Criptografía cuántica comercial

La criptografía cuántica no pertenece a la mera teoría. Pasó del papel a los laboratorios y, ahora, se materializa en productos tangibles, puestos a la venta

Gary Stix

Charles Bennett no tiene mucha experiencia en el laboratorio. De él se cuenta una de esas típicas anécdotas de físicos distraídos, de teóricos que, ausentes del mundo tangible, causan pequeños desastres; quemó, dicen, una tetera hasta cambiarle el color. Y sin embargo, a él y a sus colegas John A. Smolin y Gilles Brassard se les debe un experimento fundamental, que demostró en 1989 la existencia de una nueva criptografía basada en los principios de la mecánica cuántica.

En aquel experimento los fotones recorrieron un canal de 30 centímetros dentro de una cavidad impermeable a la luz a la que llaman "el ataúd de la tía Marta". La dirección en que oscilaban los fotones, su polarización, representaba los 0 o los 1 de una serie de bits cuánticos, o qubits. Los qubits contenían una clave criptográfica que valía para cifrar o descifrar un mensaje. Salvábase de intromisiones la clave con el principio de incertidumbre de Heisenberg, uno de los fundamentos de la física cuántica: la medida de una propiedad de un estado cuántico perturbará otra. En un sistema criptográfico cuántico, cualquier intruso que quiera fisgonear en un haz de fotones los alterará. Esa perturbación no les pasará inadvertida ni al remitente ni al receptor. Se garantiza así, al menos en principio, la perfecta seguridad de las claves criptográficas.

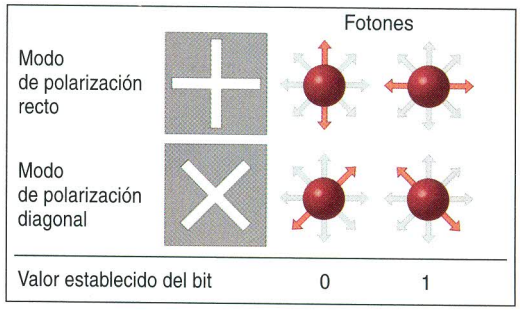
Hoy en día, la criptografía cuántica ha recorrido un largo camino desde aquella precaria exhibición. Ya hay dos pequeñas empresas que venden sistemas criptográficos cuánticos; otros productos semejantes vienen de camino. Con este nuevo método de encriptación, la ciencia de la información cuántica, que combina la mecánica cuántica y la teoría de la información, llega al mercado. El dispositivo supremo que podría darnos sería una computadora cuántica tan potente, que no hubiese otra protección contra su prodigiosa capacidad de descifrar mensajes que la criptografía cuántica.

La criptografía segura requiere que las claves con que se cifran y descifran los mensajes no puedan ser descubiertas por terceros. La criptografía de clave pública es una forma de proveer claves secretas de manera que la encriptación efectuada por una de las partes sólo pueda ser desencriptada por la otra y por nadie más; y ello, pese a que parte de la información pertinente sea de dominio público. La seguridad del procedimiento depende de la dificultad inherente a ciertos problemas matemáticos; en especial,

