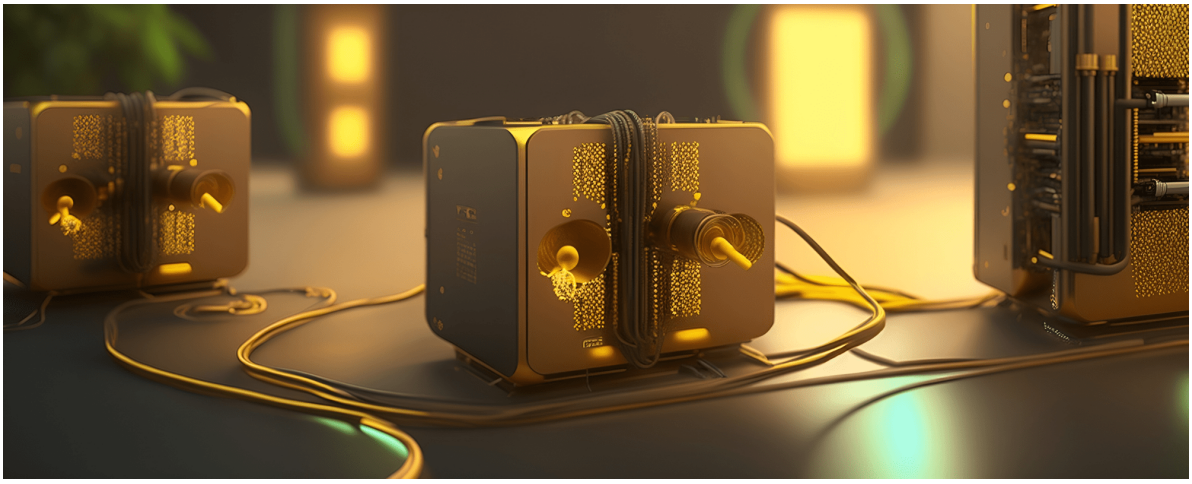
INVESTIGACIÓN Y APLICACIONES PRÁCTICAS

Las redes cuánticas e internet

Hugues de Riedmatten, Valerio Pruneri



Cables cuánticos y prototipo de miniordenador cuántico. Conceptualización: Luisa Quiroga

La comunicación es un elemento esencial de nuestra sociedad. Todos nos comunicamos entre nosotros enviando información en forma de señales que se pueden detectar y generar fácilmente. Por ejemplo, la mayor parte del tráfico de datos que sustenta hoy internet viaja por fibras ópticas en forma de dígitos binarios (bits), en secuencias de ceros y unos, conocidas como cadenas de bits. Estas cadenas están formadas por impulsos de fotones —partículas elementales de luz— cuyas propiedades se pueden describir por medio de la teoría de la física clásica. Los fotones son portadores ideales, ya que se pueden manipular fácilmente y son inmunes a las interferencias ambientales.

Cuando un solo fotón está contenido en un impulso, se convierte en un bit cuántico (qbit), una superposición de estados cuánticos 0 y 1, cuyo comportamiento se describe a partir de la teoría de la mecánica cuántica. Una propiedad fundamental de los qbits es que no se pueden medir sin alterarlos, ni tampoco se pueden clonar (copiar). Dos o más qbits también pueden formar un estado entrelazado; un conjunto de partículas fuertemente correlacionadas que se influyen mutuamente incluso a distancia.

La superposición y el entrelazamiento son dos propiedades cuánticas fundamentales de las tecnologías cuánticas, como es el caso de la comunicación cuántica —es decir, la generación, la transmisión y la detección de qbits-. De manera similar a la comunicación moderna actual, se pueden desarrollar redes cuánticas en que los dispositivos y los sistemas sean cuánticos. Y lo que es más importante: en la mayoría de los casos se pueden compartir las mismas infraestructuras de fibra y satélite por las cuales viajan actualmente los bits clásicos, hecho que hará posible la existencia de internet y redes cuánticas globales en el futuro.

Primer anteproyecto de la futura red de comunicación cuántica segura.

