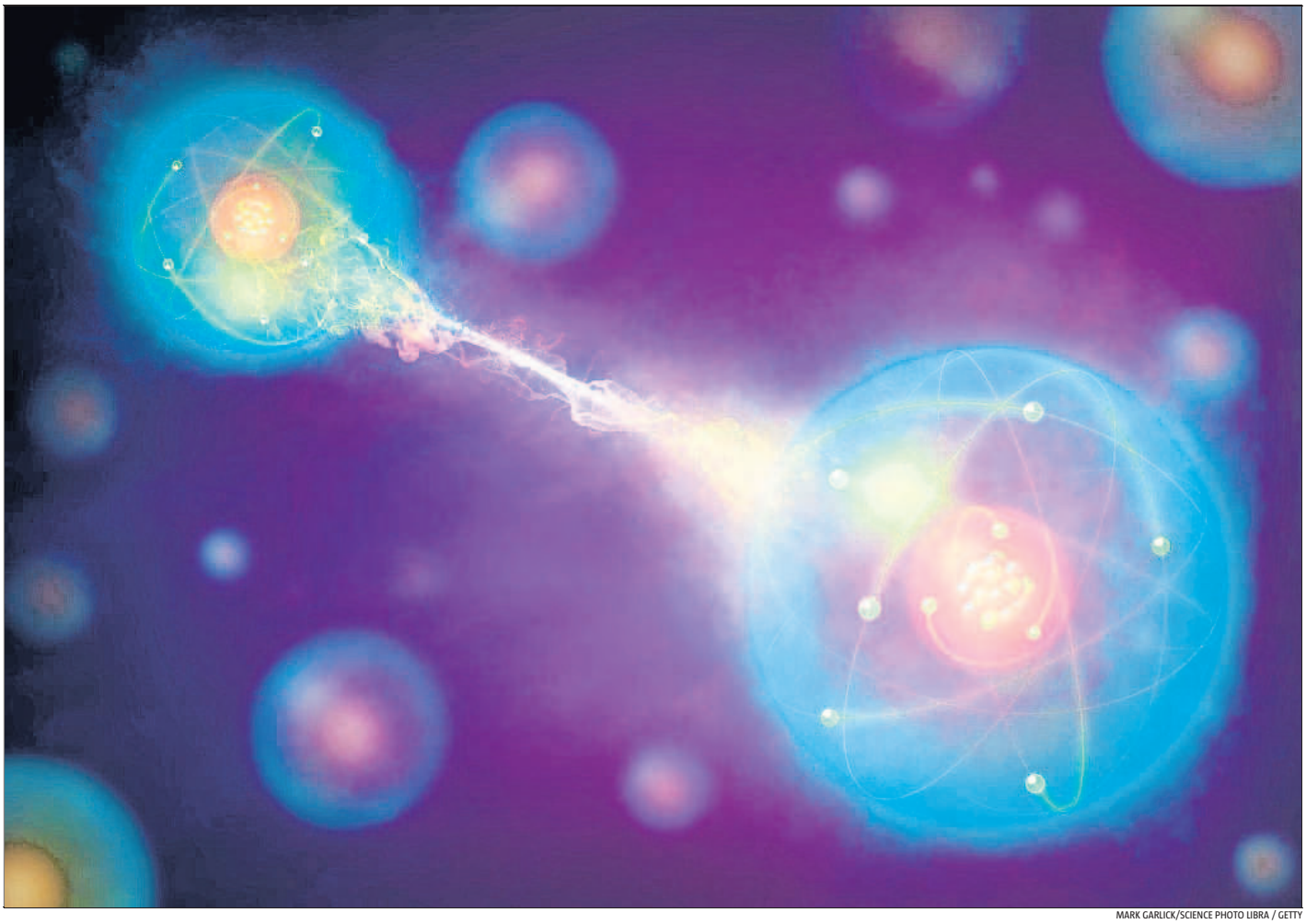
La tecnologia que ve



MARK GARLICK/SCIENCE PHOTO LIBRA / GETTY

Al món quàntic les partícules tenen comportaments radicalment diferents, que es poden aprofitar per crear tecnologies trencadores

La física quàntica canviarà les nostres vides

Promet comunicacions cent per cent segures, a prova de hackers

ELSA VELASCO
Barcelona

Internet envaeix el nostre entorn. Ordinadors, telèfons, rellotges. Durant les pròximes dècades, la interconnexió també arribarà a les nostres llars. Als vehicles. A la roba, fins i tot. Hi haurà cotxes que condueixin sols. Neveres intel·ligents que facin la compra per a nosaltres. Sensors en samarretes que monitorin la nostra salut contínuament. La nostra casa sabrà quan ha d'encendre i apagar la calefacció per mantenir-nos confortables o quan ha de trucar al metge si estem malalts.

