tecnim@p Sevilla 2006
30 mayo a 2 junio
060.es
24x7x365

Comunicación

035

COMPUTACIÓN Y CRIPTOGRAFÍA CUÁNTICAS: RETOS PARA LA SEGURIDAD EN LA SOCIEDAD DE LA INFORMACIÓN

Alberto Villafranca Ramosa
Jefe de Servicio de Sistemas de Información
Ministerio de la Presidencia

Alberto Villafranca Ramos

Palabras clave

Computación Cuántica, Criptografía Cuántica, Seguridad, Sociedad de la Información

Resumen de su Comunicación

Se repasan los aspectos fundamentales de una nueva tecnología para el procesamiento de información: la tecnología cuántica. Se describe el potencial de dicha tecnología; velocidad de procesamiento, paralelismo masivo, etc. A continuación se exponen las consecuencias que la construcción de ordenadores cuánticos tendría para la seguridad de las comunicaciones, y en particular sobre algunos de los sistemas más populares empleados para la distribución de claves de cifrado. Al mismo tiempo se describe el modo en que esta tecnología proporciona un medio, en principio, absolutamente seguro para la transmisión de información. Por último se hace referencia a los cambios potenciales que la aparición de esta tecnología puede tener en la Sociedad de la Información.

Alberto Villafranca Ramos

Computación y Criptografía Cuánticas: Retos para la seguridad en la Sociedad de la Información

"Any sufficiently advanced technology is indistinguishable from magic."
"Reading computer manuals without the hardware is as frustrating as reading sex manuals without the software."

3 ª y 69ª Leyes de Clarke

1. Introducción

Cuenta una historia, seguramente apócrifa, que en el año 1800, un miembro del Parlamento británico que visitaba al físico Michael Faraday en su laboratorio de Oxford, donde realizaba sus experimentos sobre electricidad y magnetismo, le pregunto: "Profesor, ¿Por qué se pasa la vida jugando como un niño, con esos cables y esos imanes?", a lo que Faraday respondió: "No lo sé, pero estoy seguro de que sus sucesores cobrarán cuantiosos impuestos por los resultados de mi trabajo".

En la actualidad numerosos grupos de investigación, repartidos por todo el mundo, trabajan en el desarrollo de una nueva tecnología que puede cambiar radicalmente nuestra forma de procesar, transmitir y almacenar la información. En el terreno de la seguridad de la información, el desarrollo de dicha tecnología supondría una brecha en los sistemas que protegen las comunicaciones gubernamentales, financieras y privadas, pero al mismo tiempo ofrece nuevas formas de transmitir información, en principio, de forma absolutamente segura.
.

2. Los límites físicos del procesamiento de información.

En la década de los 60 del siglo XX Rolf Landauer señaló un hecho de enorme importancia: **la información es física**, es decir, la información no puede separarse de su representación física. Siempre se encuentra almacenada en algún sistema físico, y es manipulada mediante algún proceso físico. Actualmente, la tendencia a la miniaturización de los circuitos integrados está llegando a un límite donde cobran relevancia las leyes de la materia a escala microscópica: las leyes de la física cuántica. La tecnología cuántica puede ofrecer, no sólo un avance en esta tendencia, sino algo mucho más importante: **una forma distinta de entender el procesamiento de información mediante nuevos algoritmos basados en las leyes cuánticas y nuevos métodos de conseguir su transmisión segura.**

3. Ordenadores Cuánticos.

3.1 ¿Qué es un ordenador cuántico?

A la hora de contestar a esta pregunta, la respuesta más natural es decir que un ordenador cuántico es aquel cuyo funcionamiento se rige por las leyes de la mecánica cuántica, las que gobiernan el comportamiento de la materia a escala microscópica. Esto, aunque verdad, no es del todo exacto. Nuestros ordenadores (que podemos denominar clásicos), los que tenemos en nuestras mesas de trabajo, y, de hecho cualquier objeto que tengamos a la vista, también obedecen las leyes de la mecánica cuántica, pero no decimos que son ordenadores cuánticos.

