Catalunya, pionera en la implementacio de la seguretat quantica a Internet

Avui s'han presentat els resultats del projecte ?Criptografia Quantica en Comunicacions Critiques' per transmetre informacio critica de manera ultrasegura a partir d'un sistema de claus quantiques

September 09, 2022

Exit de la primera connexio amb criptografia quantica amb tecnologia propia i embrio de la futura xarxa metropolitana, que es connectara a la Internet quantica estatal i paneurope . El vicepresident del Govern i conseller de Politiques Digitals i Territori, **Jordi Puignero**, acompanyat de la consellera de Recerca i Universitats, **Gemma Geis**, ha presidit avui la presentacio dels resultats del projecte ?Criptografia Quantica en Comunicacions Critiques', una iniciativa nascuda en el marc del Programa de Recerca i Innovacio en Tecnologies Digitals Avancades (TDA) impulsat per Politiques Digitals, que tenia per objectiu desenvolupar i validar un sistema de claus quantiques per a l'encriptacio i transmissio

ultrasegura d'informacio critica.?

El projecte**impulsat i financat amb 1,2 milions d'euros per Politiques Digitals i desenvolupat per l'Institut de Ciencies Fotoniques (ICFO)**, s'ha implementat en forma de prova pilot en un enllac de comunicacio quantica, a traves de fibra optica punt a punt i a una distancia de 30 km, entre les seus de l'ICFO, a Castelldefels, i el Centre de Telecomunicacions i Tecnologies de la Informacio de la Generalitat de Catalunya (CTTI), a l'Hospitalet del Llobregat.?

Aquesta primera i exitosa connexio quantica, que ha permes provar sobre el terreny i valida la metodologia i tecnologia emprades, s'ha reproduit avui durant la presentacio del resultats, objectius i properes passes del projecte, amb una videoconferencia entre e vicepresident**Puignero** i **Silvia Carrasco**, Directora de la Unitat de Transferencia de Coneixement i Tecnologia a l'ICFO, a traves de l'enllac de comunicacio quantica establert en el pilot. A la presentacio tambe hi han participat el director general d'Innovacio i Economi Digital,**Daniel Marco**; el director de l'ICFO, **Lluis 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 Innovacio en Tecnologies Digitals Avancades (TDA), Politiques Digitals va unir esforcos amb l'ICFO per posar en marxa u projecte que impulses les tecnologies quantiques, amb l'objectiu de desplegar le comunicacions quantiques a Catalunya

El repte proposat en el programa TDA consistia a disposar d'un sistema de comunicaci segur entre punts utilitzant la criptografia quantica sense haver de variar l'actual xarx corporativa. L'objectiu del projecte, coordinat pel Prof. ICREA de l'ICFO Valerio Pruneri,er donar resposta a la necessitat d'enfortir la seguretat en les comunicacions i superar le principals barreres detectades per democratitzar l'us de la tecnologia quantica am solucions de baix cost facilment integrables en l'ecosistema tecnologic actual

Per aixo es van desenvolupar, com a primer pas, metodes d'encriptacio de claus quantique que poguessin integrar-se com una capa addicional a les linies de telecomunicacion tradicionals i permetre comunicacions ultrasegures per a la transmissio de dades critiques

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 maquinaria i software a la xarxa de fibra optica de la Generalitat de Catalunya. La prova pilot ha consistit a establir un enllac de comunicacio quantica, punt a punt de 30 km, entre les seus de l'ICFO (Castelldefels) i el Centre de Telecomunicacions i Tecnologies de la Informacio CTTI (L'Hospitalet del Llobregat).

L'objectiu principal ha estat assajar sobre el terreny la implementacio d'un sistema de

comunicacio segura, punt a punt, que utilitzi la tecnica o protocol de comunicacio segura anomenat "Distribucio Quantica de Claus" (QKD per les sigles en angles). Aquest protocol e un metode de xifratge basat en les lleis de la fisica quantica, que fa servir fenomens quan ics per crear una clau completament segura. La clau es crea codificant els bits aleatori en fotons i es transmet a traves de les xarxes de fibra optica actuals o fins i tot a trave de l'es
ai

