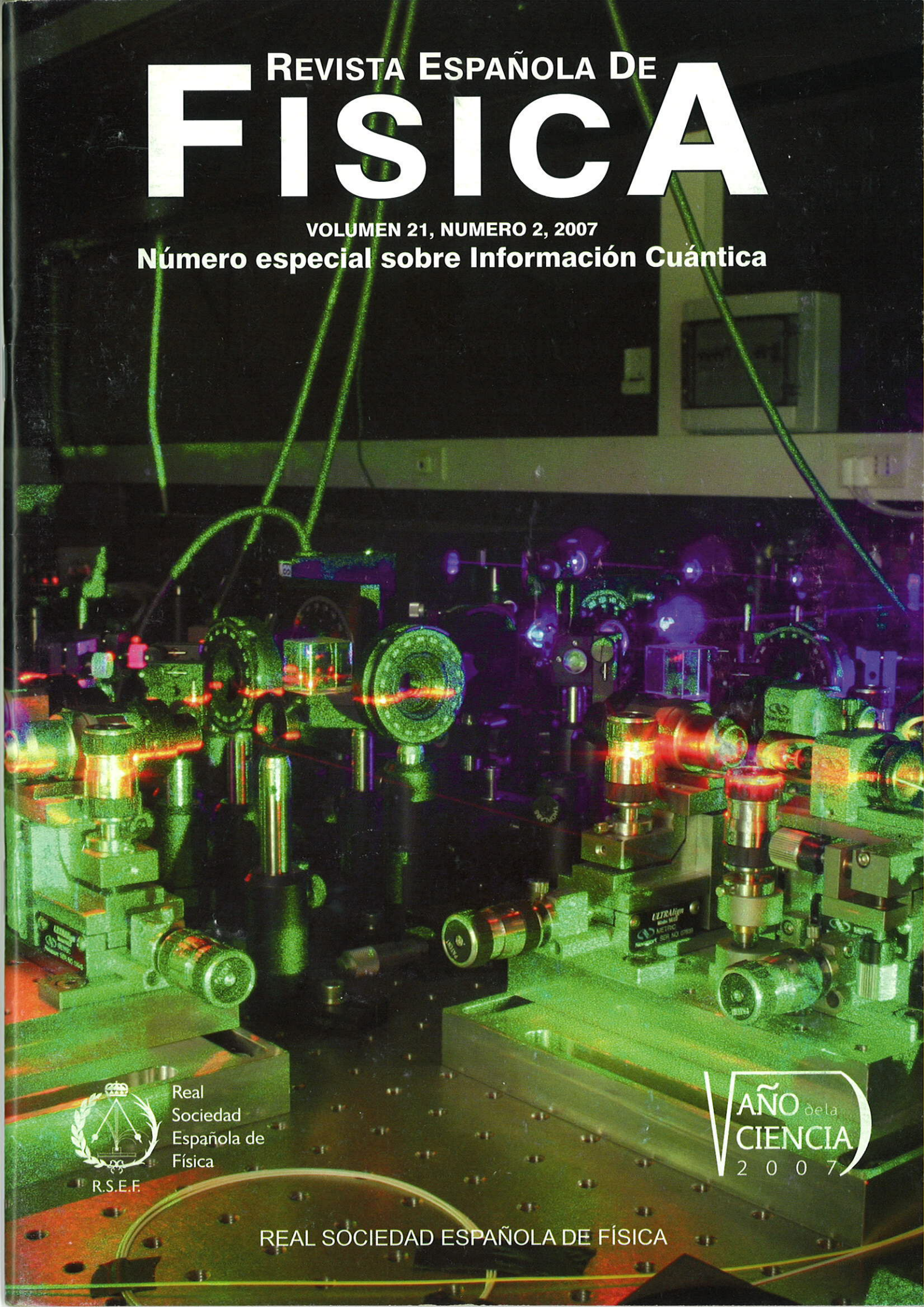
REVISTA ESPAÑOLA DE

FISICA

VOLUMEN 21, NUMERO 2, 2007

Número especial sobre Información Cuántica



Real Sociedad Española de Física

R.S.E.F.

AÑO de la CIENCIA 2007

REAL SOCIEDAD ESPAÑOLA DE FÍSICA

Criptografía cuántica en redes clásicas

Daniel Lancho, Jesús Martínez y Vicente Martín

Quantum Key Distribution (QKD) is the first technology derived from Quantum Information and Quantum Computation that is being marketed. To date, the commercial applications are in the encryption of point to point links. Now, the next logical step is about to be taken. Full quantum networks able to transport the keys to be used in symmetric key cryptography with a security level previously unattained are being designed. The proof of concept of many of the ingredients needed exist and networks with a few nodes have been implemented. The first networks will cover a metropolitan area and demonstrate the feasibility of large-scale QKD integrated with classical networks. If it succeeds in the marketplace, this could signal a major shift in how cryptography is used today.