JEAN-FRANCOIS PODEVIN

CLAVES QUE LA MECANICA CUANTICA MANTIENE SECRETAS

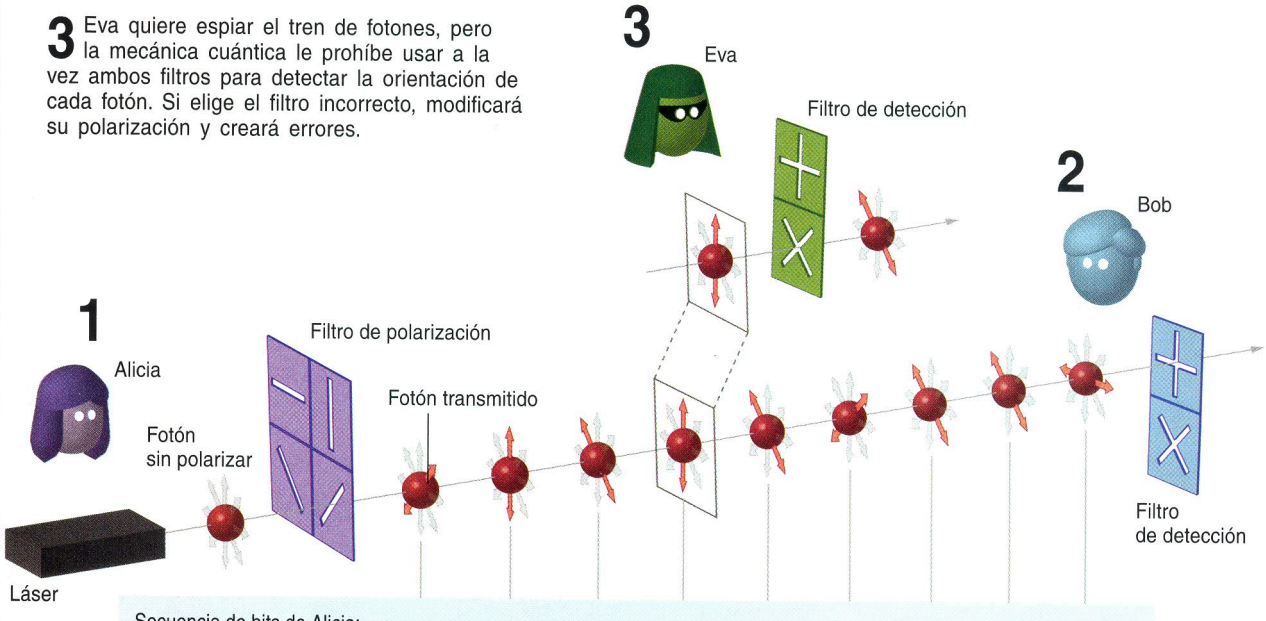
Alicia y Bob intentan mantener en secreto una clave de criptografía cuántica. Para ello, la transmiten en forma de fotones polarizados, procedimiento ideado por Charles Bennett, de IBM, y Gilles Brassard, de la Universidad de Montreal, durante los años ochenta y ahora materializado en algunos incipientes productos comerciales.



1 Para crear una clave, Alicia envía un fotón a través de la rendija 0 o de la 1 de unos filtros polarizantes rectos o diagonales; mientras, anota las distintas orientaciones.

2 Para cada bit que llega, Bob elige aleatoriamente qué filtro utiliza para la detección y anota tanto la polarización como el valor del bit.

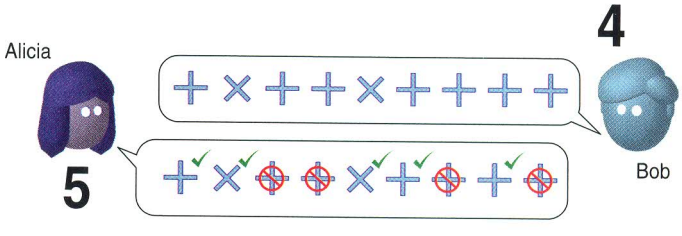
3 Eva quiere espiar el tren de fotones, pero la mecánica cuántica le prohíbe usar a la vez ambos filtros para detectar la orientación de cada fotón. Si elige el filtro incorrecto, modificará su polarización y creará errores.



Secuencia de bits de Alicia:	0	0	1	0	1	0	1	1	1
Los filtros de Alicia:	/	|	\	|	\	/	\	/	—
Los modos de detección de Bob:	+	+	+	+	×	+	+	×	+
Mediciones de bits de Bob:	1	0	1	0	1	0	0	1	1
Secuencia de bits conservados (la clave):	—	0	—	0	1	—	—	1	1

4 Una vez que todos los fotones han llegado a Bob, éste le dice a Alicia, por un canal público, quizá por teléfono o con un correo electrónico, la secuencia de modos de medición que utilizó para los fotones entrantes, pero no el valor del bit de los fotones.

5 Alicia le dice a Bob, durante la misma conversación, en qué casos eligió correctamente. Los correspondientes bits formarán la clave que Alicia y Bob utilizarán para cifrar los mensajes.



