

Image not found

Catalunya, pionera en la implementació de la seguretat quàntica a Internet

Avui s'han presentat els resultats del projecte 'Criptografia Quàntica en Comunicacions Crítiques' per transmetre informació crítica de manera ultrasegura a partir d'un sistema de claus quàntiques

September 09, 2022

Exit de la primera connexió amb criptografia quàntica amb tecnologia pròpia i embrió de la futura xarxa metropolitana, que es connectarà a la Internet quàntica estatal i paneuropea. El vicepresident del Govern i conseller de Polítiques Digitals i Territori, **Jordi Puignero**, acompanyat de la consellera de Recerca i Universitats, **Gemma Geis**, ha presidit avui la presentació dels resultats del projecte 'Criptografia Quàntica en Comunicacions Crítiques', una iniciativa nascuda en el marc del Programa de Recerca i Innovació en Tecnologies Digitals Avancades (TDA) impulsat per Polítiques Digitals, que tenia per objectiu desenvolupar i validar un sistema de claus quàntiques per a l'encriptació i transmissió ultrasegura d'informació crítica.

El projecte impulsat i finançat amb 1,2 milions d'euros per Polítiques Digitals i desenvolupat per l'Institut de Ciències Fòtoniques (ICFO), s'ha implementat en forma de prova pilot en un enllac de comunicació quàntica, a través de fibra òptica punt a punt i a una distància de 30 km, entre les seus de l'ICFO, a Castelldefels, i el Centre de Telecomunicacions i Tecnologies de la Informació de la Generalitat de Catalunya (CTTI), a l'Hospitalet del Llobregat.

Aquesta primera i exitosa connexió quàntica, que ha permès provar sobre el terreny i validar la metodologia i tecnologia emprades, s'ha reproduït avui durant la presentació dels resultats, objectius i properes passes del projecte, amb una videoconferència entre el vicepresident **Puignero** i **Silvia Carrasco**, Directora de la Unitat de Transferència de Coneixement i Tecnologia a l'ICFO, a través de l'enllac de comunicació quàntica establert en el pilot. A la presentació també hi han participat el director general d'Innovació i Economi Digital, **Daniel Marco**; el director de l'ICFO, **Lluís Torner**; i la directora de Desenvolupament de Negoci a LuxQuanta, **Vanesa Diaz**.

Primeres passes del projecte

Ara fa dos anys, en el marc del Programa de Recerca i Innovació en Tecnologies Digitals

Avancades (TDA), Politiques Digitals va unir esforços amb l'ICFO per posar en marxa un projecte que impulsi les tecnologies quàntiques, amb l'objectiu de desplegar les comunicacions quàntiques a Catalunya

El repte proposat en el programa TDA consistia a disposar d'un sistema de comunicació segur entre punts utilitzant la criptografia quàntica sense haver de variar l'actual xarxa corporativa. L'objectiu del projecte, coordinat pel Prof. ICREA de l'ICFO Valerio Pruneri, era donar resposta a la necessitat d'enfortir la seguretat en les comunicacions i superar les principals barreres detectades per democratitzar l'ús de la tecnologia quàntica amb solucions de baix cost fàcilment integrables en l'ecosistema tecnològic actual

Per això es van desenvolupar, com a primer pas, mètodes d'encriptació de claus quàntiques que poguessin integrar-se com una capa addicional a les línies de telecomunicació tradicionals i permetre comunicacions ultrasegures per a la transmissió de dades crítiques

Desenvolupament del pilot

En el marc del projecte i com a segon pas, un equip d'investigadors de l'ICFO, Cellnex Telecom -gestor de la Xarxa Oberta de Catalunya-, i l'empresa derivada de l'ICFO LuxQuanta, creada recentment, ha realitzat una prova pilot desplegant maquinària i software a la xarxa de fibra òptica de la Generalitat de Catalunya. La prova pilot ha consistit a establir un enllaç de comunicació quàntica, punt a punt de 30 km, entre les seus de l'ICFO (Castelldefels) i el Centre de Telecomunicacions i Tecnologies de la Informació CTTI (L'Hospitalet del Llobregat).

L'objectiu principal ha estat assajar sobre el terreny la implementació d'un sistema de comunicació segura, punt a punt, que utilitzi la tècnica o protocol de comunicació segura anomenat "Distribució Quàntica de Claus" (QKD per les sigles en anglès). Aquest protocol és un mètode de xifratge basat en les lleis de la física quàntica, que fa servir fenòmens quàntics per crear una clau completament segura. La clau es crea codificant els bits aleatoris en fotons i es transmet a través de les xarxes de fibra òptica actuals o fins i tot a través de l'espai lliure

