Introducción a la Criptografía Cuántica

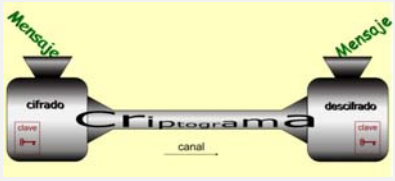
Alfonsa García, Francisco García[1] y Jesús García[1]
[1]Grupo de investigación en Información y Computación Cuántica (GIICC)

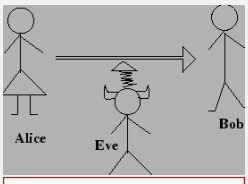
Introducción a la criptografía cuántica

1. El problema de la comunicación segura
2. Protocolo BB84
3. Seguridad del protocolo BB84
4. Otros protocolos cuánticos de distribución de claves.

1. El problema de la comunicación segura

Dos usuarios legítimos, Alicia y Bob, quieren comunicarse de manera segura a través de un canal no necesariamente seguro.





Una espía, Eva, intercepta el canal y pretende descubrir el mensaje.

Para asegurar la confidencialidad, Alicia envía a Bob el mensaje cifrado (criptograma) y Bob descifra el criptograma recuperando el mensaje.

GIEMATIC Grupo de Innovación Educativa E.U. Informática Dpto. Matemática Aplicada

Criptografía simétrica (clave secreta)

Las dos partes usan la misma clave para cifrar y descifrar.

Shannon (1949): El sistema de clave secreta es seguro, con claves de un solo uso y de longitud igual al mensaje a cifrar.

Problema → La generación y distribución de claves

GIEMATIC Grupo de Innovación Educativa E.U. Informática Dpto. Matemática Aplicada

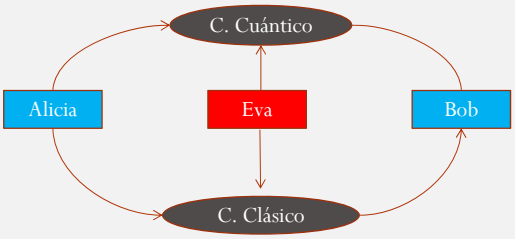
Criptografía asimétrica (clave pública)

- Cada usuario dispone de dos claves (pública y privada).
- Cualquiera puede enviar un mensaje cifrado con la clave pública del destinatario.
- Sólo el destinatario legítimo puede descifrar los mensajes recibidos, con su clave privada.
- La seguridad se basa en la hipótesis no demostrada de dificultad computacional de ciertos problemas (factorización de enteros, logaritmo discreto…).

El algoritmo cuántico de Shor pone en peligro la seguridad del sistema

Propuesta de la criptografía cuántica

Clave secreta de un solo uso, resolviendo "cuánticamente" el problema de la distribución de claves.



Se usan dos canales: uno cuántico y uno clásico autenticado.

Eva puede acceder a ambos canales. Pero no puede violar las leyes de la Mecánica Cuántica.

Protocolos cuánticos de distribución de claves (QKD)

El objetivo de un protocolo cuántico de distribución de claves (Quantum Key Distribution) es facilitar claves (cadenas aleatorias de 0's y 1's) completamente seguras a dos usuarios, Alicia y Bob, separados físicamente.

Se pueden usar fotones polarizados (enviados a través de un cable de fibra óptica) o pares EPR.

La seguridad de la QKD se basa en los principios de la mecánica cuántica

Eva no puede medir estados cuánticos sin modificarlos.
Los estados cuánticos no se pueden copiar.

Entrelazamiento cuántico

GIEMATIC
Grupo de Innovación Educativa
E.U. Informática Dpto. Matemática Aplicada

3. Protocolo BB84

- Alicia genera una cadena aleatoria de 0's y 1's.
- Codifica cada bit eligiendo aleatoriamente una de las dos bases B_1 y B_X y envía el fotón polarizado.
- Bob mide cada fotón con una de las dos bases, que también elige aleatoriamente, y descodifica con el mismo criterio que Alicia.
- Reconciliación de bases: usando el canal clásico, Bob comunica a Alicia la base usada para medir cada estado y ella le indica si ha utilizado la misma o no.
- Se quedan con los bits de la cadena en los que los dos han usado la misma base.