Però totes les connexions comporten riscos. La informació és un tresor valuós i n'hi ha que s'especialitzen a robar-la, els hackers. Les empreses que gestionen dades inverteixen una gran quantitat d'esforços i recursos a blindar-los, en una cursa constant contra aquests pirates del segle XXI.

"Avui dia hi ha sistemes molt segurs que fan difícil espiar les comunicacions, però no impossible", declara Lluís Torner, director de l'Institut de Ciències Fotòniques (Icfo) a Castelldefels. Cap dada digital no és segura al 100%, ni missatges personals, ni historials mèdics, ni informació de defensa o de transaccions comercials. I a mesura que s'expandeixen les connexions, també creix el risc.

"Si la informació no és segura, és un desastre. No podrem utilitzar tota la tecnologia que ve", explica Carlos Abellán, cofundador i director executiu de l'empresa Quside.

Però, i si algú inventés una eina per transmetre la informació d'una manera totalment segura, a prova de qualsevol hacker? Aquesta és precisament la promesa de les comunicacions quàntiques, una tecnologia en desenvolupament que pot garantir la confidencialitat no pel blindatge de protocols i algoritmes, sinó per les mateixes lleis de la física.

Aquesta mena de comunicacions s'està desenvolupant en l'anomenada segona revolució quàntica. Després que durant la primera s'aprofitessin les lleis de la mecànica quàntica per desenvolupar noves tecnologies, ara s'aspira a utilitzar directament els elements quàntics, com els àtoms o els fotons, per anar més enllà, ja que el seu comportament és radicalment diferent del de la matèria a més escala.

Al món quàntic, per exemple, una partícula pot estar en dos estats simultàniament mentre ningú no l'observa, però, si algú la intenta detectar, es decantarà per un dels dos. És el que es coneix com a superposició quàntica. Seria com si tiréssim una moneda a l'aire amb els ulls tancats. Fins que no vegem quin resultat ha sortit, pot ser tant cara com creu, amb un 50% de probabilitat per a cada opció: la moneda tindria dos estats superposats. Així que mirem, sabrem si hem tret cara o creu, o sigui que la probabilitat canviarà.

Una altra propietat estranya és l'entrellaçament quàntic. Dues partícules poden estar vinculades de manera que comparteixen el mateix estat, malgrat que les separin quilòmetres de distància.

ELS FRUITS DE LA PRIMERA REVOLUCIÓ QUÀNTICA

Principi del segle XX
Comprendre les lleis de la mecànica quàntica va obrir la porta a noves tecnologies

Llum làser
De la impressió a les comunicacions, passant per la medicina, les seves aplicacions avui són ubiqües

Ressonància magnètica
Tècnica bàsica de diagnòstic mèdic que permet veure el cos per dins amb camps magnètics i ones de ràdio, sense utilitzar rajos X

Transistors
Peces essencials dels circuits dels dispositius electrònics, sense els quals no hi hauria ordinadors

La internet de Schrödinger

Superposats i entrellaçats
La física quàntica ha obert noves portes en computació: la superposició i l'entrellaçament es poden aplicar per crear ordinadors capaços de resoldre problemes que queden fora de l'abast de la computació convencional. Es tracta d'emmagatzemar bits no a les clàssiques plaques i discos durs, sinó en partícules quàntiques. En lloc de tenir dos estats excloents com els bits convencionals (0 i 1), els bits quàntics, o qubits, poden estar en dos estats superposats: 0 i 1 alhora, cosa que multiplica les possibilitats.

La limitació principal
Els ordinadors quàntics tenen un punt feble. "El nombre de bits quàntics és molt limitat perquè són molt difícils de controlar", assenyala Hugues de Riedmatten, de l'Icfo. El rècord actual en computació quàntica està als 50 qubits i, "de moment, no hi ha cap ordinador quàntic que hagi fet una feina millor que un de clàssic".

