Cataluna, pionera en la implementacion de la seguridad cuantica en Internet

Hoy se han presentado los resultados del proyecto 'Criptografia Cuantica en Comunicaciones Criticas' para transmitir informacion critica de forma ultrasegura a partir de un sistema de claves cuanticas

September 09, 2022

Exito de la primera conexion con criptografia cuantica con tecnologia propia y embrion de la futura red metropolitana, que se conectara al Internet cuantico estatal y paneuropeo. El vicepresidente del Govern y consejero de Politicas Digitales y Territorio, **Jordi Puignero**, acompanado de la consejera de Investigacion y Universidades, **Gemma Geis**, ha presidido hoy la presentacion de los resultados del proyecto 'Criptografia Cuantica en Comunicaciones Criticas', una iniciativa nacida en el marco del Programa de Investigacion e Innovacion en Tecnologias Digitales Avanzadas (TDA) impulsado por Politicas Digitales, cuyo objetivo era desarrollar y validar un sistema de claves cuanticas para la encriptacion y transmision

ultrasegura de informacion critica.
El proyecto, **impulsado y financiado con 1,2 millones de euros por Politicas Digitales y llevado acabo por el ICFO** -Instituto de Ciencias Fotonicas, se ha implementado en forma de prueba piloto en un enlace de comunicacion cuantica, a traves de una fibra optica punto a punto de una distancia de 30 km, entre las sedes del ICFO, en Castelldefels, y el Centro de Telecomunicaciones y Tecnologias de la Informacion de la Generalidad de Cataluna (CTTI), en Hospitalet del Llobregat.
Esta primera y exitosa conexion cuantica, que ha permitido probar y validar la metodologia y tecnologia utilizadas sobre el terreno, se ha reproducido hoy durante la presentacion de los resultados, objetivos y proximos pasos del proyecto, con una videoconferencia entre el vicepresidente **Puignero** y **Silvia Carrasco** , Directora de la Unidad de Transferencia de Conocimiento y Tecnologia del ICFO, a traves del enlace de comunicacion cuantica establecido en la prueba piloto. En la presentacion tambien han participado el director general de Innovacion y Economia Digital, **Daniel Marco**; el director del ICFO, **Lluis Torner**; y la directora de Desarrollo de Negocio en LuxQuanta, **Vanesa Diaz**.

Primeros pasos del proyecto
Hace dos anos, en el marco del Programa de Investigacion e Innovacion en Tecnologias Digitales Avanzadas (TDA), Politicas Digitales unio esfuerzos con el ICFO para poner en marcha un proyecto que impulsara las tecnologias cuanticas, con el objetivo de desplegar las comunicaciones cuanticas en Cataluna.
El reto propuesto en el programa TDA consistia en disponer de un sistema de comunicacion segura entre puntos utilizando la criptografia cuantica sin tener que variar la actual red corporativa. El objetivo del proyecto, coordinado por el Prof. ICREA del ICFO Valerio Pruneri, era dar respuesta a la necesidad de fortalecer la seguridad en las comunicaciones y superar las principales barreras detectadas por democratizar el uso de las tecnologias cuanticas con soluciones de bajo coste facilmente integrables en el ecosistema tecnologico actual.
Por eso, como primer paso, se desarrollaron metodos de encriptacion de claves cuanticas que pudieran integrarse como una capa adicional a las lineas de telecomunicaciones tradicionales y permitir comunicaciones ultraseguras para la transmision de datos criticos.

Desarrollo del piloto
Dentro del marco del proyecto y como segundo paso, un equipo de investigadores del **ICFO**, **Cellnex Telecom** -gestor de la Xarxa Oberta de Catalunya-, y la empresa spin-off derivada del ICFO **LuxQuanta**, creada recientemente, ha realizado una prueba piloto desplegando maquinaria y software en la red de fibra optica de la **Generalitat de Catalunya**. La prueba piloto ha consistido en establecer un enlace de comunicacion cuantica, punto a punto de 30 km, entre las sedes del ICFO (Castelldefels) y el Centro de Telecomunicaciones y Tecnologias de la Informacion CTTI (L'Hospitalet del Llobregat).

El objetivo principal ha sido poner a prueba sobre el terreno la implementacion de un sistema de comunicacion segura, punto a punto, que utilice la tecnica o protocolo de comunicacion segura llamado "**Distribucion Cuantica de Claves**" (QKD por sus siglas en ingles). Este protocolo es un metodo de cifrado basado en las leyes de la fisica cuantica, que utiliza fenomenos cuanticos para crear una clave completamente segura. La clave se crea codificando los bits aleatorios en fotones y se transmite a traves de las actuales redes de fibra optica o incluso a traves del espacio.

El nacimiento de una nueva empresa

Como resultado de este proyecto conjunto, el ICFO fundo la spin-off LuxQuanta, empresa nacida con la mision de facilitar las comunicaciones ultraseguras mediante el uso de tecnologias cuanticas. La empresa aporto los conocimientos necesarios para la implementacion de la tecnologia, la fabricacion de los dispositivos transmisores y receptores y su integracion en la actual red de telecomunicaciones por fibra optica. Tambien permitio desarrollar los protocolos QKD que garantizaran una conexion segura.

