Criptografía Cuántica

Jesús del Pino Ruiz

Índice

Resumen

El trabajo es una breve introducción al mundo de la criptografía cuántica. En él haré un breve repaso de la historia de la criptografía clásica, sentaré los fundamentos físicos de la criptografía cuántica y por último explicaré los experimentos más relevantes que se han llevado a cabo.

1. Breve historia de la criptografía y sus conceptos más importantes.

1.1. Conceptos sobre criptografía.

La *criptografía* es la técnica, ciencia o arte de la escritura secreta. El objetivo principal de la criptografía es mantener la privacidad del comunicación entre dos personas,se altera el mensaje evitando así que una tercera pueda comprenderlo. También es importante el término *autentificación* que consiste en firmar el mensaje de forma que una tercera persona no se pueda hacer pasar por nosotros. El origen de la palabra critografía proviene del griego "cripto"(oculto, secreto) y "grafos"(escritura.)

Al paso del mensaje original al mensaje cifrado (*criptograma*) se le llama cifrado, y al paso inverso descifrado. Estos paoso se llevan mediante un acuerdo común entre los comunicantes, que se llama *clave*. Y el último concepto relevante es el de *criptoanálisis* que consiste en interceptar y descifrar el mensaje, hallando la clave oculta. La *criptología* engloba por tanto la criptografía y el criptoanálisis.

Hay que disitinguir también entre *código* y *cifra*. Con el código cambiamos una palabra o letra del mensaje original por otra, un buen ejemplo de código es la traducción de un idioma a otro. Mientras que la cifra actúa sobre los carácteres, un ejemplo de cifrado puede ser "elimina los espacios en blanco y cambia el orden de los caracteres de dos en dos". Con esto, si yo digo una frase, por ejemplo "emprender la guerra", y la pasamos por el código inglés obtendríamos "to go to war" y con el cifrado anterior obtendríamos "merpneedlrgaeurra".

Hay dos tipos de clave *simétrica* y *asimétrica*. La primera consiste en usar la misma clave para cifrar que para descifrar. La segunda emplea claves distintas para cifrado y descifrado.

1.2. Ejemplos de criptografía en la historia.

La criptografía es tan antigua como la civilización, diversas razones milita res, políticas, religiosas o comerciales impulsaron desde tiempos remotos el uso de las escrituras secretas. En el antiguo Egipto, mientras el pueblo utilizaba la lengua demótica el clero usaba la hierática (jeroglíficos) que no era comprendida nada más que por ellos. Los babilonio también empleaban esto, utilizando la escritura cuneiforme, incluso el mismo nombre de Babilonia viene codificado en la Biblia como *"Sasseh"* . El primer uso de tipo militar constatado es en la guerra entre Esparta y Atenas, el cifrado consistía en la introducción de símbolos innecesarios que desaparecían al enrollar el mensaje en un rodillo llamado "escitala" de longitud y grosor determinados. Carlomagno sustituía las letras por símbolos extraños, En Roma la técnica que empleaba César era la de sustituir las letras por la que ocupaba tres posiciones más adelante en el abecedario.

En la Edad Media, San Bernardino evitaba la regularidad de los signos. Así conseguía que el criptoanálisis por el método de la frecuencia los signos no fuese efectivo. Utilizaba un signo para cada consonante, tres distintos para cada vocal e intercalaba símbolos sin sentido.