El naixement d'una nova empresa

Com a resultat d'aquest projecte conjunt, l'ICFO va fundar l'spin-off LuxQuanta, empr sa nascuda amb la missio de facilitar les comunicacions ultrasegures mitjancant l'us de tecnologies quantiques. L'empresa va aportar els coneixements necessaris per a la implementacio de la tecnologia, la fabricacio dels dispositius transmissors i receptors i la seva integracio a la xarxa de telecomunicacions actual per fibra optica. Tambe va perme re desenvolupar els protocols QKD que garantissin una connexio se
ura. Empreses com LuxQuanta reafirmen l'enorme potencial que aquesta tecnologia pot rindar per protegir tota mena de dades en el futur, ampliant l'impacte a altres ambit de gran importancia per a la societat en general, mes enlla del sector de les telecomunicac ons, com ara infraestructures critiques, l'administracio publica o el sector sanitari, entre 'altres. Es tracta, doncs, d'un exemple d'exit del model de recerca i innovacio ?missio driven' impulsat pel Govern -on l'Administracio planteja reptes propis-, i ?dual-usei¿½, en que els resultats de la recerca son utilitzats pel sector public i transferits al sector priv t per a la generacio de creixement economic, la creacio de llocs de treball i l'assoliment d sobirania tecnologica i lidera

Validant la tecnologia

Per provar i validar l'equip, LuxQuanta va dur a terme diverses proves de comunicac o entre l'ICFO i el CTTI, utilitzant xats i videoconferencies com a exemples en que es podria er servir. Ho va fer utilitzant components de Quside, una altre spin-off de l'ICFO, que disseny i fabrica tecnologies quantiques innovadores basades en generadors de nombres aleato is quantics. Aixi, es van generar les claus quantiques i es va xifrar cada missatge. Mitjanc nt una pantalla de control, es podien monitorar el rendiment del canal de comunicacio i ve re com el sistema alertava els usuaris de la presencia d'algun ?hacker' que pog es estar escoltant la truc
da. Al contrari del que passa amb els metodes d'encriptacio tradicionals, basats en algo ismes matematics, amb aquest metode es possible detectar el moment en que algu inte cepta l'intercanvi de claus. Quan un ?hacker' intenta recuperar la informacio codificada n els fotons, les propietats d'aquests mateixos fotons canvien irreversiblement, perque els stats quantics no poden clonar-se ni copi
r-se. Es a dir, en intentar mesurar els fotons que componen la clau es modifica la informacio

ue hi ha codificada, i aixo alerta les parts que algu ha interceptat l'intercanvi de claus i a uestes queden compromeses. Aleshores, la clau es descarta i se'n genera una de nov , que es torna a enviar a cadascuna de les parts per continuar amb una comunicaci segura.

La Internet Quantica a Barcelona

Aquest enllac exitos es el primer pas cap al desplegament de **l'anell quantic a Barcelona, tracat a traves de la xarxa de fibra optica de la Generalitat de Catalunya i Cellnex Telecom**, que a la llarga formara part del desplegament de la Internet quantica en l'ambit europeu. L'anell fisic envoltara la ciutat de Barcelona, i cercara connectar diverses infraestructures i equipaments clau, demostrant, d'una banda, l'escalabilitat d'aquesta tecnologia a altres arees mes grans, i de l'altra, que la transmissio d'informacio critica es pot dur a terme de manera ultrasegura. En futures fases de desplegament esta previst que l'anell de Barcelona es connecti via terrestre i satel·lit amb altres localitzacions estatals i internacionals

Aquest anell suposa la materialitzacio inicial d'una iniciativa que situa Barcelona al mapa europeu com un important hub d'innovacio en tecnologies quantiques, posicionant-la entre els actors destacats en la materia i capdavanters en el desenvolupament i el desplegament d'aquestes tecnologies a Europa, com ara Alemanya, Franca o els Paisos Baixos.
Es tracta d'un projecte estrategic per al pais que sera un dels eixos d'actuacio de la iniciativa ?Quantica - Vall Mediterrania de la Ciencia i les Tecnologies Quantiques' impulsada pel Govern i que espera rebre financament dels fons estatals i fons europeus NextGenerationE per tal d'accelerar-ne la implantacio

L'embrio de l'EuroQCI

A mes, l'execucio de l'anell quantic a Barcelona suposara un pas mes cap a desenvolupament de la**futura infraestructura paneuropea de comunicacions quantiques**, l'anomenada EuroQCI, que es desenvolupara aviat en el marc del Programa Complementaria de Comunicaciones Cuanticas, financat per la Generalitat de Catalunya i pel Ministerio d Ciencia e Innovacion en el marc del Plan de Recuperacion, Transformacion y Resiliencia, dels programes Quantum Flagship i Digital Europe, de la Comissio Europea

Aquesta iniciativa de la Comissio Europea dotara Europa d'una xarxa de comunicacio s quantiques que es desplegara durant els deu anys vinents. Certificada punt a punt, permet a la transmissio i emmagatzematge de dades i informacio de manera totalment segu a mitjancant connexions i enllacos, terrestres i satel·litaries, entre les diferents infraestructu es clau dins de la Unio Europ

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)