



# Realidades del secreto cuántico

En abril de este año se ha puesto en marcha el proyecto *SECOQC - Development of a Global Network for Secure Communications based on Quantum Cryptology*<sup>1</sup>, dotado con 11 M€ por parte de la UE, dentro del 6º Programa Marco, y dirigido por la unidad de tecnologías cuánticas de la compañía austriaca ARC Seibersdorf Research. En este proyecto hay 41 participantes (3 pymes, 25 universidades, 5 centros nacionales de investigación y 8 empresas privadas) de doce países de la UE entre los que, como no es infrecuente, no está el nuestro.

En su nota de prensa los promotores vaticinan que pronto será sustituida la tecnología criptográfica que conocemos y que está basada en problemas matemáticos difíciles de resolver, por las tecnologías cuánticas basadas en las leyes de la naturaleza (cuántica). Para esta premonición ponen la fecha de cuatro años como el tiempo necesario para que se inicie, a costes permisibles, la producción de sistemas cuánticos de distribución de claves. De hecho, el Dr. Christian Monyk, responsable comercial de Quantum Technologies e iniciador del proyecto afirma: *"Proporcionaremos una herramienta, basada en tecnología cuántica, que permitirá a las empresas proteger sus activos frente al espionaje industrial"*, y continúa afirmando que *"En el pasado, se pueden atribuir a la vigilancia del sistema Echelon y otras redes de interceptación, el espionaje industrial que ha producido pérdidas financieras significativas"*. Para terminar, el mencionado portavoz confiesa que *"Su ánimo es hacer una contribución significativa a la independencia y competitividad de la economía europea"*.

A la vista de este tipo de afirmaciones es conveniente aclarar algunos aspectos de lo que últimamente se esconde detrás de la cada día más utilizada expresión "criptografía cuántica". Las raíces de esta disciplina están en la propuesta originaria de Stephen Wiesner llamada *"Conjugate Coding"* y que fue presentada a principios de los años 70. Este concepto fue publicado en 1983 en *Sigact News* y, en esa fecha, Bennett (IBM Research Labs.) y Brassard (Universidad de Montreal) propusieron el primer protocolo criptográfico cuántico, pero hubo que esperar

**La Unión Europea ha decidido invertir 11 M€ en un proyecto de criptografía cuántica y este término ha vuelto a aparecer, una vez más, en los medios de información. Dado que en este, como en muchos otros temas, hay intereses creados no siempre claros y bien difundidos, en esta ocasión debemos prestar cierta atención a lo que realmente puede ofrecer esta tecnología y a quienes realmente puede interesar. De este modo podremos estar "más seguros" de lo que se nos cuenta.**

hasta 1991 para que se hiciera el primer prototipo experimental de este protocolo sobre una distancia real de 32 centímetros<sup>2</sup>. Sistemas experimentales más recientes han comprobado su validez y funcionamiento en fibras ópticas extendidas a lo largo de decenas de kilómetros.

Aunque no suele resaltarse, hay que recordar que la criptografía cuántica es lenta, trabaja en distancias cortas y sólo sirve, actualmente, para el intercambio seguro de claves simétricas (la misma en los dos extremos) como las usadas en el cifrado convencional (simétrico) de las VPNs o en el envío y almacenamiento de mensajes. Investigadores en la Northwestern University (Evanston, Illinois) dicen que pronto tendrán disponible una tecnología cuántica capaz de cifrar a velocidades de 2.5-Gbit/s, por lo que podrían proteger líneas troncales importantes, pero no hablan de a qué distancia estarán los intercomunicadores.

El interés principal de la tecnología cuántica es que elimina completamente la posibilidad de que alguien esté "escuchando" en el canal de comunicación y tal acción pase inadvertida por los extremos comunicantes. Sin embargo, si los límites máximos se fijan en algunos kilómetros, las grandes distancias tendrán que cubrirse con numerosas estaciones repetidoras en las que esa característica ya no se satisfaría.