El primer libro del que se tiene constancia sobre el tema es el *"Liber Zifrorum"* de Cicco Simoneta en el siglo XIV. En el siglo XV destaca *León Battista Alberti* considerado por muchos el padre de la criptología, crea la primera máquina de criptografiar, consistente en dos círculos concéntricos, que giran independientes consiguiendo cada una un alfabeto de transposición. En el siglo XVI *Girolamo Cardano* empleó una tarjeta perforada que debía colocarse sobre el texto para poder leerlo. En el mismo siglo el francés Viete descifró los mensajes encriptados de Felpe II, siendo así uno de los primero criptoanalistas con éxito de la historia. Del mismo siglo es la obra *"Traicté des Chiffres"* del francés Blaise de Vigenére en el que contaba todas las técnicas empleadas en su tiempo. Otras claves a contar son las empleadas por Carlos I de Inglaterra que en el siglo XVII empleó códigos de sustitución silábica y Napoleón que empleó el método *Richelieu y Rossignol* que consistía en asignar números a grupos de una o más letras. (Con lo cual el argumento del "Conde de Montecristo" pierde algo de fuerza)

En el siglo XIX se usó masivamente el método de transposición consistente en la reordenación según distintos criterios del mensaje. Kerckhoffs escribe el libro *"La criptografía militar"* en el que cuenta las normas que debe cumplir un buen sistema criptográfico.

En la I Guerra Mundial los alemanes emplearon el método ADFGX que consistía en que a cada unión de dos letras de ese grupo se le asignaba otra letra del abecedario y posteriormente se le hacía una transposición en bloques de lonbgitud 20. En el periodo entreguerras la criptología sufrió un gran avance debido a la necesidad de vías seguras de comunicación diplomática. En la II Guerra Mundial los americanos utilizaron la máquina Enigma para desencriptar el código púrpura de los japoneses y lo consiguieron, mientras que ellos emplearon el código navajo, empleaban a los indios navajos y su complicado lenguaje para la transmisión, éste no fue nunca desencriptado (se puede ver en la película "Windtalkers") aquí se vez que en ocasiones un código puede sedr más útil que un cifrado.

En 1975 Diffie y Hellman establecen las bases de los algoritmos de llave pública. También hay que nombrar el cifrado Vernam, creado por Gilbert S. Vernam que trabajaba para la compañía "American Telephone and Telegraph" que consiste en una clave tan laraga como el texto a cifrar, este sistema es muy engorroso y se llamó también "Cuaderno de un solo uso" porque las claves se daban en cuadernos, en el cual cada hoja era una clave, que después de ser utilizada se arrancaba del cuaderno y se destruía.

En el año 1949 Claude E. Shannon de los laboratorios Bell demostró que cualquier mensaje cuya clave fuese más corta que el mensaje cifrado es fácilmente descifrable. También demostró que la seguridad del cifrado Vernam era limitada y que dependía del transporte de la clave, que además esta debía ser asimétrica y emplearse una sóla vez, o ser simétrica y aleatoria, cumpliéndose de nuevo la condición de un único uso de no ser así, no sería segura.

Algunos escritores famosos como Arthur Conan Doyle, Edgar Allan Poe, Francis Bacon, sociedades secretas como los templarios, etc... lo han utilizado. De hecho algunas formas de comunicarse como el código Morse o la lengua de los signos de los sordomudos son formas criptográficas.

Podemos preguntarnos, ¿A la vista de los teoremas de Shannon, puede existir un cifrado seguro? La criptografía cuántica podría dárnoslo.

2. Fundamentos físicos de la criptografía cuántica.

2.1. Consecuencias del teorema de Shannon.

Tal como he comentado la codificación será segura si:

- *La clave ha de ser aleatoria*
- *La clave debe usarse sólo una vez*

Estos requisitos no parecen muy difíciles de cumplir, sin embargo hya una tercera salvedad, la clave de un sólo uso debe estar en manos del emisor y del receptor. Y esto es complicado, porque la clave podría caer en manos de terceros, haciendo el sistema inviable.

Aquí aparece la física cuántica, dándonos métodos seguros de distribución de claves, llamados *"Quantum Key Distribution"* (a partir de ahora QKD.)

La seguridad de QKD reside en las bases físicas de la mecánica cuántica:

1. El teorema de *no cloning* (Wootters y Zurek 1982) nos asegura que un estado cuántico $|\Psi\rangle$ no puede ser copiado . Clásicamente el texto puede ser copiado, pero un sistema cuántico no puede ser copiado, y por tanto espiado.

