Criptografía cuántica

Charles H. Bennett, Gilles Brassard y Artur K. Ekert

Los matemáticos llevan milenios tratando de hallar un sistema que consienta intercambios de mensajes en secreto absoluto. La mecánica cuántica ha sumado fuerzas con la criptología para lograr grandes avances hacia tal empeño

Edgar Allan Poe fantasea, en *El escarabajo de oro*, sobre los rudimentos de la fractura de claves criptográficas y aventura, en ese relato corto de 1843, que la mente humana conseguirá descerrojar cualquier código que su ingenio pueda concebir. A lo largo del siglo y medio transcurrido, la batalla entre creadores y descifradores de claves ha sufrido vaivenes y complicaciones que hubieran hecho las delicias de Poe. En 1918 se ideó una codificación invulnerable, aunque su invulnerabilidad no fue demostrada hasta los años cuarenta. Era aquel sistema de cifrado muy poco práctico, pues exigía que destinatario y remitente conviniesen una clave de antemano, una gran ristra de números secretos generados al azar, parte de los cuales se utilizaba cada vez que se transmitía un mensaje. En los años setenta se desarrollaron sistemas más prácticos, fundados en claves breves y reutilizables; los había incluso carentes por completo de claves secretas, pero todos permanecen en el limbo matemático, sin haber sido fracturados ni haberse demostrado su invulnerabilidad.

Un giro tan reciente como inesperado ha consistido en reclamar el concurso de la mecánica cuántica para lograr proezas criptográficas inalcanzables por medios puramente matemáticos. Los dispositivos de criptografía cuántica se valen de fotones individuales y sacan provecho del principio de incertidumbre de Heisenberg, según el cual toda medida efectuada en un sistema cuántico provoca una perturbación en él, por lo que la información que proporciona sobre el estado que poseía el sistema antes de la medición es incompleta. Y así, toda escucha furtiva de un canal de comunicaciones cuántico provoca inexorablemente perturbaciones que ponen sobre aviso a los usuarios legítimos. La criptografía cuántica aprovecha tal efecto para posibilitar una comunicación secreta entre dos personas, aunque éstas no se hayan encontrado nunca ni compartan información secreta previa. Las técnicas cuánticas serían también de utilidad para conseguir objetivos criptográficos más sutiles, de gran interés en el mundo posterior a la guerra fría; por ejemplo, el de capacitar a dos partes que desconfían una de otra para alcanzar decisiones conjuntas basadas en información reservada, sin poner en peligro su confidencialidad o haciéndolo en el grado mínimo posible.

El arte de la criptografía nació hace al menos dos mil quinientos años; desde entonces ha desempeñado un papel importante en el devenir histórico. Es posible que uno de los más célebres criptogramas, la Nota Zimmermann, determinase la participación de los Estados Unidos en la primera guerra mundial. Al ser fracturada su clave y descifrado el texto, los estadounidenses se enteraron de que Alemania instaba a México a sumarse a su bando, ofreciendo en contrapartida, una vez ganada la guerra, territorios del norte.

Más o menos por entonces, Gilbert S. Vernam, de la compañía American Telephone and Telegraph, y el comandante Joseph O. Mauborgne, del Cuerpo de Señaleros del Ejército estadounidense, pusieron a punto la primera codificación invulnerable, hoy conocida por cifrado Vernam. Una peculiaridad distintiva del código Vernam es que requiere una clave al menos tan larga como el mensaje que se está transmitiendo, clave que ya no se vuelve a utilizar nunca para enviar otro mensaje. (El cifrado Vernam se conoce también por "cuaderno de un solo uso", por ser habitual proporcionar la clave a los espías en forma de cuaderno de hojas arrancables, cada una de las cuales se utilizaba una sola vez y era después cuidadosamente destruida.) El descubrimiento del cifrado Vernam no provocó demasiado revuelo en su momento, tal vez porque la invulnerabilidad de tal codificación no quedó demostrada hasta pasado mucho tiempo y a causa también de que lo voluminoso de la clave la tornaba poco práctica para uso general.

Por culpa de tal limitación, militares y diplomáticos continuaron fiando en sistemas de codificación mucho más vulnerables pero que se valían de claves mucho más breves. El resultado fue que, durante la segunda guerra mundial, los aliados pudieron leer la mayor parte de los mensajes secretos transmitidos por alemanes y japoneses. Tales sistemas de cifrado, aunque vulnerables, no eran en absoluto fáciles de decodificar; tanto es así que la formidable tarea de fracturar sistemas de cifrado más y más refinados constituyó uno de los acicates para el desarrollo de las computadoras electrónicas.

El interés del mundo académico por la criptografía se acrecentó a mediados de los años setenta, cuando Whitfield Diffie, Martin E. Hellman y Ralph C. Merkle, de la Universidad de Stanford, descubrieron el principio de criptosistema de clave pública (CSCP). Poco más tarde, en 1977, Ronald L. Rivest, Adi Shamir y Leonard M. Adleman, del Instituto de Tecnología de Massachusetts, idearon un procedimiento eficaz para llevarlo a la práctica.

Los criptosistemas de clave pública se diferencian de todos los esquemas anteriores en que las partes que desean comunicarse no necesitan convenir antes una clave secreta. La idea del CSCP es que una usuaria, a la que

