Criptografía cuántica

La **criptografía cuántica** es la criptografía que utiliza principios de la mecánica cuántica para garantizar la absoluta confidencialidad de la información transmitida. La criptografía cuántica como idea se propuso en 1970, pero hasta 1984 no se publicó el primer protocolo.

Una de las propiedades más importantes de la criptografía cuántica es que si un tercero intenta espiar durante la creación de la clave secreta, el proceso se altera detectándose al intruso antes de que se transmita información privada. Esto es consecuencia del teorema de no clonado.

La seguridad de la criptografía cuántica descansa en las bases de la mecánica cuántica, a diferencia de la criptografía de clave pública tradicional que descansa en supuestos de complejidad computacional no demostrada de ciertas funciones matemáticas.

La criptografía cuántica está cercana a una fase de producción masiva, utilizando láseres para emitir información en el elemento constituyente de la luz, el fotón, y conduciendo esta información a través de fibras ópticas.

Conceptos básicos

La criptografía es la disciplina que trata de la transmisión y almacenamiento de datos de manera que no puedan ser comprendidos ni modificados por terceros. Los diferentes métodos de criptografía actualmente utilizados necesitan que dos personas que deseen comunicar información intercambien de forma segura una o más claves; una vez que las claves han sido intercambiadas, los interlocutores pueden transferir información con un nivel de seguridad conocido. Pero esta forma de trabajar basa la seguridad de las transmisiones exclusivamente en el intercambio de claves. La forma más segura de realizar este intercambio de claves es de manera presencial, pero ello no es posible en la mayoría de los casos, dado el múltiple número de interlocutores con los que se desea intercambiar información confidencial (bancos, tiendas en Internet, colegas de trabajo en sedes distantes, etcétera). De manera que el punto donde hay menor seguridad en el intercambio de información confidencial está en el proceso de intercambio y transmisión de las claves.

La mecánica cuántica describe la dinámica de cada partícula cuántica (fotones, electrones, etc.) en términos de estados cuánticos, asignando una probabilidad a cada posible estado de la partícula por medio de una función.

Algunos aspectos a considerar de la mecánica cuántica:

- Superposición: Una partícula puede poseer más de un estado a la vez, en otras palabras, se encuentra en realidad "repartida" entre todos los estados que le sean accesibles.
- La medición no es un proceso pasivo como se suponía en la mecánica clásica, ya que altera al sistema.
- Colapso de estados: Una partícula que se encuentra repartida entre todos sus estados accesibles, al ser medida se altera su estado superpuesto determinando en qué estado particular, de entre una variedad de estados posibles, se encuentra.
- Incertidumbre: En la teoría cuántica, algunos pares de propiedades físicas son complementarias (por ejemplo, la posición y el momentum), en el sentido de que es imposible saber el valor exacto de ambas. Si se mide una propiedad, necesariamente se altera la complementaria, perdiéndose cualquier noción de su valor exacto. Cuanto más precisa sea la medición sobre una propiedad, mayor será la incertidumbre de la otra propiedad.
- Entrelazamiento: Dos partículas cuánticas pueden tener estados fuertemente correlacionados, debido a que se generaron al mismo tiempo o a que interactuaron, por ejemplo, durante un choque. Cuando esto ocurre se dice que sus estados están entrelazados, lo que provoca que la medición sobre una de ellas determina inmediatamente el estado de la otra, sin importar la distancia que las separe. Este fenómeno se explica aplicando las leyes de conservación del momento y de la energía. (ver Paradoja EPR)

Las partículas utilizadas habitualmente en la criptografía cuántica son los componentes de la luz o fotones, y los estados que se utilizan para ser entrelazados o superpuestos entre sí son sus dos estados de polarización, que es una de las características conocidas de la luz, aunque no sea directamente perceptible.

Un fotón puede ser polarizado artificialmente en una dirección en particular con respecto a su dirección de desplazamiento. Dicha polarización puede ser detectada mediante el uso de filtros, orientados en el mismo sentido en el que la luz fue polarizada. Estos filtros dejan pasar los fotones polarizados en un estado y absorben los polarizados en el otro.

Historia

La criptografía cuántica fue inicialmente propuesta por Stephen Wiesner, quien en 1970 introdujo la idea de codificación conjugada. Sin embargo, el artículo fue rechazado por la Sociedad de la Teoría de la Información (IEEE) y no fue hasta 1983 cuando fue publicado por la ASM SIGACT. En este artículo mostró cómo almacenar y transmitir dos mensajes cifrándolos en dos "observables conjugados", como luz linearmente o circularmente polarizada, de manera que uno, pero no los dos simultáneamente, pueda ser leído y descifrado.