1. Introducción

Vivimos en un mundo conectado, qué duda cabe. La mayor responsable de esta situación es "la red". La red no es en realidad una tecnología sino un conjunto de ellas que, además, evoluciona para adaptarse a las necesidades de la sociedad. Desde el nacimiento de Internet, muchas partes han sido eliminadas, modificadas o ampliadas para dar cabida a nuevas tecnologías de transmisión y a nuevos servicios, o a viejos servicios bajo nuevos aspectos: el web, nacido en el CERN, data de 1990; las últimas variantes de redes inalámbricas, del año pasado. A esta mezcla de componentes hardware y software les impone una estructura un conjunto de protocolos llamados Protocolos Internet o IP, abreviatura habitual usando las iniciales del nombre inglés. Es tal la importancia de estos protocolos que su implementación en lo que fueron los primeros nodos es la que fecha el nacimiento de la Internet: noviembre de 1977. Uno de los elementos básicos que ha estado siempre presente en estos protocolos es la capacidad de direccionar, de asignar un nombre a un dispositivo o un servicio, de manera que pueda ser localizado lógicamente. En las últimas revisiones de los IP la capacidad de direccionar es tan amplia que prácticamente se podría asignar una dirección a cualquier dispositivo electrónico, no sólo a ordenadores: lavadoras, aspiradoras, televisiones y, también, sensores y etiquetas de radiofrecuencia. En un mundo tan conectado y señalizado, con una capacidad de proceso siempre creciente, capaz de asociar los quién, qué y dónde de las comunicaciones a un coste cada vez menor, la privacidad y la seguridad cobran un nuevo sentido. Las técnicas para proteger esta privacidad, que a la vez permitan disfrutar de todas las ventajas de un mundo de acceso rápido a la información, están llamadas a desempeñar cada vez un papel más importante. Mientras estos escenarios están empezando a tomar forma, hoy en día, la seguridad y protección de la información en la red se centra en temas más concretos: cómo lograr transmitir información confidencial a un receptor, de modo que nadie más que él la reciba y que, además, emisor y receptor estén seguros de sus identidades mútuas es, quizá, el problema más importante. Un problema en el que la criptografía cuántica puede jugar un papel crucial.

2. Seguridad convencional y seguridad cuántica

Dentro de los protocolos IP se integran un conjunto de técnicas que permiten el establecimiento de canales seguros de comunicaciones. Estas técnicas de criptografía convencional son básicamente de dos tipos: sistemas de clave pública y sistemas de clave secreta.

Los sistemas de clave secreta se basan en una clave única que sirve tanto para cifrar como para descifrar, de ahí que también sean conocidos como simétricos. Los más usados trabajan con bloques del mensaje en claro, realizando operaciones entre sus bits. La función precisa que realiza estas operaciones depende de la clave y se elige de modo que sea muy difícil averiguar cuál será el texto cifrado a partir de un texto conocido y una clave desconocida, o averiguar información sobre la clave conocidos una serie de pares de mensaje en claro y su correspondiente cifrado. La operación es biyectiva y, por tanto, existe una transformación inversa dependiente de la misma clave que descifra el mensaje. Un cifrador así se considera perfecto si, para todos los textos en claro, P, y todos los cifrados, C, se cumple que las probabilidades $p(\mathrm{P}) = p(\mathrm{P}\,|\,\mathrm{C})$. En la práctica se consideran muy seguros, aunque sin datos concretos (redundancia en el mensaje, algoritmo, tamaño de clave) resulta difícil dar cotas de esta seguridad en función del tamaño del mensaje [1]. A esta familia pertenece el único criptosistema clásico demostrablemente seguro: el cifrador de Vernam o cuaderno de un solo uso. En éste se asume que emisor y receptor, habitualmente llamados Alicia y Benito, comparten una clave constituida por una cadena de bits aleatorios. Para cifrar, Alicia hace un XOR (O exclusivo, 1 XOR 1 = 0) entre el mensaje y la clave, Benito vuelve a hacer un XOR a lo recibido con la misma clave, obteniendo el mensaje original. Puesto que al hacer un XOR de un bit con otro desconocido es imposible averiguar el valor del bit original, el mensaje es seguro. Al menos mientras la clave sea completamente aleatoria y se haya usado una sola vez. Evidentemente, de esta manera sólo se puede transmitir con seguridad absoluta mensajes de la misma longitud que la clave. Los cifradores simétricos habituales usan claves mucho más cortas (entre 56 y 256 bits, típicamente 128) que se cambian cada cierto tiempo, normalmente cada 10-20 minutos. Son también algoritmos rápidos, algo muy valioso para las comunicaciones.