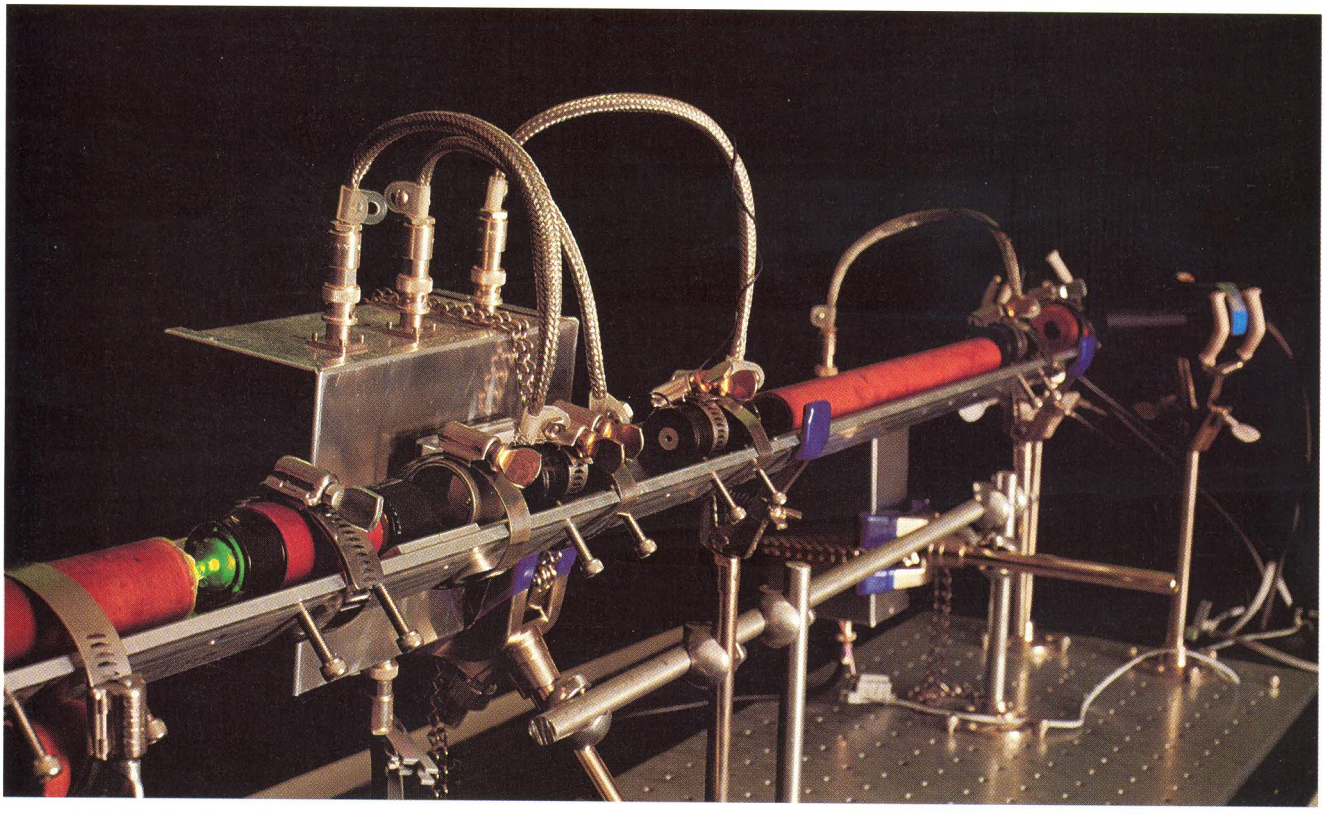
llamaremos Alicia, elige a su voluntad una pareja de transformaciones inversas una de otra, que utilizará para la codificación y la decodificación. Otro usuario, sea Benito, puede servirse entonces del algoritmo público de codificación de Alicia para preparar un mensaje que sólo ella pueda descifrar. Análogamente, todo el mundo, Alicia incluida, puede servirse del algoritmo público de codificación elegido por Benito para preparar un mensaje que sólo éste pueda descifrar. Así pues, Alicia y Benito pueden conversar en secreto, a pesar de no compartir ningún secreto. Los criptosistemas de clave pública resultan ideales para la codificación de correo electrónico y de transacciones comerciales, comunicaciones entre partes que, a diferencia de diplomáticos y espías, no tienen prevista de antemano la necesidad de comunicarse en secreto.

Frente a tales ventajas, los CSCP ofrecen un inconveniente: no está del todo demostrado que sean verdaderamente seguros. De hecho, Shamir, del Instituto Weizmann para las Ciencias, consiguió fracturar en 1982 uno de los primeros criptosistemas de clave pública, la llamada "cifra mochila".

Varios años antes de descubrirse la criptografía de clave pública se había producido otro llamativo descubrimiento: la unión de la criptografía con la mecánica cuántica. Hacia 1970, Stephen J. Wiesner, de la Universidad de Columbia, escribió un artículo titulado "Conjugate Coding" ("Codificación conjugada") donde exponía la forma en que podría utilizarse la mecánica cuántica, al menos en principio, para cumplir dos tareas imposibles desde la perspectiva de la física clásica. Consistía una de ellas en producir billetes bancarios físicamente imposibles de falsificar; la otra era un plan de combinación de dos mensajes clásicos en una sola transmisión cuántica, a partir de la cual el destinatario podría extraer uno u otro de los mensajes, pero no ambos. El artículo de Wiesner fue rechazado por la revista a la que lo presentó y permaneció inédito hasta 1983. En el ínterin, dos de los autores (Bennett y Brassard), conocedores de las ideas de Wiesner, comenzaron a pensar en combinarlas con los sistemas criptográficos de clave pública. Pronto nos percatamos de que podrían reemplazar a los CSCP: dos usuarios, que inicialmente no comparten secreto alguno, podrían comunicarse reservadamente, pero ahora podían hacerlo con seguridad absoluta y demostrable, avalándolo así las leyes físicas aceptadas.

Nuestros primeros esquemas cuántico-criptográficos, desarrollados entre 1982 y 1984, pecaban de poco prácticos; pero los refinamientos conseguidos en los años siguientes culminaron en 1989 con la puesta en servicio, en el Centro de Investigación Thomas J. Watson, de un prototipo plenamente operativo. John Smolin ayudó a construir los equipos electrónicos y ópticos del aparato y François Bessette y Louis Salvail colaboraron en la confección de los programas. Más o menos por entonces, las nociones teóricas de David Deutsch, de la Universidad de Oxford, llevaron a uno de nosotros (Ekert) a concebir un sistema criptográfico ligeramente distinto, basado en correlaciones cuánticas. A principios de 1991, aplicando ideas de Massimo Palma, de la Universidad de Palermo, John Rarity y Paul Tapster, de la Agencia Británica de Investigación para la Defensa, emprendieron experimentos que llevaban a la práctica el criptosistema ideado por Ekert.

Para explicar el funcionamiento de tales sistemas es preciso describir con detalle algo mayor ciertos aspectos matemáticos de la criptografía clá-



1. DISPOSITIVO CUANTICO que genera y mide destellos sumamente débiles de luz polarizada, proporcionando una vía segura de transmisión de información. La intensidad media de cada destello es sólo de una décima de fotón.

sica, en especial el papel desempeñado por la clave. En los primeros días de la criptografía la seguridad de los sistemas de cifrado estaba determinada por la discreción con que se efectuase el proceso completo de codificación y decodificación. En la actualidad tales procedimientos suelen ser de conocimiento público; lo que se conserva en secreto es la clave. En tales sistemas de codificación la clave se utiliza para controlar y adaptar a la medida de cada usuario los procesos de codificación y decodificación, de modo tal que un adversario que haya interceptado el criptograma no pueda, falto de la clave, extraer del mismo ninguna información útil relativa al mensaje original, por muy bien que conozca el procedimiento general de codificación. La consecuencia es que el criptograma podría ser difundido por un canal de uso público; por ejemplo, podría ser radiado o publicado en la prensa. La clave, empero, ha de ser enviada por conducto reservado y muy seguro. Aunque la distribución de una clave mediante canales privados pueda ser onerosa, permite la posterior comunicación secreta a través de canales públicos económicos.

La seguridad de un criptograma depende en última instancia de la longitud de la clave. En dos brillantes artículos publicados en los años cuarenta, Claude E. Shannon, de los Laboratorios Bell, demostró que, si la clave es más breve que el mensaje que con ella se está codificando, un adversario hábil podría inferir alguna información sobre el mensaje. Tal fuga de información se produce independientemente de lo enrevesado que pueda ser el proceso de codificación. El mensaje puede, por el contrario, quedar completa e incondicionalmente oculto y protegido de fisgones mediante sistemas como la codificación Vernam, cuya clave es tan larga como el mensaje, es aleatoria y se utiliza una sola una vez.