En 1984 Charles H. Bennett y Gilles Brassard propusieron un método de comunicación segura basado en el trabajo de Wiesner, conocido hoy como el protocolo BB84. En 1991 Artur Ekert desarrolló el protocolo E91 o EPR, un enfoque diferente para la distribución de claves cuánticas basado en correlaciones cuánticas peculiares conocidas como entrelazamiento cuántico.

Intercambio de claves cuánticas

El intercambio de claves cuánticas (QKD, del inglés "quantum key distribution", distribución cuántica de claves) es un método de comunicación seguro que implementa un protocolo criptográfico utilizando propiedades de la mecánica cuántica. Permite que dos partes produzcan una clave secreta aleatoria compartida que solo ellos conocen, que luego puede usarse para cifrar y descifrar mensajes.

Una propiedad importante y única de la QKD es la capacidad de los dos usuarios que se comunican para detectar la presencia de un tercero que intenta obtener conocimiento de la clave. Esto resulta de un aspecto fundamental de la mecánica cuántica: el proceso de medición de un sistema cuántico en general perturba el sistema. Un tercero que intente espiar la clave debe de alguna manera medirla, introduciendo así anomalías detectables. Mediante el uso de superposiciones cuánticas o entrelazamiento cuántico y transmisión de información en estados cuánticos, se puede implementar un sistema de comunicación que detecte la escucha. Si el nivel de escucha está por debajo de un cierto umbral, se puede producir una clave que se garantiza que es segura (es decir, el espía no tiene información al respecto), de lo contrario, no es posible una clave segura y se interrumpe la comunicación.

La distribución de claves cuánticas solo se usa para producir y distribuir una clave, no para transmitir ningún dato de mensaje. Esta clave se puede usar con cualquier algoritmo de cifrado elegido para encriptar (y descifrar) un mensaje, que luego puede

transmitirse a través de un canal de comunicación estándar. El algoritmo más comúnmente asociado con la QKD es la libreta de un solo uso.

El cifrado de la libreta de un solo uso es demostrablemente seguro. Consiste en emparejar el mensaje con una clave. La longitud de esta clave debe ser igual a la del mensaje, así cada bit del texto inicial se combina con otro bit de la clave realizando una suma modular.

Por ejemplo, se supone que se quiere enviar el mensaje “HOLA”. Para ello, a cada letra del abecedario se le adjudicará un número de 0 a 26 (“A” es 0, “B” es 1, etc). Si se quiere encriptar el mensaje, se necesita una clave con el mismo número de letras, por ejemplo “ZUMO”.

```
      H       O       L       A    mensaje
   7 (H)   14 (O)  11 (L)    0(A)  mensaje
+  25 (Z)  20 (U)  12 (M)  14 (O)  clave
=  32      34      23      14      mensaje + clave
=  6 (G)    8 (I)  23 (X)  12 (M)  mensaje + clave (mod 26)
      G       I       X       M   mensaje cifrado
```

Cada letra del mensaje se suma modularmente con la letra correspondiente de la clave, para asegurarnos de que el resultado de esta suma vuelve a ser un número entre 0 y 26 (es decir, una letra del abecedario). Por tanto, el mensaje que se envía en lugar de “HOLA” es “GIXM”. Con el mensaje cifrado en su poder, el receptor solo tiene que realizar el proceso inverso para descifrar el mensaje. Es decir, ahora hay que restar la clave al mensaje encriptado.

```
      G       I       X       M   mensaje cifrado
    6 (G)   8 (I)  23 (X)  12 (M)  mensaje cifrado
-  25 (Z)  20 (U)  12 (M)  14 (O)  clave
= -19     -12     11      -2      mensaje cifrado - clave
=   7 (H)  14 (O)  11 (L)   0(A)   mensaje cifrado - clave (mod 26)
      H       O       L       A    mensaje
```

Protocolo general

Situación de partida

La información cuántica permite que un emisor (Alice) envíe un mensaje a un receptor (Bob). Para ello disponen de lo siguiente

- Objetos cuánticos, es decir, objetos físicos que se comportan siguiendo las leyes de la física cuántica. En la práctica, estos objetos son fotones que pueden encontrarse en diferentes estados de polarización: pueden estar

polarizados verticalmente (0), horizontalmente (1) o en cualquiera de los estados resultantes de superponer ambos. Dicha polarización puede ser detectada mediante el uso de filtros, que dejan pasar los fotones polarizados en un estado y absorben los polarizados en el otro.

- Un canal cuántico, que no es más que un canal físico de comunicación que puede transmitir información cuántica, así como clásica. Un ejemplo de canal cuántico es la conocida fibra óptica.
- Un canal clásico de comunicación que debe estar autentificado, es decir, Alice tiene que estar segura de que es a Bob a quien está enviando la información.