TOMMY MOORMAN; ADAPTADO DE *THE CODE BOOK: THE SCIENCE OF SECRECY FROM ANCIENT EGYPT TO QUANTUM CRYPTOGRAPHY*, POR SIMON SINGH (1999)

el de factorizar un número. Es fácil calcular el producto de dos números grandes, pero dificilísimo volverlo a factorizar en números primos. En esa asimetría se basa el algoritmo de cifrado RSA, muy usado en la criptografía de clave pública. El mensaje confidencial que se transfiere entre el remitente y el receptor, previamente convertido por un procedimiento estándar en un número, se encripta mediante una operación matemática en la que intervienen un número grande, digamos que 408508091 (en la práctica sería mucho mayor), y otro número relacionado con los factores primos —en este caso 18.313 y 22.307— del primero.

Quebrar un cifrado de clave pública resulta tan difícil, que el secreto de las claves se puede mantener durante una docena de años, como poco. Pero el advenimiento de la era de la información cuántica, y en particular de computadores cuánticos capaces de realizar con rapidez factorizaciones monstruosas, supondría seguramente el declive final del RSA y de otros métodos criptográficos.

Al contrario que la criptografía de clave pública, la criptografía cuántica seguiría siendo segura, aunque se dispusiese de ordenadores cuánticos. Una forma de enviar una clave criptográfica cuántica entre el remitente y el receptor consiste en que un láser transmita fotones, cada uno polarizado de una de dos maneras. En la primera, la polarización es vertical u horizontal (lo denominaremos "modo recto"); en la segunda, se orienta 45 grados hacia la izquierda o la derecha de la vertical ("modo diagonal"). En cualquiera de los modos, las polarizaciones opuestas de los fotones representan un 0 o un 1 digitales.

El remitente, a quien los criptógrafos acostumbran llamar Alicia, envía una cadena de bits; para cada fotón, que codificará uno de esos bits, elegirá aleatoriamente si lo envía en el modo recto o en el diagonal. El receptor, al que se llama Bob, decide al azar qué les medirá a los bits entrantes, si el modo recto o el diagonal. El principio de incertidumbre de Heisenberg dicta que podrá medir a los bits nada más que un modo. Bob sólo obtendrá con toda certeza el valor correcto cuando le mida a un bit el mismo modo en que lo envió Alicia.

QUIEN VENDE CLAVES "ABSOLUTAMENTE SEGURAS"

EMPRESA	TECNICA
id Quantique Ginebra	Envía por fibra óptica claves criptográficas cuánticas a distancias de decenas de kilómetros
MagiQ Technologies Nueva York	Envía por fibra óptica claves criptográficas cuánticas a cien kilómetros de distancia, como máximo; incluye componentes y programas para la integración en redes ya existentes
NEC Tokio	Venderá un producto de fibra óptica muy pronto; en 2004 transfirió en un ensayo claves a la mayor distancia conseguida por ahora, 150 kilómetros
QuinetiQ Farnborough	Ofrece por contrato sistemas que transfieren claves a través del aire a distancias de hasta 10 kilómetros; ha proporcionado uno a BBN Technologies, de Cambridge, Massachusetts

Después de la transmisión, Bob se comunica con Alicia, intercambio que no tiene ya por qué ser secreto, para decirle cuál de los dos modos le midió a cada fotón. Sin embargo, no revela el valor, 0 o 1, que obtuvo en cada caso. Alicia le dice entonces a Bob cuáles se midieron en el modo que correspondía; ambos descartan los demás. Los modos medidos correctamente constituyen la clave que se introducirá en el algoritmo empleado para encriptar o descifrar el mensaje.

