Criptografía Cuántica

Gregoria Blanco y Ángeles Martínez[1]

Resumen

La posibilidad de factorizar números en tiempo polinómico mediante el algoritmo de Shor y un ordenador cuántico supone un claro ataque a la seguridad del criptosistema de clave pública RSA. Sin embargo lo que la Mecánica Cuántica quita con una mano, lo da con la otra y es posible diseñar protocolos de distribución de claves privadas cuya seguridad está garantizada por las propias leyes de la Mecánica Cuántica.

El objetivo de este artículo es dar a conocer los protocolos más relevantes de generación de claves privadas usando técnicas cuánticas y esbozar una línea de trabajo encaminada a analizar algunas estrategias de espionaje que se pueden efectuar y su repercusión en la generación de una clave segura.

1 Introducción

Uno de los problemas de mayor dificultad práctica a la hora de llevar a cabo una comunicación segura mediante un sistema de clave privada es la distribución segura de las claves. Un resultado de Shannon de 1949 [4] establece que si la clave es aleatoria, de la misma longitud que el mensaje a cifrar y se usa una única vez, la codificación es segura. De hecho es el único sistema que está probado que es seguro. Sin embargo, la necesidad de distribuir y almacenar de manera segura las claves en general largas y de un solo uso, claramente apuntan al limitado uso que puede hacerse de este sistema.

Precisamente una de las razones del éxito obtenido por el sistema de codificación con clave pública es que permitía prescindir de acordar y distribuir la clave secreta. Sin embargo la seguridad de este sistema nunca ha sido probada matemáticamente. No se sabe si factorizar un número puede hacerse en tiempo polinómico, simplemente no se ha encontrado un algoritmo que lo haga, de modo que la seguridad práctica de este sistema viene proporcionada por el coste computacional de la factorización. La construcción de un ordenador cuántico en el que se implemente el algoritmo de Shor que permite factorizar en tiempo polinómico supondría claramente la fractura definitiva del RSA.

Las leyes de la mecánica cuántica, sin embargo, proporcionan herramientas para abordar el problema de la distribución segura de claves privadas. Esencialmente consiste en que los comunicantes se transmiten la clave privada a través de un canal cuántico y la aportación cuántica a la seguridad del proceso es que un espía no puede extraer información sin revelar su presencia a los comunicantes.

2 Sistema cuántico del fotón

Un fotón puede interpretarse físicamente como un campo eléctrico ortogonal a su dirección de propagación (pongamos el eje $0Z$). La polarización de este campo determina el estado cuántico del fotón y se representa por una dirección en el plano XY, es decir por un vector unitario. Experimentalmente se ha observado que con un dispositivo físico de medida capaz de distinguir entre la polarización horizontal $|\rightarrow\rangle$ y la vertical $|\uparrow\rangle$, cuando recibe un fotón con polarización $a|\rightarrow\rangle + b|\uparrow\rangle$, el dispositivo detecta el estado $|\rightarrow\rangle$ con probabilidad $|a|^2$ y $|\uparrow\rangle$ con probabilidad $|b|^2$.

El modelo matemático de un sistema cuántico es un espacio de Hilbert complejo. A los vectores unitarios de este espacio se les denomina *estados*. En el caso concreto del sistema cuántico de un fotón estaremos en el espacio bidimensional generado por una base ortonormal y con el producto hermítico que hace que esa base sea ortonormal. A los estados de este espacio se les denomina *qubits* y al espacio se le denomina *espacio de 1-qubit*. Consideremos

[1]Dpto. Matemática Aplicada. E.U. Informática. Universidad Politécnica de Madrid. E-mail: {gblanco,ams}@eui.upm.es

la base $[|\rightarrow\rangle, |\uparrow\rangle]$ y $\mathcal{V} = \mathcal{L}(|\rightarrow\rangle, |\uparrow\rangle)$. Si $\psi = a|\rightarrow\rangle + b|\uparrow\rangle$ es un estado, a los coeficientes a, b se les denomina *amplitudes* y el cuadrado de sus módulos tienen un significado probabilístico que ya apuntabamos y que precisaremos en breve.

