Criptografía cuántica

Alfonsa García López
Jesús García López de la Calle

Dpto. Matemática Aplicada
Escuela Universitaria de Informática, Universidad Politécnica de Madrid
Cr. Valencia Km.7 28031 Madrid
garcial@eui.upm.es
jglopez@eui.upm.es

La criptografía cuántica es una de las aplicaciones más importantes de la computación cuántica. En este modelo de computación la unidad elemental de información es el qubit, que se define a partir de dos estados básicos denotados por $|0\rangle$ y $|1\rangle$. Un estado cuántico de un qubit es una combinación lineal de estos dos estados, $\phi = a|0\rangle + b|1\rangle$, tal que $|a|^2 + |b|^2 = 1$. Es decir ϕ es un vector unitario del espacio de Hilbert complejo $\mathcal{H}$, en el que $B = [|0\rangle, |1\rangle]$ es una base ortonormal.

Al medir un estado cuántico, éste se proyecta sobre uno de los vectores de la base ortonormal considerada. De este modo, al medir el estado ϕ, usando la base B, se obtendrá $|0\rangle$ con probabilidad $|a|^2$, o $|1\rangle$, con probabilidad $|b|^2$.

Un estado cuántico de n qubits es un vector de norma 1 del espacio de Hilbert complejo $\mathcal{H}_n = \mathcal{H} \otimes \cdots \otimes \mathcal{H}$, de dimensión 2^n, cuya base es $B_n = [|x_0\rangle, \cdots, |x_{2^n-1}\rangle]$, donde cada $x_j \in \{0,1\}^n$ es la representación binaria del número $j \in \{0 \cdots 2^n - 1\}$. (Los vectores de B_n son todos los productos tensoriales de n vectores de B.)

La potencia de la computación cuántica se basa en el paralelismo cuántico, derivado del hecho de que aplicar una transformación a un estado cuántico, superposición de todos los estados de la base, es como operar simultámeamente con todas las posibles cadenas de n bits.

En 1994 aparece el primer resultado verdaderamente importante en computación cuántica. Se trata de los algoritmos polinomiales para la factorización de números enteros y cálculo de logaritmos discretos propuestos por P. Shor, que abren la posibilidad de que los ordenadores cuánticos puedan romper los criptosistemas de clave pública.

Sabemos que la codificación usando claves privadas aleatorias de un solo uso permite llevar a cabo una comunicación segura. Pero presenta la dificultad práctica de la distribución segura de las claves. Afortunadamente, las leyes de la mecánica cuántica proporcionan herramientas para abordar el problema de la distribución segura de claves privadas. La aportación cuántica a la seguridad del proceso consiste

esencialmente en que un espía no puede extraer información sin revelar su presencia a los comunicantes, ya que por las leyes de la mecánica cuántica no es posible copiar estados.

Existen diversos protocolos para la distribución cuántica de claves privadas. El más sencillo fue propuesto en 1984 por C.H. Bennett y G. Brassard y se conoce como $BB84$. Después se propusieron diversas modificaciones que dan lugar a otros protocolos esencialmente equivalentes.

En un proceso de distribución cuántica de claves, intervienen un emisor y un receptor y dos canales de comunicación, uno cuántico para enviar fotones y otro clásico para reconciliar y depurar la información. Los dos comunicantes usan un trozo de su clave para detectar la presencia de espías. El posible espía puede acceder al canal clásico, 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.