ai

El naixement d'una nova empresa

Com a resultat d'aquest projecte conjunt, l'ICFO va fundar l'spin-off LuxQuanta, empresa nascuda amb la missió de facilitar les comunicacions ultrasegures mitjançant l'ús de tecnologies quàntiques. L'empresa va aportar els coneixements necessaris per a la implementació de la tecnologia, la fabricació dels dispositius transmissors i receptors i la seva integració a la xarxa de telecomunicacions actual per fibra òptica. També va permetre desenvolupar els protocols QKD que garantissin una connexió segura. Empreses com LuxQuanta reafirmen l'enorme potencial que aquesta tecnologia pot brindar per protegir tota mena de dades en el futur, ampliant l'impacte a altres àmbits de gran importància per a la societat en general, més enllà del sector de les telecomunicacions

ons, com ara infraestructures crítiques, l'administració pública o el sector sanitari, entre altres. Es tracta, doncs, d'un exemple d'èxit del model de recerca i innovació 'mission driven' impulsat pel Govern -on l'Administració planteja reptes propis-, i 'dual-use', en que els resultats de la recerca són utilitzats pel sector públic i transferits al sector privat per a la generació de creixement econòmic, la creació de llocs de treball i l'assoliment d sobirania tecnològica i lídera

Validant la tecnologia

Per provar i validar l'equip, LuxQuanta va dur a terme diverses proves de comunicació entre l'ICFO i el CTTI, utilitzant xats i videoconferències com a exemples en que es podria servir. Ho va fer utilitzant components de Qside, una altra spin-off de l'ICFO, que dissenya i fabrica tecnologies quàntiques innovadores basades en generadors de nombres aleatoris quàntics. Així, es van generar les claus quàntiques i es va xifrar cada missatge. Mitjançant una pantalla de control, es podien monitorar el rendiment del canal de comunicació i veure com el sistema alertava els usuaris de la presència d'algun 'hacker' que pogués estar escoltant la trucada.

Al contrari del que passa amb els mètodes d'encriptació tradicionals, basats en algorismes matemàtics, amb aquest mètode és possible detectar el moment en que algú intercepta l'intercanvi de claus. Quan un 'hacker' intenta recuperar la informació codificada en els fotons, les propietats d'aquests mateixos fotons canvien irreversiblement, perquè els stats quàntics no poden clonar-se ni copiar-se. És a dir, en intentar mesurar els fotons que componen la clau es modifica la informació que hi ha codificada, i això alerta les parts que algú ha interceptat l'intercanvi de claus i aquestes queden compromeses. Aleshores, la clau es descarta i se'n genera una de nova, que es torna a enviar a cadascuna de les parts per continuar amb una comunicació segura.

La Internet Quàntica a Barcelona

Aquest enllaç exitós és el primer pas cap al desplegament de **l'anell quàntic a Barcelona, tractat a través de la xarxa de fibra òptica de la Generalitat de Catalunya i Cellnex Telecom**, que a llarga formara part del desplegament de la Internet quàntica en l'àmbit europeu. L'anell físic envoltarà la ciutat de Barcelona, i cercarà connectar diverses infraestructures i equipaments clau, demostrant, d'una banda, l'escalabilitat d'aquesta tecnologia a altres àrees més grans, i de l'altra, que la transmissió d'informació crítica es pot dur a terme de manera ultrasegura. En futures fases de desplegament està previst que l'anell de Barcelona es connecti via terrestre i satel·lità amb altres localitzacions estatals i internacionals

Aquest anell suposa la materialització inicial d'una iniciativa que situa Barcelona al mapa europeu com un important hub d'innovació en tecnologies quàntiques, posicionant-la entre els actors destacats en la matèria i capdavanters en el desenvolupament i el desplegament

d'aquestes tecnologies a Europa, com ara Alemanya, França o els Països Baixos. Es tracta d'un projecte estratègic per al país que serà un dels eixos d'actuació de la iniciativa 'Quantica - Vall Mediterrània de la Ciència i les Tecnologies Quàntiques' impulsada pel Govern i que espera rebre finançament dels fons estatals i fons europeus NextGenerationE per tal d'accelerar-ne la implantació

L'embrió de l'EuroQCI

A més, l'execució de l'anell quàntic a Barcelona suposarà un pas més cap a desenvolupament de la **futura infraestructura paneuropea de comunicacions quàntiques**, l'anomenada EuroQCI, que es desenvoluparà aviat en el marc del Programa Complementari de Comunicacions Quàntiques, finançat per la Generalitat de Catalunya i pel Ministeri de Ciència e Innovació en el marc del Plan de Recuperación, Transformación y Resiliencia, dels programes Quantum Flagship i Digital Europe, de la Comissió Europea

Aquesta iniciativa de la Comissió Europea dotarà Europa d'una xarxa de comunicacions quàntiques que es desplegarà durant els deu anys vinents. Certificada punt a punt, permetrà la transmissió i emmagatzematge de dades i informació de manera totalment segura mitjançant connexions i enllaços, terrestres i satel·litàries, entre les diferents infraestructures clau dins de la Unió Europea

Image not found

Image not found

Image not found



Quantum Cryptography in Critical Communications



How does quantum cryptography work? (v. Eng)



Com funcion la criptografia quantica (v. CAT)



¿Como funciona la encriptacion cuantica? (v. CAST)