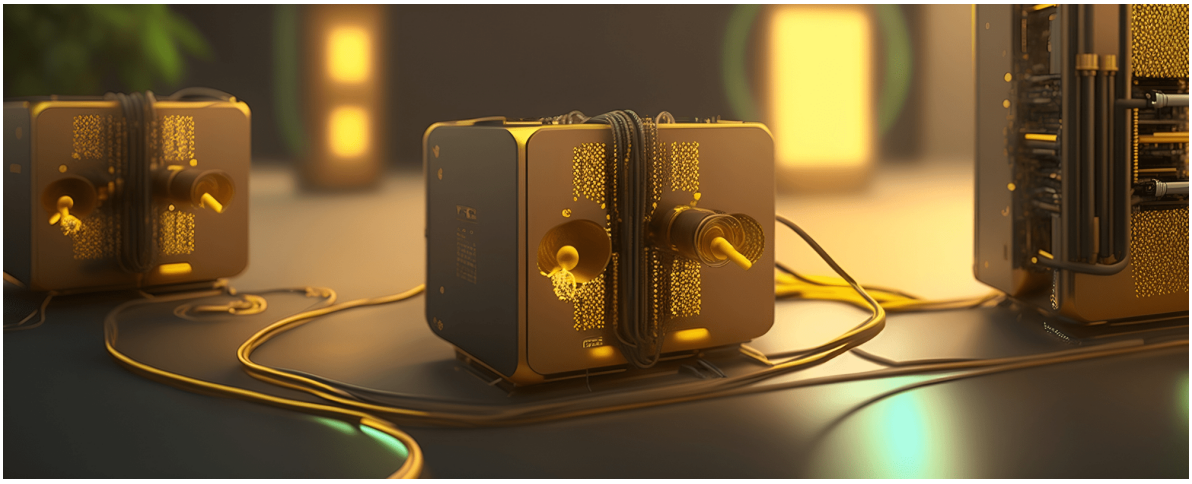
RECERCA I APLICACIONS PRÀCTIQUES

# Les xarxes quàntiques i internet

Hugues de Riedmatten, Valerio Pruneri



Cables quàntics i prototip de miniordinador quàntic. Conceptualització: Luisa Quiroga

La comunicació és un element essencial de la nostra societat. Tots ens comuniquem entre nosaltres enviant informació en forma de senyals que es poden detectar i generar fàcilment. Per exemple, la major part del trànsit de dades que sustenta avui internet viatja per fibres òptiques en forma de dígits binaris (bits), en seqüències de zeros i uns, conegudes com a cadenes de bits. Aquestes cadenes estan formades per impulsos de fotons —partícules elementals de llum— les propietats dels quals es poden descriure per mitjà de la teoria de la física clàssica. Els fotons són portadors ideals, ja que es poden manipular fàcilment i són immunes a les interferències ambientals.

Quan un sol fotó està contingut en un impuls, es converteix en un bit quàntic (qbit), una superposició d'estats quàntics 0 i 1, el comportament dels quals es descriu a partir de la teoria de la mecànica quàntica. Una propietat fonamental dels qbits és que no es poden mesurar sense alterar-los, ni tampoc es poden clonar (copiar). Dos o més qbits també poden formar un estat entrellaçat; un conjunt de partícules fortament correlacionades que s'influeixen mútuament fins i tot a distància.

La superposició i l'entrellaçament són dues propietats quàntiques fonamentals de les tecnologies quàntiques, com és el cas de la comunicació quàntica —és a dir, la generació, la transmissió i la detecció de qbits—. De manera similar a la comunicació moderna actual, es poden desenvolupar xarxes quàntiques en què els dispositius i els sistemes siguin quàntics. I el que és més important: en la majoria dels casos es poden compartir les mateixes infraestructures de fibra i satèl·lit per les quals viatgen actualment els bits clàssics, fet que farà possible l'existència d'internet i xarxes quàntiques globals en el futur.

Primer avantprojecte de la futura xarxa de comunicació quàntica segura.