Internet y las redes cuánticas ofrecen un número significativo de funcionalidades y servicios únicos que no son posibles en la comunicación clásica. [1] La criptografía cuántica, que describiremos detalladamente más adelante, es probablemente la más avanzada de estas funcionalidades, y consiste en distribuir claves secretas hechas de qbits (claves cuánticas), que después se utilizan para encriptar y desencriptar mensajes entras dos partes que se comunican. En la práctica, la criptografía cuántica combina la distribución de claves cuánticas (QKD, por las siglas en inglés) y los protocolos de criptografía clásica para llegar a una comunicación segura imposible de piratear, incluso con recursos computacionales ilimitados (por ejemplo, ordenadores cuánticos) y algoritmos potentes. En junio de 2019, los 27 estados miembros de la Unión Europea acordaron construir la Infraestructura Europea de Comunicación Cuántica (EuroQCI), una infraestructura de comunicación cuántica segura que abarcará toda la UE, incluidos los territorios de ultramar. En el último apartado de este artículo, presentaremos el plan inicial para desplegar el EuroQCI en el área metropolitana de Barcelona.

La distancia máxima de la comunicación cuántica en las fibras ópticas se limita a unos pocos centenares de kilómetros, a causa de las pérdidas de la fibra óptica y también por el hecho de que los bits cuánticos no se pueden amplificar sin añadir un ruido que impediría una comunicación fiel. Las redes cuánticas ofrecen una solución a este problema mediante la implantación de repetidores cuánticos que combinan la distribución del entrelazamiento y un dispositivo denominado memoria cuántica, que permite almacenar el entrelazamiento en un sistema material. La implantación de repetidores cuánticos permitirá enlaces completamente cuánticos a distancias continentales. Sin embargo, habrá que superar muchas dificultades técnicas antes de poder implantar un repetidor cuántico completo.

Además de la distribución de claves cuánticas (QKD), también se han propuesto varias aplicaciones futuras que podrían utilizar la distribución del entrelazamiento cuántico, sobre todo en los campos de la computación y la metrología cuánticas. Con respecto a la

computación, los primeros ordenadores cuánticos serán probablemente grandes máquinas ubicadas en laboratorios específicos, parecidos a los superordenadores actuales. El internet cuántico permitirá a usuarios distantes conectarse a estos ordenadores cuánticos en la nube de una manera segura y confidencial, de manera que nadie —ni siquiera el mismo ordenador cuántico— sabrá qué cálculo se está llevando a cabo. Otra potente aplicación futurista será reunir ordenadores cuánticos. Dado que cada ordenador cuántico tiene un número limitado de qbits, el hecho de conectarlos mediante enlaces fotónicos permitirá acceder a un número mucho mayor de qbits y, por lo tanto, aumentar considerablemente la potencia de cálculo. Además de las aplicaciones de computación, las futuras redes cuánticas también tendrán aplicaciones en metrología cuántica. Por ejemplo, se ha demostrado que las redes de relojes ópticos entrelazados permitirían una sincronización más precisa. Igualmente, se ha constatado que la construcción de conjuntos de telescopios que compartieran entrelazados podría elevar la línea de base y aumentar la sensibilidad, hecho que daría lugar a aplicaciones en astronomía.

> La criptografía cuántica permitirá llegar a una comunicación segura imposible de piratear, incluso con recursos computacionales ilimitados y algoritmos potentes

Las funcionalidades del internet cuántico son fundamentalmente diferentes del internet clásico, por lo cual los dos tipos de red son complementarios. El internet cuántico no sustituirá el clásico, sino que lo complementará con capacidades antes imposibles. Aunque ya hay varias aplicaciones del internet cuántico, hay que señalar que la mayoría de las aplicaciones actuales que permite el internet clásico no estaban previstas cuando se desarrollaron las primeras versiones de internet. Por lo tanto, es razonable esperar que se produzca una evolución similar con el internet cuántico y que se descubran nuevas aplicaciones en las diferentes etapas de despliegue.