2. Cualquier intento de acceder a la información de un sistema cuántico conlleva una alteración del sistema (colapso) por tanto no se puede obtener información sin destruir el sistema.

3. Las medidas cuánticas son irreversibles. Después de realizar una medida el sistema colapsa a uno de los estados propios del operador correspondiente a la magnitud que se ha medido, y no se puede volver a llevar el sistema al estado antes de medir. Por tanto, un espía siempre dejará huella.

Veamos con más detalle estos efectos. Supongamos que queremos distinguir entre dos estados cuánticos $|\Psi\rangle$ y $|\Phi\rangle$ que no sean ortogonales, es decir, que $|\langle\Phi|\Psi\rangle|^2 \neq 0$.

El aparato de medida que usaremos para medir lo denotaremos por $|u\rangle$. El estado global del sistema será por tanto $|\Phi\rangle \otimes |u\rangle$ o bien $|\Psi\rangle \otimes |u\rangle$. La evolución del sistema durante la medida nos llevará a que $|u\rangle$ evolucionará a

$|u_\Phi\rangle$ ó $|u_\Psi\rangle$ pero la evolución será unitaria, por lo que si queremos que los estados a medir queden inalterados será imposible que $|u_\Phi\rangle$ y $|u_\Psi\rangle$ sean distintos.

2.2. Fenomenología.

Podemos aplicar el principio de incertidumbre a la creación de un canal seguro basado en las propiedades cuánticas de la luz. Nos basaremos en la polarización de los fotones. La luz, habitualmente, posee fotones con todas las polarizaciones posibles. Empleando un polarizador seleccionamos aquellos fotones que tienen una determinada polarización. Para transmitir un mensaje cifrado cuánticamente necesitaremos, un emisor con un polarizador y un receptor que puede tener o bien otro polarizador, o un cristal birrefringente que hace lo mismo, pero no absorbe fotones. Un fotón en el dispositivo birrefringente tiene dos opciones, si llega polarizado verticalmente pasará en una dirección, y si no en otra, si no está polarizado tendrá una cierta probabilidad de pasar por uno o por otro lado, si su polarizacion son 45º tendrá la misma posibilidad de seguir su camino que de desviarse. De estos fotones no sabremos en que dirección estaban polarizados, ya que lo "olvidan."

A partir de ahora vamos a tener dos nuevos amigos, Bob y Alicia, que intentan comunicarse, y una tercera persona, Eva, que intentará interceptar su mensaje.

El proceso de QKD se da de la siguiente manera: Alicia emite los fotones polarizados según una dirección al azar, y anota en que dirección los ha polarizado. Según la mecánica cuántica Bob puede elegir en que base quiere medir la polarización del fotón, o en vertical - horizontal, o en diagonal,(que a partir de ahora denotaremos base + y base x) pero no en las dos.

Cada fotón que emite Alicia irá polarizado en una dirección, elegida por ella al azar, Bob decide en que base medir en + ó x. Después anota los resultados y los mantiene en secreto, Bob anuncia públicamente las bases en las que mide y Alicia le comunica donde ha acertado. Ellos dan por buenos los aciertos que convierten en 1 y 0, y desde ese momento son la clave. Alicia y Bob utilizarán la clave en la forma Vernam. Si un supuesto espía, Eva, intercepta el mensaje y lo cambia, este ya no valdrá, más adelante veremos como se comprueban estas escuchas. Lo que hacen es comprobar cuantas medidas correctas ha realizado Bob, si Eva cambia el mensaje, habrá un alto índice de error y la clave se tiraría.