L'internet i les xarxes quàntiques ofereixen un nombre significatiu de funcionalitats i serveis únics que no són possibles en la comunicació clàssica [1]. La criptografia quàntica, que descriurem detalladament més endavant, és probablement la més avançada d'aquestes funcionalitats, i consisteix a distribuir claus secretes fetes de qbits (claus quàntiques), que després s'utilitzen per encriptar i desencriptar missatges entres dues parts que es comuniquen. A la pràctica, la criptografia quàntica combina la distribució de claus quàntiques (QKD, per les sigles en anglès) i els protocols de criptografia clàssica per arribar a una comunicació segura impossible de piratejar, fins i tot amb recursos computacionals il·limitats (per exemple, ordinadors quàntics) i algoritmes potents. El juny de 2019, els 27 estats membres de la Unió Europea van acordar construir la Infraestructura Europea de Comunicació Quàntica (EuroQCI), una infraestructura de comunicació quàntica segura que abastarà tota la UE, inclosos els territoris d'ultramar. En l'últim apartat d'aquest article, presentarem el pla inicial per desplegar l'EuroQCI a l'àrea metropolitana de Barcelona.

La distància màxima de la comunicació quàntica en les fibres òptiques es limita a uns pocs centenars de quilòmetres, a causa de les pèrdues de la fibra òptica i també pel fet que els bits quàntics no es poden amplificar sense afegir un soroll que impediria una comunicació fidel. Les xarxes quàntiques ofereixen una solució a aquest problema mitjançant la implantació de repetidors quàntics que combinen la distribució de l'entrellaçament i un dispositiu anomenat memòria quàntica, que permet emmagatzemar l'entrellaçament en un sistema material. La implantació de repetidors quàntics permetrà enllaços completament quàntics a distàncies continentals. Tanmateix, caldrà superar moltes dificultats tècniques abans de poder implantar un repetidor quàntic complet.

A més de la distribució de claus quàntiques (QKD), també s'han proposat diverses aplicacions futures que podrien utilitzar la distribució de l'entrellaçament quàntic, sobretot en els camps de la computació i la metrologia quàntiques. Pel que fa a la computació, els

primers ordinadors quàntics seran probablement grans màquines ubicades en laboratoris específics, semblants als superordinadors actuals. L'internet quàntic permetrà a usuaris distants connectar-se a aquests ordinadors quàntics al núvol d'una manera segura i confidencial, de manera que ningú —ni tan sols el mateix ordinador quàntic— sabrà quin càlcul s'està duent a terme. Una altra potent aplicació futurista serà reunir ordinadors quàntics. Atès que cada ordinador quàntic té un nombre limitat de qbits, el fet de connectar-los mitjançant enllaços fotònics permetrà accedir a un nombre molt més gran de qbits i, per tant, augmentar considerablement la potència de càlcul. A més de les aplicacions de computació, les futures xarxes quàntiques també tindran aplicacions en metrologia quàntica. Per exemple, s'ha demostrat que les xarxes de rellotges òptics entrellaçats permetrien una sincronització més precisa. Igualment, s'ha constatat que la construcció de conjunts de telescopis que compartissin estats entrellaçats podria elevar-ne la línia de base i augmentar-ne la sensibilitat, fet que donaria lloc a aplicacions en astronomia.

> La criptografia quàntica permetrà arribar a una comunicació segura impossible de piratejar, fins i tot amb recursos computacionals il·limitats i algoritmes potents

Les funcionalitats de l'internet quàntic són fonamentalment diferents de l'internet clàssic, per la qual cosa tots dos tipus de xarxa són complementaris. L'internet quàntic no substituirà el clàssic, sinó que el complementarà amb capacitats abans impossibles. Tot i que ja hi ha diverses aplicacions de l'internet quàntic, cal assenyalar que la majoria de les aplicacions actuals que permet l'internet clàssic no estaven previstes quan es van desenvolupar les primeres versions d'internet. Per tant, és raonable esperar que es produeixi una evolució similar amb l'internet quàntic i que es descobreixin noves aplicacions en les diferents etapes de desplegament.