Criptografía cuántica

La seguridad de los esquemas criptográficos actuales que protegen la transmisión de datos financieros, sanitarios y gubernamentales se basa en la dificultad en resolver problemas matemáticos complejos. El más utilizado es el llamado protocolo criptográfico RSA (por el nombre de sus inventores, Rivest, Shamir y Adleman), cuya seguridad se basa en la dificultad práctica en factorizar números grandes. Peter Shor, profesor del MIT, descubrió un algoritmo de factorización cuántica eficiente que permitiría factorizar estos números. Así pues, la única razón por la cual el RSA sigue siendo un protocolo de encriptación viable hoy día es que el algoritmo de Peter Shor requiere un ordenador cuántico tolerante a fallos con el fin de poder funcionar; esta tecnología, aunque no está disponible en la actualidad, está evolucionando rápidamente y se espera que sea una realidad en las próximas décadas. Y, cuando lo haga, los algoritmos de clave asimétrica que se utilizan hoy en internet dejarán de ser seguros.

Una alternativa para contrarrestar ataques futuros es crear algoritmos y protocolos que requieran la solución de problemas que no se pueden abordar fácilmente con ninguna tecnología computacional. Los algoritmos de criptografía postcuántica (PQC, por las siglas en inglés), concebidos para proporcionar seguridad computacional, no son, en principio, susceptibles de sufrir los ataques que actualmente se llevan a cabo con un ordenador cuántico. Se espera que los algoritmos de criptografía postcuántica puedan funcionar como una herramienta de software, con una posible aceleración de hardware. La complejidad computacional para los usuarios de confianza —es decir, los recursos necesarios para encriptar y desencriptar el mensaje con la clave— tendría que ser aceptable para la aplicación en cuestión.

A diferencia de los algoritmos que ofrecen seguridad computacional, la distribución de claves cuánticas puede proporcionar seguridad teórica de la información; es decir, una seguridad que no se base en la dificultad en resolver determinados problemas, sino que se demuestre mediante pruebas matemáticas sólidas basadas en principios fundamentales de la mecánica cuántica —por ejemplo, el principio de incertidumbre y el teorema de no clonación. Aunque pueden utilizar componentes diferentes, las numerosas variantes de la distribución de claves cuánticas se basan en el mismo esquema, que implica dos partes (A y B) que confían la una en la otra y quieren compartir una clave secreta que pueden utilizar para comunicaciones confidenciales futuras. La clave secreta se transmite enviando qbits fotónicos o entrelazamientos entre A y B mediante un canal cuántico (por ejemplo, una fibra óptica) que los conecta. Si una persona que escucha clandestinamente (C) ataca el canal cuántico, sus parámetros se alterarán invariablemente. A y B pueden cuantificar esta alteración, cosa que puede garantizar que la clave secreta final se genere a partir de una información desconocida para la tercera persona (C). [2]

La seguridad perfecta es intrínsecamente imposible en escenarios realistas, pero podemos diseñar sistemas que, si se implantan correctamente, tengan una probabilidad de fallar ante un posible ataque que se limite a un valor muy pequeño, ϵ (del orden de 10-10 o menos), incluso utilizando futuros ordenadores cuánticos de gran potencia. Para algunos esquemas criptográficos, como la distribución de claves cuánticas, el valor ϵ es fácil de calcular en determinadas condiciones; en cambio, para los sistemas que se basan en la seguridad computacional, el progreso matemático podría, en el peor de los casos, destruir la seguridad en cualquier momento y, por lo tanto, la probabilidad de fallo no es fácil de calcular. Además, la probabilidad de éxito de un ataque desde el punto de vista computacional aumenta con el tiempo, a medida que los avances tecnológicos ponen más recursos a disposición del atacante. Eso genera una situación inaceptable en aplicaciones que necesitan seguridad a largo plazo. Los flujos de información especialmente sensible podrían ser objeto de intentos de “almacenar ahora y atacar después”, en los cuales los intrusos capturan información encriptada en determinados momentos con la esperanza de desencriptarla en el futuro, cuando dispongan de recursos computacionales o algoritmos más potentes..