Los sistemas de clave pública tienen una filosofía radicalmente distinta: usan una clave de cifrado y otra de descifrado, de ahí que también sean conocidos como asimétricos. La clave de descifrado se mantiene privada por el receptor mientras que la clave de cifrado es pública y puede ser enviada por cualquier medio o mantenida en algún almacén central de acceso público. Los procedimientos de cifrado (C) y descifrado (D) son tales que a partir de la clave pública es muy difícil inferir la privada. Para poder enviar mensajes

secretos estos procedimientos deben ser inversos para todo mensaje M: $D(C(M)) = M$. Si Alicia quiere enviar un mensaje secreto a Benito, toma C_{Benito} del lugar público y cifra el mensaje M que sólo Alicia con su D_{Benito} privado, haciendo D_{Benito} $(C_{Benito}(M)) = M$, podrá descifrar. Este proceso es computacionalmente mucho más ineficiente que el equivalente simétrico.

El criptosistema de clave pública más usado es el debido a Rivest, Shamir y Adleman, o RSA. Su fortaleza reside en la suposición de complejidad computacional de la factorización. El mejor algoritmo conocido corre en tiempo exponencial en el número de bits de la clave, n. A pesar de lo enormemente seguro que puede parecer esto, conviene recordar que no es un hecho demostrado y que mañana puede aparecer un algoritmo que resuelva el problema de la factorización en tiempo polinomial. Conviene también repasar la historia reciente de records de factorización y observar cómo han ido variando las estimaciones del tiempo que se tardaría en romper una clave de una longitud dada. En el artículo original [2], en 1977, se calculaba que claves con 100 dígitos (decimales) permanecerían seguras durante unos 74 años. Esas claves fueron rotas por primera vez en 1991 y hoy, con los nuevos algoritmos y un PC moderno, podríamos romperlas en cuestion de horas. Claves de 200 dígitos fueron estimadas seguras por una duración similar a la edad de la tierra; de 193 dígitos fueron rotas en el 2005 usando un cluster de 80 CPUs normales durante cinco meses. Por poner este coste computacional en perspectiva: los ordenadores más grandes de este país disponen de 10.000[1] y 2.500[2] CPUs. En la actualidad no se consideran seguras, al menos para aplicaciones importantes que requieran seguridad a largo plazo, claves de menos de 2048 bits, para las que originalmente se estimaba una resistencia superior en varios órdenes de magnitud a la edad del universo. Y todo esto sin considerar el algoritmo de Shor, para el que se requerirá un ordenador cuántico pero que resuelve el problema de la factorización en tiempo polinomial. Esto, además de abrir interesantes conjeturas sobre la potencia de la computación cuántica y sobre la complejidad real del problema de la factorización, supone la muerte de la criptografía RSA y sistemas afines para información que deba ser mantenida secreta a largo plazo.

Puede que la computación e información cuántica destruya una parte de la criptografía convencional, pero también provee una alternativa que podría resultar extremadamente útil. De hecho, sienta las bases de una infraestructura que podría jugar un papel fundamental en las comunicaciones del futuro. La imposibilidad de hacer copias perfectas de estados cuánticos desconocidos es la idea básica que hace posible que la criptografía cuántica sea completamente segura. La primera referencia es más antigua (Wiesner, *circa* 1970) de lo que la juventud del campo podría dar a entender, aunque no se llegase a publicar hasta 1983. Pero no sería ésta, sino la publicación en unas actas en 1984 del protocolo BB84 [3] la que realmente marcó el inicio de la criptografía cuántica. Este protocolo establece una serie de pasos que permiten que una cadena de bits aleatoria (la clave) sea compartida entre los dos operadores del mismo, reduciendo el conocimiento que un tercero pudiera tener de ésta a valores arbitrariamente bajos.