Pero incluso la seguridad del cifrado Vernam está limitada por la que ofrezca la distribución y almacenamiento de la clave. En vista de la gran dificultad de suministrar nuevas claves para cada mensaje, el cifrado Vernam no resulta práctico para uso comercial general, aun cuando se emplee de manera rutinaria en las comunicaciones diplomáticas, como las intercambiadas a través del "teléfono rojo" entre Moscú y Washington. El cifrado comercial corriente, Data Encryption Standard (o brevemente, DES), se funda en cambio en una clave de 56 bits, que se utiliza reiterada-

El cifrado de Ché Guevara

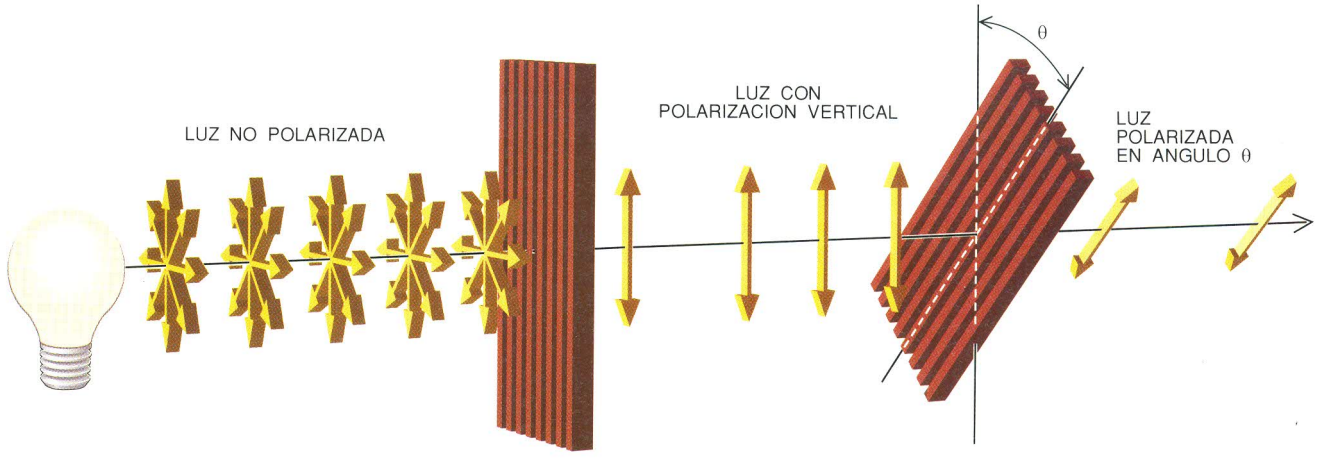
En 1967, cuando el ejército boliviano capturó y ejecutó a Ché Guevara, hallaron en su bolsillo una planilla que mostraba la forma en que preparaba los mensajes que habrían de transmitirse a Fidel Castro. Guevara utilizaba el cifrado invulnerable inventado por Gilbert Vernam en 1918. Las letras del mensaje del Ché se traducían primero a cifras de uno o dos guarismos mediante una regla fija, a saber:

A 6	E 8	I 39	M 70	Q 71	U 52	Y 1
B 38	F 30	J 31	N 76	R 58	V 50	Z 59
C 32	G 36	K 78	O 9	S 2	W 56	
D 4	H 34	L 72	P 79	T 0	X 54	

Por sí solo, este procedimiento no supone prácticamente ninguna protección. Los guarismos del mensaje se agrupaban a continuación en bloques de cinco dígitos y se llevaban a la línea superior de cada grupo de tres líneas de la planilla. La línea central de cada grupo es la clave, una sucesión de dígitos aleatorios que solamente conocían Guevara y Castro.

Luego se sumaban el mensaje y la clave (sin acarreo), generando un criptograma constituido por la tercera línea de cada grupo de tres. Por haberse sumado dígitos aleatorios, el propio criptograma forma una sucesión aleatoria de guarismos, que no aporta información relativa al mensaje original salvo para quienes conozcan la clave. El criptograma se transmitía por último a Cuba a través de un canal inseguro, como pudiera ser la radio de onda corta. El destinatario, la sección de cifrado de Castro, restaría la misma serie de dígitos aleatorios de la clave, reconstruyendo la sucesión numérica de la primera hilera, con lo que podría traducir los números a las letras que constituían el mensaje original.

Son muchos los espías y diplomáticos que han utilizado la codificación Vernam durante el siglo xx. En lugar de guarismos decimales, la clave puede consistir en una larga ristra de dígitos binarios, 0 y 1, y las sumas y restas pueden realizarse en base 2 y a máquina, en vez de hacerlo manualmente en base 10. Sin embargo, sigue siendo necesario portar en mano la clave desde el lugar de su creación hasta los puntos de utilización y guardarse cuidadosamente durante todas las fases de entrega y almacenamiento, para evitar que caiga en manos enemigas.



2. LA LUZ NO POLARIZADA entra en un filtro, que absorbe parte de la luz y confiere al resto polarización vertical. Un segundo filtro, inclinado en cierto ángulo, absorbe parte de la luz verticalmente polarizada y transmite el resto.

mente para efectuar muchas codificaciones a lo largo de un período de tiempo. Este sistema simplifica el problema de la distribución y almacenamiento de una clave segura, pero no lo elimina.

Subsiste a pesar de todo una dificultad. En principio, todo canal privado clásico es susceptible de supervisión pasiva, sin que ni remitente ni destinatario se percaten de ello. Una clave portada por un correo de confianza podría ser leída en ruta con un escáner de rayos X de alta resolución, o mediante otras refinadas técnicas de obtención de imágenes, sin que el correo se enterase. Con mayor generalidad, la física clásica —que se ocupa de cuerpos macroscópicos y de fenómenos como los documentos de papel, las cintas magnéticas o las señales de radio— consiente la medición de todas las propiedades de un objeto sin que tales propiedades resulten perturbadas. Dado que toda la información, incluidas las claves criptográficas, se encuentra codificada en propiedades físicas de objetos o de señales, la teoría clásica deja abierta la posibilidad de supervisión pasiva, pues consiente que el supervisor mida las propiedades físicas sin perturbarlas.

No sucede lo mismo en la teoría cuántica, fundamento de la cuántico-criptografía. Se cree que la teoría cuántica gobierna todos los objetos, grandes y pequeños, pero sus consecuencias se hacen notar sobre todo en sistemas microscópicos, como los átomos o las partículas subatómicas. La acción de medir constituye parte integrante de la mecánica cuántica, a diferencia de la física clásica, donde es una acción positiva y externa. Cabe, pues, diseñar un canal cuántico, esto es, un canal que porta señales basándose en fenómenos cuánticos, de forma tal que toda tentativa de supervisión del canal provoque perturbaciones detectables en la señal. Tal efecto se da porque, en teoría cuántica, ciertas parejas de propiedades físicas son complementarias, lo que significa que la medición de una propiedad perturba necesariamente a la otra. Tal enunciado, conocido por principio de incertidumbre de Heisenberg, no se refiere meramente a las limitaciones de una determinada técnica de medición: es válido para toda medición posible.