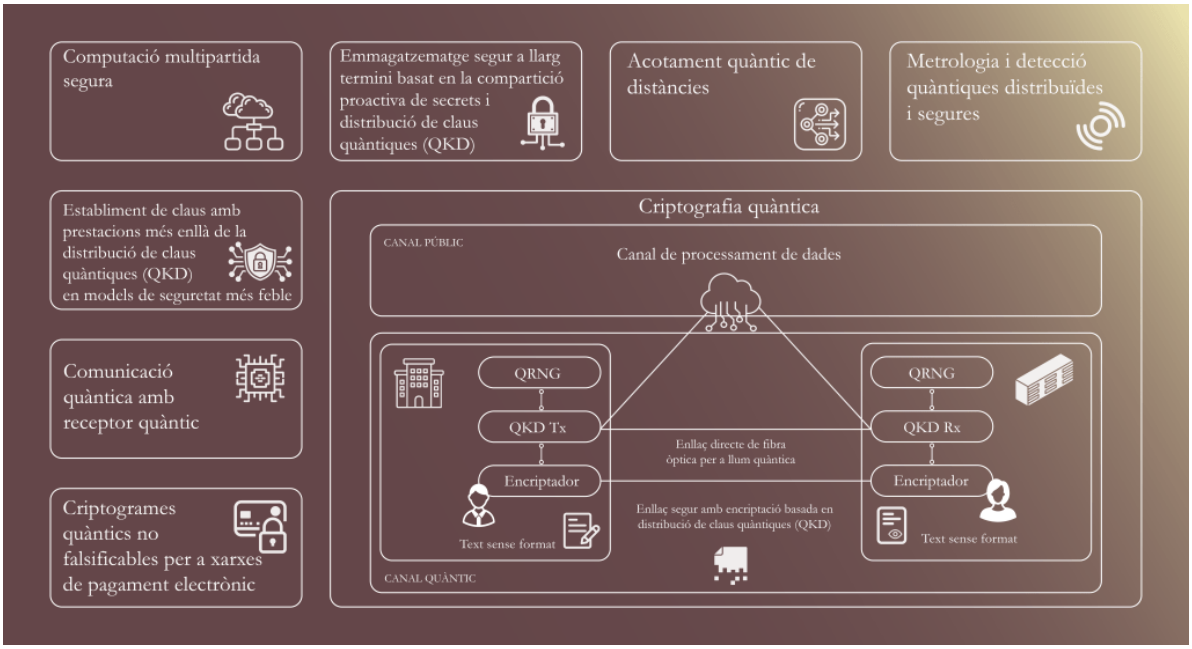


Figura 1. Criptografía cuántica: se puede conseguir una comunicación ultrasegura mediante la distribución de claves cuánticas y la encriptación, mientras que una gama adicional de aplicaciones, como el cálculo seguro multipartito, el almacenaje seguro a largo plazo y la detección distribuida segura se pueden implantar con ventaja cuántica en la red.

La criptografía cuántica es un ámbito muy interesante de investigación, con aplicaciones que van más allá de la distribución de claves cuánticas; por ejemplo, el cálculo seguro multipartito, el almacenaje seguro a largo plazo (LTSS, por las siglas en inglés) basado en el intercambio proactivo y la distribución de claves cuánticas, y también la metrología y la detección cuánticas. A pesar de que menos maduras que la distribución de claves cuánticas, estas aplicaciones tienen el potencial de alcanzar ventajas cuánticas en las redes básicas.

Memorias y repetidores cuánticos

La comunicación cuántica se suele alcanzar enviando fotones a través de fibras ópticas a largas distancias. Sin embargo, las fibras ópticas sufren una atenuación que aumenta exponencialmente con la distancia. Aunque la fibra óptica estándar es uno de los materiales más transparentes que hay, las pérdidas se vuelven muy significativas al cabo de unas decenas de kilómetros. Por ejemplo, sólo el 1% de la luz se transmite al cabo de 1.000 kilómetros. En la comunicación clásica, esta pérdida se compensa colocando dispositivos amplificadores de luz cada 50 o 100 kilómetros a lo largo de la red de fibra instalada. Estos amplificadores son los que hacen posible internet tal como hoy lo conocemos, al permitir que la luz se transmita a través de fibras ópticas a distancias globales. Ahora bien, el uso de estos amplificadores no es posible en la comunicación cuántica, porque los qbits no se pueden copiar sin añadir ruido al canal cuántico y no hacer imposible la comunicación. Eso, en la práctica, limita las comunicaciones cuánticas a través de fibra óptica a unos centenares de kilómetros como máximo.