Xarxes d'ordinadors
Però hi ha una manera d'esquivar aquesta limitació: la internet quàntica. Els físics s'han proposat de desenvolupar una xarxa d'ordinadors quàntics connectada a través de l'entrellaçament dels seus qubits. Així, com que se sumen les capacitats de les diferents màquines, la potència total del sistema augmentarà exponencialment, segons De Riedmatten, que participa en el projecte QIA del Quantum Flagship per aconseguir aquest objectiu. La internet quàntica també pot ajudar a incrementar les distàncies de les comunicacions quàntiques i millorar-ne la seguretat.

Noves possibilitats
Però "el més important és que amb la computació quàntica es podran fer coses que un ordinador clàssic no pot fer", afirma De Riedmatten. Els ordinadors quàntics permetrien estudiar el comportament de la matèria a una escala avui impossible. Per exemple, un simulador quàntic podria servir per estudiar com les proteïnes es pleguen de diferents maneres, un procés clau en malalties com l'alzheimer o el parkinson; o ajudar a desenvolupar nous fàrmacs o materials amb propietats físiques inusuals i que avui dia no es comprenen del tot, com alguns tipus de superconductors. Segons De Riedmatten, és difícil predir quan la computació quàntica serà una realitat, però "serà un canvi de paradigma".

"Seria com si jo estigués a Castelldefels i tu aquí, a Barcelona, que tots dos tiréssim una moneda diferent a l'aire i sempre tinguéssim el mateix resultat. Si jo trec cara, tu també. I si em surt creu, a tu igual", il·lustra Hugues de Riedmatten, investigador Icrea a l'Icfo.

"La veritat és que no sabem per què l'univers es comporta així. Però ho podem aprofitar", afirma Carlos Abellán. Segons els experts, a mitjà termini el de les comunicacions serà el camp que més es beneficiï de les tecnologies quàntiques.

La ciberseguretat actual es basa a encriptar les dades a través de dos factors. En primer lloc, cal crear un pany que protegeixi la informació, en forma d'algoritme. El problema és que tots els algoritmes es construeixen seguint seqüències lògiques i, per tant, a través de la lògica es poden arribar a desenvolupar claus que obrin aquests panys amb relativa facilitat. Per evitar-ho, s'elaboren forrellats que es poden obrir només amb claus creades aleatòriament, és a dir, claus de nombres generats a l'atzar, de manera que per forçar-los ja no n'hi ha prou amb la lògica.

MÓN INTERCONNECTAT

La seguretat de les connexions és vital per poder utilitzar la tecnologia que ve

PROTECCIÓ BASADA EN ÀTOMS

Receptor i emissor sabran a l'acte si algú intenta interceptar el missatge

Però hi ha un segon problema: els receptors dels missatges encriptats han de poder desxifrar-los. Per això, també cal enviar les claus que permeten desencriptar-los. I, si algú intercepta aquesta clau sense deixar rastre, la seguretat s'esfuma.

Aquí és on entren les tecnologies quàntiques. L'objectiu és crear un canal de comunicació basat en bits quàntics per distribuir les claus. És a dir, partícules com àtoms o fotons que tenen dos estats superposats, que comparteixen a distància amb altres partícules, explica Valerio Pruneri, investigador Icrea a l'Icfo. Gràcies a l'entrellaçament i a la superposició dels bits quàntics, és possible enviar claus de manera que, si algú intenta aconseguir-les, tant el receptor com l'emissor del missatge s'adonin que els estan espiant. "Si algú intenta escoltar d'amagat, canvia l'estat dels bits quàntics i les dues parts ho saben", assenyala Pruneri. Així, quan descobreixen que els han robat la clau, poden interrompre la comunicació i generar un nou pany de seguretat.

Pruneri lidera el projecte CiViQ, amb l'objectiu de desenvolupar aquesta tecnologia perquè es pugui aplicar a gran escala. S'emmarca dins del programa europeu Quantum Flagship, que es va presentar al públic del Mobile World Congress, que va tenir lloc a Barcelona entre el 25 i el 28 de febrer, i que juntament amb el Human Brain Project i el Graphene Flagship és un dels projectes d'investigació més ambiciosos d'Europa, amb una inversió de mil milions d'euros.

La idea no és transmetre quànticament tota la informació encriptada, sinó només les claus per desencriptar-la. "El principal repte és treure la tecnologia quàntica del laboratori, aplicar-la al món real i comprovar que es pot integrar amb les xarxes clàssiques a un cost assumible", declara Valerio Pruneri. "Les xarxes de comunicacions són molt agressives amb els elements quàntics", explica Vicente Martín, catedràtic de la Universitat Politècnica de Madrid (UPM) i director del Centre de Simulació Computacional (CCS), que també participa a CiViQ en estreta col·laboració amb Telefónica. "Un senyal clàssic de fibra òptica té uns 100 milions de fotons", mentre que un senyal quàntic està codificat per un únic fotó. "És molt difícil compatibilitzar les comunicacions clàssiques amb les quàntiques", subratlla Martín. El projecte CiViQ disposa de gairebé 10 milions d'euros per perseguir aquest objectiu.