El sistema cuántico de dos fotones se modeliza mediante el espacio producto tensorial de los espacios asociados a cada fotón, con el producto escalar inducido. Análogamente se define el sistema cuántico de n fotones como el producto tensorial de los n espacios asociados a cada uno de los fotones. Tiene dimensión 2^n y se le denomina *espacio de n-qubits*.

Medir un estado cuántico consiste esencialmente en proyectar ortogonalmente el estado. Medir respecto de una base ortonormal $[|\xi_1\rangle, |\xi_2\rangle]$ el estado de un fotón $\psi = a|\xi_1\rangle + b|\xi_2\rangle$ consiste en un proceso en el que se observa el estado $|\xi_1\rangle$ con probabilidad $|a|^2$, el estado $|\xi_2\rangle$ con probabilidad $|b|^2$ y tras el cual el estado resultante ψ' es $\frac{a}{|a|}|\xi_1\rangle$ en el primer caso y $\frac{b}{|b|}|\xi_2\rangle$ en el segundo, es decir, ψ' es la proyección ortogonal (normalizada) sobre el espacio generado por el elemento de la base observado.

Cuando se tiene un sistema cuántico de dos fotones en estado $\psi = a|\xi_1\rangle \otimes |\xi_1\rangle + b|\xi_1\rangle \otimes |\xi_2\rangle + c|\xi_2\rangle \otimes |\xi_1\rangle + d|\xi_2\rangle \otimes |\xi_2\rangle = a|\xi_1\xi_1\rangle + b|\xi_1\xi_2\rangle + c|\xi_2\xi_1\rangle + d|\xi_2\xi_2\rangle$, medir el estado del primer fotón respecto de la base $[|\xi_1\rangle, |\xi_2\rangle]$ consiste en un proceso en el que se observa el estado $|\xi_1\rangle$ con probabilidad $|a|^2 + |b|^2$, el estado $|\xi_2\rangle$ con probabilidad $|c|^2 + |d|^2$ y tras el cual el estado resultante ψ' es la proyección ortogonal (normalizada) sobre el espacio generado por el elemento de la base observado: $\psi' = \frac{a}{\sqrt{|a|^2+|b|^2}}|\xi_1\xi_1\rangle + \frac{b}{\sqrt{|a|^2+|b|^2}}|\xi_1\xi_2\rangle$ en el primer caso y $\psi' = \frac{c}{\sqrt{|c|^2+|d|^2}}|\xi_2\xi_1\rangle + \frac{d}{\sqrt{|c|^2+|d|^2}}|\xi_2\xi_2\rangle$ en el segundo.

Nótese esta peculiaridad de la mecánica cuántica de que cuando se mide un estado éste cambia irreversiblemente, salvo los estados de la propia base respecto de la que se mide (o múltiplos de ellos).

Existen una serie de resultados que se deducen de los postulados de la mecánica cuántica que permiten derivar protocolos de generación y distribución de claves privadas a través de un canal cuántico (por ejemplo un cable de fibra óptica si la clave se codifica mediante estados de polarización de fotones) de modo que la presencia de espías no autorizados no sea transparente.

El primero de ellos ya se ha comentado anteriormente: cuando se mide un estado para obtener información sobre él, éste se destruye. El segundo es que no es posible clonar estados, es decir, hacer copias idénticas de un estado desconocido. El tercero es la imposibilidad de distinguir estados no ortogonales.

3 Protocolos de distribución de claves

En un proceso de distribución cuántica de claves, intervienen un emisor y un receptor, comúnmente denominados Alicia y Benito, un espía, Eva, y dos canales de comunicación, uno cuántico para enviar fotones y otro clásico para reconciliar y depurar información. Eva puede acceder al canal clásico sin alterar los datos que observa, y también puede acceder al canal cuántico y usar todos los medios que desee con la única restricción de que sean compatibles con las leyes de la mecánica cuántica.