## Criptografia quàntica

La seguretat dels esquemes criptogràfics actuals que protegeixen la transmissió de dades financeres, sanitàries i governamentals es basa en la dificultat de resoldre problemes matemàtics complexos. El més utilitzat és l'anomenat protocol criptogràfic RSA (pel nom dels seus inventors, Rivest, Shamir i Adleman), la seguretat del qual es basa en la dificultat pràctica de factoritzar nombres grans. Peter Shor, professor del MIT, va descobrir un algoritme de factorització quàntica eficient que permetria factoritzar aquests nombres. Així doncs, l'única raó per la qual l'RSA continua sent un protocol d'encriptació viable avui dia és que l'algoritme de Peter Shor requereix un ordinador quàntic tolerant a fallades per tal de poder funcionar; aquesta tecnologia, tot i que no està disponible en l'actualitat, està evolucionant ràpidament i s'espera que sigui una realitat en les pròximes dècades. I, quan ho faci, els algoritmes de clau asimètrica que s'utilitzen avui a internet deixaran de ser segurs.

Una alternativa per contrarestar atacs futurs és crear algoritmes i protocols que requereixin la solució de problemes que no es poden abordar fàcilment amb cap tecnologia computacional. Els algoritmes de criptografia postquàntica (PQC, per les sigles en anglès), concebuts per proporcionar seguretat computacional, no són, en principi, susceptibles de patir els atacs que actualment es duen a terme amb un ordinador quàntic. S'espera que els algoritmes de criptografia postquàntica puguin funcionar com una eina de programari, amb una possible acceleració de maquinari. La complexitat computacional per als usuaris de confiança —és a dir, els recursos necessaris per encriptar i desencriptar el missatge amb la clau— hauria de ser acceptable per a l'aplicació en qüestió.

A diferència dels algoritmes que ofereixen seguretat computacional, la distribució de claus quàntiques pot proporcionar seguretat teòrica de la informació; és a dir, una seguretat que no es basi en la dificultat de resoldre determinats problemes, sinó que es demostri mitjançant proves matemàtiques sòlides basades en principis fonamentals de la mecànica quàntica —per exemple, el principi d'incertesa i el teorema de no clonació—. Tot i que poden utilitzar components diferents, les nombroses variants de la distribució de claus quàntiques es basen en el mateix esquema, que implica dues parts (A i B) que confien l'una en l'altra i volen compartir una clau secreta que poden utilitzar per a comunicacions confidencials futures. La clau secreta es transmet enviant qbits fotònics o entrellaçaments entre A i B mitjançant un canal quàntic (per exemple, una fibra òptica) que els connecta. Si una persona que escolta clandestinament (C) ataca el canal quàntic, els seus paràmetres s'alteraran invariablement. A i B poden quantificar aquesta alteració, cosa que pot garantir que la clau secreta final es generi a partir d'una informació desconeguda per a la tercera persona (C) [2].

La seguretat perfecta és intrínsecament impossible en escenaris realistes, però podem dissenyar sistemes que, si s'implanten correctament, tinguin una probabilitat de fallar davant d'un possible atac que es limiti a un valor molt petit, $\epsilon$ (de l'ordre de 10-10 o menys), fins i tot utilitzant futurs ordinadors quàntics de gran potència. Per a alguns esquemes criptogràfics, com ara la distribució de claus quàntiques, el valor $\epsilon$ és fàcil de calcular en determinades condicions; en canvi, per als sistemes que es basen en la seguretat computacional, el progrés matemàtic podria, en el pitjor dels casos, destruir la seguretat en qualsevol moment i, per tant, la probabilitat de fallada no és fàcil de calcular. A més, la probabilitat d'èxit d'un atac des del punt de vista computacional augmenta amb el temps, a mesura que els avenços tecnològics posen més recursos a disposició de l'atacant. Això genera una situació inacceptable en aplicacions que necessiten seguretat a llarg termini. Els fluxos d'informació especialment sensible podrien ser objecte d'intents d'"emmagatzemar ara i atacar després", en els quals els intrusos capturen informació encriptada en determinats moments amb l'esperança de desencriptar-la en el futur, quan disposin de recursos computacionals o algoritmes més potents.

