Los secretos mejor guardados del mundo

Dos empresas utilizan un sistema basado en la física cuántica para transmitir datos imposibles de interceptar

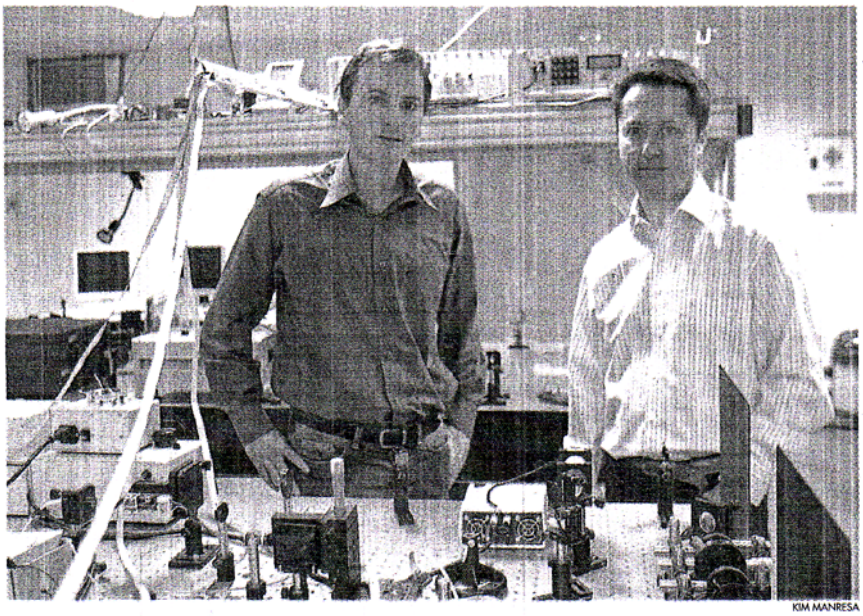
JOSEP CORBELLA

BARCELONA. – Son datos que nadie puede interceptar sin delatarse. Aprovechando los principios de la física cuántica, que dicen que no se puede observar una partícula sin modificarla, una empresa suiza y una estadounidense han empezado a comercializar ya un sistema de transmisión de datos invulnerable. El sistema tiene aún sus limitaciones: permite transmitir un máximo de un megabit por segundo, a un máximo de cien kilómetros de distancia, y cuesta entre 50.000 y 100.000 euros por unidad. Todo ello restringe su uso, por ahora, a unos pocos gobiernos –en particular, sus ejércitos– y unos pocos bancos. Pero en el futuro la llamada criptografía cuántica puede ayudar a mejorar la seguridad de las transacciones por internet y otras transmisiones de datos privados.

Físicos del Institut de Ciències Fotòniques (ICFO) de Barcelona han presentado desde principios de año tres investigaciones que sientan las bases para ampliar las posibilidades de la criptografía cuántica. Las investigaciones publicadas en *Physical Review Letters*, considerada la revista de física más importante, permiten establecer hasta qué punto un canal de comunicación es seguro, cómo hay que codificar la información para obtener una seguridad máxima y qué volumen de datos se puede encriptar.

"No es que los sistemas actuales no sean seguros", advierte Ignacio Cirac, investigador del Instituto Max Planck en Munich (Alemania), asesor del ICFO y coautor de una de las investigaciones. Pero los ordenadores cuánticos que los físicos esperan crear en las próximas décadas tendrán una capacidad de cálculo tan fabulosa que podrán descifrar cualquiera de los códigos de seguridad actuales. "Para lo que sirve la criptografía cuántica –advierte Cirac– no es para evitar que alguien intercepte nuestras transmisiones hoy día. Pero si transmitimos datos que queremos que sigan siendo secretos dentro de 30 años, como puede ocurrir en relaciones entre gobiernos, debemos enviar la información de un modo que no la pueda leer ni un ordenador cuántico".

Una prueba de su interés estratégico es que el Laboratorio Nacional de Los Álamos, donde Estados Unidos desarrolla parte de su investigación militar, ha reclutado uno de los grupos de trabajo más potentes del mundo. La nueva tecnología se basa en codificar la información en fotones que se transmiten por cables de fibra óptica. Un emisor llamado Alicia envía información a un receptor llamado Bob, y un espía llamado Eva intenta interceptarla. "La gente se aburrió de hablar del emisor A y el receptor B, y a la A ahora todos los investigadores la llamamos Alicia y a la B, Bob", explica Antonio Acín, coautor de las investigaciones del Icfo. "Eva viene del inglés *eavesdropper* [persona que escucha conversaciones ajenas], que se abrevió a Eve, o sea, Eva".