El protocolo BB84 se explica habitualmente en términos de los estados de polarización de un fotón, aunque se podría utilizar cualquier sistema cuántico de dos niveles o qubit. El protocolo funciona en dos fases: una cuántica y otra clásica. La parte cuántica hace uso de dos bases máximamente conjugadas. En términos de estados de polarización usaríamos la base "recta" con estados de polarización horizontal (H) y vertical (V) y la base "oblicua" con estados de polarización a $+45^0$ (+) y -45^0 (–). El solapamiento entre dos estados, uno de cada base es 1/2. Si ahora Alicia y Benito quieren crear una clave que sólo ellos dos conozcan, Alicia comienza eligiendo dos bits aleatorios. Uno para la base y otro para el valor que quiere codificar. Podrían establecer que el "1" representa la base recta y el "0" la oblicua y que "1" se representa por H en la base recta y por "+" en la oblicua, de modo que si los bits aleatorios son "11", Alicia prepararía un fotón en el estado H y se lo enviaría a Benito. éste espera la llegada del fotón y lo mide en la base recta u oblicua según otro bit aleatorio que ha obtenido de manera independiente. Está claro que según este procedimiento, Benito obtendrá el mismo valor que Alicia cuando ambas bases coincidan, que será la mitad de las veces, y, del resto, tendrá el mismo valor la mitad de las veces, ya que la posibilidad de errar o acertar cuando las bases son distintas es del 50%. Un espía introduciría inevitablemente un error mayor y, por tanto, podría ser detectado. Para que ambas partes finalicen con una cadena de bits idéntica, se continúa con la parte clásica del protocolo. Benito anuncia por un canal clásico público cuales fueron las bases que utilizó para cada fotón que le llegó. Este canal puede ser escuchado por cualquiera, pero para que el protocolo sea seguro Alicia necesita saber que es realmente Benito quien anuncia las bases y no alguien que se haga pasar por él. En criptografía convencional esto se conoce como un canal autenticado. Cuando escucha a Benito, Alicia responde, por el mismo canal, diciendo para qué fotones las bases de Benito han coincidido con las suyas. El conjunto de bits que corresponden a los fotones medidos en la misma base compondrían la clave si todo el proceso hubiese sido perfecto: sin pérdidas en el canal, sin problemas en los emisores/detectores de fotones y, por supuesto, sin espía. Como nada es así, ahora hay que corregir todos estos errores, por lo que se procede a la detección de los mismos. El proceso habitual pasa por tomar bloques de la clave y calcular su paridad. Esto lo hacen tanto Alicia como Benito, comparando sus resultados. Cuando la paridad difiere es que hay, al menos, un error, de modo que se subdivide el bloque y se repite el proceso hasta que se encuentra. Para no dar información, por cada paridad revelada se descarta un bit de clave. Este proceso de corrección de errores permite la estimación de una magnitud clave: la "tasa de error de bits cuánticos", TEBC, definida como el número de bits erróneos dividido por las detecciones totales.

El valor de la TEBC sirve para guiar el mismo proceso de corrección de errores y la fase siguiente, la amplificación de privacidad. Es, además, la cantidad que nos permite asegurar si podremos obtener una clave secreta final o no. Si tenemos

[1]Centro Nacional de Supercomputación, Barcelona. www.bsc.es.
[2]Centro de Supercomputación y Visualización de Madrid. cesvima.upm.es.

un espía dotado de todo el poder que le diese un computador cuántico, incluyendo la capacidad de atacar coherentemente un número ilimitado de los qubits usados durante la transmisión, aún sería posible que Alicia y Benito obtuvieran una clave completamente segura si el valor de la TEBC fuese menor que un 11% [4]. En la práctica el proceso de depuración clásico asociado es tan costoso que con valores de la TEBC bastante menores del 11% es preferible interrumpir la transmisión y asumir que se está siendo atacado o que el canal de comunicaciones está estropeado. TEBC típicas van del 1% al 3%. Después de la corrección de errores es todavía posible que un hipotético espía conozca parte de la clave, por ello se hace una fase de amplificación de privacidad. La idea es dispersar el conocimiento que pudiese tener el espía entre el resto de los bits desconocidos de clave, de modo que cada vez sepa menos. Si, por ejemplo, un espía conoce el valor del bit 16 pero no el del 15, y hacemos un XOR (15,16) tendremos un valor completamente desconocido para el espía. Si hiciesemos XOR entre todos los pares contiguos de bits de la clave el espía perdería toda la información que conociese de bits aislados. Sólo le quedaría la información que tuviese de pares de bits contiguos. El precio a pagar sería alto: la clave se reduce a la mitad. En la práctica lo que se hace es utilizar ciertas familias de funciones *hash*, más eficientes en términos de clave perdida/privacidad ganada. El proceso clásico es costoso y, por dar cifras ilustrativas, si asumimos una transmisión con una TEBC del 3% y obtenemos una clave bruta de 8 kb, debemos hacer dos transmisiones con un total de 144 kb en la reconciliación de bases (unos 20 ms en redes modernas) que nos deja la clave en la mitad. Unas 1000 transmisiones para comunicar unos 20 kb en la parte de corrección de errores (10 s) que nos deja una clave de unos 3 kb. Finalmente hay que hacer otra transmisión más para la amplificación de privacidad, que nos deja unos 2 kb de clave final privada útil. Las cifras dadas se corresponden con una implementación directa del método habitual, sin optimizaciones ni mejoras algorítmicas, pero sirve para ilustrar el hecho de que la parte clásica puede ser el cuello de botella de un sistema de criptografía cuántica.

Una vez ha terminado el protocolo Alicia y Benito comparten una clave, que ha sido generada simultáneamente por ambos y de la que se ha excluido el conocimiento que una tercera persona pudiera tener de ella. Este proceso se conoce como "distribución cuántica de claves" o DCC. Obsérvese que la exigencia de que el canal esté autenticado requiere que Alicia y Benito compartan previamente una clave común. Obsérvese también que parte de la nueva clave generada puede utilizarse para renovar la utilizada en la autenticación, de modo que un nombre más correcto para este proceso sería "crecimiento cuántico de claves".