Hay dos soluciones a este problema. La primera es enviar qbits fotónicos por el espacio

libre mediante satélites; este método ha demostrado la posibilidad de llevar a cabo la comunicación cuántica además de 1.000 kilómetros de distancia. Si, al contrario, queremos quedarnos en el suelo y utilizar fibra óptica, se ha propuesto el uso de repetidores cuánticos que utilizan el entrelazamiento como recurso principal. La idea básica que hay detrás del repetidor cuántico es dividir la distancia total en varios enlaces elementales, generar entrelazamiento de manera independiente entre los nodos cuánticos de cada enlace y, a continuación, extender el entrelazamiento a nodos cada vez más distantes mediante una técnica denominada intercambio de entrelazamiento (ved la figura 2). Una vez distribuido el entrelazamiento entre nodos distantes, se puede utilizar para varias tareas, como la distribución de claves cuánticas mediante estados entrelazados o la transmisión de un qbit con una técnica denominada teleportación cuántica.

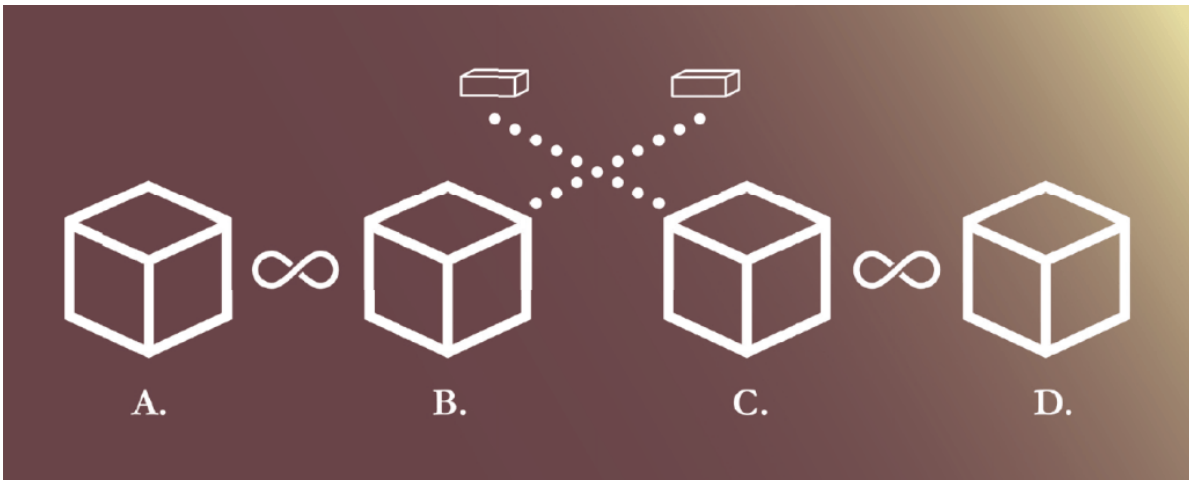


Figura 2. Arquitectura del repetidor cuántico. La distancia total se divide en diferentes enlaces. El entrelazamiento se distribuye de manera independiente en cada enlace y se almacena en memorias cuánticas. Una vez los enlaces adyacentes están entrelazados, la distancia aumenta por medio del intercambio de entrelazamiento.