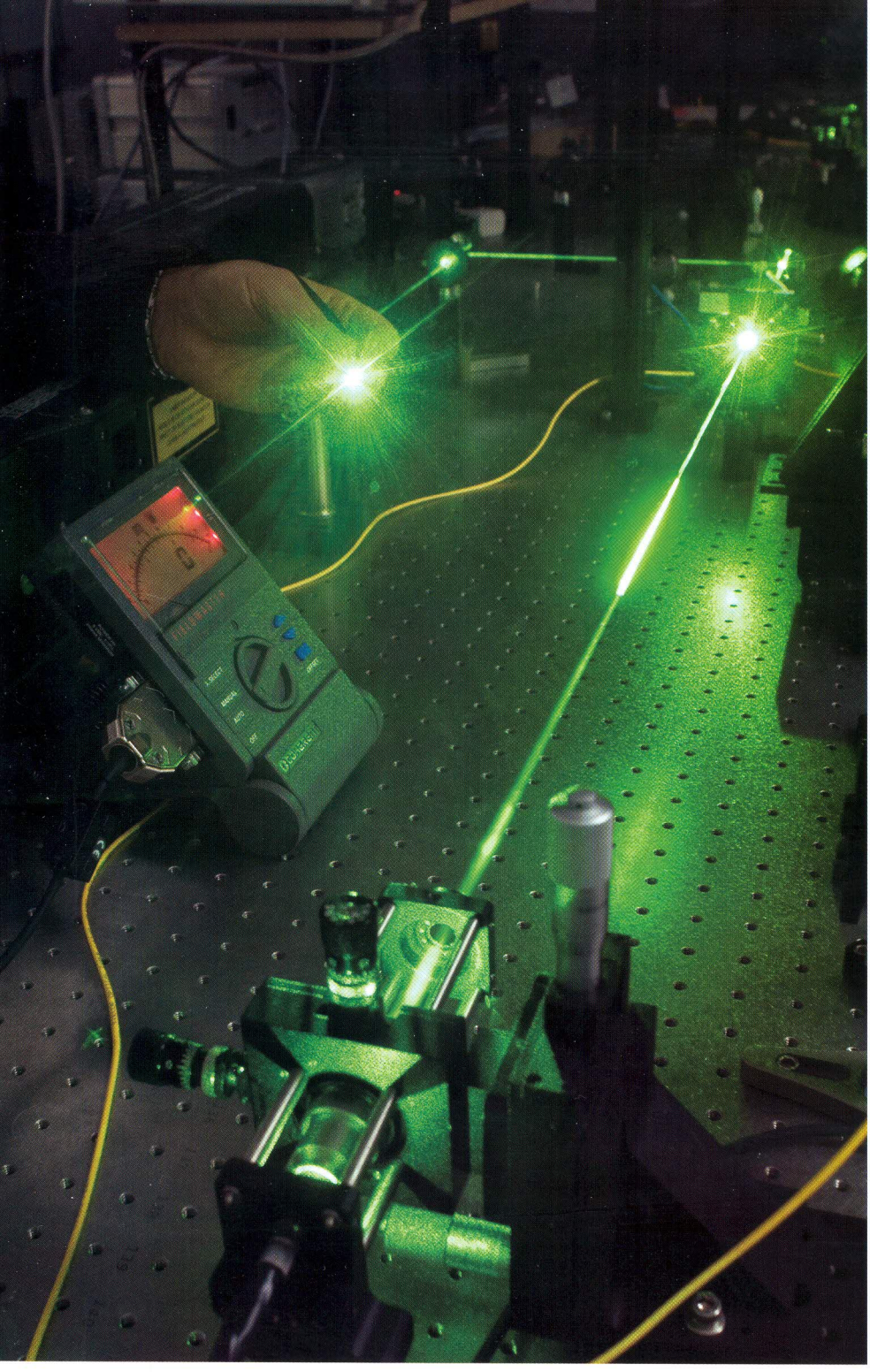
Si alguien —llamémosla Eva— intenta interceptar esta serie de fotones, no podrá medir ambos modos, gracias a Heisenberg. Si Eva mide en el modo incorrecto, aunque reenvíe los bits a Bob en el mismo modo en que los midió, introducirá errores. Alicia y Bob pueden detectar la presencia de la espía comparando bits seleccionados y comprobando si hay errores.

Desde 2003, dos compañías —id Quantique, de Ginebra, y MagiQ Technologies, de Nueva York— han presentado productos comerciales que envían una clave de criptografía cuántica a más de los 30 centímetros recorridos en el experimento de Bennett. Tras exhibir una distancia de transmisión de 150 kilómetros —la mayor conseguida—, se espera que NEC presente un producto en el mercado el año que viene. IBM, Fujitsu y Toshiba trabajan en lo mismo.

Los productos ya comercializados pueden enviar claves por un enlace de fibra óptica a decenas de kilómetros. Un sistema de MagiQ cuesta de 70.000 a 100.000 dólares. El número de clientes es aún pequeño; el sistema no se ha implantado en ninguna red a gran escala.