¿Qué diferencia a un ordenador cuántico de los nuestros?: que el primero aprovecha las propiedades cuánticas de las partes que lo forman para efectuar tareas que, en principio, estarían más allá de las posibilidades de los ordenadores comunes.

3.2 Bits clásicos y bits cuánticos.

Para tener una idea de las nuevas capacidades de los ordenadores cuánticos nos centraremos en el elemento más sencillo de cualquier teoría o tecnología de la información, su unidad básica: **el bit.**

Un ordenador clásico opera con cadenas de 0s y 1s y las convierte en otras cadenas. Cada elemento de la cadena constituye un **bit** que puede tomar dos valores: 0 ó 1. Para representarlos, los ordenadores contienen un conjunto de sistemas físicos capaces de encontrarse, de forma inequívoca, en uno de dos estados posibles: 0/1, abierto/cerrado, lleno/vacío, cargado/descargado, arriba/abajo, etc. En principio nada impediría construir un ordenador en el que los bits estuviesen representados por botellas de agua llenas o vacías, si bien su velocidad de procesamiento dejaría mucho que desear (además de no ser aconsejable en tiempos de sequía).

Del mismo modo que podemos utilizar un condensador cargado o descargado para implementar físicamente un bit, podríamos utilizar un átomo en dos estados posibles, por ejemplo, en su estado fundamental (el de más baja energía), que representaría el 0 o en su primer estado excitado, que representaría el 1. Sin embargo, según las leyes de la mecánica cuántica, dicho átomo, además de poder encontrarse en esos dos posibles estados puede hallarse en una mezcla de ambos. Técnicamente se dice que el átomo se encontraría en una **superposición de estados**. Esto significa que el átomo puede estar **en ambos estados al mismo tiempo.**

Esta es la diferencia fundamental entre la tecnología clásica y la cuántica: mientras que los dispositivos físicos que implementan un bit clásico sólo pueden codificar un único estado en un momento determinado, un bit cuántico **puede codificar dos estados a la vez**. Indudablemente esto está mas allá de nuestra experiencia cotidiana: abusando del lenguaje podríamos decir que un "interruptor clásico" puede estar abierto o cerrado, pero no en ambos estados al mismo tiempo. En cambio un "interruptor cuántico" sí que podría estarlo. Para ver las posibilidades que ofrece esta superposición (mezcla) de estados estudiaremos, como ejemplo, un registro formado por tres bits.

3.3 Muchos por el precio de uno: Superposiciones de Bits.

Imaginemos un registro formado por tres bits físicos, es decir, tres dispositivos físicos idénticos y que cada uno de ellos nos sirve para representar un bit. Un registro **clásico** almacenará, en un instante dado, sólo uno de los ocho posibles números distintos que podemos codificar con esos tres bits, a saber: 000, 001, 010, 011, 100, 101, 110 ó 111.

En un registro **cuántico** formado por tres bits podemos almacenar, en cualquier instante, **todos los números** mediante una superposición de todos los estados posibles. De esta forma los ocho números están físicamente presentes a la vez. Si vamos añadiendo bits cuánticos al registro aumentaremos exponencialmente la capacidad de almacenamiento: si 3 bits cuánticos pueden almacenar 8 números distintos al mismo tiempo, 4 bits cuánticos almacenarán 16 números distintos, y en general, con N bits cuánticos podremos almacenar 2^N números **al mismo tiempo y en un único registro.**

3.4 Paralelismo Cuántico.

Una vez que tenemos un registro preparado como una superposición de todos números que podamos

representar podemos empezar a realizar operaciones sobre ellos; sobre todos ellos al mismo tiempo.

Si queremos abordar dos problemas con un ordenador corriente, habría que introducir el primero y esperar el resultado, luego introducir el segundo y volver a esperar. Es decir, nuestros ordenadores sólo se ocupan de un problema cada vez, y si tienen que resolver varios los tratan uno detrás de otro. Sin embargo, en un ordenador cuántico, ambos problemas podrían combinarse e introducirse en el ordenador simultáneamente, ejecutándose al mismo tiempo.