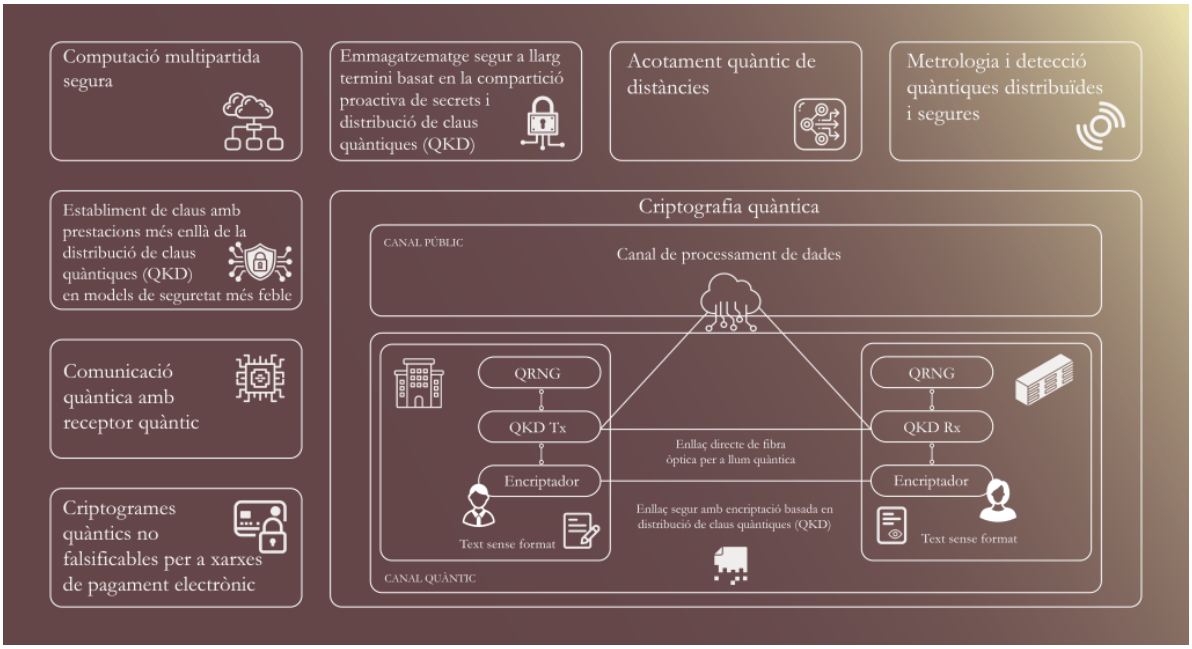



Figura 1. Criptografia quàntica: es pot aconseguir una comunicació ultrasegura mitjançant la distribució de claus quàntica i l'encriptació, mentre que una gamma addicional d'aplicacions, com el càlcul segur multipartit, l'emmagatzematge segur a llarg termini i la detecció distribuïda segura es poden implantar amb avantatge quàntic a la xarxa.

La criptografia quàntica és un àmbit molt interessant de recerca, amb aplicacions que van més enllà de la distribució de claus quàntiques; per exemple, el càlcul segur multipartit, l'emmagatzematge segur a llarg termini (LTSS, per les sigles en anglès) basat en l'intercanvi proactiu i la distribució de claus quàntiques, i també la metrologia i la detecció quàntiques. Tot i que menys madures que la distribució de claus quàntiques, aquestes aplicacions tenen el potencial d'assolir avantatges quàntics en les xarxes bàsiques.

