob. Veamos todos los posibles casos:

Supongamos que Alice envia el estado $|+\rangle$, codificando un 0.

- Alice, Eve y Bob usaron la misma base para medir:

  En este caso Eve mide en X con $1/2$ de probabilidad, descifrando un 0. Como midió en la misma base original el estado no cambia y a Bob le llega el mismo $|+\rangle$. Luego Bob mide también en X con una probabilidad de $1/2$, obteniendo exitosamente un 0. Luego de la publicación de las bases, Alice, Eve y Bob comparan resultados y al coincidir los de Alice y Bob la información es guardada. Eve logra robar la información sin ser detectada exitosamente.

- Alice y Eve usaron la misma base pero Bob una diferente:

  Eve mide en X con una probabilidad de $1/2$, descifrando un 0 sin cambiar el estado. Aquí la información es descartada a finalizar el proceso pues las bases de Alice y Bob son diferentes. Eve no logra robar la información pero sigue sin ser detectada.

- Eve y Bob usaron la misma base pero Alice una diferente:

Eve mide en Z, descifrando un 0 o 1 con 1/2 de probabilidad. En este caso el estado que sale de Eve colapso a uno muy diferente del que envio Alice. Bob tambien utiliza Z obteniendo el mismo resultado de Eve. Como las bases de Alice y Bob no coinciden la información es descartada. Eve no logra robar la informacion pero no es detectada.

- Alice y Bob usaron la misma base y Eve una diferente:

  Eve mide en Z, descifrando un 0 o 1 y haciendo colapsar el estado a $|0\rangle$ o $|1\rangle$ con 1/2 de probabilidad respectivamente. Ahora Bob utiliza la base X igual que Alice, pero lo que el recibe es el estado $|0\rangle$ o $|1\rangle$. Veamos que ocurre con las probabilidades:

  Asumamos que la medida proyectiva de Bob en X es:

$$P_+ = |+\rangle \langle +| . \tag{10}$$

  Aplicado a $|0\rangle$ o $|1\rangle$, asumamos que el estado de Eve colapso a $|0\rangle$. Para que Eve siga sin ser detectada Bob tendría que medir un 0, es decir un $|+\rangle$. La probabilidad de eso es:

$$\begin{aligned} |c_+|^2 &= \langle 0| P_+ |0\rangle = \langle 0| (|+\rangle \langle +|) |0\rangle \\ &= \frac{1}{\sqrt{2}}(\langle +| + \langle -|)(|+\rangle \langle +|)\frac{1}{\sqrt{2}}(|+\rangle + |-\rangle) \\ &= \frac{1}{2}(\langle +|+\rangle + \langle +|-\rangle)(\langle +|+\rangle + \langle +|-\rangle) \\ &= \frac{1}{2}(1+0)(1+0) \\ &= \frac{1}{2}. \end{aligned} \tag{11}$$

Para que Eve pueda continuar robando información debe permanecer indetectado. Entonces la probabilidad de exito de Eve corresponde a que Alice, Bob y ella midan en la misma base:

$$P(1) = P(X)^3 = \left(\frac{1}{2}\right)^3 = \frac{1}{8} \tag{12}$$

O, que Alice y Bob midan en la misma base y que la medida de Eve colapse convenientemente:

$$P(2) = P(X)P(+)P(X) = \frac{1}{2} \cdot \frac{1}{2} \cdot \frac{1}{2} = \frac{1}{8} \tag{13}$$

Sumando ambas probabilidades tenemos, finalmente que la probabilidad de exito en un intento de Eve de no ser detectada es de:

$$P(Exito) = P(1) + P(2) = \frac{1}{4} \tag{14}$$

Sin embargo, Alice y Bob desean intercambiar n estados, la probabilida de éxito de Eve en cada uno de esos intentos es $P(Exito)$. Pero para que tenga exito en todo el proceso de comunicación es:

$$P(Com) = P(Exito)^n = \frac{1}{4^n} = 2^{-2n} \tag{15}$$

Si la cantidad de información que quieren compartir Alice y Bob es muy grande, es casi imposible para Eve no ser detectada. Lo que le da una seguridad al protocolo muy alta.

3. BB92

Como ya se menciono antes, el protocolo BB92 es una versión más flexible de su predecesor BB84. En este caso los pasos son identicos, lo diferente radica en las bases y medidas a implementar. En este protocolo se establece que no es necesario una base ortogonal. El protocolo enuncia:

Sean $|u_0\rangle$ y $|u_1\rangle$ dos estados diferentes no ortogonales, y sean $P_0 = 1 - |u_1\rangle \langle u_1|$ y $P_1 = 1 - |u_0\rangle \langle u_0|$ dos proyectores que no conmutan en los subespacios ortogonales a $|u_1\rangle$ y $|u_0\rangle$, respectivamente. Veamos que ocurre al aplicar P_0 sobre las distintas bases:

$$
\begin{aligned}
|c_1|^2 = \langle u_1| P_0 |u_1\rangle &= \langle u_1| (1 - |u_1\rangle \langle u_1|) |u_1\rangle \\
&= \langle u_1| (|u_1\rangle - \langle u_1| (\langle u_1|u_1\rangle |u_1\rangle)) \\
&= \langle u_1| (|u_1\rangle - |u_1\rangle) \\
&= 0
\end{aligned}
\tag{16}
$$

$$
\begin{aligned}
|c_0|^2 = \langle u_0| P_0 |u_0\rangle &= \langle u_0| (1 - |u_1\rangle \langle u_1|) |u_0\rangle \\
&= \langle u_0| (|u_0\rangle - \langle u_0|u_1\rangle |u_1\rangle) \\
&= \langle u_0|u_0\rangle - \langle u_0|u_1\rangle \langle u_0|u_1\rangle \\
&= 1 - \langle u_0|u_1\rangle^2
\end{aligned}
\tag{17}
$$

Vemos que P_0 aplicado a $|u_1\rangle$ hace la probabilidad nula. Pero aplicado a $|u_0\rangle$, como las bases no son ortogonales el producto interno $\langle u_0|u_1\rangle \neq 0$, asi la probabilidad $1 - \langle u_0|u_1\rangle^2 > 0$.

De nuevo, Alice prepara y envia a Bob un secuencia aleatoria de bits codificados en $|u_0\rangle$ y $|u_1\rangle$. Bob mide aleatoriamente cada sistema en los proyectores P_0 o P_1. Luego, comparan y ven cuales obtuvieron una medida positiva descartando las demás. El protocolo continua de la misma manera que en su versión BB84.

Referencias

1. Bennett, C.H., Brassard, G.: Quantum cryptography: public key distribution and coin tossing. In: Proceedings IEEE International Conference on Computers, Systems and Signal Processing, Bangalore, India, 1984, pp. 175–179. IEEE, New York (1984)

2. Bennett, C.H., Brassard, G., Mermin, N.D.: Quantum cryptography without Bell's theorem. Phys. Rev. Lett. 68, 557 (1992)

3. Bennett, C.H.: Quantum Cryptography Using Any Two Nonorthogonal States. IBM Research Division, T.J. Watson Research Center, Yorktown Heights, New York, USA, 1992, pp. 3121-3124. (1992)