Si tenemos una superposición de bits representando un conjunto de números, y ésta cambia, los números que representa también lo hace. El resultado será que habremos efectuado una operación con todos los números al mismo tiempo.

Con un registro formado por N bits, un **ordenador cuántico podría ejecutar en un solo paso la misma operación sobre 2^N números distintos codificados en forma de superposición de esos N bits**; esto es lo que se conoce como **paralelismo cuántico**. Y lo más importante es que sólo habríamos necesitado un registro, una única pieza de hardware. Para que un ordenador clásico pueda realizar esta tarea tendría que repetir la misma operación **2^N** veces, una con cada número (input) diferente o bien tendría que utilizar **2^N** procesadores trabajando el paralelo.

En resumen, un ordenador cuántico posibilitaría el ahorro de una enorme cantidad de recursos, y realizaría el mismo trabajo que un ordenador clásico necesitando mucho menos tiempo y memoria. Pero, además de ser más rápido y consumir menos recursos, ¿podría un ordenador cuántico resolver problemas intratables para un ordenador ordinario?.

4. Nuevos métodos para viejos problemas: Algoritmos Cuánticos.

4.1 Secretos al descubierto.

Imaginemos que se nos pide realizar la siguiente operación:

277 x 599 = ?

Su solución nos llevaría menos de un minuto, sin necesidad de utilizar una calculadora. Esto es así gracias a que conocemos, desde la escuela primaria, un algoritmo "rápido" para la multiplicación. Pero su tuviésemos que hacer la operación inversa:

? x ? = 165923

esto es, averiguar dos números (primos) cuyo resultado sea el que aparece, podríamos tardar horas. Si nos planteásemos factorizar números de cientos de dígitos, el tiempo necesario para hacerlo sería mayor que la edad del Universo, incluso utilizando nuestros computadores más potentes.

En 1.994 Peter Shor, un matemático que en aquel entonces trabajaba en la división de investigación de los laboratorios AT&T Bell en New Jersey, asombró a todo el mundo presentando un algoritmo que podría ejecutarse en un ordenador cuántico y que era capaz de resolver, en un tiempo razonable, la factorización de números enteros grandes. Lejos de ser una curiosidad académica, la repercusión práctica de este hallazgo es enorme. Actualmente, los sistemas más utilizados para proteger las comunicaciones a través de Internet, (desde los mensajes cifrados, a las compras pasando por las transacciones bancarias) se apoyan, en su mayoría, en algoritmos de cifrado cuya fortaleza se basa en la existencia de operaciones matemáticas muy fáciles de realizar en un sentido pero intratables en sentido contrario: por ejemplo, la multiplicación y

la factorización. En esto reside la fortaleza de sistemas como el popular RSA.

Si se construyese un ordenador cuántico, los sistemas que garantizan la seguridad de nuestras comunicaciones electrónicas quedarían obsoletos de un plumazo. Pero al mismo tiempo, la tecnología cuántica es capaz de proporcionar nuevos métodos para garantizar la transmisión de información de forma **absolutamente** segura.

5. Criptografía Cuántica.

5.1 El que hace la trampa, hace la ley.

El propósito de la criptografía es la transmisión de información de forma que sólo pueda acceder a ella su legítimo destinatario. La pieza fundamental de los sistemas criptográficos actuales reside en un parámetro conocido como clave, que consistirá en cualquier cadena aleatoria de bits, suficientemente larga, y la seguridad de un sistema de cifrado reside, enteramente, en mantener en secreto esta clave.

Esto parece garantizar una comunicación segura. Sin embargo sigue quedando un problema por resolver: ¿Cómo se ponen de acuerdo el emisor y el receptor sobre la clave que van a utilizar?. Deben encontrar una forma segura de comunicarse para intercambiar este dato. Esto es lo que se conoce como el **problema de la distribución de claves.**

Como solución a este dilema aparecieron **los sistema de cifrado de clave pública.** En éstos los usuarios utilizan dos claves, una para cifran el mensaje y otra para descifrarlo. Todo el mundo puede tener acceso a una de las claves (denominada pública) para cifrar un mensaje, pero sólo su legítimo destinatario tiene la otra clave (llamada privada) para descifrarlo. Los sistemas de cifrado de clave pública más populares, como RSA, basan su seguridad en la dificultad de factorizar números enteros muy grandes. Pero esto no sería un obstáculo para un ordenador cuántico que ejecutase el algoritmo de factorización de Shor.

