INTEGRANDO LA CRIPTOGRAFÍA CUÁNTICA EN REDES CLÁSICAS

D. Lancho, J. Martínez y V. Martín

Departamento LSIIS-Análisis Numérico. Facultad de Informática. Universidad Politécnica de Madrid. Campus de Montegancedo, 28660 Boadilla del Monte, Madrid.

Vicente.Martin@fi.upm.es

Resumen: Algunos aspectos de la criptografía cuántica son realidades tecnológicas hoy en día. Esto es lo que ocurre con la generación y distribución cuántica de claves para sistemas criptográficos convencionales de clave simétrica. De momento esta distribución se hace tan solo entre dos puntos directamente conectados por el canal de transmisión cuántico, lo que limita su utilidad a usuarios dispuestos a correr con los gastos derivados de un equipamiento caro y una línea punto a punto que, además, no puede ser de longitud ilimitada. Para lograr que esta tecnología acabe siendo de uso común hay que integrarla en las redes de comunicaciones clásicas. Esto abarataría su uso e incrementaría su disponibilidad geográfica, aumentando el número de usuarios potenciales. En este artículo discutimos las limitaciones y ventajas de la distribución cuántica de claves y los primeros pasos hacia su inclusión dentro de la infraestructura de seguridad en las redes de comunicaciones convencionales.

1. Introducción

La distribución cuántica de claves es una tecnología que está madurando rápidamente. La imposibilidad de hacer copias perfectas de estados cuánticos desconocidos es lo que hace posible que esta técnica sea completamente segura. Cualquier intento de un espía para leer el canal cuántico dejará una huella que será detectable y que permitirá eliminar aquellos bits de clave sospechosos de ser conocidos por el espía. Desde la formalización del primer protocolo en 1984 [1] hasta la fecha se ha avanzado mucho: su primera implementación en 1986 despertó un gran interés precisamente por demostrar su factibilidad, no por las distancias, la velocidad de transmisión o los niveles de seguridad alcanzados. Hoy en día se pueden realizar transmisiones seguras en fibra óptica hasta distancias cercanas a los 200 Km con dispositivos experimentales, aunque sea a una velocidad de tan sólo unos pocos bits por segundo. La tecnología mejora continuamente y se están construyendo sistemas especializados en cortas y en largas distancias, dependiendo del uso que se les vaya a dar. No obstante, las limitaciones impuestas por la relación inversa entre la distancia máxima alcanzada y la velocidad de transmisión, que lleva aparejada la existencia de una distancia máxima de transmisión debida a las imperfecciones del canal cuántico -indistinguibles de un espía- y el que la generación de claves sea punto a punto, imponen restricciones muy fuertes al diseño de la red.

2. La red cuántica como subestructura de la red clásica

La red cuántica no transporta datos, su objetivo es generar y transportar claves. Funciona como una estructura independiente de la red clásica y puede ser vista como un mecanismo para proveerla de una materia básica, las claves, sobre la que construir nuevos mecanismos de seguridad. En este sentido su estructura lógica puede ser establecida en tres niveles [2]. En el primero están los dispositivos hardware. Estos son conexiones punto a punto entre nodos considerados seguros que están continuamente ejecutando un protocolo cuántico

