Cataluna da el primer paso hacia la implementacion de la 'EuroQCI', la gran infraestructura de comunicacion cuantica europea

La Generalitat de Cataluna, el ICFO y Cellnex ponen en marcha el proyecto 'Criptografia Cuantica en Comunicaciones Criticas' para desarrollar y validar un sistema de claves cuanticas para la encriptacion y transmision de informacion de manera ultrasegura

March 04, 2021

El proyecto '**Criptografia Cuantica en Comunicaciones Criticas**' desarrollara y validara un sistema de distribucion cuantica de claves criptograficas que se implementara en forma de prueba piloto en un enlace punto a punto entre el ICFO - Instituto de Ciencias Fotonicas, ubicado en Castelldefels, y el Centro de Telecomunicaciones y Tecnologias de la Informacion (CTTI), ubicado en Hospitalet del Llobregat.

El proyecto se inscribe en el Programa de Investigacion e Innovacion en Tecnologias Digitales Avanzadas que impulsa la **Generalitat de Cataluna** a traves del **Departamento de**

Politicas Digitales y Administracion Publica, siendo coordinado por el **ICFO** en colaboracion con la empresa **Cellnex**, gestora de la Xarxa Oberta de Catalunya (Red Abierta de Cataluna), y de la **Fundacion i2CAT**, proveedora de una parte del software necesario para llevarlo a cabo.
El objetivo principal del piloto es ejecutar una prueba de campo para la implementacion de un sistema de comunicacion segura, punto a punto, que incluya tecnologia d comunicaciones cuanticas utilizando el metodo de comunicacion segura denominado " **Quantum Key Distribution**" (QKD). Esta prueba implica la materializacion de conceptos en implementaciones tangibles para la industria y la ciudadania en general, mientras busca validar las verdaderas ventajas de esta tecnologia respecto a los sistemas actuales gracias a su facil integrabilidad, su coste y, sobre todo, su importante potencial de mercado.
El proyecto forma parte del conjunto de iniciativas que se implementaran para el desarrollo de la futura infraestructura paneuropea de comunicaciones cuanticas EuroQCI. EuroQCI es una iniciativa de la Comision Europea que proveera a Europa de una red de comunicaciones cuanticas y que se desplegara a lo largo de los proximos 10 anos.
Esta futura infraestructura, certificada punto a punto, permitira la transmision y almacenamiento de datos e informacion de manera completamente segura, a traves de conexiones entre los diferentes activos clave en el territorio de la Union Europea, mediante enlaces terrestres y satelitales.
EuroQCI buscara demostrar diferentes casos de uso donde esta iniciativa es un primer paso para tener, en un futuro, un rol relevante en areas como la ciberseguridad para centros de datos, comunicacion entre satelites y la Tierra, asi como proteccion de redes de distribucion electrica y comunicacion gubernamental, entre otros.
Para el consejero de Politicas Digitales, **Jordi Puignero**, "el impulso de las tecnologias cuanticas es una prioridad para el Gobierno y especialmente en el campo de la criptografia cuantica para las comunicaciones, el cual nos permitira mejorar la seguridad y privacidad de nuestras redes de comunicaciones y a la vez generar una nueva industria basada en el conocimiento y tecnologia punta".
Por otra parte, el profesor **Lluis Torner**, director del ICFO, asegura que "las tecnologias de la informacion que emergeran de la segunda revolucion cuantica, que ya ha comenzado y de la que EuroQCI es solo un ejemplo, crearan oportunidades inmensas en la era post COVID-19. Cataluna tiene grandes activos para crear empresas y puestos de trabajo en este ambito y los debemos aprovechar ".
Finalmente, el director global de Negocio e Innovacion de Cellnex, **Oscar Pallarols**, destaca "el papel que una red resiliente de infraestructuras de telecomunicaciones debe jugar en el desarrollo de las condiciones necesarias para hacer posible un ecosistema favorable a unas comunicaciones seguras basadas en protocolos cuanticos ".

Sobre la encriptacion cuantica

Internet ha supuesto un cambio radical en la manera de hacer e interaccionar en el nuestro

dia a dia: cada minuto enviamos millones de mensajes alrededor de todo el mundo, conectandonos al instante de manera global. Los moviles se han convertido en una extension de nuestras manos, facilitandonos mucho la forma en que nos relacionamos con nuestro entorno, pero, aunque los usamos para hacer todo tipo de operaciones, a menudo no nos detenemos a pensar que nuestras transacciones bancarias, nuestros correos electronicos, nuestros datos privados o incluso nuestras fotografias pueden ser vulneradas.

Para evitar el hackeo de informacion y mantener la red segura, los sistemas de encriptacion actuales se basan en operaciones matematicas conceptualmente muy simples, pero extremadamente dificiles de resolver en la practica: con los algoritmos conocidos y que se utilizan en la actualidad, serian necesarios ordenadores de capacidades totalmente inalcanzables para descifrarlos.

Sin embargo, a lo largo de la historia se ha visto que los codigos secretos se han descifrado mucho antes que los afectados se dieran cuenta. Por otro lado, los avances computacionales y algoritmicos que tendran lugar durante los proximos anos haran mas sencilla la tarea de descifrar, y por tanto, pueden llegar a comprometer la seguridad, las redes de comunicaciones, las infraestructuras criticas y los datos sensibles/ personales, de salud, financieros, de seguridad o defensa, entre otros.

Teniendo presente esta vulnerabilidad, las tecnologias cuanticas proporcionan sistemas de encriptacion, basados en las leyes fundamentales de la fisica cuantica y en operaciones computacionales clasicas, y se convierten asi en mas seguras ante las nuevas tecnicas computacionales. Las claves criptograficas cuanticas presentan, ademas, dos ventajas clave: son compatibles con las tecnologias actuales, integrandose facilmente en los sistemas como un "add-on", y permanecen seguras a largo plazo.