¿Significa esto que no habría ninguna forma de intercambiar una clave de cifrado de forma segura?. No. Del mismo modo que la tecnología cuántica demolería la seguridad de nuestros sistemas de cifrado actuales, también acude al rescate proporcionando un método para la transmisión de información de forma segura de modo que si el canal de comunicación estuviese siendo espiado, tanto el emisor como el receptor lo sabrían al instante.

5.2 Ideas básicas de criptografía cuántica.

En los años 80 del siglo pasado apareció el primer protocolo que utiliza las leyes cuánticas para conseguir una distribución segura de claves.

El método de distribución de claves mediante tecnología cuántica se basa en propiedades de los fotones, las partículas que forman la luz. Cuando un fotón viaja por el espacio vibra. Cuando hay muchos fotones en juego, cada uno puede vibrar en ángulos diferentes. Este ángulo de vibración se conoce como **polarización del fotón.** Al encender una bombilla se están creando fotones con todas las polarizaciones, vibrando en todos los ángulos posibles, pero podemos seleccionar fotones con una polarización determinada. Esto no es algo nuevo; cuando nos ponemos unas buenas gafas de sol, lo que está sucediendo es que el cristal actúa como un filtro que sólo deja pasar los fotones que están polarizados en un ángulo determinado (ver figura 1).

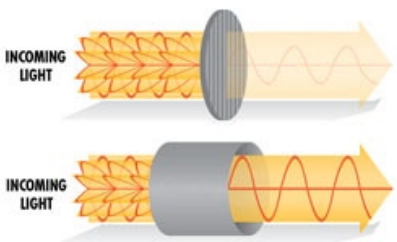

Figura 1.

Para explicar el protocolo de distribución cuántica de claves, recurriremos a los tres personajes más célebres de la literatura sobre criptografía: por un lado Alice y Bob (que quieren intercambiar una clave) y Eve, la espía.

Alice quiere acordar una clave con Bob para poder cifrar mensajes futuros, mediante el envío de fotones polarizados, utilizando una fuente de luz y haciendo pasar los fotones por un filtro polarizador. De este modo, los fotones que envíe tendrán la polarización que ella desee. Para ello utilizará dos filtros polarizadores orientados según ángulos de 90° y 45°, y los fotones que envíe con estas polarizaciones representarán los bits 0 y 1 respectivamente. En el otro extremo Bob tiene otros dos filtros con orientaciones de 0° y 135° (ver tabla 1 y figuras 2a y 2b). (Consideramos todos los ángulos respecto a la horizontal).

Filtros de Alice	90° (Codifica: 0)	45° (Codifica: 0)
Filtros de Bob	0°	135°

Tabla 1.

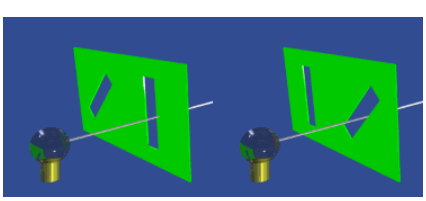

Figura 2a: Filtros de Alice.

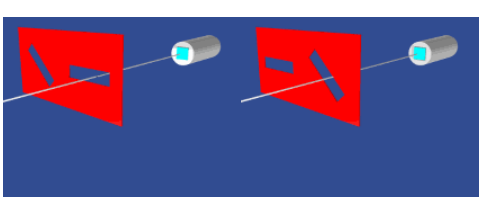

Figura 2b: Filtros de Bob

Para transmitir la clave, Alice manda a Bob una serie de fotones polarizados, eligiendo para cada uno un filtro al azar; es decir, unas veces enviará un fotón polarizado 90° y otras 45°. Como resultado le enviará una cadena aleatoria de 0s y 1s.

