MOOC: Computación y Criptografía Cuánticas

Lección 2: Criptografía Cuántica

Soluciones a los ejercicios propuestos

Ejercicio 2.2.1 Suponiendo que se ha llevado a cabo el protocolo BB84, sin espías ni interferencias, ¿por qué se puede asegurar que la clave bruta es común y que su longitud es aproximadamente la mitad de la de la cadena inicial?

Recordemos que al medir un estado u, usando una base B, éste se proyecta sobre el subespacio generado por los vectores de la base, por lo que si el estado u es uno de los vectores de B, el estado resultante tras la medición será el propio u con probabilidad 1.

En la fase de reconciliación de bases, Alicia y Bob se han asegurado que, para cada uno de los bits de la clave bruta, han usado la misma Base (Alicia para codificar y Bob para descodificar). Por tal motivo, han de tener el mismo bit con probabilidad 1.

Por otra parte, la probabilidad de que los dos hayan elegido la misma base es del 50%, por tanto en la clave bruta habrá aproximadamente la mitad de bits que en la cadena inicial.

Ejercicio 2.2.2 Completa la tabla de la figura, que muestra un ejemplo en el que Eva sigue una estrategia de espionaje Interceptar-Reenviar.

Cadena de Alicia	0	0	1	0	1	1	0	0	0	1
Base elegida por Alicia	B_1	B_X	B_1	B_X	B_1	B_X	B_1	B_1	B_X	B_X
Polarización	$\rightarrow$	$\nearrow$	$\uparrow$	$\nearrow$	$\uparrow$	$\searrow$	$\rightarrow$	$\rightarrow$	$\nearrow$	$\searrow$
Base elegida por Eva	B_X	B_X	B_1	B_X	B_X	B_1	B_1	B_X	B_1	B_X
Resultado	$\|+\rangle$	$\|+\rangle$	$\|1\rangle$	$\|+\rangle$	$\|-\rangle$	$\|0\rangle$	$\|0\rangle$	$\|-\rangle$	$\|1\rangle$	$\|-\rangle$
Eva envía a Bob										
Base usada por Bob	B_1	B_1	B_X	B_X	B_X	B_1	B_1	B_1	B_X	B_X
Resultado de la medida										
Cadena de Bob tras la reconciliación de bases										
Cadena de Eva										

Rellénala varias veces poniendo posibles resultados diferentes en las medidas

A continuacón, se muestra una posible forma de rellenar la tabla, el contenido de las filas 8ª y 9ª puede cambiar según los resultados de las mediciones realizadas por Bob. Los resultados que aparecen en color rojo, se obtienen con probabilidad 1/2, los que aparecen en negro, con probabilidad 1.

Cadena de Alicia	0	0	1	0	1	1	0	0	0	1
Base elegida por Alicia	B_1	B_X	B_1	B_X	B_1	B_X	B_1	B_1	B_X	B_X
Polarización	$\rightarrow$	$\nearrow$	$\uparrow$	$\nearrow$	$\uparrow$	$\searrow$	$\rightarrow$	$\rightarrow$	$\nearrow$	$\searrow$
Base elegida por Eva	B_X	B_X	B_1	B_X	B_X	B_1	B_1	B_X	B_1	B_X
Resultado	$\|+\rangle$	$\|+\rangle$	$\|1\rangle$	$\|+\rangle$	$\|-\rangle$	$\|0\rangle$	$\|0\rangle$	$\|-\rangle$	$\|1\rangle$	$\|-\rangle$
Eva envía a Bob	$\nearrow$	$\nearrow$	$\uparrow$	$\nearrow$	$\searrow$	$\rightarrow$	$\rightarrow$	$\searrow$	$\uparrow$	$\searrow$
Base usada por Bob	B_1	B_1	B_X	B_X	B_X	B_1	B_1	B_1	B_X	B_X
Resultado de la medida	$\|1\rangle$	$\|1\rangle$	$\|-\rangle$	$\|+\rangle$	$\|-\rangle$	$\|0\rangle$	$\|0\rangle$	$\|0\rangle$	$\|-\rangle$	$\|-\rangle$
Cadena de Bob tras la reconciliación de bases	1			0			0	0	1	1
Cadena de Eva	0			0			0	1	1	1

En cada caso contesta a las siguiente preguntas:

¿Cuántos bits tiene la clave tras la reconciliación de bases? 6

¿En cuántos de estos bits son coincidentes las cadena de Alicia y Eva? 4

¿Qué discrepancia se ha introducido en la cadena de Bob? 2/6

Con los resultados marcados en las mediciones, Eva tiene 2/3 de acierto e introduce una discrepancia de 1/3. Si, por ejemplo el resultado de la primera medición de Bob hubiera sido $|0\rangle$, la discrepancia habría sido sólo de 1/6. Pero si, como resultado de la octava medición, hubiera obtenido $1\rangle$, la discrepancia sería del 50%.