Ciertos organismos gubernamentales e instituciones financieras temen que un mensaje cifrado espiado hoy se guarde hasta el día en que un ordenador cuántico pueda descifrarlo. Entre los posibles clientes de los sistemas de criptografía cuántica se hallan también los abastecedores de servicios de telecomunicaciones que prevén ofrecer a sus clientes un servicio ultraseguro.

Están en marcha los primeros intentos de dotar con criptografía cuántica, no a conexiones punto a punto, sino a verdaderas redes. DARPA —la Agencia de Proyectos de Investigación Avanzados para la Defensa—, el organismo estadounidense que patrocinó los inicios de lo que luego se llamaría Internet, ha financiado una conexión en red de seis nodos pertenecientes a la Universidad de Harvard, la Universidad de Boston y BBN Technologies, empresa de Cambridge, Massachusetts, que también desempeñó un papel fundamental en aquellos orígenes de Internet. Las claves cifradas se envían por enlaces reservados, por Internet los mensajes cifrados con ellas. Es la primera red de criptografía cuántica que opera sin interrupción fuera de un laboratorio. Se ha creado sólo para demostrar la viabilidad del procedimiento; no transmite informaciones confidenciales. El pasado otoño, id Quantique, junto con Deckpoint, proveedor de servicios de Internet, exhibió una red que un grupo de servidores de Ginebra utilizó para almacenar sus



LA ENCRIPTACION que involucra estados cuánticos utiliza técnicas tan avanzadas que mucha parte del trabajo todavía se hace en laboratorios; así, éste de MagiQ Technologies.

SAM OGDEN

datos a 10 kilómetros de distancia. Un enlace con encriptación cuántica repartía —se trata de una operación frecuente— nuevas claves.

La actual criptografía cuántica está destinada a aplicarse a redes de alcance geográfico limitado. En su mayor virtud —que al espiar un mensaje o clave encriptados cuánticamente se cambie sin remedio— está su peor defecto: los dispositivos que restauran en la red las señales debilitadas para que se las pueda transmitir hasta el repetidor siguiente no podrían ejecutar esa tarea con las señales que codificarían las claves cuánticas. Un amplificador óptico corrompería los bits cuánticos, los qubits.

Para que pueda haber una mayor distancia entre enlaces, se persigue que un medio diferente de la fibra óptica distribuya las claves cuánticas. Se ha subido a montañas —donde la altitud reduce al mínimo la turbulencia atmosférica— para probar la viabilidad de enviar los fotones a través del aire. Un experimento, realizado en el año 2002 en el Laboratorio Nacional de Los Alamos, estableció un enlace de 10 kilómetros.

Otro ensayo, ese mismo año, de QinetiQ, en Farnborough, y la Universidad Ludwig Maximilian de Múnich, cubrió 23 kilómetros entre dos cumbres de los Alpes meridionales. Optimizando esta técnica —con mayores telescopios para la detección y mejores filtros y recubrimientos antirreflectantes—, se podría construir un sistema capaz de transmitir y recibir señales a más de 1000 kilómetros; bastaría para llegar a los satélites situados en una órbita terrestre baja. Una red de satélites de ese tipo ofrecería una cobertura mundial.

La Agencia Espacial Europea ha empezado a proyectar un experimento que conectaría un satélite a tierra. (En abril del año pasado, la Unión Europea puso en marcha también planes para desarrollar la encriptación cuántica en redes de comunicaciones; la ha movido a ello, en parte, el deseo de prevenir el espionaje de Echelon, sistema que intercepta mensajes electrónicos para los servicios de inteligencia de los Estados Unidos, Gran Bretaña y otras naciones.)

En última instancia, los criptógrafos desean algún tipo de repetidor cuántico, que vendría a ser una forma elemental de computador cuántico capaz de superar las limitaciones de la distancia. Funcionaría gracias a las que Albert Einstein llamó *spukhafte Fernwirkungen*, "fantasmagóricas acciones a distancia". Un equipo del Instituto de Física Experimental de Viena, dirigido por Anton Zeilinger, ha dado un primer paso hacia un repetidor así: en el número de *Nature* del 19 de agosto de 2004 informaron de que habían tendido bajo el Danubio, por un conducto del alcantarillado, un cable de fibra óptica con un fotón "entrelazado" en cada extremo. La medida del estado de polarización de uno de esos fotones establecía

inmediatamente en el otro un estado de polarización correlacionado con el primero —justo en eso consiste el entrelazamiento.