Hace más de un año, MagiQ Technologies<sup>3</sup> anunció la puesta en el mercado el primer sistema criptográfico comercial basado en principios cuánticos, y fue seguida rápidamente por su homóloga ID Quantique<sup>4</sup>. Actualmente, la tecnología disponible está limitada a conexiones punto-a-punto y a distancias máximas de 50 km. El precio de uno de esos sistemas es, hoy en día, prohibitivo (la unidad de MagiQ cuesta entre 50 y 100 mil dólares). Estas unidades son una combinación de las técnicas de criptografía cuántica y la criptografía tradicional para montar redes virtuales privadas (VPNs) sobre fibras ópticas. A pesar de su alto precio, uno puede imaginar que en el futuro estas unidades puedan estar incluidas dentro de las propias infraestructuras de comunicaciones, muy lejos de los usuarios

finales de la misma. Así, estos sistemas, de terminar instalándose, no serán de uso común y, probablemente, queden reservados para redes con transacciones financieras muy sensibles y para aplicaciones militares. Actualmente, las compañías que explotan grandes redes de fibra óptica han demostrado algún interés en esta tecnología como mecanismo comercial diferenciador ya que estiman poder aumentar un 30 ó 40 % su valor comercial ofertando "líneas de comunicación ultra seguras".

El reciente interés práctico por la criptografía cuántica anida en los aspectos más preocupantes de la criptografía de clave pública que sustenta servidores web, herramientas personales de seguridad (PGP) y muchos protocolos de comunicaciones (SSL, SSH, etc.). Todas esas aplicaciones se basan en el tiempo que requiere descomponer números grandes en sus factores primos y cuya complejidad los matemáticos no han sido capaces de demostrar. Por ello, algunos piensan, y a unos pocos les va el negocio en hacer pensar, que la criptografía de clave pública puede tener los pies de barro y que agencias estatales como la NSA americana o el contraespionaje israelí sí pueden factorizar los módulos que los usuarios finales y empresas estamos utilizando.

La teoría criptológica afirma que las claves secretas uniformes, aleatorias, de un solo uso y de longitud igual a la del mensaje que cifran, permiten asegurar que sólo el receptor del mensaje puede terminar descifrándolo (cifrado Vernam); pero en la práctica las claves no son tan largas (56- 256 bits) por lo que se emplean varias veces para cifrar mensajes más largos. En este y muchos otros casos, hasta la clave más secreta siempre puede descubrirse por "prueba y error", por lo que la seguridad real la marcan las velocidades a las que el atacante puede probar un número suficiente de claves.

La criptografía cuántica puede terminar siendo una solución tecnológica válida en algunos escenarios muy concretos, pero es poco probable que logre salir de tan estrechos confines. Los desarrollos realizados

en los últimos doce años nos sugieren que ese escenario serán largas líneas de comunicaciones troncales basadas en fibras ópticas o comunicaciones aéreas con satélites artificiales volando encima de nuestras cabezas pero, por el momento, no parece que vaya a

afectar al usuario individual final. Quizás las grandes compañías, capaces de mantener enlaces transnacionales, necesiten de la criptografía cuántica pero no va a ser una solución, como alegremente invocan los promotores del proyecto *SECOQC*, al espionaje industrial o a los mecanismos de vigilancia electrónica de los norteamericanos y de sus fieles aliados de peso. Por mucho que se aseguren algunos elementos o tramos de los sistemas de información, la seguridad depende del más débil de todos ellos. Aún haciendo inquebrantable las comunicaciones cuando transitan por una fibra óptica, la información podrá ser interceptada en muchos otros puntos y mediante una abundante colección de herramientas o métodos. Por ello, un excesivo fervor a la hora de hablar de los métodos cuánticos quizás lo que esté consiguiendo es hacer que nos olvidemos de lo mucho que no puede hacer esta tecnología, y su seguridad real va estar definida más por lo que no puede hacer que por lo que sí hace.

Pensar en el papel que puede jugar hoy en día la criptografía cuántica nos remonta al mes de octubre de 1861, fecha en la que se termina la primera línea telegráfica transcontinental norteamericana y momento en el que han transcurrido seis meses de guerra civil. Ya en aquel conflicto, la información era tan importante como las tropas o los cañones, y los agentes de ambos bandos podían subirse a los postes telegráficos y conocer los planes del enemigo. Ya en aquel momento se utilizaron curiosos, antiguos y vetustos sistemas criptográficos europeos (*nomenclators* o libros de códigos) para resolver—con dispar éxito por cierto—, este problema. Muchos de los códigos utilizados entonces no fueron rotos a tiempo, pero el espionaje clásico y al estilo Mata Hari ya tuvo su efecto en la resolución final del conflicto. ■

**JORGE DÁVILA MUÑOZ**

Director  
Laboratorio de Criptografía  
**LSSI - Facultad  
de Informática - UPM**  
jdavila@fi.upm.es

<sup>1</sup>Ver <http://www.quantenkryptographie.at/>

<sup>2</sup>Ver <http://monet.mercersburg.edu/henle/bb84/>

<sup>3</sup>Ver <http://www.magiqtech.com/>

<sup>4</sup>Ver <http://www.idquantique.com/index.html>