## Memòries i repetidors quàntics

La comunicació quàntica se sol assolir enviant fotons a través de fibres òptiques a llargues distàncies. Tanmateix, les fibres òptiques pateixen una atenuació que augmenta exponencialment amb la distància. Tot i que la fibra òptica estàndard és un dels materials més transparents que hi ha, les pèrdues es tornen molt significatives al cap d'unes desenes de quilòmetres. Per exemple, només l'1% de la llum es transmet al cap de 1.000 quilòmetres. En la comunicació clàssica, aquesta pèrdua es compensa col·locant dispositius amplificadors de llum cada 50 o 100 quilòmetres al llarg de la xarxa de fibra instal·lada. Aquests amplificadors són els que fan possible internet tal com avui el coneixem, en permetre que la llum es transmeti a través de fibres òptiques a distàncies globals. Ara bé, l'ús d'aquests amplificadors no és possible en la comunicació quàntica, perquè els qbits no es poden copiar sense afegir soroll al canal quàntic i fer impossible la comunicació. Això, a la pràctica, limita les comunicacions quàntiques a través de fibra òptica a uns centenars de quilòmetres com a màxim.

Hi ha dues solucions a aquest problema. La primera és enviar qbits fotònics per l'espai

lliure mitjançant satèl·lits; aquest mètode ha demostrat la possibilitat de dur a terme la comunicació quàntica a més de 1.000 quilòmetres de distància. Si, al contrari, volem quedar-nos a terra i utilitzar fibra òptica, s'ha proposat l'ús de repetidors quàntics que utilitzen l'entrellaçament com a recurs principal. La idea bàsica que hi ha al darrere del repetidor quàntic és dividir la distància total en diversos enllaços elementals, generar entrellaçament de manera independent entre els nodes quàntics de cada enllaç i, a continuació, estendre l'entrellaçament a nodes cada cop més distants mitjançant una tècnica anomenada intercanvi d'entrellaçament (vegeu la figura 2). Un cop distribuït l'entrellaçament entre nodes distants, es pot utilitzar per a diverses tasques, com la distribució de claus quàntiques mitjançant estats entrellaçats o la transmissió d'un qbit amb una tècnica anomenada teleportació quàntica.