Por su parte Bob intentará medir la polarización de cada fotón que le llega, eligiendo, también al azar, entre sus dos filtros. En consecuencia, unas veces utilizará el filtro de 0° y otras el de 135°.

¿Cómo se comportan los fotones polarizados de Alice cuando se encuentran con los filtros de Bob?. Existen tres posibilidades:

- Cuando un fotón llegue al un filtro con la misma orientación que su polarización, lo atravesará **siempre.** (ver figura 3a y tabla 2)
- Si un fotón se encuentra con un filtro con una orientación perpendicular a su polarización no

pasará **nunca**; quedará bloqueado (ver figura 3b y tabla 2)

- Si el fotón se encuentra con un filtro orientado diagonalmente respecto a su polarización (formando un ángulo de 45° con ésta; por ejemplo, un fotón polarizado 90° ↕ que se encuentra con un filtro de 135° ↘), tendrá un 50% de posibilidades de atravesarlo y otro 50% de quedar bloqueado. Esto significa que si lanzamos muchos fotones hacia un filtro, según las condiciones que acabamos de describir, aproximadamente la mitad de ellos lo atravesará, la otra mitad no (ver figuras 3c y 3d y tabla 2). Pero no hay forma de saber qué le sucederá a un fotón individual. Que pase o no es algo completamente aleatorio.

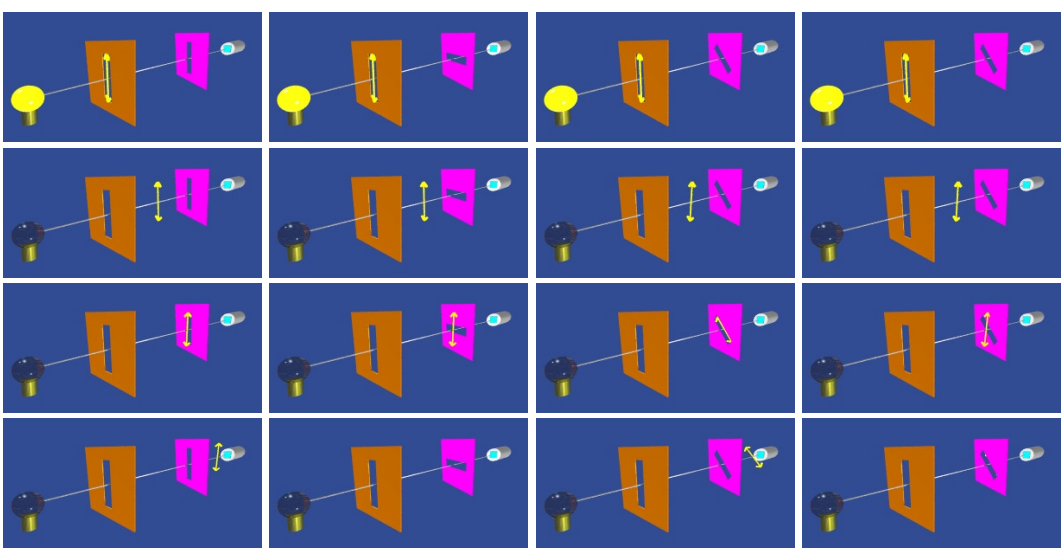

Figura 3a **Figura 3b** **Figura 3c (50%)** **Figura 3d (50%)**

Polarización del Fotón de Alice	90°	90°	45° ↗	45° ↗
Filtro que utiliza Bob	0° ↔	135° ↘	0° ↔	135° ↘
¿Atraviesa el filtro de Bob?	Nunca	50% Si 50% No	50% Si 50% No	Nunca

Tabla 2.

Analicemos un ejemplo concreto. Si Bob elige su filtro de 135° ↘ para medir un fotón que le llega de Alice, pueden ocurrir dos cosas:

- **El fotón no pasa el filtro;** Entonces, y teniendo en cuenta lo dicho más arriba, Bob no sabrá si Alice mandó un fotón polarizado 45° ↗ (que codifica un bit 1) y que siempre será bloqueado por su filtro, o si mandó un fotón polarizado 90° ↕ (que codifica un bit 0), en cuyo caso había una probabilidad del 50% de que su filtro de 135° ↘ lo bloquease (ver figura 3d).