Podemos aplicar el principio de incertidumbre a la creación de un canal seguro basado en las propiedades cuánticas de la luz. La unidad mínima o cuanto de luz es el fotón, al que podemos imaginar como un campo eléctrico diminuto y oscilante. La dirección de la oscilación se denomina polarización del fotón. La luz ordinaria está formada por fotones que poseen muchas polarizaciones diferentes. Pero si la luz atraviesa un filtro polarizador, como los utilizados en algunas gafas de sol, solamente podrán pasar a su través los fotones que posean cierta polarización. La polarización transmitida depende de la orientación del filtro. Los filtros de las gafas de sol se hallan orientados de manera que permitan el paso de la luz con polarización vertical, porque esa luz es la que, al reflejarse de superficies horizontales, provoca menor reverberación y deslumbramiento. Si se hace girar las gafas 90 grados, los cristales quedarán uno encima del otro y la luz transmitida con preferencia será la de polarización horizontal, lo que acentúa la reverberación en vez de amortiguarla.

La construcción de un canal cuántico requiere un filtro polarizador o algún otro método idóneo que permita al remitente la preparación de fotones con polarización determinada; también es preciso que el destinatario pueda medir la polarización de los fotones que recibe. Esta última tarea podría encomendársele a un segundo filtro polarizador, que absorbería parte de los fotones que llegasen a él. Una solución más conveniente consistiría en utilizar un cristal birrefringente (la calcita), que tiene la propiedad de encaminar los fotones incidentes por una de dos posibles rutas, según su polarización, sin absorberlos.

Un fotón que incida sobre un cristal de calcita puede actuar de dos formas, según sea su polarización con respecto al cristal: o lo atraviesa en línea recta y emerge con polarización perpendicular a su eje óptico o bien resulta desviado y emerge polarizado según tal eje. En el caso de que el fotón incidente se encuentre ya polarizado en una de estas dos direcciones, no sufrirá cambio de polarización y se verá determinísticamente encaminado a la ruta directa (o a la desplazada, según). Sin embargo, un fotón que incida en el cristal con polarización intermedia tiene cierta probabilidad de ser asignado a cada uno de los dos haces y quedará polarizado según el haz que le haya correspondido, perdiendo con ello su polarización primitiva. La conducta más aleatoria se da cuando la polarización del fotón biseca exactamente a las direcciones de polarización del cristal, esto es, cuando forma con ellas ángulos de 45 o de 135 grados. Tales fotones tienen la misma probabilidad de ingresar en uno u otro haz, por lo que no revelan nada acerca de su polarización original, perdiendo, por así decirlo, todo recuerdo de ella.

Supongamos que Benito esté informado de antemano de que un fotón dado se encuentra polarizado en una

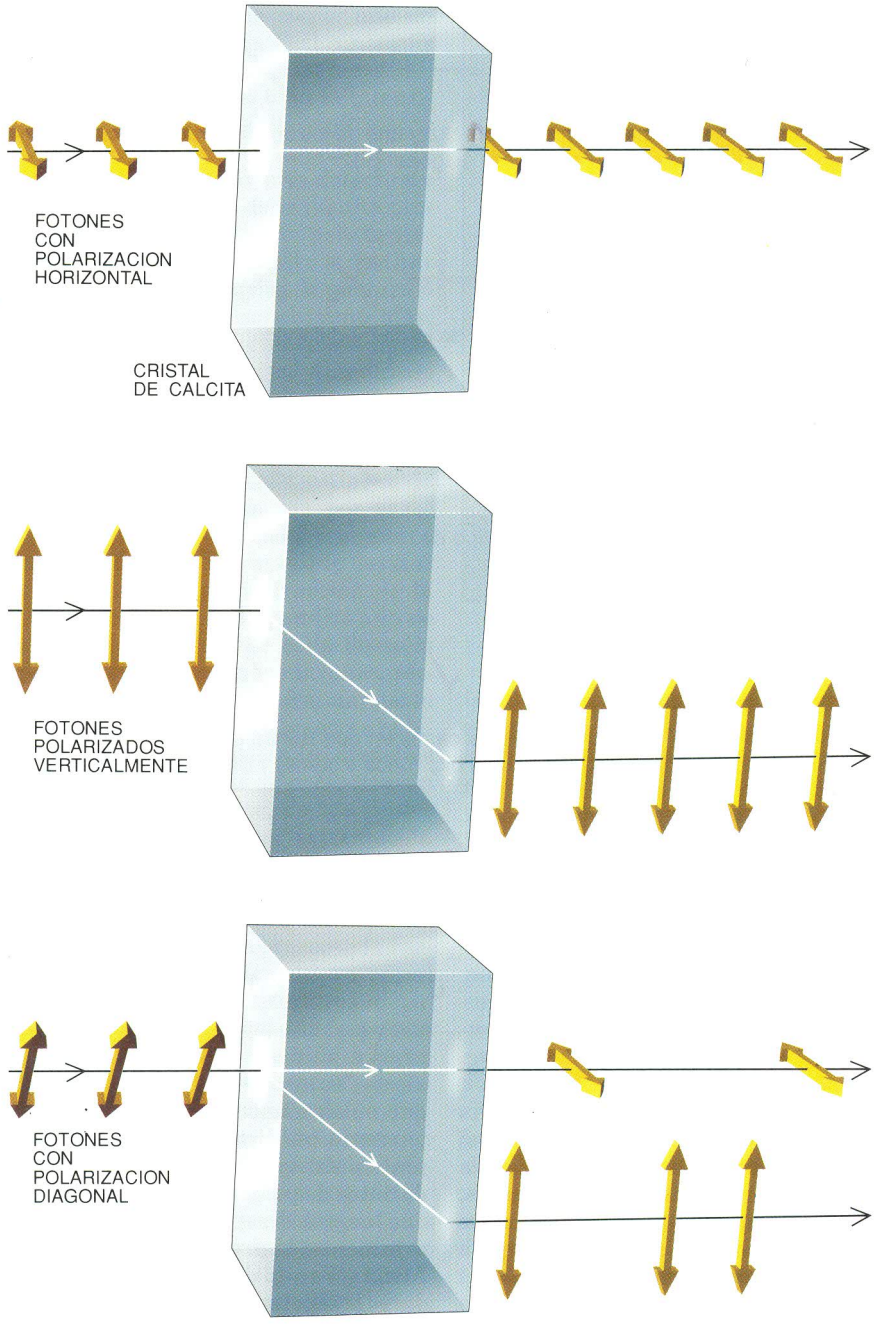
de las dos direcciones "rectilíneas", vertical (90 grados) u horizontal (0 grados), pero no sepa específicamente en cuál de ellas. Puede entonces determinar fiablemente de qué dirección se trata enviando el fotón a un instrumento consistente en un cristal de calcita con orientación vertical más dos detectores, por ejemplo, dos tubos fotomultiplicadores, capaces de registrar la llegada de fotones individuales. El cristal de calcita encaminaría al fotón incidente hacia el detector superior, si aquél estuviera polarizado horizontalmente, y hacia el inferior de estarlo verticalmente. Tal aparato no serviría para detectar fotones "diagonales" (orientados a 45 o 135 grados), que pueden a su vez reconocerse mediante un aparato similar girado 45 grados con respecto a la orientación del primero. El aparato girado es incapaz de distinguir los fotones horizontales de los verticales. De acuerdo con el principio de incertidumbre, tales limitaciones valen no sólo para el aparato concreto de medida aquí descrito, sino también para cualquier dispositivo de medición, sea el que fuere. Las polarizaciones rectilínea y diagonal constituyen propiedades complementarias, en el sentido de que la medición de una de las dos introduce un elemento de azar en la otra.