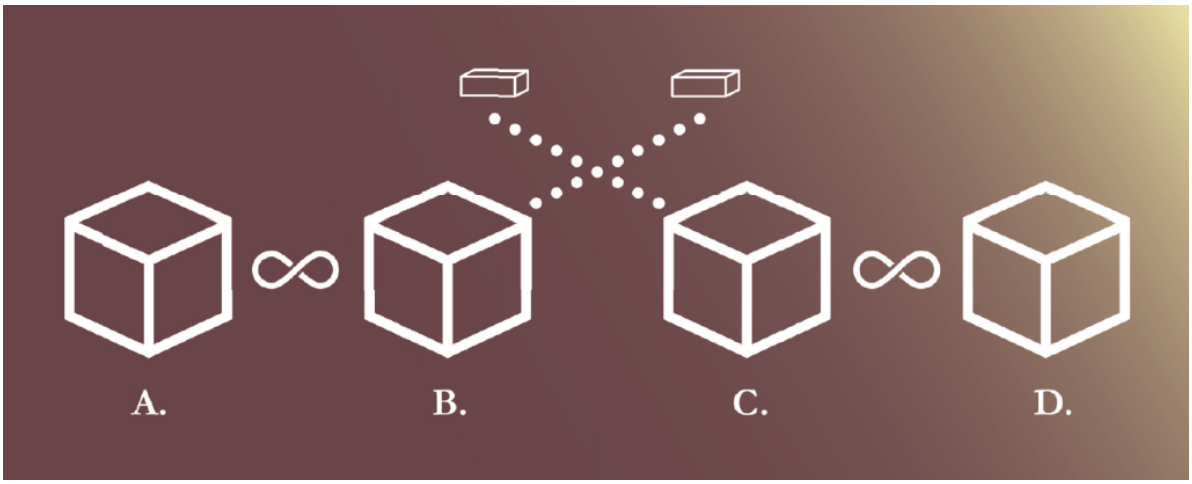


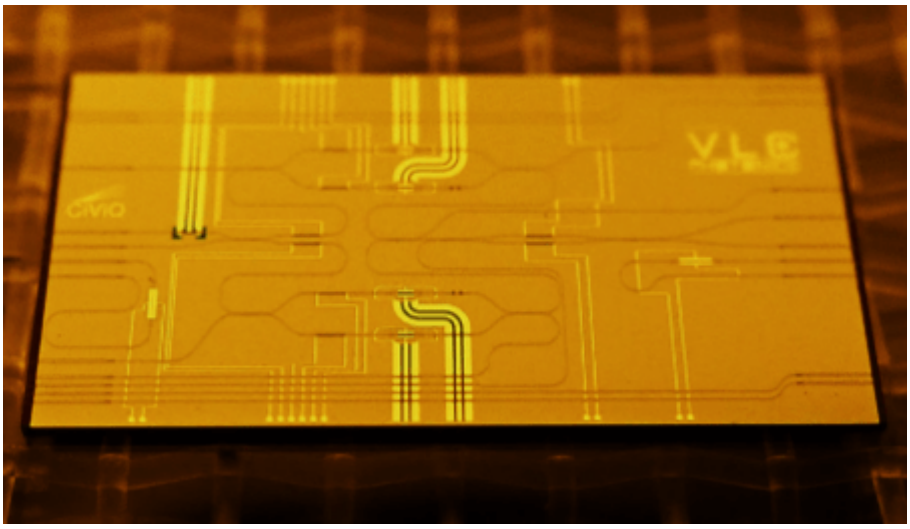

Figura 2. Arquitectura del repetidor quàntic. La distància total es divideix en diferents enllaços. L'entrellaçament es distribueix de manera independent en cada enllaç i s'emmagatzema en memòries quàntiques. Un cop els enllaços adjacents estan entrellaçats, la distància augmenta per mitjà de l'intercanvi d'entrellaçament.

Un component clau dels repetidors quàntics és un dispositiu que permet emmagatzemar l'entrellaçament en un enllaç fins que els altres enllaços estiguin preparats: és el que es coneix com a memòria quàntica [3]. L'emmagatzematge de l'entrellaçament permet que els diferents enllaços elementals s'entrellacin de manera independent (és a dir, no han de funcionar simultàniament), la qual cosa possibilita la distribució de l'entrellaçament a un ritme que no disminueix exponencialment amb la distància. En general, la implantació d'una memòria quàntica per llum requereix una interacció coherent i forta entre fotons i algun tipus de sistema atòmic que permeti emmagatzemar informació quàntica en coherències atòmiques de llarga durada. Actualment, s'estan explorant diversos sistemes físics, com els gasos atòmics freds i els sistemes d'estat sòlid basats en cristalls dopats amb terres rares. Tot i que en l'última dècada s'han fet avenços importants, la construcció d'una memòria quàntica eficient, duradora i d'alta fidelitat, capaç de suportar un nivell alt de multiplexació que permeti una taxa elevada d'entrellaçament, continua sent un repte experimental pendent i un camp de recerca actiu. Més enllà dels dispositius de memòria quàntica, un altre repte per als repetidors quàntics és desenvolupar fonts adequades d'entrellaçament fotònic per interactuar amb les memòries quàntiques, és a dir, que emetin fotons capaços d'interactuar eficaçment amb el sistema de memòria atòmica.

La construcció d'un repetidor quàntic funcional que pugui transmetre entrellaçament quàntic a distàncies superiors amb la transmissió directa és un repte experimental i tècnic formidable, que implicarà la generació eficient d'entrellaçament d'alta fidelitat entre sistemes materials remots, cosa que, al seu torn, requerirà nodes quàntics d'alt rendiment, que combinin memòria quàntica i font d'entrellaçament. A més, la tecnologia utilitzada ha de ser robusta i capaç de funcionar fora d'un entorn de laboratori controlat. Tots aquests reptes s'estan abordant actualment sota els auspicis d'un important programa europeu, la Quantum Internet Alliance, i s'espera que en els pròxims anys es facin avenços significatius.