El protocolo descrito es el más usado, pero es tan solo uno de los disponibles. Hay protocolos de solo una base y de más de dos. Hay protocolos basados en pares EPR y protocolos especialmente diseñados para ser resistentes frente a determinados tipos de ataques, etc.

3. Integración con redes clásicas y servicios

Un protocolo de DCC puede utilizar cualquier realización física de un qubit. Hasta el momento en DCC éste ha sido invariablemente el fotón. Los fotones son qubits realmente buenos para esto: hay maneras relativamente fáciles de manipular el grado de libertad en el que se codifica la información, ya sea polarización, fase, etc. así como buenos canales de transmisión: aire y fibra óptica. Sin embargo, también hay problemas. El proceso físico de DCC se inicia emitiendo un único fotón. Puesto que en la actualidad no hay dispositivos, más allá de la fase de prototipo, que generen fotones individualmente y bajo demanda, se suele usar un pulso láser atenuado. Esto implica la posibilidad de que haya pulsos con más de un fotón, con la consiguiente pérdida de seguridad, y pulsos con ningún fotón, lo que supone una pérdida en la eficiencia del sistema. El medio por el que se propaga el fotón no es perfecto, de modo que éste puede perderse. En fibra óptica, en la ventana de máxima transparencia (1550 nm), estas pérdidas son de alrededor de 0,2 dB/km. Los detectores existentes son muy ineficientes, especialmente a 1550 nm, donde más crítico es para la fibra óptica. Tienen también otros problemas, como la velocidad máxima de conteo o la inestabilidad temporal de la señal generada, lo que puede hacer complicado mantener la marca de tiempo que nos permite indizar cada qubit detectado para usarlo luego en la parte clásica del procolo. Estos problemas hacen que las distancias máximas seguras alcanzables estén limitadas y que la eficiencia sea muy baja. En la actualidad hasta unos 200 km aproximadamente, pero ya con ratios de clave segura del orden del bit/s [5].

Por reducir todas estas magnitudes a una situación práctica en un sistema real[3]: con una fibra de 13 km, de cada millón de pulsos, generados en 0,2 s, sólo se tienen unas 6000 detecciones válidas que podrán pasar a la parte clásica

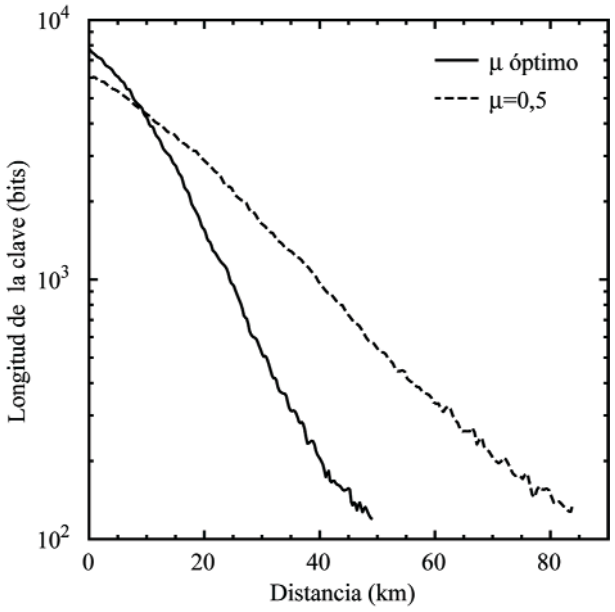


Figura 1. Bits de clave por Mbit de pulsos generados en un sistema de haz atenuado frente a la distancia, después de la corrección de errores y para distintos valores de μ, el número de fotones promedio en el pulso atenuado. El intercambio completo dura 0,2 s. El valor óptimo de μ se elige para reducir la probabilidad de éxito de determinados ataques al protocolo BB84, para el que se ha obtenido esta gráfica. Valores de μ más altos se pueden usar con nuevos protocolos, lo que aumenta la distancia máxima segura.

[3]id Quantique id-3000.

del protocolo que nos dará 1,5 kb de clave útil. Una situación real para distintas distancias se puede ver en la figura 1.

Las redes de comunicaciones convencionales están mucho menos limitadas. Las señales que transmiten pueden ser copiadas y amplificadas, de modo que se puede introducir redundancia fácilmente y el alcance es ilimitado. Las redes cuánticas llevan información que no se puede copiar ni amplificar. En ausencia de un medio de transmisión perfecto, esto significa que el alcance es limitado y que las transmisiones son punto a punto: sólo Benito y Alicia podrán compartir directamente la misma cadena de bits secreta. Además de estas limitaciones intrínsecas hay otras limitaciones relacionadas con el momento tecnológico actual: la baja eficiencia, el alto coste de los componentes y su escasa variedad –en términos de optimización para tareas especializadas– y la relativa incompatibilidad entre el hardware cuántico y el usado habitualmente para comunicaciones. Las redes cuánticas, además, necesitan la colaboración de una red clásica preexistente y lo que transportan son claves, no datos, de modo que requieren una infraestructura software capaz de integrar todos los dispositivos y canales físicos para ofrecer servicios fiables. Todos estos problemas no son imposibles de superar y hay ya redes de prueba que incluyen soluciones para algunos [6]. De hecho, existen ya servicios comerciales usando criptografía cuántica.