	0	1
B_1	$\|0\rangle$ →	$\|1\rangle$ ↑
B_X	$\|+\rangle$ ↗	$\|-\rangle$ ↘

GIEMATIC
Grupo de Innovación Educativa
E.U. Informática Dpto. Matemática Aplicada

Un ejemplo

Mensaje	0	0	1	0	1	1	0	0	0	1
Base elegida	B_1	B_X	B_1	B_X	B_1	B_X	B_1	B_1	B_X	B_X
Codificación	$\|0\rangle$	$\|+\rangle$	$\|1\rangle$	$\|+\rangle$	$\|1\rangle$	$\|-\rangle$	$\|0\rangle$	$\|0\rangle$	$\|+\rangle$	$\|-\rangle$
Polarización	→	↗	↑	↗	↑	↘	→	→	↗	↘
B mide con	B_1	B_1	B_X	B_X	B_X	B_1	B_1	B_1	B_X	B_X
Resultado	$\|0\rangle$	$\|0\rangle$	$\|+\rangle$	$\|+\rangle$	$\|-\rangle$	$\|0\rangle$	$\|0\rangle$	$\|0\rangle$	$\|+\rangle$	$\|-\rangle$
Reconciliación	0			0			0	0	0	1

Clave bruta y clave depurada

- Si no ha habido espías ni interferencias, tras el protocolo descrito, A y B tienen una clave común, cuya longitud es aproximadamente la mitad de la cadena inicial.
- Esta clave se denomina **clave bruta**.
- Cualquier estrategia de espionaje introduce alteraciones en los qubits que Bob recibe.
- A y B usarán un subconjunto aleatoriamente elegido de la clave bruta para chequear discrepancias, comunicándose por el canal clásico. En ausencia de ruido, las discrepancias denotan la presencia de Eva y, si las hay, la clave debe ser rechazada.
- Si no hay discrepancias (o son pocas), se pueden quedar con el resto de la clave como **clave depurada**.
- Esta clave, antes de ser usada, se someterá a un proceso de corrección de errores y amplificación de privacidad, dando lugar a la **clave secreta final**.

Sistemas que se comercializan

www.idquantique.com

Ya se comercializan soluciones tecnológicas para implementar el BB84

3. Seguridad del protocolo BB84

Estudio de seguridad frente a ataques individuales (a cada qubit enviado)

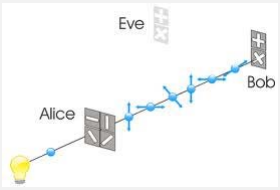
La seguridad de la KQD se basa en detectar la presencia del espía, usando una parte de la clave para estimar discrepancias.

Pero cualquier canal tiene ruidos y puede haber discrepancias no debidas a la actuación de Eva.

Es necesario analizar las posibles estrategias de espionaje para establecer una cota de error admisible, que depende de relación entre la información de Eva y la discrepancia introducida.

Estrategia Intercepta-Reenvía

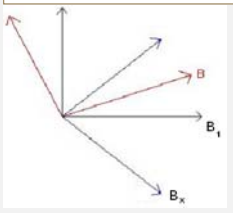
- Eva intercepta el fotón enviado por Alicia, lo mide usando una de las bases B_1 ó B_X, elegida aleatoriamente, y envía a Bob el qubit resultante de la medida.
- Consigue una coincidencia del 75% con la clave de Alicia.
- Introduce una discrepancia del 25% en la clave de Bob.