## Miniaturització i integració mitjançant circuits fotònics integrats

Com passa amb qualsevol nova tecnologia, per tal que l'internet i les xarxes quàntiques tinguin un impacte industrial i social és obligatori assolir un alt nivell de miniaturització i integració. La integració permet reduir les dimensions dels dispositius i els sistemes que proporcionen les funcionalitats requerides, disminueix el consum d'energia i fa possible la producció de grans volums de maquinari a baix cost. Per simplificar, es poden definir dos nivells diferents d'integració: en primer lloc, el nivell tecnològic, l'objectiu del qual és miniaturitzar els subsistemes de comunicació quàntica en una combinació de circuits fotònics i electrònics integrats; i, en segon lloc, el nivell de xarxa, que implica la integració de la comunicació quàntica en la infraestructura clàssica, com també el programari de gestió, el desplegament a gran escala i la capacitat d'actualització de l'internet i les xarxes quàntiques.



Circuit fotònic integrat per a la distribució de claus quàntica desenvolupada a través del projecte CiViQ.

Pel que fa a la integració de tecnologies, com els xips electrònics que manipulen spins electrònics, els circuits fotònics integrats permeten la miniaturització gràcies al fet que els fotons, portadors primaris dels senyals, són guiats i processats en petites dimensions. Els

circuits fotònics integrats també permeten assolir un rendiment sense precedents en aplicacions quàntiques com, per exemple, la generació quàntica de nombres aleatoris [4], les fonts d'entrellaçament, les memòries quàntiques i la computació, per citar-ne només algunes. De fet, en les tecnologies de la informació i la comunicació que utilitzen fotons sempre hi ha una interconnexió optoelectrònica que permet convertir els senyals elèctrics en homòlegs fotònics i viceversa. Això significa que calen plaques de circuits electrònics per dur a terme la conducció i la lectura dels circuits fotònics integrats. El maquinari de les xarxes quàntiques i d'internet inclourà circuits fotònics integrats i plaques de circuits electrònics, i la integració optoelectrònica tindrà un paper essencial. El maquinari, doncs, requereix una interfície de programari que permeti a l'usuari final utilitzar-lo en aplicacions [5].

Pel que fa a la integració de les xarxes, per tal de facilitar el desplegament a gran escala, la tecnologia de les xarxes quàntiques ha de ser compatible amb la infraestructura de fibra existent [6]. Un requisit important és que els fotons utilitzats per transmetre la informació quàntica han d'estar en la longitud d'ona de les telecomunicacions, per minimitzar les pèrdues i permetre l'ús de les fibres òptiques estàndard ja instal·lades. Per facilitar el desplegament dels nodes sobre el terreny, en centres de dades, per exemple, la tecnologia utilitzada ha de ser compacta, robusta i fiable, i ha de funcionar de manera automatitzada, amb una intervenció humana mínima. Fins ara només s'han dut a terme demostracions de prova del concepte en un entorn controlat de laboratori, i cal un desenvolupament important per construir nodes desplegables. Finalment, les xarxes quàntiques necessitaran una interfície de programari específica que faci que els diferents components funcionin conjuntament i permeti als usuaris utilitzar la xarxa d'una manera senzilla, sense conèixer els detalls de la plataforma física utilitzada. És el que s'anomena pila de xarxa quàntica. Hi ha una interfície similar per accedir a l'internet clàssic, però, com que l'internet quàntic funciona d'una manera radicalment diferent, caldrà una pila de xarxa específica, que s'està desenvolupant actualment.

## Node Barcelona – Q-Network

La Comissió Europea i l'Agència Espacial Europea promouen i donen suport al desenvolupament de l'EuroQCI, una xarxa paneuropea de comunicació quàntica formada tant per elements terrestres (fibra) com espacials (satèl·lit). En la seva fase inicial, l'EuroQCI se centra sobretot en el desenvolupament de nodes metropolitans en les principals ciutats europees com Barcelona; en la segona fase, aquests nodes quàntics metropolitans es connectaran entre si.