Empresas como LuxQuanta reafirman el enorme potencial que esta tecnologia puede brindar para proteger todo tipo de datos en el futuro, ampliando el impacto a otros ambitos de gran importancia para la sociedad en general, mas alla del sector de las telecomunicaciones, como infraestructuras criticas, la administracion publica o el sector sanitario, entre otros.

Se trata, pues, de un ejemplo de exito del modelo de investigacion e innovacion 'mission driven' impulsado por el Gobierno -donde la Administracion plantea retos propios-, y de 'dual-use', donde los resultados de la investigacion son utilizados por el sector publico y transferidos al sector privado para la generacion de crecimiento economico, la creacion de puestos de trabajo y la consecucion de soberania tecnologica y liderazgo global.

Validando la tecnologia

Para probar y validar el equipo, LuxQuanta llevo a cabo diversas pruebas de comunicacion entre el ICFO y el CTTI, utilizando chats y videoconferencias como ejemplos en los que se podria implementar. Lo hizo utilizando componentes de Quside, otra spin-off del ICFO, que disena y fabrica tecnologias cuanticas innovadoras basadas en generadores de numeros aleatorios cuanticos. Asi, se generaron las claves cuanticas y se cifro cada mensaje. Mediante una pantalla de control, se podian monitorear el rendimiento del canal de comunicacion y ver como el sistema alertaba a los usuarios de la presencia de algun hacker que pudiera estar escuchando la llamada.

Al contrario de lo que ocurre con los metodos de encriptacion tradicionales, basados en algoritmos matematicos, con este metodo es posible detectar el momento en que alguien intercepta el intercambio de claves. Cuando un hacker intenta recuperar la informacion codificada en los fotones, las propiedades de estos mismos fotones cambian irreversiblemente, porque los estados cuanticos no pueden clonarse ni copiarse.

Es decir, al intentar observar los fotones que componen la clave se modifica la informacion que hay codificada, y esto alerta a las partes que alguien ha interceptado el intercambio de claves y estas quedan comprometidas. Entonces, la clave se descarta y se genera una nueva, que se vuelve a enviar a cada una de las partes para continuar con una comunicacion segura.

El Internet Cuantico en Barcelona

Este enlace exitoso es el primer paso hacia el despliegue del **anillo cuantico** en Barcelona, trazado a traves de la red de fibra optica de la **Generalidad de Cataluna** y **Cellnex Telecom**, que a la larga formara parte del despliegue de la Internet cuantica en el ambito europeo. El anillo fisico rodeara la ciudad de Barcelona, y buscara conectar diversas infraestructuras y equipamientos clave, demostrando, por un lado, la escalabilidad de esta tecnologia en otras areas mas grandes, y por otro, que la transmision de informacion critica se puede llevar a cabo de forma ultrasegura. En futuras fases de despliegue esta previsto que el anillo de Barcelona se conecte via terrestre y satelital con otras localizaciones estatales e internacionales.

Este anillo supone la primera materializacion de una iniciativa que situa a Barcelona en el mapa europeo como un importante hub de innovacion en tecnologias cuanticas, posicionandola entre los actores destacados en la materia y lideres en el desarrollo y el despliegue de estas tecnologias en Europa, como Alemania, Francia o Paises Bajos.

Se trata de un proyecto estrategico para el pais que sera uno de los ejes de actuacion de la iniciativa 'Cuantica - Valle Mediterraneo de la Ciencia y las Tecnologias Cuanticas' impulsada por el Gobierno y que espera recibir financiacion de los fondos estatales y fondos europeos NextGenerationEU con el fin de acelerar su implantacion.

El embrion del EuroQCI

Por otra parte, la ejecucion del anillo cuantico en Barcelona supondra un paso mas hacia el desarrollo de la **futura infraestructura paneuropea de comunicaciones cuanticas**, la llamada **EuroQCI**, que se desarrollara en breve en el marco del Programa Complementarias de Comunicaciones Cuanticas, financiado por la Generalidad de Cataluna y por el Ministerio de Ciencia e Innovacion en el marco del Plan de Recuperacion, Transformacion y Resiliencia, y de los programas Quantum Flagship y Digital Europe, de la Comision Europea.

Esta iniciativa de la Comision Europea dotara a Europa de una red de comunicaciones cuanticas que se desplegara durante los proximos diez anos. Certificada punto a punto, permitira la transmision y almacenamiento de datos e informacion de forma totalmente segura mediante conexiones y enlaces, terrestres y satelitales, entre las diferentes infraestructuras clave dentro de la Union Europea.

Criptografia Cuantica en Comunicaciones Criticas

How does quantum cryptography work? (v. Eng)

Com funcion la criptografia quantica (v. CAT)

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