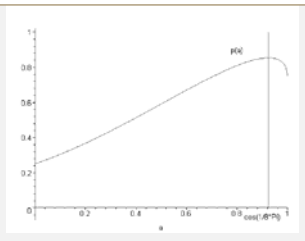


Estrategia de la base intermedia

Eva usa para medir una base elegida para maximizar la probabilidad de acierto

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





a=cos(α)

El máximo de la probabilidad de acierto de Eva se alcanza con $\alpha = \pi/8$ y es $\cos^2(\pi/8) \sim 0.854$

Discrepancia introducida: 0.25

Otras estrategias de espionaje

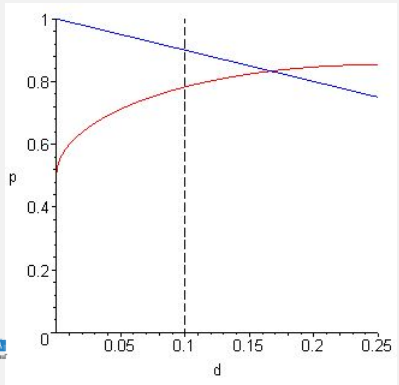
Eva puede llevar a cabo cualquier estrategia compatible con las leyes de la Mecánica Cuántica.

Un modelo de estrategia general:

1. Eva intercepta cada qubit enviado por Alicia
2. Le añade un n-qubit prueba en estado |0> y aplica una transformación unitaria T.
3. Envía a Bob el primer qubit del estado resultante.
4. Tras la reconciliación de bases, Eva puede aplicar otra transformación unitaria.
5. Mide un qubit de su estado para obtener su clave.

Garantizar la seguridad

Para una estrategia general de espionaje, interesa establecer la relación entre la máxima probabilidad de acierto de Eva (p) y la discrepancia introducida (d).



Se puede estimar cuánto mayor es la coincidencia entre las claves de A y B que entre las de A y E

Medida de la información

Entropía de Shannon

X variable aleatoria discreta

$$H(X) = H(p_1, p_2, \cdots, p_n) = -\sum_{j=1}^{n} p_j \log_2(p_j)$$

Es un promedio de la incertidumbre

Si X sólo toma dos valores, con probabilidades p y 1–p, se tiene la entropía binaria:

$$h(p) = H(p, 1-p) = -p\log_2(p) - (1-p)\log_2(1-p)$$

Si X corresponde a una cadena aleatoria de n bits, hay 2^n valores equiprobables y es $H(X)=n$

Información mutua

Dadas dos variables aleatorias X e Y se puede hablar de entropía conjunta H(X,Y) y condicionada H(X|Y)

La información mutua se define por:
I(X,Y)=H(X)+H(Y)-H(X,Y)=H(X)-H(X|Y)

Mide la diferencia de incertidumbre sobre X antes y después de conocer Y.

- La información mutua siempre es mayor o igual que 0.
- I(X,Y)=0 cuando las variables son independientes.
- I(X,Y)=I(Y,X)

Información mutua en el BB84

A →variable aleatoria correspondiente a la cadena de Alicia,
B→ v. a. de la cadena de Bob y E→ v. a. de la cadena de Eva.

Sabemos que $H(A)= n$ (pues hay 2^n valores equiprobables)

Si Eva tiene una probabilidad p de acierto en cada bit e introduce una discrepancia d resulta: $I(A,E)=n(1-h(p))$, $I(A,B)=n(1-h(1-d))$.

$$I(A,B)+I(A,E)\leq n$$

Criterio de seguridad exigible: $I(A,B)>I(A,E)$

Se obtiene que el protocolo BB84 es seguro frente ataques individuales si d<11%

Limitaciones de seguridad del BB84

La seguridad del BB82 está condicionada al supuesto de que Alicia dispone de una fuente capaz de emitir fotones individuales.

Pero experimentos, basados en pulsos débilmente coherentes, han puesto de manifiesto que la probabilidad de multifotón es bastante apreciable.

Eva puede hacer un ataque PNS (Photon Number Splitting) basado en pulsos con dos fotones.

Para mejorar la seguridad, se utilizan técnicas de corrección de errores y **amplificación de la privacidad.**

Otros protocolos QKD

- Protocolo B92. Generalización del BB84 que usa sólo dos estados.
- Protocolo SARG04. Se puede llevar a cabo con la misma tecnología del BB84 y pretende evitar ataques PNS
- Protocolo E91. Basado en el uso de partículas entrelazadas.