El conjunto de protocolos IP está distribuido en siete niveles, cada uno con unas tareas bien definidas. El nivel más bajo, denominado físico, es el que se ocupa del hardware. Estándares para este nivel tienen que detallar información como los voltajes, la duración o la forma de los pulsos para codificar los bits. USB (Universal Serial Bus), RS-232 u 802.11g son nombres que alguna vez hemos oído de protocolos que están a este nivel. El nivel más alto es el de aplicación, que da servicios directamente al programa que esté utilizando el usuario. Dada la variedad de aplicaciones posibles, estos servicios son muy diversos. HTTP, TELNET, SSH son ejemplos de servicios a este nivel. Aquí se incluyen algunos mecanismos para mantener la privacidad y la autenticación de las partes involucradas en una comunicación. Niveles intermedios se ocupan de tareas que van desde el cifrado hasta el encaminamiento a través de la red. El nivel dos es conocido como nivel de enlace y su misión es mantener la fiabilidad de la conexión de nivel uno. En él se definen cómo se empaquetan las señales en tramas, se les da una interpretación, cómo detectar errores y qué hacer cuando se encuentra uno, etc. Ethernet, WiFi, son algunos de estos protocolos. Es en el nivel dos en el único en el que hasta ahora se han ofrecido servicios comerciales de criptografía cuántica. Son sistemas punto a punto que pueden ser vistos como si se tratase de un cable mágico. Se instalan por pares Alicia/Benito: digamos el sistema Alicia en una oficina en el centro de la ciudad y el sistema Benito en un parque tecnológico de las afueras, donde la empresa tenga su centro de proceso de datos. La conexión entre ambos debe ser una fibra óptica, ininterrumpida y de uso exclusivo, para el canal cuántico y otra, no necesariamente de uso exclusivo, para el canal público y la transmisión de los datos cifrados. Entre Alicia y Benito se está ejecutando continuamente un protocolo de DCC. Las claves resultantes se utilizan para alimentar un cifrador simétrico, normalmente un AES (Advanced Encryption Standard), que cifra todas las comunicaciones que pasan a través de la conexión clásica Alicia/Benito. La clave cambia tantas veces por segundo como la vaya generando el protocolo cuántico. Los ordenadores que utilizan esta conexión envían y reciben los datos sin cifrar del mismo modo que lo harían con una conexión cualquiera: es transparente para los niveles superiores, que no necesitan "saber" que está allí. Con este esquema las claves no pueden ser utilizadas por ningún otro nivel en la pila IP, pero aún así se pueden hacer cosas interesantes, como una copia de respaldo contra un centro de proceso de datos remoto o crear una red virtual privada en la que dos enclaves seguros, separados varios kilómetros y con una red privada cada uno, se comportan como si fuesen una sola red dentro de un único perímetro seguro.

La integración en nivel de enlace tiene la ventaja de la transparencia: no hay que modificar nada en niveles IP superiores, pero es caro y poco versátil. Necesita una fibra óptica dedicada y el hardware cuántico no puede ser compartido entre varios usuarios. Las claves generadas no se pueden gestionar fuera del enlace ni usar en otra aplicación o para otros propósitos. Con esto no tenemos una verdadera red de distribución de claves. Con la tecnología existente se puede pensar de manera realista en construir una red de área metropolitana, de hecho, varias de estas se encuentran ya en proyecto o en fase experimental. Las distancias típicas en una de estas redes no excede los 10-20 km, que están dentro del rango donde los dispositivos de DCC tienen un buen rendimiento. La arquitectura básica es un conjunto de pares conectados de sistemas Alicia/Benito cuyos extremos residen en lugares considerados seguros. Estos pares están continuamente intercambiando claves, de modo que en cada extremo del par se mantienen almacenes de claves que serán los que se usen para dar servicios en la red clásica. La conexión cuántica entre dos nodos no tiene por qué ser única y, de hecho, para poder garantizar el ancho de banda (la cantidad de bits de clave por segundo generadas) y la disponibilidad del sistema, hay que dotar de una cierta redundancia al sistema. Tanto en términos de añadir pares Alicia/Benito extra como en unirlas con más de un camino de fibra óptica o de ser capaces de reconfigurar las parejas. La redundancia encarece el sistema e introduce una serie de complicaciones técnicas en los algoritmos de encaminamiento o el restablecimiento de la sincronización del sistema: no hay que olvidar que Benito espera que Alicia le envíe la información en intervalos temporales muy precisos. Benito activa sus detectores sólo en esos intervalos, que en la actualidad son del orden de unos pocos nanosegundos. Estos problemas técnicos pueden ser resueltos y la ventaja ahora es que la red será compartida por muchos más usuarios.