Ya es posible describir el sencillo plan de distribución de claves por medios cuánticos, que propusimos en 1984 y al que bautizamos "BB84". La finalidad de aquel esquema era permitir que Alicia y Benito se intercambiasen una clave aleatoria secreta, posteriormente utilizable a la manera del cifrado Vernam, para enviar, llegado el caso, mensajes secretos inteligibles. Lo mismo que otros esquemas cuánticos para la distribución de claves, el BB84 recurre a un canal cuántico, a través del cual Alicia y Benito envían fotones polarizados, en conjunción con un canal público clásico, por el que envían mensajes "llanos" ordinarios. Una escucha no autorizada, a la que llamaremos Esther, es libre de medir los fotones del nivel cuántico, pero no puede hacerlo sin perturbarlos. Aunque cabe también que Esther llegue a conocer el contenido completo de los mensajes enviados por el canal público, supondremos provisionalmente que no puede perturbarlos ni alterarlos.

Alicia y Benito se sirven del canal público para comentar y comparar las señales enviadas por el canal cuántico, verificando si existen pruebas de inspección por terceros. De no hallarlas, pueden destilar de sus datos un cuerpo de información que es certificablemente compartido, aleatorio y secreto, con independencia del refinamiento técnico de Esther y de la capacidad informática que tenga a su disposición. El funcionamiento esquemático es el siguiente:

En primer lugar, Alicia genera y envía a Benito una serie de fotones cuyas polarizaciones han sido elegidas al azar entre los valores 0, 45, 90 y 135 grados. Benito va recibiendo los fotones y decidiendo, en cada caso y también al azar, si mide la polarización rectilínea o la diagonal.

Benito anuncia luego públicamente qué tipo de medida ha efectuado (rectilínea o diagonal) respecto de cada uno de los fotones, pero no informa de su resultado (es decir, de si ha sido 0, 45, 90 o 135 grados). Alicia le informa entonces públicamente de si la



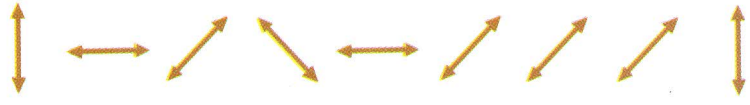
3. UN CRISTAL DE CALCITA permite la discriminación de los fotones polarizados vertical y horizontalmente. Los fotones con polarización horizontal atraviesan directamente el cristal; los de polarización vertical experimentan una deflexión que los desplaza. Cuando llegan al cristal fotones con polarización oblicua quedan repolarizados al azar en dirección horizontal o vertical y sufren el desplazamiento correspondiente.

Distribución cuántica de claves

Un sistema de criptografía cuántica permitiría que dos personas, Alicia y Benito, intercambiasen una clave secreta. El sistema dispone de un transmisor y un receptor. Alicia utiliza el transmisor para enviar fotones polarizados en una de cuatro posibles direcciones: 0, 45, 90 y 135 grados. Benito se vale del receptor para medir la polarización. Según las leyes de la mecánica cuántica, el receptor puede distinguir entre polarizaciones rectilíneas (0 y 90), o ser reconfigurado para distinguir polarizaciones diagonales (45 y 135); empero, no es capaz nunca de discriminar ambos tipos a la vez. La distribución de claves comporta varias etapas. Alicia envía fotones, cada uno con una de cuatro polarizaciones, elegidas por ella al azar.

Benito opta, también al azar, por realizar uno de los dos tipos de medida para cada fotón, ora rectangular (+), ora diagonal (×).

Benito va registrando el resultado de cada medida y conserva el registro en secreto.



Benito anuncia abiertamente el tipo de medidas que ha realizado y Alicia le dice cuáles han sido correctas.

Alicia y Benito dan por buenos los casos en que Benito efectuó la medición correcta, datos que son traducidos a bits (unos y ceros) y desde ese momento se convierten en la clave.

medida realizada de cada fotón ha sido la pertinente o no. Desechan así todos los casos en que Benito haya efectuado mediciones improcedentes, junto con aquellos otros en los que los detectores no registrasen la llegada del fotón (dado que su eficacia no es del ciento por ciento). En el caso de que nadie haya fisgoneado en el canal cuántico, las polarizaciones restantes constituirían la información secreta compartida por Alicia y Benito, quienes verificarían entonces si han sido objeto de inspección por terceros, lo que pueden hacer, por ejemplo, comparando públicamente un subconjunto entresacado al azar de la serie de datos de polarización, subconjunto que luego se desecha. Si la verificación denunciase la presencia de escuchas, Alicia y Benito descartarían todos los datos y repetirían el proceso con una nueva tanda de fotones; en caso negativo, adoptarían las polarizaciones restantes, que no han sido públicamente mencionadas, con el carácter de bits secretos compartidos, interpretando como ceros los fotones cuyas polarizaciones fuesen horizontales y de 45 grados, y como unos los polarizados verticalmente o a 135 grados.

En virtud del principio de incertidumbre, Esther no puede medir las polarizaciones rectilínea y oblicua de un mismo fotón. Si efectuase una medición incorrecta de un fotón concreto, introduciría elementos aleatorios en la serie de polarizaciones enviadas por Alicia, aunque luego enviase a Benito un fotón coherente con el resultado de su medida. El efecto neto sería la provocación de errores en la cuarta parte de los bits de los datos de Benito que hayan sido objeto de espionaje.