2.3. Protocolos de QKD.

2.3.1. BB84

Este protocolo fue presentado por Bennet y Brassard en la International Conference on Computers en Bangalore, en el año 1984. Poalrizaremos fotones en la base + y elegiremos los ejes X e Y para polarizarlos. Podremos escribir entonces un vector polarización

$$|\Psi\rangle \ = a|\rightarrow\rangle + b|\uparrow\rangle \tag{1}$$

donde se denotan los estados de base como $|\rightarrow\rangle$ y $|\uparrow\rangle$. No obstante la elección es totalmente arbitraria, y podríamos haber considerado la base x, el mismo estado tiene su representación en esta base, mediante las ecuaciones de cambio de base.

$$|\nearrow\rangle = \frac{1}{\sqrt{2}}(|\rightarrow\rangle + |\uparrow\rangle) \tag{2}$$

$$|\nwarrow\rangle = \frac{1}{\sqrt{2}}(|\rightarrow\rangle - |\uparrow\rangle) \tag{3}$$

Por convenio representaremos el bit 0 por el vector $|\rightarrow\rangle$ en la base + y por $|\nearrow\rangle$ en la base x.

El proceso entonces consiste en comparación de bases, empleadas al emitir y al medir. En los procesos en que han compartido base, tanto Alicia como Bob teiene el mismo bit, en los que no ha habido coincidencia los bits serán aleatorios. Sin consiguen eliminar esos bits aleatorios, tendrán una clave de un sólo uso. ¿Cómo pueden eliminar esos bits erróneos? Pues basta en que Alicia y Bob hagan públicas las secuencias de bases empleadas para prepara y medir los estados. Comparando las dos listas, ambos sabrán que resultados deben desechar.

La pregunta obvia es, ¿no es esto peligroso? No mientras Alicia no diga que bits han codificado ni Bob que resultado ha obtenido.

2.3.2. B92

Bennet publicó en 1992 un protocolo distinto. Consideramos el sistema anterior, pero ahora el bit 0 será $|\rightarrow\rangle$ y el bit 1 $|\nwarrow\rangle$ que serán denominados $|0\rangle$ y $|1'\rangle$ donde la prima nos recuerda que es igual que el estado que habíamos

llamado 1 en la base diagonal.

Alicia prepara su sistema de igual manera que antes, pero ahora Bob no utiliza un sistema de medida Von Neumann, sino que aplica unos proyectores a lo que mide de la siguiente manera:

Si su bit es 0 (base +) aplica el proyector $P_{not0} = (1 - |0\rangle\langle 0|)$ y si el bit es 1 (base x) $P_{not1'} = (1 - |1'\rangle\langle 1'|)$ el resultado de aplicar esos proyectores será 0 ó 1, ¿cómo interpretamos los resultados?

Si la aplicación de P_{not0} sobre un sistema lo deja invariante (autovalor 1) puede estar seguro de su estado no es $|0\rangle$ y que ha recibido un $|1'\rangle$, pero si obtiene 0 no puede deducir que estado ha recibido, de forma similar ocurre con el otro proyector.

La estrategia a seguir es eliminar todos los bit en lo que Bob ha obtenido 0 y comunicarle a Alicia cuales debe desechar, en los demás el acuerdo será total.

2.3.3. E91

Este protocolo propuesto por Ekert en 1991 funciona de forma distinta, ya que emplea pares de fotones "enlazados" de una fuente EPR. Preparamos tres tipos de parejas distintas:

$$|\Omega_0\rangle = \frac{1}{\sqrt{2}}(|0\rangle_1|\frac{3\pi}{6}\rangle_2 - |\frac{3\pi}{6}\rangle_1|0\rangle_2) \tag{4}$$

$$|\Omega_1\rangle = \frac{1}{\sqrt{2}}(|\frac{\pi}{6}\rangle_1|\frac{4\pi}{6}\rangle_2 - |\frac{4\pi}{6}\rangle_1|\frac{\pi}{6}\rangle_2) \tag{5}$$

$$|\Omega_2\rangle = \frac{1}{\sqrt{2}}(|\frac{2\pi}{6}\rangle_1|\frac{5\pi}{6}\rangle_2 - |\frac{5\pi}{6}\rangle_1|\frac{2\pi}{6}\rangle_2) \tag{6}$$