Sobre este nivel físico de sistemas cuánticos se construye un nivel lógico por el que se garantiza que dos nodos cualesquiera de la red DCC pueden crear una clave común, aunque no estén directamente conectados como pareja Alicia/Benito. Los nodos intermedios sencillamente hacen un reenvío de la clave creada en el primer par usando un cifrado Vernam hasta alcanzar el destino. Este nivel se conoce como nivel de secretos. Es posible dotarle de infraestructuras adicionales para dar servicios globales más allá del transporte punto a punto de claves. Este sería el caso, por ejemplo, de la creación de un almacén de claves centraliza-

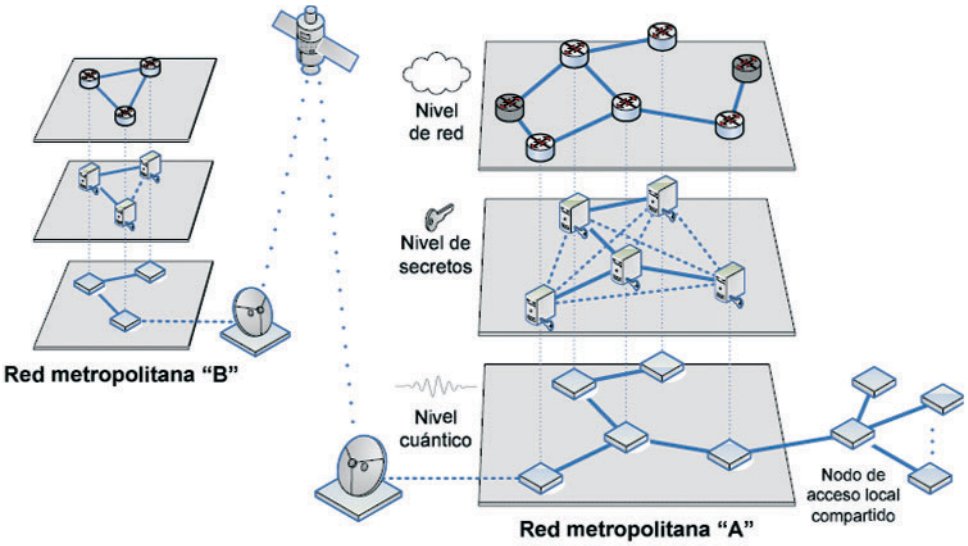


Figura 1. Esquema de la arquitectura de las redes DCC [6]. En el nivel cuántico están los dispositivos físicos y los canales cuánticos de conexión punto a punto. A este nivel también se encuentran las conexiónes a larga distancia con otras redes (a la izquierda de la gráfica) y los nodos de acceso local compartidos (A la derecha. Por claridad en estos solo se ha dibujado el nivel cuántico). El nivel de secretos establece una arquitectura lógica con la cual cualquier nodo conectado a nivel cuántico, incluyendo los usuarios de nodos de acceso, pueden establecer un canal seguro con cualquier otro nodo de la red cuántica. El nivel más alto se corresponde con la red clásica, algunos de estos nodos tendrán un equivalente en el de secretos y podrán acceder continuamente a los servicios asegurados por criptografía cuántica. Otros nodos (marcados con un color más oscuro) no tendrán conexión directa y podrían incluso ser móviles. Estos deberán conectarse a la red DCC de vez en cuando para recargar sus almacenes de secretos.

do común que se podría usar, por ejemplo, como autoridad de certificación. Esta autoridad podría dar servicios de autenticación y comunicación segura a dos o más usuarios que quisieran asegurar su identidad mútua y establecer un canal criptográfico convencional fuera de la red DCC. Además, estos servicios pueden ser ofrecidos sin necesidad de estar conectados en ese momento a la red cuántica: basta con que se haya hecho un intercambio seguro previamente. Esto se correspondería ya con el nivel de red convencional. Una representación de estos tres niveles se muestra en la figura 2. En ella aparecen también dos partes que se ocupan de la larga y corta distancia. Para convertir una red metropolitana en global hace falta ser capaz de generar claves en segmentos con longitudes que vayan desde los centenares a los millares de kilómetros. Aunque es en principio posible construir repetidores cuánticos, la tecnología requerida es todavía inaccesible y es previsible que tarden años en fabricarse. Podrían utilizarse puntos seguros intermedios, del mismo modo que se usan en la red metropolitana, pero esto no permitiría cruzar un océano. Una tercera tecnología con posibilidades a corto plazo es el uso de DCC con dispositivos al aire libre. El aire es un buen medio para transmitir fotones y se han desarrollado sistemas especializados para ello, de los cuales algunos se están aproximando ya a la fase de comercialización. Con ellos es posible hacer nodos en los que Alicia está en tierra mientras que Benito se encuentra en un satélite. El satélite se puede considerar un punto seguro dada su inaccesibilidad. La comunicación entre satélites puede hacerse por medios clásicos, abriendo así la posibilidad de una red DCC de alcance global.