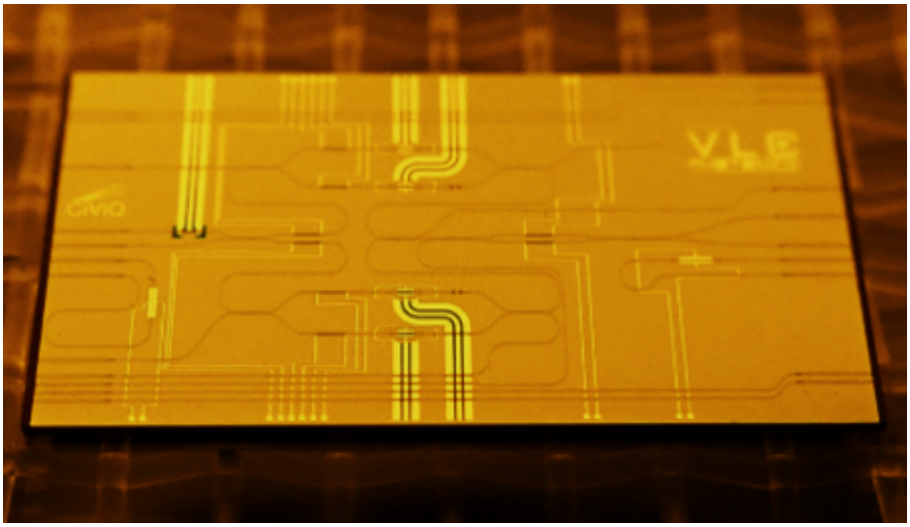
Un componente clave de los repetidores cuánticos es un dispositivo que permite almacenar el entrelazamiento en un enlace hasta que los otros enlaces estén preparados: es lo que se conoce como memoria cuántica. [3] El almacenaje del entrelazamiento permite que los diferentes enlaces elementales se entrelacen de manera independiente (es decir, no tienen que funcionar simultáneamente), lo cual posibilita la distribución del entrelazamiento a un ritmo que no disminuye exponencialmente con la distancia. En general, la implantación de una memoria cuántica por luz requiere una interacción coherente y fuerte entre fotones y algún tipo de sistema atómico que permita almacenar información cuántica en coherencias atómicas de larga duración. Actualmente, se están explorando varios sistemas físicos, como los gases atómicos fríos y los sistemas de estado sólido basados en cristales dopados con tierras raras. Aunque en la última década se han hecho avances importantes, la construcción de una memoria cuántica eficiente, duradera y de alta fidelidad, capaz de soportar un nivel alto de multiplexación que permita una tasa elevada de entrelazamiento, sigue siendo un reto experimental pendiente y un campo de investigación activo. Más allá de los dispositivos de memoria cuántica, otro reto para los repetidores cuánticos es desarrollar fuentes adecuadas de entrelazamiento fotónico para interactuar con las memorias cuánticas, es decir, que emitan fotones capaces de interactuar eficazmente con el

sistema de memoria atómica.

La construcción de un repetidor cuántico funcional que pueda transmitir entrelazamiento cuántico a distancias superiores con la transmisión directa es un reto experimental y técnico formidable, que implicará la generación eficiente de entrelazamiento de alta fidelidad entre sistemas materiales remotos, cosa que, a su vez, requerirá nodos cuánticos de alto rendimiento, que combinen memoria cuántica y fuente de entrelazamiento. Además, la tecnología utilizada tiene que ser robusta y capaz de funcionar fuera de un entorno de laboratorio controlado. Todos estos retos se están abordando actualmente bajo los auspicios de un importante programa europeo, la Quantum Internet Alliance, y se espera que en los próximos años se hagan avances significativos.

Miniaturización e integración mediante circuitos fotónicos integrados

Como pasa con cualquier nueva tecnología, con el fin de que internet y las redes cuánticas tengan un impacto industrial y social es obligatorio alcanzar un alto nivel de miniaturización e integración. La integración permite reducir las dimensiones de los dispositivos y los sistemas que proporcionan las funcionalidades requeridas, disminuye el consumo de energía y hace posible la producción de grandes volúmenes de hardware a bajo coste. Para simplificar, se pueden definir dos niveles diferentes de integración: en primer lugar, el nivel tecnológico, el objetivo del cual es miniaturizar los subsistemas de comunicación cuántica en una combinación de circuitos fotónicos y electrónicos integrados; y, en segundo lugar, el nivel de red, que implica la integración de la comunicación cuántica en la infraestructura clásica, como también el software de gestión, el despliegue a gran escala y la capacidad de actualización de internet y las redes cuánticas.