Con una cadena más larga el porcentaje de aciertos de Eva debe esta cerca del 75% y la discrepancia introducida cerca del 25%.

Ejercicio 2.2.3 Demuestra que con la estrategia de la base intermedia la máxima probabilidad de acierto se alcanza con $\alpha = \pi/8$. Calcula en ese caso, la probabilidad de acierto y la discrepancia introducida.

En la estrategia de la base intermedia, Eva considera una base ortonormal $B = [|u\rangle, |v\rangle]$, de la forma

$$|u\rangle = \cos(\alpha)|0\rangle + \sin(\alpha)|1\rangle, \quad |v\rangle = -\sin(\alpha)|0\rangle + \cos(\alpha)|1\rangle$$

y la usa para medir y descodificar su clave, poniendo 0 si obtiene $|u\rangle$, y 1 si obtiene $|v\rangle$.

En este caso, la expresión respecto de B de los vectores de las bases B_1 y $B_\times$ es

$$\begin{pmatrix} |0\rangle \\ |1\rangle \end{pmatrix} = \begin{pmatrix} \cos(\alpha) & -\sin(\alpha) \\ \sin(\alpha) & \cos(\alpha) \end{pmatrix} \begin{pmatrix} |u\rangle \\ |v\rangle \end{pmatrix}$$

$$\begin{pmatrix} |+\rangle \\ |-\rangle \end{pmatrix} = \begin{pmatrix} \cos(\frac{\pi}{4} - \alpha) & \sin(\frac{\pi}{4} - \alpha) \\ \sin(\frac{\pi}{4} - \alpha) & -\cos(\frac{\pi}{4} - \alpha) \end{pmatrix} \begin{pmatrix} |u\rangle \\ |v\rangle \end{pmatrix}$$

Con esta estrategia, la probabilidad de acierto de Eva es

$$p(\alpha) = \frac{1}{2}\left(\cos^2(\alpha) + \cos^2(\frac{\pi}{4} - \alpha)\right),$$

que se hace máxima máxima cuando $\alpha = \dfrac{\pi}{4} - \alpha$, en cuyo caso $\alpha = \pi/8$.

La discrepancia es constante e igual a 1/4.

Luego, de acuerdo con el plantemiento de espionaje propuesto, la base que debe elegir Eva es $B_i = [|u\rangle, |v\rangle]$, con

$$|u\rangle = \cos(\pi/8)|0\rangle + \sin(\pi/8)|1\rangle \quad \text{y} \quad |v\rangle = -\sin(\pi/8)|0\rangle + \cos(\pi/8)|1\rangle,$$

que es la denominada base intermedia.

En este caso, la probabilidad de acierto de Eva es

$$p = \cos^2(\pi/8) = \frac{1}{2} + \frac{\sqrt{2}}{4} \approx 0.854.$$

Ejercicio 2.4.1: Pon un ejemplo de aplicación del protocolo B92 con una cadena de al menos 12 bits.

A continuación se muestra una tabla con un ejemplo de aplicación del B92. Los resultados de las mediciones realizadas por Bob, que aparecen en color rojo, se obtienen con probabilidad 1/2, los que aparecen en negro, con probabilidad 1.

Cad. inicial Alicia (a)	0	0	1	0	1	1	0	0	0	1	0	1
Polarización	$\rightarrow$	$\rightarrow$	$\nearrow$	$\rightarrow$	$\nearrow$	$\nearrow$	$\rightarrow$	$\rightarrow$	$\rightarrow$	$\nearrow$	$\rightarrow$	$\nearrow$
Cad.inicial Bob (a')	0	1	1	0	0	1	1	0	1	1	0	0
Base usada por Bob	B_1	B_X	B_X	B_1	B_1	B_X	B_X	B_1	B_X	B_X	B_1	B_1
Resultado de la medida	$\|0\rangle$	$\|+\rangle$	$\|+\rangle$	$\|0\rangle$	$\|0\rangle$	$\|+\rangle$	$\|-\rangle$	$\|0\rangle$	$\|-\rangle$	$\|+\rangle$	$\|0\rangle$	$\|1\rangle$
Cadena (b) Bob	0	0	0	0	0	0	1	0	1	0	0	1

Una vez completada la tabla, por el canal clásico, Bob publica las posiciones en las que el valor de la cadena b es 1 y con esas posiciones forman la clave común: (a) para Alicia y (1-a') para Bob. En este caso la clave común es 001, cuya longitud es la cuarta parte de la de la cadena inicial.