

Catalunya fa el primer pas cap a la implementacio de l??EuroQCI?, la gran infraestructura de comunicacio quantica europea

La Generalitat de Catalunya, l'ICFO i Cellnex engeguen el projecte ?Criptografia Quantica en Comunicacions Critiques' per desenvolupar i validar un sistema de claus quantiques per a la l'encriptacio i transmissio ultrasegura d'informacio

March 04, 2021

El projecte ?**Criptografia Quantica en Comunicacions Critiques'** desenvolupara i validara un sistema de distribucio quantica de claus criptografiques que s'implementara en forma de prova pilot en un enllac punt a punt entre l'Institut de Ciencies Fotoniques (ICFO), a Castelldefels, i el Centre de Telecomunicacions i Tecnologies de la Informacio (CTTI), a l'Hospitalet del Llobregat.

El projecte s'inscriu en el Programa de Recerca i Innovacio en Tecnologies Digitals Avancades que impulsa la **Generalitat de Catalunya** a traves del **Departament de Politiques Digitals i Administracio Publica**, essent coordinat per l'**ICFO** en col·laboracio amb l'empresa **Cellnex**, gestora de la xarxa oberta de Catalunya, i de la **Fundacio i2CAT**, proveidora de part del software necessari per dur-lo a terme.

L'objectiu principal del pilot es executar una prova de camp per a la implementacio d'un sistema de comunicacio segur, punt a punt, que inclogui tecnologia de comunicacions quantiques utilitzant el metode de comunicacio segura denominat i¿½**Quantum Key Distribution**i¿½ (QKD). Aquesta prova implica la materialitzacio de conceptes n implementacions tangibles per a la industria i la ciutadania en general, mentre busca valid r els veritables avantatges d'aquesta tecnologia respecte als sistemes actuals gracies a la se a facil integrabilitat, el seu cost i, sobre tot, el seu important potencial de merca . El projecte forma part del conjunt d'iniciatives que s'implementaran per al desenvolupame t de la futura infraestructura paneuropea de comunicacions quantiques EuroQCI. L'EuroQCI s una iniciativa de la Comissio Europea que proveira Europa d'una xarxa de comunicacio s quantiques i que es desplegara al llarg dels propers 10 any . Aquesta futura infraestructura, certificada punt a punt, permetra la transmissio i emmagatzematge de dades i informacio de manera completament segura, a traves e connexions entre els diferents actius clau en el territori de la Unio Europea, mitjanca t enllacos terrestres i via satel·l t. EuroQCI buscara demostrar diferents casos d'us on aquesta iniciativa es un primer pas pe a, en un futur, tenir un rol rellevant en arees com la ciberseguretat per a centres de dades la comunicacio entre satel·lits i la Terra, la proteccio de xarxes de distribucio electrica i la comunicacio govername tal. Per al conseller de Politiques Digitals, **Jordi Puignero**, i¿½l'impuls de les tecnologi s quantiques es una prioritat pel Govern i especialment en el camp de la criptografia quant ca en les comunicacions, que ens permetra millorar la seguretat i privacitat de les nost es xarxes de comunicacions a la vegada que generem una nova industria basada en tecnolo ia puntera i coneixementi¿½.

Per la seva banda, el professor **Lluis Torner**, director de l'ICFO, assegura que i¿½les tecnologies de la informacio que sortiran de la segona revolucio quantica que ja s'ha iniciat i de la qual EuroQCI n'es nomes un exemple, crearan oportunitats immenses a l'era pos COVID-19. Catalunya te grans actius per crear empreses i llocs de treball en aquest ambit i el hem d'aprofitari¿?

. Finalment, el director global de Negoci i Innovacio de Cellnex, **Oscar Pallarols**, destaca i¿½el paper que una xarxa resilient d'infraestructures de telecomunicacions ha de jugar en el desplegament de les condicions necessaries per fer possible un ecosistema favorable a unes comunicacions segures basades en protocols quanticsi¿½

ICFO

Sobre l'encriptacio quantica

Internet ha suposat un canvi radical en la manera de fer i interaccionar en el nostre dia a dia: cada minut s'envien milions de missatges arreu del mon, connectant-nos a l'instant de manera global. Els mobils s'han convertit en una extensio de les nostres mans, facilitant-nos molt la manera com ens relacionem amb el nostre entorn, pero tot i que els fem servir per fer tot tipus d'operacions, sovint no ens aturem a pensar que les nostres transaccions bancaries, els nostres correus electronics, les nostres dades privades o fins i tot les nostres fotografies poden ser vulnerades.

Per tal d'evitar el hackeig d'informacio i mantenir la xarxa segura, els sistemes d'encriptacio actuals es basen en operacions matematiques conceptualment molt simples, pero extremadament dificils de resoldre a la practica: amb els algoritmes coneguts i qu s'utilitzen en l'actualitat, caldrien ordinadors de capacitats totalment inabastables pe desxifrar-los

Tot i aixo, al llarg de la historia s'ha vist que els codis secrets s'han desxifrat molt abans q e els afectats se n'adonessin. A mes, els avencos computacionals i algoritmics que tindran ll c durant els propers anys faran mes senzilla la tasca de desxifrar, i per tant, poden arriba a comprometre la seguretat, les xarxes de comunicacions, les infraestructures critiques i es dades sensibles/personals, de salut, financeres, de seguretat o defensa, entre d'altr s. Tenint en compte aquesta vulnerabilitat , les tecnologies quantiques proporcionen sist mes d'encriptacio, basats en les lleis fonamentals de la fisica quantica i en operac ons computacionals classiques, i esdevenen aixi mes segures davant de noves tecni ues computacionals. Les claus criptografiques quantiques presenten, a mes, dos avantatges c au: son compatibles amb les tecnologies actuals, integrant-se facilment als sistemes co un i¿½add-oni¿½, i romanen segures a llarg termini.