Pese a que el entrelazamiento cuántico le pareciese fantasmagórico a Einstein, les valió a Zeilinger y su equipo para que la conexión por fibra óptica entre los dos fotones entrelazados "teletransportase" la información contenida en un tercer fotón al otro lado del Danubio, a 600 metros de distancia. Se podría extender el montaje mediante repetidores múltiples, hasta que los qubits de una clave se transmitiesen a través de continentes o de océanos. Pero ese cambio de escala requeriría la creación de componentes muy peculiares, memorias cuánticas, por ejemplo, que almacenasen los qubits sin corromperlos antes de que se los reexpidiera al enlace siguiente. Falta mucho para siquiera acercarse a la fabricación de elementos de esa especie. [Acerca de un experimento un poco anterior, en que se comprobó que el entrelazamiento de fotones transmitidos por el aire se mantenía entre ambas orillas del Danubio, pero sin que se teletransportase un estado, véase "Experimento en el Danubio", de Gabriel Molina Terriza, INVESTIGACIÓN Y CIENCIA, agosto de 2004, págs. 40-41].

Quizá se realizaría mejor una memoria cuántica con átomos que con fotones. Un experimento, publicado en el número del 22 de octubre de 2004 de *Science*, ha mostrado una manera de hacerlo. Basándose en una idea de Lu Ming Duan, Mikhail Lukin, Ignacio Cirac y Peter Zoller, dos investigadores del Instituto de Tecnología de Georgia, Alex Kuzmich y Dzmitry Matsukevich, entrelazaron un par de nubes de átomos de rubidio ultraenfriados para inscribirles un qubit —las nubes los almacenan mucho más tiempo que los fotones— y transferirlo después a un fotón. Traspasaron, pues, información de la materia a la luz, y una memoria cuántica entregó un bit. Esperan crear mediante ese procedimiento repetidores que transmitan qubits a largas distancias.

La supuesta inviolabilidad de la criptografía cuántica se apoya sobre un conjunto de hipótesis que quizá no se cumplan en el mundo real. Según una de ellas, cada qubit está representado por un fotón y sólo uno. Para efectuar un encriptado cuántico, se disminuye la energía de un láser que funciona a impulsos hasta que sea poco probable que más de uno de cada diez de esos impulsos contenga un fotón —el resto son "oscuros"—; por esa razón es el ritmo de transmisión de datos tan bajo. Pero sólo se trata de una probabilidad estadística. El pulso puede contener más de un fotón. Un espía podría, en teoría, robar los fotones adicionales y descifrar con ellos un mensaje. Un algoritmo de programación —una "amplificación de la intimidad"— protege de esta posibilidad enmascarando los valores de los qubits.

Los criptógrafos quisieran contar con mejores detectores y fuentes de fotones. El norteamericano Instituto Nacional de Pesos y Medidas (NIST) es una de las muchas organizaciones que investigan en esa línea. Tienen interés en construir detectores que distingan entre la llegada simultánea de uno, dos o más fotones. Allí también intentan paliar el problema de la lenta velocidad de transmisión mediante la generación de claves cuánticas a un ritmo de un megabit por segundo, cien veces más deprisa que hasta ahora. Bastaría para distribuir claves en aplicaciones de vídeo.

La criptografía cuántica, con todo, seguiría siendo vulnerable a cierto tipo de ataques. Un espía podría sabotear el detector que recibe los fotones haciendo que los qubits que le llegan pasasen a una fibra, donde se los interceptaría. Y contra la defección interna, contra la mera traición, no hay defensa cuántica que valga.

Bibliografía complementaria

CRIPTOGRAFÍA CUÁNTICA. Charles H. Bennett, Gilles Brassard y Artur K. Ekert en *Investigación y Ciencia*, págs. 14-22; diciembre, 1992.

THE CODE BOOK. Simon Singh. Anchor Books, 1999.

Se puede encontrar información sobre productos de criptografía cuántica en las páginas Web de id Quantique (id-quantique.com) y MagiQ Technologies (magiqtech.com).