El procedimiento explicado, que consiste en la comparación directa de bits seleccionados para ver si hay errores, no es muy eficaz. Son demasiados los bits que hay que sacrificar para alcanzar una razonable seguridad de que los datos de Alicia y de Benito son idénticos, sobre todo si la escucha no ha sido continua, sino esporádica, y ha producido sólo unos cuantos errores. Una idea mucho mejor consiste en que Alicia y Benito comparen la "paridad" (si el número de elementos es par o non) de un subconjunto aleatorio públicamente convenido que contenga alrededor de la mitad de los bits de sus datos. Alicia, por ejemplo, podría decirle a Benito: "He examinado los bits primero, tercero, cuarto, noveno, 996 y el 999 de mis 1000 bits de datos, y he hallado que hay un número par de unos en esa colección." Benito contaría entonces el número de unos que ocupan en su serie esas mismas posiciones. Si descubriera un número impar de unos podría deducir que sus datos difieren de los de Alicia. Se puede demostrar que, en el caso de que los datos de Alicia y de Benito sean diferentes, la comparación de la paridad de un subconjunto aleatorio permitirá detectar tal hecho con probabilidad 1/2, independientemente del número y ubicación de los errores. Basta repetir la prueba veinte veces con otros tantos subconjuntos aleatorios distintos para reducir la probabilidad de error indetectado a menos de uno por millón.

El esquema BB84 hubo de modificarse para producir en IBM un equipo cuántico-criptográfico operativo. Las modificaciones fueron necesarias para afrontar problemas prácticos, como el del ruido de los detectores o el hecho de que el prototipo no utiliza en realidad fotones individuales, sino débiles destellos luminosos.

El canal cuántico, con el aparato

emisor de Alicia en un extremo y el equipo receptor de Benito en el otro, ha sido alojado en una cámara oscura. El funcionamiento del sistema está gobernado por un ordenador personal provisto de programas que representan a Alicia, a Benito y en su caso a Esther.

La porción izquierda del aparato emisor de Alicia consta de un diodo fotoemisor de luz verde, de una lente, de un orificio diminuto y de un sistema de filtros polarizadores que proporcionan un haz colimado de luz polarizada horizontalmente. Vienen luego unos dispositivos optoelectrónicos conocidos por células Pockels, que permiten pasar de la primitiva polarización horizontal a cualquiera de los cuatro estados de polarización preconvenidos, siguiendo las órdenes de Alicia. Su efecto equivale al giro mecánico del filtro polarizador, pero puede realizarse mucho más rápidamente.

El equipo receptor de Benito contiene, en el otro extremo, otra célula Pockels similar, que le permite elegir el tipo de polarización que desea medir sin necesidad de hacer girar tampoco su detector materialmente. En cuanto el haz atraviesa la célula Pockels de Benito, es escindido mediante un prisma de calcita en dos haces perpendicularmente polarizados, que son dirigidos a dos tubos fotomultiplicadores para detectar los fotones individuales.

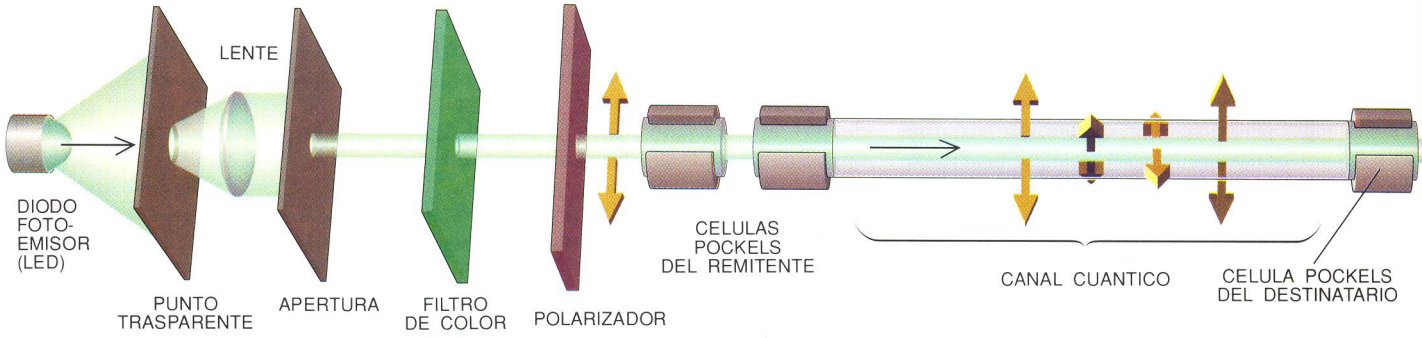
Los equipos emisor y receptor del prototipo no están separados más que unos treinta centímetros, para que el artilugio quepa sobre una mesa, mas nada impediría en principio aplicar esta técnica a distancias mucho mayores. Podrían, por ejemplo, efectuarse transmisiones cuánticas por fibra óptica hasta distancias de algunos kilómetros; prescindiendo del costo y de los inconvenientes que supondría la instalación, se podrían efectuar transmisiones cuánticas a distancias arbitrariamente grandes, con pérdidas despreciables, a través de un tubo en el que se haya hecho el vacío. Ahora bien, la distribución cuántica de claves ha de competir con las técnicas clásicas, que a distancias grandes son mucho más económicas y capaces de ofrecer una seguridad suficiente.

Recordemos que el esquema BB84 codifica cada bit en un solo fotón polarizado, mientras que el prototipo lo hace en un tenue destello luminoso. Ello entraña un nuevo riesgo de que pueda espiarse el sistema: si Esther "pinchase" el haz mediante un dispositivo similar a un espejo semirreflectante podría escindir cada destello en dos de menor intensidad, uno de los cuales llegaría hasta Benito con su polarización intacta, reservándose ella el otro para su lectura. Si la fracción de haz así desviada fuese muy modesta, es posible que Benito no detectase el debilitamiento de su señal, o que lo atribuyese a pérdidas naturales de la transmisión por el canal. Tal ataque puede neutralizarse eficazmente, al costo de reducir la velocidad de transmisión por el canal cuántico, haciendo que los destellos emitidos por Alicia sean debilísimos (por ejemplo, de una intensidad media menor que un fotón por destello). Es fácil conseguir destellos de debilidad extrema eliminando con filtros casi toda la intensidad de los destellos brillantes.

Al utilizar destellos tan débiles, la posibilidad de que Benito detecte un fotón en un destello dado resulta proporcionalmente reducida, pero la probabilidad de que Benito y Esther detecten a la vez fotones de un mismo destello se reduce muchísimo más, pues depende del cuadrado de la intensidad. El equipo disponible genera intensidades vecinas a una décima de fotón por destello. Por otra parte, si los destellos de Alicia fuesen mucho más brillantes (millares de fotones por destello, sea por caso) resultarían presa fácil del ataque por escisión del haz: sin más que desviar para sí una pequeña fracción de la intensidad, Esther dispondría aún de suficientes fotones de cada destello para efectuar las dos mediciones, rectilínea y diagonal, y determinar así la polarización correcta. Con otras palabras, cuanto más brillen los destellos de Alicia, tanto más se comportarán como señales clásicas, de las cuales puede el espía obtener información completa introduciendo en ellas una perturbación imperceptible.