A Espanya, a CiViQ hi participen també dues empreses emergents, VLC Photonics, sorgida de la Universitat Politècnica de València (UPV), i Quside, que va néixer d'un projecte de l'Icfo. Quside ha creat el primer xip integrat per generar claus d'encriptació a partir de principis quàntics. "Els nombres aleatoris actuals utilitzats en encriptació en realitat no són aleatoris, ja que neixen d'algoritmes", declara Carlos Abellán. Això constitueix un altre punt feble, perquè una màquina prou potent, o un ordinador quàntic, podria arribar a desxifrar-los. "La quàntica és l'única manera de generar aleatorietat real". Segons Abellán, el xip de Quside es començarà a aplicar els pròxims anys en centres de dades, cotxes autònoms i altres dispositius connectats a la internet de les coses.

"Ja som capaços d'establir comunicacions segures d'un punt a l'altre separats per una distància d'uns 400 quilòmetres", destaca Pruneri. "A llarg termini, l'objectiu és que qualsevol punt del món es pugui connectar de manera segura amb qualsevol altre punt utilitzant satèl·lits combinats amb cables de fibra òptica i repetidors quàntics, que s'estan desenvolupant i permetran distribuir l'entrellaçament a distàncies més llargues".●

WLADIMIR BULGAR/SCIENCE PHOTO LI / GETTY
Un processador quàntic

L'impuls de les tecnologies quàntiques és una oportunitat per a ciutadans, empreses i governs

ELSA VELASCO
Barcelona

Gràcies al seu ric ecosistema de recerca, Catalunya té l'oportunitat de convertir-se en una regió líder del sud d'Europa en tecnologies quàntiques. "Tenim *start-ups*, centres d'investigació, universitats i persones molt capdavanteres en aquest àmbit", afirma Lluís Torner, director de l'Icfo. "Podem ser un centre del sud d'Europa en tecnologies quàntiques".

L'Icfo participa en set projectes diferents del Quantum Flagship i en lidera dos; unes xifres que superen qualsevol altra institució a Europa. A més, recentment els centres científics de Catalunya que treballen en tecnologies quàntiques s'han aliat per crear una versió local del Quantum Flagship, QuantumCAT, que té el suport del Fons Europeu de Desenvolupament Regional i la Generalitat de Catalunya. Hi participen el mateix Icfo, que el coordina, el Barcelona Supercomputing Center (BSC-CNS), l'Institut Català de Nanociència i Nanotecnologia (ICN2), la Fundació i2CAT, la Universitat Autònoma de Barcelona (UAB), la Universitat de Barcelona (UB) i la Universitat Politècnica de Catalunya (UPC). "L'objectiu és impulsar projectes orientats a la indústria i que puguin tenir un impacte en l'economia catalana", informa Maria Martí, directora de projectes dels portafolis de tecnologies quàntiques de l'Icfo.

A Catalunya hi ha centres, universitats i empreses emergents que investiguen aquest àmbit

L'impuls de les tecnologies quàntiques servirà per formar científics, tant de Catalunya com d'altres zones, "que poden tenir idees per crear nous negocis", assenyala Hugues de Riedmatten, de l'Icfo. A més, el coneixement generat agilitarà l'aplicació d'aquestes tecnologies a nivell públic i privat. "Això interessa tant als governs com als ciutadans", subratlla Torner.

A la cursa per les tecnologies quàntiques la Xina i els EUA hi anaven al capdavant. Ara, amb el Quantum Flagship i la inversió de governs estatals, Europa ha esdevingut un sòlid competidor. "Hi ha un esforç genuí d'Europa per posar-se al dia en un camp que no va cuidar tant com hauria pogut en el passat", afirma Vicente Martín, de la UPM.

D'altra banda, "Espanya és dels pocs països europeus que no ha fet una inversió específica en aquest àmbit", critica Lluís Torner. "Encara hi som a temps i hauríem de fer-ho per situar millor investigadors i empreses", reclama. "A Espanya tenim bons científics en tecnologies quàntiques i s'han fet grans esforços, però en la part econòmica anem una mica curts", valora Vicente Martín. ●