Ahora bien, la criptografía cuántica es lo que permite que Alice y Bob se comuniquen en secreto. En otras palabras, la criptografía cuántica hace posible detectar si el mensaje ha sido interceptado por un espía (Eva). Para llevar a cabo el protocolo de encriptamiento son necesarios dos elementos:

- Un algoritmo, que se encarga de manipular el mensaje para ocultarlo y hacerlo ilegible a terceros. Es decir, su función es la de encriptar el mensaje y desencriptarlo posteriormente para que pueda ser leído por el receptor. El algoritmo es conocido por las dos partes que se intercambian el mensaje, pudiendo llegar a ser incluso público. Es por ello que se necesita un elemento más para poder encriptar un mensaje.
- Una clave (secuencia de ceros y unos) conocida previamente por ambas partes, que es la que asegura que el proceso se mantenga privado, ya que como se ha dicho, el algoritmo puede ser de conocimiento público.

En función de la clave se pueden dividir los protocolos de encriptación en dos categorías: protocolos simétricos y antisimétricos. Los protocolos simétricos son aquellos en los que la clave es la misma para ambas partes, y los antisimétricos son aquellos en los que emisor y receptor poseen claves diferentes.

El establecimiento de la clave es el principal problema de la criptografía cuántica, ya que no hay forma de que Alice y Bob compartan una clave incondicionalmente segura mediante la información clásica.

No obstante, existen algunos algoritmos cuya seguridad está demostrada matemáticamente (como el cifrado de Vernam), o se basan en la complejidad de descifrarlo sin la clave secreta (sistema RSA, cuya seguridad no está rigurosamente probada). Algoritmos tales como el de Vernam y RSA son los más empleados hoy en día.

Detección de espionaje

La información clásica puede ser copiada sin que la información original se vea modificada. Por ello, trabajando con sistemas de comunicación clásicos no se puede saber con certeza si un mensaje ha sido manipulado por una tercera parte. Dicho de otro modo, en física clásica, Eva puede espiar y manipular el mensaje que Alice envía a Bob sin que ellos puedan descubrirlo.

Sin embargo, en mecánica cuántica el hecho de medir hace que el estado cuántico inicial se perturbe, se modifique. Esto se traduce en que si Eva intercepta el mensaje, Alice y Bob pueden descubrirlo fácilmente. Este hecho viene garantizado por:

- El teorema de no clonado. Este teorema nos asegura que "no pueden existir máquinas o dispositivos de clonación cuánticas". En otras palabras, no es posible hacer copias exactas de la información cuántica.
- El tercer postulado de la mecánica cuántica o de la reducción del paquete de ondas, que asegura que, al realizar una medida sobre un estado cuántico, este se está modificando.

Así, cuando Eva intercepta el mensaje entre Alice y Bob introduce anomalías (ruidos o errores), que pueden ser detectados por Alice y Bob.

Se puede demostrar que existe una relación entre la cantidad de anomalías introducidas en el mensaje y la cantidad de información que Eva ha interceptado, de esta manera es posible saber, no solo que Eva ha interceptado información, sino también la cantidad. Esta inspección es posible llevarla a cabo con las llamadas pruebas de seguridad, que combinan las leyes de la física cuántica y de la teoría de la información.

Información secreta

Primero, Alice y Bob evalúan el nivel de error y ruido que separan los dos conjuntos de datos. Las diferencias entre estos pueden provenir de:

- La intervención de Eva, que añade errores y ruido.
- Los errores y ruido de fondo, que no pueden ser evitados completamente.

Sin embargo, como los errores en la comunicación y los efectos de la observación de Eva no pueden ser distinguidos, por seguridad Alice y Bob deben suponer que todas las incoherencias son debidas a un espía.

Luego, gracias a las pruebas de seguridad y a ese nivel de ruido, Alice y Bob pueden evaluar la cantidad de información que ha interceptado Eva, llamada I_E. A la misma vez, la teoría de la información les permite evaluar la cantidad de información que comparten después de la transmisión I_{AB}.

Finalmente, si la cantidad de información $\Delta I = I_{AB} - I_E$ es superior a cero, es decir, la cantidad de espionaje permanece por debajo de cierto umbral, entonces se puede extraer una clave secreta de tamaño máximo ΔI de la trasmisión.

En el caso contrario, ninguna extracción es posible y la transmisión debe ser interrumpida.

Extracción de la clave

En el caso en el que la información secreta, ΔI, sea superior a cero, Alice y Bob pueden empezar la extracción de la clave. Alice y Bob no comparten todavía una clave, sino datos correlacionados.

La extracción se compone por dos etapas: la reconciliación y la amplificación de la confidencialidad.