- **El fotón pasa el filtro:** Entonces Bob sabrá, con certeza absoluta, que Alice mandó un fotón polarizado 90°, pues es la única polarización que tenía alguna posibilidad (50%) de atravesar su filtro de 135°. Luego si un fotón pasa su filtro, Bob puede estar seguro de que Alice le habrá mandado un fotón polarizado 90° que codifica un 0 (cero).

Por el mismo razonamiento, si Bob utiliza un filtro de 0° y un fotón de Alice lo atraviesa, tendrá la certeza de que ésta lo mandó con una polarización de 45° y que por tanto codifica un bit 1 (uno). Esto se resume en el siguiente cuadro:

Si un fotón atraviesa el filtro de 135° ( ) de Bob, entonces sabrá que Alice le envió un bit 0 (cero).
Si un fotón atraviesa el filtro de 0° ( ) de Bob, entonces sabrá que Alice le envió un bit 1 (uno).

Tabla 3.

Por tanto, cuando Alice envía fotones polarizados a Bob, éste será capaz de determinar, para los que atraviesen sus filtros, el valor del bit que representan. La tabla 4 muestra un ejemplo de esta comunicación para 6 fotones.

Bit que quiere enviar Alice	0	0	1	1	0	1
Filtro Polarizador de Alice	90	90	45	45	90	90
Filtro Polarizador de Bob	135	0	135	0	135	0
Resultado	Pasa	No	No	Pasa	No	Pasa
Bit de la clave	0	____	____	1	____	1

Tabla 4.

Luego en este caso sencillo, la clave sería: **011** (Nótese que Alice envía los fotones 1° y 5° con la misma polarización (90°), y se encuentran con el mismo filtro de Bob, el de 135° . Sin embargo, uno pasa y el otro no. Este es un ejemplo del comportamiento cuántico que se mencionó anteriormente).

Si Alice mandase 1 millón de fotones a Bob, con polarizaciones elegidas al azar entre las dos de las que dispone (90° y 45°), y a su vez Bob los va midiendo según le llegan eligiendo, también al azar, cuál de sus filtros va a utilizar (0° 135°), entonces, aproximadamente tres de cada cuatro fotones (750.000) quedarán bloqueados y no pasarán los filtros de Bob, pero al mismo tiempo sabrá con certeza qué bit codifica cada uno de los restantes fotones que pasan sus filtros; uno de cada cuatro (250.000). Estos bits formarán la clave con la que cifrar los mensajes entre ellos.

Bob puede decirle a Alice (por teléfono) **qué fotones son los que han pasado sus filtros** (por ejemplo, los que, según el orden en que Alice los envió, ocupan las posiciones, 7ª, 129ª, 7.315ª, etc), **pero no le dice qué filtro utilizó para medirlos**, es decir, **no revela la polarización de esos fotones**. Por tanto, si alguien está espiando su conversación no conseguirá ninguna información sobre la clave. Y lo que es aún más importante, **si un espía (Eve) interceptase los fotones que viajan entre Alice y Bob, su presencia sería detectada**. Veamos por qué.

Supongamos que Alice manda a Bob un fotón polarizado 90° , que representa un bit 0 (cero), y que Eve, que dispone de los mismos filtros para medir que Bob, lo intercepta utilizando un filtro de 135°. Si el

fotón queda bloqueado Eve no tiene forma de saber si es porque su polarización era de 45° (y por tanto nunca podría haber pasado su filtro) o si era de 90° ↕ y pertenece al 50% que queda bloqueado. Eve puede aventurar que era un fotón polarizado 45° ↗, preparar otro fotón con esta polarización y reenviarlo a Bob. Si resulta que éste lo mide con un filtro de 0° ↔, el fotón reenviado por Eve tendrá un 50% de probabilidades de pasar y en este caso Bob lo interpretará como un bit 1 (uno), justo lo contrario de lo que le envió Alice (ver figura 4).