de QKD[1] [3]. Las claves generadas se guardan en almacenes en los extremos de la conexión. Estas claves serán utilizadas cuando sean solicitadas por la red clásica o dentro de la misma red cuántica para cifrar claves provenientes de otro nodo que deban ser reenviadas a un nodo lejano de la red. Si se quiere hacer manteniendo seguridad absoluta, hay que utilizar en cada salto entre nodos una cantidad de clave igual a la que se está transmitiendo. De esta manera la red física de canales cuánticos se convierte en una red lógica, el segundo nivel, que asegura que entre dos nodos cualesquiera se puede establecer una clave común, incluso aunque no exista una conexión punto a punto entre ellos. El tercer nivel lo compone la red clásica normal. Esta podrá acceder directamente a los servicios de la red cuántica en tanto coincidan los nodos de las dos redes físicas. Si no es así, en algún momento deberán conectarse para rellenar sus almacenes de claves. La red cuántica genera y repone sus almacenes de claves de manera continua, pero su función no es mantener estos almacenes siempre llenos, sea cual sea el nodo, sino disponer de claves suficientes para los servicios que requiera la red de datos clásica. Si en la red clásica se va a realizar un gran movimiento de datos que necesita ser cifrado con niveles altos de seguridad, como en una copia de respaldo remota, se requiere que los dos nodos que van a realizarla compartan una gran cantidad de clave. Esto significa que en la red cuántica deben construirse mecanismos que permitan el encaminamiento de claves bajo petición, pudiéndose incluso requerir la garantía de determinadas calidades de servicio. Estos mecanismos se denominan protocolos de red. En la actualidad no hay un conjunto completo de estos protocolos en la red cuántica análogo al que existe en las redes clásicas, aunque se parte con la ventaja de que algunos de los ya existentes son adaptables.

Otro tema problemático es la compatibilidad de la red cuántica con la convencional. La compatibilidad software obliga a que el conjunto de protocolos de control y servicios se adapten a los protocolos IP (Internet Protocols). Esto no es un perjuicio en si mismo: limita la libertad de adaptación, pero hace que cualquier red cuántica pueda ser usada desde la convencional. La compatibilidad física es más importante desde el punto de vista económico. Si la red cuántica no es capaz de usar las fibras preexistentes ni los equipos ser compatibles con los ya instalados en los nodos de comunicaciones, estaría destinada a convertirse en una tecnología nicho con casi total seguridad. En la actualidad se estudia la posibilidad de multiplexar el canal cuántico junto con canales clásicos en la misma fibra. La tecnología WDM[2] permite tener varias entradas en la misma longitud de onda, que el multiplexor desplaza en frecuencias para introducir todas en la misma fibra óptica. Al final de la misma, otro dispositivo WDM hace la inversa, tomando las distintas frecuencias de la fibra, pasándolas a la frecuencia base y mandando cada una a una salida distinta. Esto hace sobre una sola fibra el mismo efecto que si se hubiesen tenido tantas fibras ópticas como pares de entrada/salida. El problema aquí es que el canal cuántico es muy frágil, siendo muy sensible frente a cualquier tipo de dispersión de los canales viajando a frecuencias próximas. Hasta ahora se tienen buenos resultados cuando la separación entre canales es de unos 4nm, pero una mayor densidad sería preferible: En el estándar D[ense]WDM hay hasta 160 canales viajando por la misma fibra con una separación de 0,8 nm.

[1] Iniciales inglesas, utilizadas habitualmente, de Distribución Cuántica de Claves: Quantum Key Distribution.

[2] Multiplexación por división de longitud de onda: Wavelength Division Multiplexing.

Estos problemas son menores en el prototipo de red en el que estamos trabajando [figura 2]. La idea es construir una red cuántica de área metropolitana cuya topología básica sea un anillo. Esto permite simplificar mucho los protocolos de gestión de la red cuántica -aún cuando la parte de integración con IP mantenga su complejidad- y reduce el número de puntos seguros intermedios necesarios, lo que hace que sea más barata. En cada nodo del anillo un dispositivo conocido como ROADM[3] extrae dos canales de la fibra óptica existente. Uno será usado como canal cuántico y otro como canal para la parte clásica de los protocolos cuánticos. La distancia típica entre nodos del anillo (~10 Km) está bien dentro del rango donde se puede obtener un buen rendimiento con los sistemas de distribución de claves disponible [figura 1], incluyendo las pérdidas inevitables en los conectores y multiplexores (~3 dB, equivalentes a ~15 Km de fibra óptica). En el anillo se están generando y transmitiendo claves de manera continua que son repartidas a los usuarios finales a través de conexiones especiales donde se sitúa un sistema modificado para que la conexión punto a punto pueda hacerse cambiando uno de los extremos bajo demanda. Este funcionamiento en tiempo compartido abarata notablemente los costes de servicio.