Otro problema que presenta la realización práctica de un canal cuántico es que los detectores disponibles producen a veces una respuesta positiva sin haber recibido ningún fotón. Tales "falsos recuentos", sumados a otras imperfecciones del instrumental, determinan errores aunque no haya habido escucha ni interferencia, haciendo que sea poco práctico que Alicia y Benito procedan sin más a prescindir de los datos en cuanto hallen un error en ellos, como prescribía el protocolo ideal BB84. Si el número de errores encontrados fuese pequeño, lo que tendrían que hacer sería idear una forma de corregirlos y de proseguir, mientras que, si fuese grande, deberían desecharlos y empezar de nuevo.

Hay todo un abanico de técnicas que les permitirían corregir un pequeño número de errores comunicándose abiertamente. Podrían utilizar códigos de corrección de errores, por ejemplo. Pero tales métodos pudieran filtrar información a una Esther atenta a sus comunicaciones públicas. En consecuencia, tras la transmisión cuántica y la conversación de enmienda de errores, Alicia y Benito pudieran encontrarse con una clave corrupta o impura, un cuerpo de datos compartido que sólo es secreto en parte. Cabe que se haya filtrado hasta Esther información sobre la clave en diversas fases del proceso; puede que haya conseguido información escindiendo algunos destellos, o por medición directa de algunos otros (no muchos, ya que provocaría errores en los datos de Benito) y alguna más prestando oído a las comunicaciones públicas entre Alicia y Benito. Como éstos conocen la intensidad de los destellos luminosos y el número de errores descubiertos y corregidos, podrían estimar cuánta es la información que se ha filtrado hasta Esther por todos estos conductos.



4. UN SISTEMA CUANTICO permite la distribución de información en secreto absoluto. El transmisor produce débiles destellos de luz verde generada por un diodo fotoemisor. El punto transparente, la lente y el filtro crean un haz colimado de destellos tenues. La luz es polarizada luego horizontalmente. Dos células Pockels modulan la polarización a 0, 45, 90 o 135 grados. Los destellos de luz polarizada salen del transmisor del remitente y acaban alcanzando el receptor del destinatario. Otra célula Pockels deja intacta la polarización o le imprime un giro de 45 grados. Su acción permite al destinatario optar por medir la polarización rectilínea o la oblicua. En el caso rec-

Una clave impura tal es, en sí, completamente inútil. De ser utilizada, pongamos por caso, como clave de un cifrado Vernam, podría resultar muy insegura, de darse la casualidad de que la parte sustantiva del mensaje coincidiera con la porción de clave conocida por el espía. Pero, por suerte y en colaboración con Jean-Marc Robert, pusimos a punto la "amplificación de privacidad". Merced a esta técnica matemática, Alicia y Benito pueden, comunicándose abiertamente, tomar esa clave semisecreta y destilar de ella una cantidad menor reservadísima, de la que el fisgón no conocería siquiera un bit. La idea esencial de la amplificación de privacidad es que Alicia y Benito, tras la intervención del fisgón, elijan públicamente una transformación que comprima la longitud de su clave impura de forma tal que el conocimiento parcial de la clave suministrada a la transformación produzca un conocimiento prácticamente nulo de la clave comprimida.

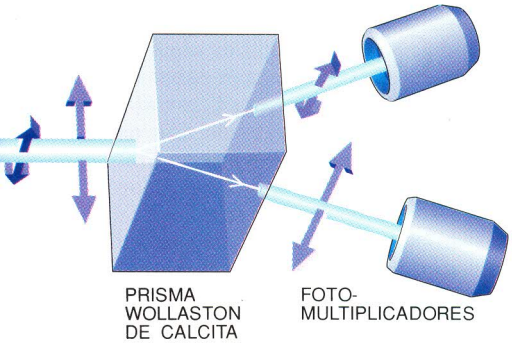
Supongamos que la clave a comprimir constase de mil bits, de los cuales Esther conozca a lo sumo doscientos. Alicia y Benito podrían seguir destilando por compresión casi ochocientos bits de información secretísima. Se puede demostrar que bastan para lograrlo técnicas sencillas; además, Alicia y Benito no necesitarían saber cuál pueda ser la información parcial que está en manos del fisgón para elegir una función compresora de cuya salida Esther no posea información. Basta con que definan que cada bit de la salida ha de ser la paridad de un subconjunto independiente y públicamente convenido de los bits suministrados a la función, de forma muy parecida a como habían hecho para estar muy seguros de que sus datos cuánticos "en rama" eran idénticos (la diferencia es que ahora deben mantener secreta la paridad en lugar de compararla públicamente).

El problema de la seguridad de las claves no queda resuelto con las garantías en la seguridad de la distribución. Otro de sus puntos débiles radica en el almacenamiento de la clave. Suponiendo que Alicia y Benito ya hayan establecido la clave, es preciso que la guarden y la conserven hasta que sea necesaria. Pero cuanto más tiempo hayan de conservar la clave en su —digamos— "caja de seguridad secreta", tanto más vulnerable será a inspecciones no autorizadas. Aunque pueda conseguirse que la caja de seguridad resulte difícil de abrir aplicando principios de ingeniería, según las leyes de la física cabe siempre la posibilidad de una brecha en la seguridad. Resulta sorprendente que sea posible diseñar un sistema criptográfico, basado en correlaciones cuánticas, capaz de garantizar tanto la seguridad de la distribución de claves como la de su almacenamiento. El criptosistema se funda en la versión de David Bohm del célebre efecto Einstein-Podolsky-Rosen (efecto EPR).

El efecto EPR tiene lugar cuando un átomo que posee simetría esférica emite dos fotones en direcciones opuestas hacia sendos observadores, Alicia y Benito. El estado de polarización inicial de los dos fotones producidos es indefinido. Ahora bien, en razón de la simetría del estado inicial, si se miden las polarizaciones de los dos fotones los valores obtenidos han de ser opuestos (siempre que las mediciones sean del mismo tipo). Por ejemplo, si Alicia y Benito midiesen ambos la polarización rectilínea, ambos tendrían idéntica probabilidad de registrar ya un 0 (polarización horizontal) ya un 1 (polarización vertical), pero si Alicia obtuviese un 0, es seguro que Benito obtendría un 1, y viceversa.

La faceta insólita e interesante del efecto EPR es que la polarización de ambos fotones queda determinada en cuanto uno de ellos es objeto de medida, pero no antes. Así ocurre por muy alejados que puedan hallarse en ese momento. Esta explicación "clásica" del efecto EPR resulta un tanto contraria a la intuición; a decir verdad, todas las explicaciones clásicas del efecto EPR entrañan elementos implausibles, como la acción instantánea a distancia. Y, sin embargo, el formalismo matemático de la mecánica cuántica explica con suma sencillez el efecto EPR, fenómeno, por otra parte, confirmado por vía experimental.