Para la codificación emplearemos tres alfabetos alternativos A_0, A_1 y A_2 con la representación de bits (0, 1) como:

Bits	0	1
A_0	$\|0\rangle$	$\|\frac{3\pi}{6}\rangle$
A_1	$\|\frac{\pi}{6}\rangle$	$\|\frac{4\pi}{6}\rangle$
A_2	$\|\frac{2\pi}{6}\rangle$	$\|\frac{5\pi}{6}\rangle$

Como operadores de medida podemos utilizar $M_0 = |0\rangle\langle 0|$, $M_1 = |\frac{\pi}{6}\rangle\langle\frac{\pi}{6}|$

ó $M_2 = |\frac{2\pi}{6}\rangle\langle\frac{2\pi}{6}|$

El protocolo sigue los siguientes pasos:

1. Se genera una estado $|\Omega_j\rangle$ con j = 0,1,2 de forma aleatoria.
2. Se manda uno de los fotones a Alicia y el otro a Bob.
3. Alice y Bob separadamente y de forma aleatoria eligen uno de los tres operadores de medida y lo aplican al fotón.
4. Después de las medidas Alicia y Bob hacen públicas las listas con los operadores empleados en cada medida (manteniendo en secreto los resultados obtenidos).
5. En los casos en que han empleado la misma base tienen la concordancia asegurada, en los demás casos los eliminan, y ya tienen la clave común.

2.4. Dropping

¿Cómo podría un espía interferir en el proceso? Evidentemente si Eva pincha el cable de fibra óptica, no puede "apuntar" los fotones que pasan ya que lo prohíbe el teorema de no-cloning. Lo que si puede hacer es interceptar la comunicación ¿se puede medir este efecto?

Si. Lo que se hace es hacer pública una serie de bits emitidos y bits medidos. Es fácil averiguar que si Eva no está presente la probabilidad de acierto es de 1/4 (para el protocolo BB84), sin embargo, si Eva interfiere la probabilidad de acierto es de 5/8, por tanto la presencia de Eva es detectada y se desechará la clave. No se puede evitar esta intrusión, pero si sabremos si hay alguien escuchando, lo único que podemos hacer es esperar a que se "aburra" la espía.

3. Realización experimental de Criptografía Cuántica

3.1. Underwater quantum coding

Este experimento se publico por Muller, Zbinden y Gisin en la revista Nature en 1995. Utilizaron un cable de 23 km en el fondo del lago Ginebra. Utilizaron un laser de pulsos de 1300 nm con pulsos de 1 ns y un rate del pulso de 1.1 Mhz. Los fotones fueron polarizados con una lámina de $\lambda/4$. En el artículo explica que han conseguido una tasa del 3.4 % de error polarizando el láser de 1300 nm. Demostrando así que es una canal fiable y que se puede utilizar la criptografía cuántica.

3.2. Criptografía cuántica con pares de fotones "enredados"

Jenneweinn, Simons y otros, presentaron un sistema basado en pares "enlazados" y en el protocolo BB84 modificado. De esta manera ponen a Alicia y a Bob separados unos 360 m los fotones son analizados, detectados y registrados independientemente, así evitamos problemas que teníamos con el láser que podría ser atacado con la técnica "beam splitter." Con este método se transmitió con éxito la *Venus de Willendorf* de un tamaño de 50000 bits con un 3 % de error.

Referencias

[1] M. Baig. Grupo de física teórica - IFAE. *Criptografía Cuántica.*

[2] Nicolas Gisin, Grégoire Ribordy, Wolfang Tittel and Hugo Zbinden. Group of applied physics. University of Geneva. *Quantum Criptography.*

[3] www.iec.csic.es/criptonomicon *Criptonomicón*