A grandes rasgos las fases de un protocolo de generación de claves son: generación y distribución de la clave, análisis de errores, y correción de errores y amplificación de la privacidad. A continuación se describe cada una de ellas a través de los dos protocolos más representativos.

3.1 Generación y distribución de claves

Uno de los esquemas más sencillos para la generación aleatoria de claves es el protocolo $BB84$. En este protocolo Alicia utiliza un canal cuántico para enviar a Benito una cadena de qubits, eligiendo aleatoriamente cada uno de ellos entre los cuatro estados de las bases $B_1 = [|\rightarrow\rangle, |\uparrow\rangle]$ y $B_2 = [|\nearrow\rangle, |\searrow\rangle]$ que se identifican con las polarizaciones horizontal, vertical, 45° y -45° respectivamente. Cuando Benito los recibe, mide, también aleatoriamente, cada uno de ellos en la base B_1 o en B_2, y a continuación ambos utilizan un canal público para localizar y eliminar los casos en que las mediciones se han realizado en la base inadecuada o los detectores no han registrado la llegada de un fotón. Si ambos conservan únicamente los estados

que se han medido en la base a la que pertenecen, la cadena de estados de los dos es la misma.

Finalmente traduciendo como 0 los estados que corresponden a los primeros vectores de cada base, y como 1 los segundos, si no ha habido interferencia de espías, Alicia y Benito tienen una clave común.

Otros protocolos, un poco más complicados, usan estados de dos qubits y se basan en el efecto EPR (Einstein - Podolsky - Rosen). Este efecto, comprobado por vía experimental, se pone de manifiesto cuando un átomo con simetría esférica emite dos fotones en direcciones opuestas. El estado de polarización inicial de los fotones es indefinido, pero en el instante en que se mide uno de ellos, la polarización del otro queda automáticamente determinada. Este tipo de estados se denominan *estados entrelazados* o pares EPR, y matemáticamente corresponden a los vectores del espacio de 2-qubits que no se pueden expresar como producto vectorial de dos qubits.

Si dos fotones en estado entrelazado $\varphi = \frac{1}{\sqrt{2}}(|\rightarrow\rightarrow\rangle + |\uparrow\uparrow\rangle)$ se imaginan como dos monedas tan distantes como se desee, el efecto EPR significa que cuando una de las monedas se tira al aire y sale cara, lo cual ocurre con probabilidad $\frac{1}{2}$, la otra también sale cara y lo mismo sucede si al lanzar una de ellas sale cruz.

Este fenómeno de acción instantánea tiene aplicaciones inmediatas en la generación automática de claves y además la mecánica cuántica permite construir dispositivos que se rigen por dicho principio.

En efecto, si en el estado φ anterior se quiere medir el primer qubit en la base B_1, el estado resultante tras la medida será $|\rightarrow\rightarrow\rangle$ con probabilidad $\frac{1}{2}$ o bien el estado $|\uparrow\uparrow\rangle$ con probabilidad $\frac{1}{2}$. Es evidente que si a continuación se mide el segundo qubit de nuevo en la base B_1, la medida no altera el estado, y esto significa en particular que la medida del primer qubit y del segundo coinciden. Este resultadoes el fundamento del protocolo para generar una clave aleatoria.

Supongamos que se tiene una fuente capaz de generar pares EPR, por ejemplo el estado φ anterior, y que envía el primer qubit a Alicia y el segundo a Benito. Si envía según este procedimiento un determinado número de pares, Alicia y Benito pueden generar una cadena de bits del modo siguiente: ambos miden aleatoriamente cada una de sus mitades en la base B_1 o en B_2, y tras la medida traducen el resultado a 0 o a 1, con el mismo esquema que se sigue en el protocolo $BB84$. Por las propiedades de medida del estado φ, es claro que, en ausencia de espías, Alicia y Benito van a tener los mismos resultados siempre que midan en la misma base, y por tanto, basta utilizar un canal público para analizar la coincidencia de bases y descartar los casos de discrepancia para obtener una clave común.