En la figura también se muestra el acceso del usuario final. Un tema activo de investigación es la creación de clientes (Alicias) ligeros desde los que acceder al transporte de claves ofrecido por la red DCC. Estos clientes estarían optimizados para ser baratos y trabajar en distancias cortas, posiblemente utilizando en tiempo compartido un único Benito, más caro pero con mayores capacidades. De esta manera bastaría con poner un punto de acceso de la red DCC en un edificio o parque industrial para ofrecer servicios relativamente baratos al grupo de empresas en un entorno cercano, del orden de los cientos o pocos miles de metros.

Un punto clave para el éxito de las redes DCC es la compatibilidad con la infraestructura de comunicaciones y la criptografía convencionales. La compatibilidad software se puede hacer integrando un nuevo conjunto de protocolos en los IP, tarea que se está realizando en este momento. En cuanto al hardware, la red DCC funciona de manera paralela a las redes de datos, con canales cuánticos dedicados. Si para construirla es necesario crear todos estos segmentos cuánticos desde cero, sin reaprovechar las inversiones existentes en comunicaciones convencionales, las probabilidades de éxito estarían muy mermadas. La compatibilidad hardware, para poder usar líneas de comunicación y equipos preexistentes, es una característica vital para las redes DCC. El punto clave es lograr utilizar las fibras ópticas en uso como canales cuánticos. Hacer pasar cada vez más información por una única fibra óptica es un tema importante en comunicaciones convencionales. Para esto existen varias tecnologías, una de las más usadas es la multiplexación en longitud de onda (WDM, Wavelength Division Multiplexing). Estos multiplexores toman la frecuencia de entrada y la cambian ligeramente. En el dispositivo físico el cambio que hacen depende de cuál es el puerto de entrada que se está utilizando. Se pueden conectar varios equipos estándar de comunicaciones, todos usando canales a la longitud de onda de 1550 nm, a uno de estos WDM que los va separando en saltos de entre 0,2 y 20 nm, dependiendo de la variante que se use, y los introducen en una única fibra óptica de salida. En el otro extremo de la fibra, un aparato similar separa las distintas frecuencias mandándolas a distintas salidas, todas a 1550 nm. De este modo se tiene que una sola fibra óptica puede transportar hasta 160 canales distintos. En la actualidad se trabaja en la posibilidad de usar como canal cuántico una de las frecuencias, de modo que no se necesite una fibra óptica dedicada. Los resultados son alentadores cuando la separación entre el canal cuántico y el clásico más próximo está en el entorno de 3–4 nm, pero una mayor cercanía sería preferible. Una complicación adicional

surge con las pérdidas introducidas por estos dispositivos, que son típicamente de 3 a 5 dB, lo que hace que la distancia óptica real, en términos de la atenuación que sufre el canal cuántico, sea mayor que la distancia geográfica (3 dB ≅ 15 km). Esto hace que, para poder mantener el flujo de claves requerido, el diseño de la red pueda necesitar de pares Alicia/Benito conectados por un canal cuántico exclusivo.

4. Conclusión y Futuro

Los enlaces punto a punto para la distribución cuántica de claves son una realidad comercial. El siguiente paso, las redes de distribución cuántica de claves, son una posibilidad tecnológica al alcance de la mano. Pruebas de concepto para casi todos los componentes han sido realizadas en redes experimentales. Inicialmente estarán limitadas a un entorno metropolitano y a servicios especializados, bien por requerimientos de muy alta seguridad o bien por necesitar canales cifrados en tiempo real con un gran ancho de banda. A medida que se extiendan, las redes convencionales podrán contar con una nueva infraestructura de distribución de claves simétricas, con lo que servicios que antes se daban usando esquemas de clave pública podrán pasar a darse, más eficientemente y con niveles de seguridad mejorados, utilizando esquemas de clave simétrica.

Bibliografía

[1] B. Preneel *et al.*, IST-1999-12324 (2004), https://www.cosic.esat.kuleuven.ac.be/nessie/.
[2] R. Rivest *et al.*, *Communications of the ACM* **21** (2), 120 (1978).
[3] C. H. Bennett y G. Brassard, *Proceedings of the International Conference on Computer Systems and Signal Processing* (IEEE, New York, 1984), p. 175.
[4] P. W. Shor y J. Preskill, *Phys. Rev. Lett.* **85**, 441 (2000).
[5] F. F. Chi-Hang *et al., Phys. Rev. A* **73**, 012337 (2006).
[6] C. Elliot *et al*., quant-ph/0503058 (2005) y SECOQC, www.secoqc.net.

Daniel Lancho, Jesús Martínez y Vicente Martín
están en el DLSIIS-Análisis Numérico, Facultad de Informática, Universidad Politécnica de Madrid, Boadilla del Monte