3. Resultados y conclusiones

Los próximos años serán clave para el despegue de QKD como tecnología de uso común. En la actualidad, aunque se sigan haciendo esfuerzos importantes en mejorar las técnicas básicas -especialmente en la extensión de las distancias máximas y el aumento de la velocidad de generación de clave- se ha pasado del estatus de tecnología emergente a ser un candidato serio que podría cambiar radicalmente la manera de usar la criptografía en la red. Ya se está trabajando en integrar los servicios añadidos que ofrece con las redes tradicionales. Los operadores de red se involucran activamente en este tipo de proyectos y los objetivos y técnicas para lograr redes QKD capaces de dar servicio a usuarios finales están bien definidos. También se están diseñando prototipos de red como el presentado y están construyéndose instalaciones piloto. Si no se logran estos objetivos de integración con la presente generación de dispositivos -y los que ahora mismo están en su fase final de desarrollo- habría que esperar hitos tecnológicos importantes, como la creación de fuentes de fotones individuales y detectores muy eficientes, para que QKD volviese a generar interés económico y dejase de una tecnología nicho.

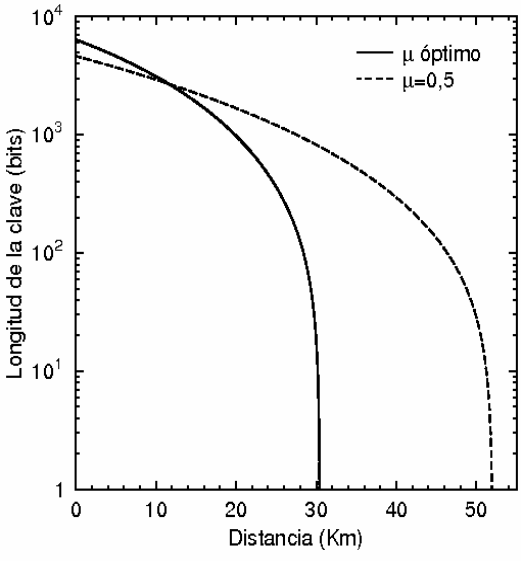

Figura 1. Longitud de clave final, después de realizar la parte clásica del protocolo BB84, frente a distancia de transmisión en un sistema de criptografía cuántica moderno (id Quantique id3000). La amplificación de privacidad se realiza utilizando la entropía de BBBSS92 [4], que es especialmente restrictiva, en la versión para ataques de intercepción/reenvío. Los sistemas de QKD actuales usan como fuente de fotones láseres atenuados con un número promedio de fotones, μ, por pulso, lo que les hace vulnerables a ataques que tomen sólo un fotón de aquellos pulsos que contengan más de uno. Aquí presentamos resultados para un número fijo μ=0.5 y para un valor óptimo definido como el

[3] Reconfigurable Optical Add and Drop Multiplexer.

mayor valor de μ que hace que estos ataques no puedan tener una eficacia del 100%.