GIEMATIC Grupo de Innovación Educativa E.U. Informática Dpto. Matemática Aplicada

Protocolo B92

- Alicia genera una cadena aleatoria **a** de 0's y 1's.
- Alicia envía a Bob cada bit de la cadena **a**, codificado del siguiente modo: Un 0 lo codifica con |0> y un 1 con |+>
- Bob genera una cadena **a'** de 0's y 1's y mide cada estado recibido usando B_1 si en la posición correspondiente a'=0 y B_X, cuando a'=1.
- A partir de esta medición Bob obtiene una cadena b de 0's y 1's, del siguiente modo:

  Si ha usado B_1 y obtiene |0> pone b=0 y si obtiene |1>, pone b=1.
  Si ha usado B_X y obtiene |+> pone b=0 y si obtiene |->, pone b=1
- Bob publica las posiciones en que b=1 y, sólo con estas posiciones, las claves son a para Alicia y 1-a' para Bob.

Las claves coinciden (salvo ruidos o espías) con probabilidad 1.
La longitud de la clave es ¼ de la de la cadena original

GIEMATIC Grupo de Innovación Educativa E.U. Informática Dpto. Matemática Aplicada

Protocolo SARG04

Se puede llevar a cabo con la misma tecnología del BB84 y pretende evitar ataques PNS

- Alicia genera aleatoriamente una cadena de 0's y 1's.
- Codifica cada bit usando aleatoriamente uno de los dos estados de la base B_1 para el 0 y uno de los de la base B_X para el 1, enviando a Bob cada fotón polarizado.
- Bob mide el fotón, con una de las dos bases elegida al azar.
- Contraste de información en el canal público.

GIEMATIC Grupo de Innovación Educativa E.U. Informática Dpto. Matemática Aplicada

Fase de Contraste en SARG04

Alicia no dice qué base ha usado sino que da uno de los siguientes conjuntos en el que se encuentre el qubit enviado junto con uno de los que se usa para codificar el otro bit.

$$S_{-+} = \{|1\rangle, |+\rangle\}, S_{--} = \{|1\rangle, |-\rangle\}$$
$$S_{++} = \{|0\rangle, |+\rangle\}, SS_{+-} = \{|0\rangle, |-\rangle\}$$

Bob descodifica de acuerdo con la tabla adjunta, donde *D* significa que se descarta el bit

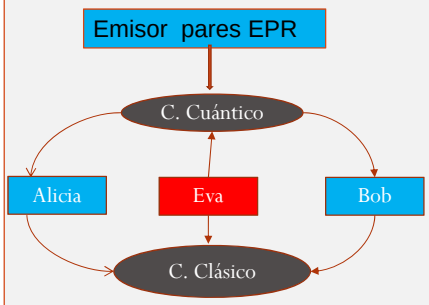
	$\|0\rangle$	$\|1\rangle$	$\|+\rangle$	$\|-\rangle$
S_{++}	D	1	D	0
S_{+-}	D	1	0	D
S_{-+}	1	D	D	0
S_{--}	1	D	0	D

La longitud de la clave bruta resultante es ¼ de la original

GIEMATIC Grupo de Innovación Educativa E.U. Informática Dpto. Matemática Aplicada

Protocolo E91

- Alicia y Bob disponen de un emisor de pares EPR, que podrían ser fotones polarizados
- Un par EPR es un estado de 2 partículas entrelazadas. Por ejemplo $\frac{1}{\sqrt{2}}(|00\rangle + |11\rangle) = \frac{1}{\sqrt{2}}(|++\rangle + |--\rangle)$.
- Estas partículas son separadas. Alicia recibe, a través del canal cuántico, el primer qubit de cada par y Bob el segundo.
- Alicia y Bob miden cada qubit recibido, usando una de las dos bases B_1 ó B_X.
- Si han usado la misma base, deben obtener el mismo resultado.
- La reconciliación de bases se hace por el canal público, como en el BB84.
- Consiguen una clave común por el principio del entrelazamiento cuántico.



GIEMATIC
Grupo de Innovación Educativa
E.U. Informática Dpto. Matemática Aplicada