3.2 Análisis de errores

En condiciones ideales (dispositivos de emisión y medida perfectos, ausencia de espías), los pocedimientos anteriores conducen a una clave aleatoria común, pero si un espía intercepta la emisión de los estados y lo hace midiendo, por las leyes de la mecánica cuántica, en general el estado resultante tras la medición va a ser diferente del original y los interlocutores van a poder detectarlo.

Para estudiar la presencia de espías, Alicia y Benito eligen un subconjunto de los elementos de sus cadenas y usan un canal público para compararlo. Si hay discrepancias significa que ha habido un espía. En particular, es fácil probar que si la estrategia que usa el espía es medir en la base B_1 o en B_2 aleatoriamente, en el protocolo $BB84$ y en el de los pares EPR, su probabilidad de acierto en un bit es del 75% y Benito pasa del 100% de aciertos al 75%. Además, analizando el número de discrepancias se puede estimar la cantidad de información que el espía ha podido obtener, y el número total de errores de los elementos restantes de la cadena. En función del resultado obtenido se puede decidir si es posible depurarla o es necesario abortar el protocolo y empezar de nuevo.

3.3 Corrección de errores y amplificación de la privacidad

Una vez que se tiene una clave y se sabe que contiene un número de errores menor que una cota establecida de antemano, hay varias técnicas que permiten corregir dichos errores y reducir la información del espía.

La primera de ellas, que es la más elemental y conocida, consiste en usar métodos de partición en bloques y test de paridad para eliminar los errores. Suponiendo que se puede partir la clave en

bloques que contengan solo un error, y comparando las paridades de cada bloque, con alta probabilidad se detectan todos los errores, pero no se reduce la información del espía. A continuación, de nuevo se usan las paridades de un determinado número de subconjuntos de la cadena obtenida en el paso anterior para elaborar una nueva clave que, de nuevo con alta probabilidad, el espía no conoce.

Otra forma, más elegante que la anterior, consiste en usar dos códigos clásicos correctores de errores. Si t es una cota superior del número de errores que contiene la clave, basta usar un código $t-corrector$ para obtener una nueva clave sin errores. La idea consiste en que Alicia elige aleatoriamente una palabra x del código y le envía a Benito la suma de su cadena con x. Cuando Benito la recibe, primero le suma su cadena y después descodifica el resultado obtenie ndo, con alta probabilidad, la palabra x. Como en el procedimiento anterior, este primer paso no reduce la información del espía, y por eso es necesario usar un segundo código que a partir de la clave sin errores, proporcione otra clave segura.

4 Seguridad de los protocolos

Un protocolo de distribución cuántica de claves se dice que es *seguro* si, para cada par de parámetros de seguridad $s > 0, l > 0$ elegidos por Alicia y Benito, y para cada estrategia de espionaje de Eva, o bien el esquema aborta o bien aporta una clave aleatoria con probabilidad al menos $1 - O(2^{-s})$, y garantiza que la información de Eva sobre la clave final es menor que 2^{-l}.

Existen varias demostraciones de que los dos protocolos citados son seguros [5, 2]. Nuestro trabajo está centrado en estudiar algunas estrategias concretas de espionaje basadas en la capacidad del espía de realizar entrelazamiento de qubits y computación cuántica.

Referencias

[1] N. Gisin, G. Ribordy, W. Tittel and H. Zbinden. *Quantum cryptography.* http://arxiv.org/pdf/quant-ph/0101098. 2001.

[2] H. Inamori, N. Lütkenhus and D. Mayers. *Unconditionaly Security of the BB84 Quantum Key Distribution Protocol.* http://arxiv.org/pdf/quant-ph/0107017 v1. 2001.

[3] M. A. Nielsen and I. L. Chuang *Quantum Computation and Quantum Information.* Cambridge Univerity Press, 2000.

[4] C. E. Shannon. *Communication theory of secrecy systems.* Bell System Technical Journal. vol. 28 pp.656-715. 1949.

[5] P. W. Shor and J. Preskill. *Simple Proof of Security of Practical Quantum Key Distribution.* http://arxiv.org/pdf/quant-ph/0003004 v2. 2000.