Ekert ha ideado, valiéndose del efecto EPR, un criptosistema que garantiza la seguridad tanto de la distribución como del almacenamiento de la clave. Según una versión simplificada de este sistema, descrita por N. David Mermin, Alicia genera cierto número de pares fotónicos EPR, guardando para sí uno de los miembros del par y enviando el otro a Benito. Alicia y Benito proceden a medir algunos de sus fotones para comprobar si están sometidos a espionaje, mientras que almacenan los restantes sin medirlos. Más tarde, justamente cuando va a ser necesario utilizar la clave, miden y comparan algunos de los fotones almacenados. Si nadie ha manipulado los fotones "en conserva", Benito obtendrá siempre un 1 cuando Alicia obtenga 0, y viceversa. En el caso de que no aparezcan discrepancias, Alicia y Benito proceden a medir los fotones restantes para hacerse con la clave deseada.



tilíneo, los fotones dotados de polarización horizontal serán desviados hacia el fotomultiplicador de la derecha, mientras que los verticalmente polarizados lo serán hacia el de la izquierda.

Aunque este procedimiento funcione en teoría, no es posible su utilización práctica, porque no hay técnica capaz de almacenar fotones más allá de una pequeña fracción de segundo. El efecto EPR no consiente, pues, una certificación práctica de la seguridad del almacenamiento de claves.

Aunque la aplicación más conocida de la criptografía sea el secreto de las comunicaciones, es probable que en tiempos de paz haya otras dos aplicaciones de mayor importancia. La primera consiste en el problema de la autenticación: la certificación de que el mensaje se ha enviado por quien dice remitirlo y no ha sufrido alteración en el tránsito. La segunda estriba en el mantenimiento de la confidencialidad de la información privada utilizada para llegar a decisiones públicas.

Desde que existen registros históricos, la autenticación ha solido confiarse a objetos materiales difíciles de copiar, como sellos o firmas. Tales recursos proporcionan una seguridad bastante pobre; además no pueden utilizarse en los documentos electrónicos digitales —caso de las transacciones bancarias—, que suelen transmitirse por líneas de telecomunicaciones apenas protegidas.

Existen, por fortuna, diversas técnicas matemáticas para la autenticación de mensajes digitales. Mark N. Wegman y J. Lawrence Carter descubrieron en 1979 un sistema de autenticación digital que proporciona una seguridad matemáticamente demostrable. Pero, al igual que con la codificación Vernam, es preciso que remitente y destinatario posean de antemano una clave secreta compartida, parte de la cual se utiliza cada vez que se certifica un mensaje.

La autenticación Vernam-Carter y la distribución cuántica de claves pueden beneficiarse recíprocamente. La técnica cuántica proporciona, por su parte, los bits constitutivos de la clave secreta que el método de certificación ha de consumir. El método de autenticación Vernam-Carter, por la suya, puede servir para llevar a cabo con éxito la distribución de claves, incluso en presencia de un adversario más poderoso, esto es, de una entidad capaz no sólo de escuchar los mensajes enviados por canales de comunicaciones públicas, sino también de alterarlos.

La criptografía cuántica puede resultar útil, asimismo, en la protección de información privada mientras se está utilizando en decisiones públicas. El ejemplo clásico a este respecto es el llamado "problema de la cita". Dos personas solteras buscan la forma de concertar una cita para salir juntas, aunque solamente si a cada una de ellas le agrada la otra, sin desvelar ninguna otra información. Por ejemplo, si Benito le gusta a Alicia, pero ésta no le es simpática a aquél, la cita no debe llegar a concertarse y además Benito no debe enterarse de que Alicia le mira con buenos ojos (por otra parte, es lógicamente inevitable que Alicia sepa que no le agrada a Benito, pues de ser así habrían concertado el encuentro).

Hay muchas otras situaciones en las que las decisiones que han de tomar instituciones públicas y privadas, individuos y organizaciones, dependen de datos particulares y reservados que las partes negociadoras no desean revelar. Una solución mediocre del problema de la cita, o de cualquier otro problema de decisión conjunta basada en datos privados, consiste en que Alicia y Benito confíen tales datos a un intermediario de confianza (Esther, sea por caso), dejando que sea ésta quien tome la decisión. Saltan a la vista los riesgos de semejante proceder: Alicia y Benito han de confiar no sólo en que Esther tome la decisión correcta, sino además en que nunca llegue a revelar la información particular que les concierne.

Otras técnicas permiten alcanzar decisiones públicas basadas en datos particulares sin el concurso de un intermediario de confianza. Por ejemplo, si el número de participantes es grande podría establecerse un protocolo que sólo fallase si una mayoría de los partícipes conspiran para hacer fracasar el resultado o desvelar los datos aportados. Por otra parte, si dos partes están convencidas de la seguridad de los sistemas criptográficos de clave pública, pueden llegar reservadamente a tomar decisiones sin intermediario alguno. Este problema ya fue abordado en 1982 por Andrew C.-C. Yao.

Claude Crépeau y su discípula Marie-Hélène Skubiszewska, en colaboración con Bennett y Brassard, han demostrado que cabe utilizar un aparato cuántico similar al ya construido para la distribución de claves en la toma de decisiones conjunta, sin intermediarios ni presunciones matemáticas no demostradas. La adopción de decisiones en condiciones de discreción absoluta puede realizarse por aplicación reiterada de un curioso procedimiento de procesado de información, conocido por transferencia olvidadiza. Tal procedimiento es una versión de la hazaña de Wiesner, consistente en enviar dos mensajes de tal modo que el destinatario pudiera leer uno cualquiera de ellos, pero no ambos. Michael O. Rabin formalizó la noción de transferencia olvidadiza en 1981, sin conocer los trabajos realizados por Wiesner un decenio antes, que no se habían publicado. Crépeau, Joe Kilian y otros investigadores demostraron luego que la transferencia olvidadiza era aplicable a la toma de decisiones reservadas.

Una de las características más atractivas de la adopción cuántica de decisiones reservadas es que tiene importancia incluso a distancias cortas, a diferencia de la distribución de claves. Pero las formas conocidas de ponerla en práctica son muy poco eficaces matemáticamente, exigiendo el envío y recepción de muchos millares de fotones para alcanzar incluso decisiones sencillas. Si pudiese mejorarse su rendimiento matemático, la adopción reservada de decisiones podría convertirse en la principal aplicación práctica de la criptografía cuántica.

BIBLIOGRAFIA COMPLEMENTARIA

QUANTUM CRYPTOGRAPHY BASED ON BELL'S THEOREM. Artur K. Ekert en *Physical Review Letters*, volumen 67, número 6, páginas 661-663; 5 de agosto de 1991.

EXPERIMENTAL QUANTUM CRYPTOGRAPHY. Charles H. Bennett, François Bessette, Louis Salvail y John Smolin en *Journal of Cryptology*, volumen 5, número 1, páginas 3-28; 1992.

QUANTUM CRYPTOGRAPHY WITHOUT BELL'S THEOREM. Charles H. Bennett, Gilles Brassard y N. David Mermin en *Physical Review Letters*, volumen 68, número 5, págs. 557-559, 3 de febrero de 1992.