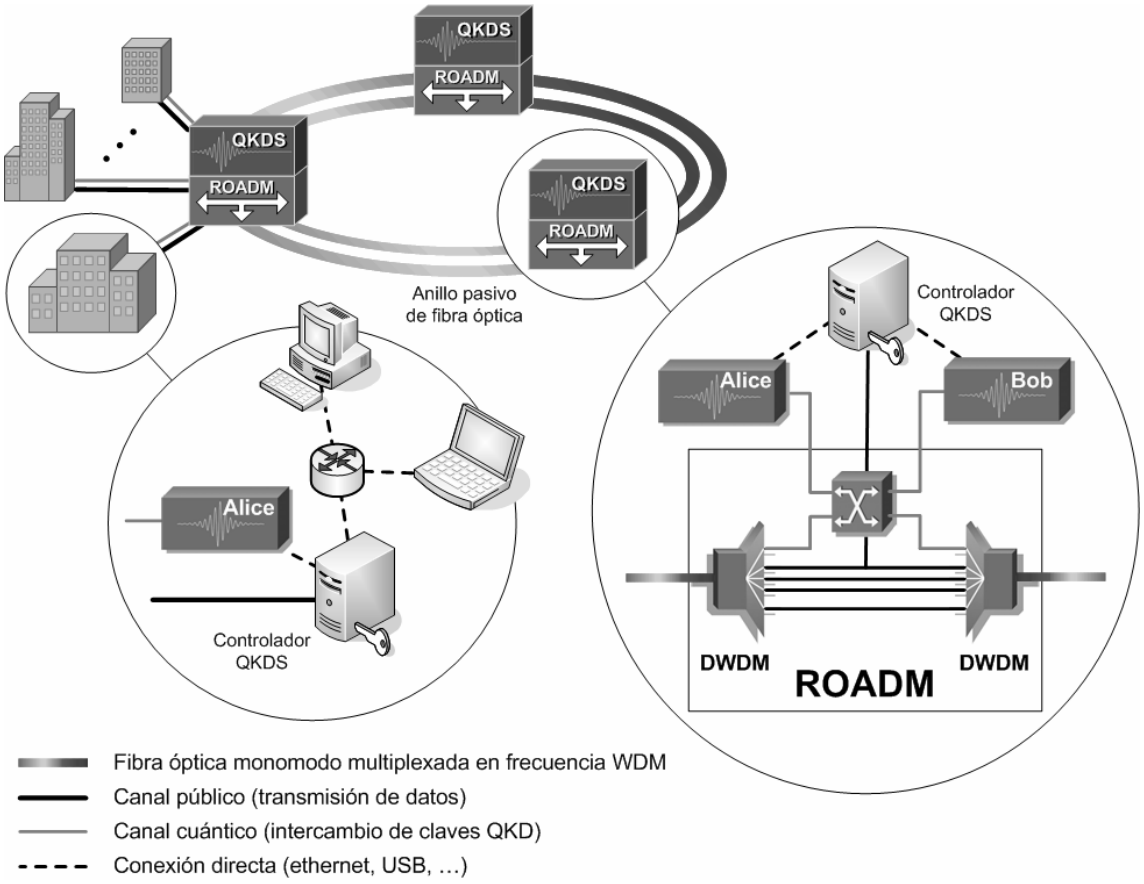

Figura 2. Esquema del anillo de pruebas (arriba). Los nodos del anillo son puntos seguros de una red clásica conectados por una fibra óptica. En estos nodos (abajo a la derecha) se extraen dos de los canales multiplexados para su uso en las partes cuántica y clásica del protocolo por los pares de emisor/receptor cuántico (Alice/Bob) y su ordenador de control. El anillo mantiene una generación constante de claves punto a punto y utiliza unos protocolos de encaminamiento de modo que cualesquiera dos de los puntos de acceso al anillo (abajo a la izquierda) puedan establecer una clave compartida secreta que les permitiría acceder a servicios de seguridad a través de un canal público cualquiera.

Bibliografía

[1] Bennett, C.H. and Brassard, G. ``Quantum Cryptography: Public Key Distribution and Coin Tossing" IEEE International Conference on Computers, Systems and Signal Processing. Bangalore, 1984. Pags. 175-179.
[2] Alléaume, R. et al. “SECOQC White Paper on Quantum Key Distribution and Cryptography”, arXiv:quant-ph/0701168v1. Ver también www.secoqc.net.
[3] Gisin, N. *et al.* Rev. Mod. Phys. 74 (2002) 145, arXiv:quant-ph/0101098v2.
[4] BBBSS92. Bennett, C.H. et al. “Experimental quantum cryptography” Journal of Cryptography Vol. 5, No. 1, 1192.