Amb el suport de projectes finançats per la Generalitat de Catalunya (SmartCAT, Qollserola, Qsunset, Qinfinity, Complementarias en comunicació quàntica), el Ministeri de Ciència i Innovació espanyol (Q-networks i Complementarias en comunicació quàntica) i la Comissió Europea (EuroQCI, QSNP, QIA), s'han ideat diverses arquitectures de xarxa quàntica per demostrar casos d'ús d'interès. A tall d'exemple, la figura 3 mostra una demostració recent d'una videotrucada segura, basada en distribució de claus quàntiques i criptografia quàntica, entre dos llocs (CTTI i ICFO) situats al sud del node de Barcelona.


Figura 3. Demostració en el node de Barcelona de transmissió de la distribució de claus quàntica (QKD) i videotrucada segura entre el CTTI I l'ICFO utilitzant tecnologia de base europea: el sistema QKD de variable contínua de l'ICFO, tecnologia desenvolupada en part sota el projecte CiViQ i ara transferida i produïda per la nova empresa derivada Luxquanta i el QRNG de Quside.

Pel que fa a la tecnologia, s'utilitzaran recursos tant de superposició com d'entrellaçament. Això inclourà nous dispositius i sistemes per a transmissors, receptors, memòries i repetidors quàntics desenvolupats en instituts de recerca de Catalunya, com també altres recursos homòlegs produïts per empreses locals (per exemple, Quside i Luxquanta) i empreses europees amb un grau de preparació tecnològica més elevat. Des del punt de vista de l'arquitectura de xarxa, el node Barcelona – Q-network es desenvoluparà entorn de la torre de Collserola, que és un emplaçament ideal per captar senyals quàntics per satèl·lit, transmetre i rebre comunicacions en l'espai lliure i connectar-se a la xarxa central de fibra terrestre de l'àrea metropolitana. Amb aportacions decisives de Cellnex i altres empreses, s'utilitzaran tecnologies i xarxes quàntiques per demostrar usos en els sectors financer, sanitari, de transports i governamental, per citar-ne només alguns: en un futur pròxim es produirà la transferència segura entre dues sucursals bancàries, per exemple, o la transmissió de dades sanitàries entre clíniques i hospitals públics. La xarxa també es farà servir per provar tecnologies quàntiques per a la propera generació de xarxes quàntiques de fibra per mitjà de repetidors quàntics i, més endavant, per implantar connexions entre sensors o ordinadors quàntics.

## REFERÈNCIES I NOTES

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 és professor ICREA i cap del grup de Fotònica Quàntica de l'ICFO des de l'any 2010. La investigació del seu grup se centra en la construcció de maquinari experimental per a les xarxes quàntiques i els repetidors quàntics, incloent-hi memòries quàntiques per a la llum, fonts de llum quàntica, nodes de xarxes quàntiques i conversió quàntica de freqüències. Doctorat per la Universitat de Ginebra l'any 2003, és membre de l'equip executiu de la European Quantum Internet Alliance. Ha contribuït a fer realitat fites clau en la tecnologia de repetidors quàntics, com les primeres demostracions de teletransportació quàntica allarga distància i enllaços de repetidors quàntics utilitzant àtoms freds i memòries quàntiques d'estat sòlid.

**Valerio Pruneri**

Valerio Pruneri és professor ICREA, president de l’empresa tecnològica especialitzada en materials Corning Inc. i cap de grup a l’Institut de Ciències Fotòniques (ICFO). Té més de seixanta famílies de patents concedides o pendents, i ha fet un centenar de conferències com a convidat en el camp de la fotònica i les tecnologies quàntiques. Doctorat el 1996 per la Universitat de Southampton, actualment coordina l’Associació de Xarxes Quàntiques Segures (QSNP) del programa Quantum Flagship de la Comissió Europea. També és coordinador del projecte EuroQCI Espanya de la Infraestructura Europea de Comunicació Quàntica. Ha desenvolupat tecnologies per a la generació quàntica de nombres aleatoris i la distribució de claus quàntiques, comercialitzades actualment per Quside i Luxquanta, respectivament.