Circuito fotónico integrado para la distribución de claves cuánticas desarrollado a través del proyecto CiViQ.

Con respecto a la integración de tecnologías, como los chips electrónicos que manipulan

spins electrónicos, los circuitos fotónicos integrados permiten la miniaturización gracias al hecho que los fotones, portadores primarios de las señales, son guiados y procesados en pequeñas dimensiones. Los circuitos fotónicos integrados también permiten alcanzar un rendimiento sin precedentes en aplicaciones cuánticas como, por ejemplo, la generación cuántica de números aleatorios, [4] las fuentes de entrelazamiento, las memorias cuánticas y la computación, para citar sólo algunas. De hecho, en las tecnologías de la información y la comunicación que utilizan fotones siempre hay una interconexión optoelectrónica que permite convertir las señales eléctricas en homólogos fotónicos y viceversa. Eso significa que hacen falta placas de circuitos electrónicos para llevar a cabo la conducción y la lectura de los circuitos fotónicos integrados. El hardware de las redes cuánticas y de internet incluirá circuitos fotónicos integrados y placas de circuitos electrónicos, y la integración optoelectrónica tendrá un papel esencial. El hardware, pues, requiere una interfaz de software que permita al usuario final utilizarlo en aplicaciones. [5]

Con respecto a la integración de las redes, con el fin de facilitar el despliegue a gran escala, la tecnología de las redes cuánticas tiene que ser compatible con la infraestructura de fibra existente. [6] Un requisito importante es que los fotones utilizados para transmitir la información cuántica tienen que estar en la longitud de onda de las telecomunicaciones, para minimizar las pérdidas y permitir el uso de las fibras ópticas estándar ya instaladas. Para facilitar el despliegue de los nodos sobre el terreno, en centros de datos, por ejemplo, la tecnología utilizada tiene que ser compacta, robusta y fiable, y tiene que funcionar de manera automatizada, con una intervención humana mínima. Hasta ahora sólo se han llevado a cabo demostraciones de prueba del concepto en un entorno controlado de laboratorio, y hace falta un desarrollo importante para construir nodos desplegables. Finalmente, las redes cuánticas necesitarán una interfaz de software específica que haga que los diferentes componentes funcionen conjuntamente y permita a los usuarios utilizar la red de una manera sencilla, sin conocer los detalles de la plataforma física utilizada. Es lo que se denomina pila de red cuántica. Hay una interfaz similar para acceder al internet clásico, sin embargo, como el internet cuántico funciona de una manera radicalmente diferente, hará falta una pila de red específica, que se está desarrollando actualmente.

Nodo Barcelona – Q-Network

La Comisión Europea y la Agencia Espacial Europea promueven y dan apoyo al desarrollo del EuroQCI, una red paneuropea de comunicación cuántica formada tanto por elementos terrestres (fibra) como espaciales (satélite). En su fase inicial, el EuroQCI se centra sobre todo en el desarrollo de nodos metropolitanos en las principales ciudades europeas como Barcelona; en la segunda fase, estos nodos cuánticos metropolitanos se conectarán entre sí.

Con el apoyo de proyectos financiados por la Generalitat de Catalunya (SmartCAT, Qollserola, Qsunset, Qinfinity, Complementarias en comunicación cuántica), el Ministerio de Ciencia e Innovación español (Q-networks i Complementarias en comunicación cuántica) y la Comisión Europea (EuroQCI, QSNP, QIA), se han ideado varias arquitecturas de red cuántica para demostrar casos de uso de interés. A modo de ejemplo, la figura 3 muestra una demostración reciente de una videollamada segura, basada en distribución de claves

cuánticas y criptografía cuántica, entre dos lugares (CTTI e ICFO) situados en el sur del nodo de Barcelona.

Figura 3. Demostración en el nodo de Barcelona de transmisión de la distribución de claves cuánticas (QKD) y videollamada segura entre el CTTI I el ICFO utilizando tecnología de base europea: el sistema QKD de variable continua del ICFO, tecnología desarrollada en parte bajo CiViQ y ahora transferida y producida por la nueva empresa derivada Luxquanta y el QRNG de Quside.