Bit que quiere enviar Alice	0°
Filtro Polarizador de Alice	90° ↕
Filtro Polarizador de Eve	45° ↗
Filtro Polarizador de Bob	0° ↔
Resultado	Pasa
Bit que registra Bob	1

Figura 4.

Esta discrepancia es la que pone a Eve al descubierto, ya que, según este procedimiento, si nadie estuviese interceptando los fotones, Bob sólo puede obtener: O bien nada (cuando sus filtros bloquean los fotones que le llegan) o bien el resultado correcto con certeza absoluta, pero en ningún caso resultados opuestos a los de Alice. De esta manera, para saber si Eve estuvo espiando, Alice y Bob comprueban si hay discrepancias de este tipo. Para ello, una vez que han terminado la transmisión de fotones (y saben cuáles son los que han proporcionado a Bob alguna información) y cada uno tiene apuntada su cadena de Os y 1s, escogen unos cuantos al azar y se comunican por teléfono sus valores. Si hay alguna discrepancia, sabrán inmediatamente que Eve estuvo espiando. Si no, podrán utilizar esa cadena de Os y 1s como clave para cifrar sus comunicaciones futuras, después de tirar a la basura los bits que han utilizado para buscar errores, ya que para compararlos utilizaron un medio inseguro como el teléfono.

Siempre existe la posibilidad de que Eve tenga suerte y tras interceptar y medir un fotón de Alice, lo retransmita a Bob con la polarización correcta; la que Alice preparó. Al fin y al cabo, tiene la misma probabilidad de acertar que de errar. Si Alice y Bob utilizasen el bit que codifica este fotón para el proceso de búsqueda de discrepancias, no notarían nada y no les ayudaría a descubrir a Eve. Pero si Alice y Bob hacen su comprobación de discrepancias utilizando más y más bits, las oportunidades de Eve de pasar desapercibida serán prácticamente nulas. Por emplear una analogía sencilla, sería como adivinar todos los números que van a salir en un sorteo de lotería y además en qué orden.

El resultado final es que Alice y Bob tienen una clave segura para cifrar sus mensajes. Este es el método de distribución de claves más seguro jamás concebido. La razón de esto es sencilla: para que un posible espía consiguiese información sobre la clave, no bastaría que fuese capaz de vencer un complicado algoritmo o resolver un ingenioso problema matemático; tendría de saltarse las leyes de la física.

Al contrario de lo que ocurre con los ordenadores, ya existen productos comerciales de criptografía cuántica. Empresas como la norteamericana MagiQ o la suiza ID Quantique ofrecen soluciones de distribución cuántica de claves para comunicaciones ultraseguras (ver figura 5).

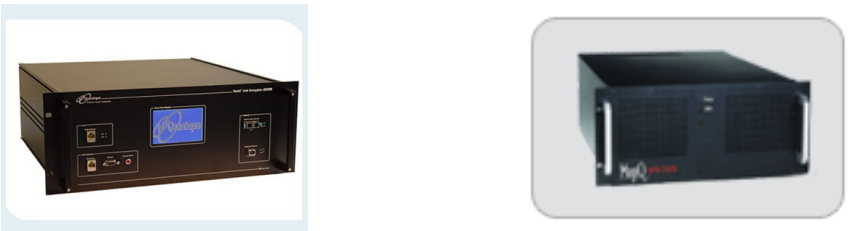

Figura 5: Productos criptográficos comerciales.

6. Tecnología Cuántica y Sociedad de la Información.

Siempre resulta arriesgado hacer predicciones y más aún en el terreno de los avances tecnológicos y sus consecuencias. Hace 50 años nadie habría podido imaginar el impacto de las tecnologías de la información sobre la sociedad. Hoy en día, el activo más importante de muchas organizaciones es la información y en consecuencia los medios para obtenerla, manipularla, transmitirla o, en resumen, para sacar partido de ella, han adquirido un valor estratégico.