KIM MANRESA

Antonio Acín (izquierda) e Ignacio Cirac, en el laboratorio del Institut de Ciències Fotòniques de Barcelona

En los trabajos de Acín, los fotones se envían de dos en dos para aprovechar un extraño principio de la física cuántica llamado entrelazamiento. Dos partículas entrelazadas vienen a ser como un matrimonio: están relacionadas entre ellas incluso cuando estén separadas. Y

Físicos del Institut de Ciències Fotòniques trabajan en las técnicas de la criptografía cuántica

si una de las dos partículas cambia, de manera instantánea cambia la otra. Los físicos no saben muy bien cómo ocurre, pero múltiples experimentos han confirmado que ocurre.

Aquí es donde entra en juego otro extraño principio, también comprobado experimentalmente, según el cual basta con observar una partícula –en este caso, un fotón– para que sus propiedades cambien. Si Alice envía fotones entrelazados a Bob y Eva lee la información, las partículas que le lleguen a Bob habrán cambiado por el camino –concretamente, habrá cambiado lo que los físicos llaman el spin, que es la característica que se utiliza para codificar la información–. En este momento, Bob aún no sabrá que el mensaje que recibe no es el que le ha enviado Alice. Pero cuando instantes después Alice le envíe un segundo mensaje complementario y Bob lo coteje con el primero, descubrirá si un espía lo ha interceptado. "No evitamos que el espía lea la información, pero detectamos el espía inmediamente", explica Acín.

Una de las investigaciones ha demostrado que, siempre que se puedan enviar fotones entrelazados, se puede verificar si un canal es seguro. Una segunda investigación, en la que ha participado Cirac, ha aclarado cómo hay que procesar los fotones en el laboratorio para sacar el máximo beneficio de la criptografía cuántica. Y la tercera establece, en función de la información que se pierde de manera espontánea durante una transmisión y del ruido del canal, qué volumen de datos es posible encriptar.

Id Quantique, de Ginebra, y Magio Technologies, de Nueva York, llevan dos años comercializando sistemas de criptografía cuántica. IBM, Fujitsu, Toshiba y NEC desarrollan productos que aún no han llegado al mercado. "Nos encontramos en el punto en que se encontraba el láser cuando se inventó –explica Cirac–. Nadie sabía para qué serviría y ahora está en todas partes. Con la criptografía cuántica puede ocurrir lo mismo".●

Diez tecnologías que cambiarán el mundo

El Instituto de Tecnología de Massachusetts (MIT) presentó en el 2003 el informe *Diez tecnologías emergentes que cambiarán el mundo*:

CRIPTOGRAFÍA CUÁNTICA. Técnica en que trabajan Acín y otros investigadores del ICFO. Permite transmitir datos que no pueden ser interceptados sin que el emisor se dé cuenta

SEGURIDAD DE SOFTWARE. Nuevas técnicas permitirán evaluar la seguridad de los programas informáticos antes de que los programadores empiecen a escribirlos

COMPUTACIÓN EN GRID. Red de ordenadores en la que todos ellos comparten datos y cada uno realiza una parte del trabajo

TEJIDOS INYECTABLES. Para regenerar articulaciones dañadas, los traumatólogos dispondrán de papillas de células, proteínas y polímeros que se inyectarán, por ejemplo, en la cadera o las rodillas

IMAGEN MOLECULAR. Distintas técnicas de imagen (resonancia magnética, tomografías...) confluyen para observar, tras ser procesadas por ordenador, cómo actúan las moléculas en el cuerpo humano, por ejemplo, para diagnósticos de cáncer

GLICÓMICA. Es la línea de investigación destinada a comprender cómo actúan los azúcares del propio cuerpo humano para mejorar la salud y combatir enfermedades

MECATRÓNICA. Combinación de sistemas mecánicos, componentes electrónicos y software capaces de identificar y corregir errores de forma inmediata en sistemas complejos como coches y aviones

RED DE SENSORES. Pequeños aparatos robóticos dotados de sensores, procesadores y memoria monitorizan su entorno inmediato. Envían sus datos a otros robots por radioondas, creando una red con aplicaciones en gestión de tráfico, de edificios y de ecosistemas

NANOCÉLULAS SOLARES. Capas de cristales y polímeros de 0,2 milímetros de grosor que sirven para crear una nueva generación de paneles solares

LITOGRAFÍA NANOIMPRESA. Nueva técnica de impresión basada en los principios de la nanotecnología