Con respecto a la tecnología, se utilizarán recursos tanto de superposición como de entrelazamiento. Eso incluirá nuevos dispositivos y sistemas para transmisores, receptores, memorias y repetidores cuánticos desarrollados en institutos de investigación de Catalunya, como también otros recursos homólogos producidos por empresas locales (por ejemplo, Quside y Luxquanta) y empresas europeas con un grado de preparación tecnológica más elevado. Desde el punto de vista de la arquitectura de red, el nodo Barcelona – Q-network se desarrollará en torno a la torre de Collserola, que es un emplazamiento ideal para captar señales cuánticas por satélite, transmitir y recibir comunicaciones en el espacio libre y conectarse a la red central de fibra terrestre del área metropolitana. Con aportaciones decisivas de Cellnex y otras empresas, se utilizarán tecnologías y redes cuánticas para demostrar usos en los sectores financiero, sanitarios, de transportes y gubernamentales, para citar sólo algunos: en un futuro próximo se producirá la transferencia segura entre dos sucursales bancarias, por ejemplo, o la transmisión de datos sanitarias entre clínicas y hospitales públicos. La red también se utilizará para probar tecnologías cuánticas para la próxima generación de redes cuánticas de fibra por medio de repetidores cuánticos y, más adelante, para implantar conexiones entre sensores u ordenadores cuánticos.

REFERENCIAS Y NOTAS

1 — S. Wehner, S., Elkouss, D., Hanson, R. (2018). Science 362, 6412.
2 — Bennett, C. H., G. Brassard, G., Ekert, A. K. (1992). Scientific American 267, 50–57.
3 — Afzelius, M., Gisin, N., de Riedmatten, H. (2015). Physics Today 68 (12), 42.

4 — Abellan, C., Amaya, W., Domenech, D., Muñoz, P. Capmany, J., Longhi, S., M. W. Mitchell, M. W., Pruneri, V. (2016). *Optica* 9, 989.
5 — Aldama, J., Sarmiento, S. López Grande, I. H., Signorini,, S., Trigo Vidarte, L., Pruneri, V. & Light, J. (2022) *Technol* 40, 7498.
6 — Lago-Rivera, D., Grandi, S., Rakonjac, J.V., Seri, A., de Riedmatten, H. (2021). Nature 594, 37.

Hugues de Riedmatten

Hugues de Riedmatten es profesor ICREA y jefe del grupo de Fotónica Cuántica del ICFO desde el año 2010. La investigación de su grupo se centra en la construcción de hardware experimental para las redes cuánticas y los repetidores cuánticos, incluyendo memorias cuánticas para la luz, fuentes de luz cuántica, nodos de redes cuánticas y conversión cuántica de frecuencias. Doctorado por la Universidad de Ginebra en 2003, es miembro del equipo ejecutivo de la European Quantum Internet Alliance. Ha contribuido a alcanzar metas clave en la tecnología de repetidores cuánticos, como las primeras demostraciones de teletransportación cuántica a larga distancia y enlaces de repetidores cuánticos utilizando átomos fríos y memorias cuánticas de estado sólido.

Valerio Pruneri

Valerio Pruneri es profesor ICREA, presidente de la empresa tecnológica especializada en materiales Corning Inc. y jefe de grupo en el Instituto de Ciencias Fotónicas (ICFO). Tiene más de sesenta familias de patentes concedidas o pendientes, y ha realizado un centenar de conferencias como ponente en el campo de la fotónica y las tecnologías cuánticas. Doctorado en 1996 por la Universidad de Southampton, actualmente coordina la Asociación de Redes Cuánticas Seguras (QSNP) del programa Quantum Flagship de la Comisión Europea. También es coordinador del proyecto EuroQCI España de la Infraestructura Europea de Comunicación Cuántica. Ha desarrollado tecnologías para la generación cuántica de números aleatorios y la distribución de claves cuánticas, comercializadas actualmente por Quside y Luxquanta, respectivamente.