Son muchos los campos donde la tecnología puede tener profundas consecuencias; desde la investigación científica, pudiéndose realizar simulaciones de sistemas microscópicos con una exactitud fuera del alcance de los computadores actuales, hasta la protección de comunicaciones que requieran una privacidad absoluta. Uno de los pilares sobre los que se debe apoyar el desarrollo de la Sociedad de la Información es la confianza para intercambiar datos con plena seguridad. Esto es fundamental, por ejemplo, para Gobiernos, comunicaciones diplomáticas, para las entidades financieras que apuesten por la banca a través de Internet o para cualquier empresa de comercio electrónico. Los mismo se puede decir de la interacción de los ciudadanos con la Administración a través de las tecnologías de la información.

La primera consecuencia práctica de la tecnología cuántica, es que por primera vez se dispone de un medio de transmitir información de forma absolutamente segura. Esto es sólo el primer ejemplo de la aplicación de esta tecnología para la solución de un problema práctico. Como toda tecnología de cifrado, puede ser utilizada para fines loables (por ejemplo, comunicaciones a través de Internet entre médico y paciente) o perversos (delincuencia organizada, terrorismo, etc), dependiendo de quién tenga acceso a ella.

Al tratarse de un tema de investigación candente, es imposible decir hasta dónde se puede llegar. Como sucede en cualquier área de la ciencia, desarrollos que hoy parecen prometedores no llevarán a ninguna parte y al mismo tiempo, como ya ha ocurrido en el pasado, nuevas ideas conducirán a conocimientos y aplicaciones que hoy no podemos imaginar. Es muy difícil predecir el resultado de una investigación científica y más aún cuando ésta puede suponer una mejor comprensión de los mecanismos fundamentales de la naturaleza. En lo que se refiere a los ordenadores cuánticos, David Mermin de la Universidad de Cornell lo expresa con claridad: “Sólo un incauto podría predecir que no habrá ordenadores cuánticos útiles en el año 2.050, pero sólo un incauto podría decir los habrá”.

Aún queda un largo camino por recorrer hasta que esta tecnología pueda, alguna vez, formar parte de nuestra vida cotidiana. Pero ¿Cuánta gente podía imaginar que hoy podríamos escuchar a Mozart mediante un dispositivo láser capaz de leer un disco óptico y que podemos llevar en el bolsillo?.

Como dijo el físico danés Niels Bohr: “Hacer predicciones es difícil, especialmente si son del futuro”. No podemos tener certezas respecto a dónde nos llevará esta tecnología ni sobre sus impacto en la Sociedad

de la Información. Pero si se produce, sin duda, superará todas las previsiones. E incluso, quién sabe, puede que alguien termine cobrando impuestos por ello.

7. Bibliografía.

Existe una enorme cantidad de bibliografía sobre computación y criptografía cuánticas. Exceptuando la mención a algún libro, se da a continuación una pequeña lista de sitios de Internet donde se puede ampliar lo expuesto anteriormente:

- Centre for Quantum Información: www.qubit.org .
- Institute for Quantum Información: www.iqi.caltech.edu .
-"Quantum Computation and Quantum Information". Michael A. Nielsen & Isaac L. Chuang. Cambridge University Press (2000).
-"The Code Book: The Secret History of Codes and Code Breaking", Simon Singh. Anchor (2000). www.simonsingh.com . (Figs. 2a, 2b, 3a, 3b, 3c y 3d).
- www.idquantique.com . (Fig 5).
- www.magiqtech.com (Fig. 5).
- "Quantum Information Science: An Emerging Field of Interdisciplinary Research and Educacion in Science and Engineering". Quantum Information Science Workshop (Proceedings). National Science Foundation (1999). www.nsf.gov/publications/ .
- "Quantum Computing", Andrew Steane: http://xxx.lanl.gov/abs/quant-ph/9708022 .
- "Quantum Cryptography", Richard J. Hughes et al. http://xxx.lanl.gov/abs/quant-ph/9504002
- Reliable Quantum Computers", John Preskill: http://xxx.lanl.gov/abs/quant-ph/9705031