Catalonia, pioneer in the implementation of quantum security on the Internet

Today the results of the 'Quantum Cryptography in Critical Communications' project were presented, focusing on the transmission of critical information in an ultra-secure manner using a system of quantum keys

September 09, 2022

Presentation of the first succesful connection with quantum cryptography using proprietary technolgy, the embryo of the future metropolitan network, to be connected to the state and pan-European quantum Internet. The Vice President of the Government and Minister for Digital Policies and Territory, **Jordi Puignero**, accompanied by the Minister for Research and Universities, **Gemma Geis**, officiated the presentation today of the results of the **'Quantum Cryptography in Critical Communications' project**, an initiative born in the framework of the Research and Innovation Program in Advanced Digital Technologies (TDA) promoted by Digital Policies, whose objective was to develop and validate a system of quantum keys for

the encryption and ultra-secure transmission of critical information.?

The project**promoted and funded with 1.2 million euros by Digital Policies and carried out by ICFO** -The Institute of Photonic Sciences, was implemented as a pilot test in a quantum communication link, through a point-to-point fiber optics link, covering a distance of 30 km, between the headquarters of ICFO, in Castelldefels, and the Center for Telecommunications and Information Technologies of the Government of Catalonia (CTTI), in Hospitalet del Llobregat.

This first and successful quantum connection, which has permitted the testing and validation of the methodology and technology used in the field, was reproduced today during the presentation of the project's results, objectives and next steps, with a videoconference between Vice President **Puignero** and **Silvia Carrasco**, Director of the ICFO Knowledge and Technology Transfer Unit, through the quantum communication link established in the pilot test. Also participating in the presenation were the general director of Innovation and Digital Economy, **Daniel Marco**; the director of ICFO, **Lluis Torner**; and the director of Business Development at LuxQuanta, **Vanesa Diaz**.

First steps of the project

Two years ago, within the framework of the Advanced Digital Technologies Research and Innovation Program (TDA), Digital Policies joined forces with ICFO to launch a project that would promote quantum technologies, with the aim of deploying quantum communications in Catalonia.

The challenge proposed by the TDA program was to have a secure communication system between points using quantum cryptography without having to change the current corporate network. The objective of the project, coordinated by ICREA Prof at ICFO Valerio Pruneri, was to respond to the need to strengthen the security in communications and overcome the main barriers detected in the democratization of the use of quantum technologies with low-cost solutions that can be easily integrated into the current technological ecosystem.

Therefore, as a first step, quantum key encryption methods were developed that could be integrated as an additional layer to traditional telecommunications lines and allow ultra-secure communications for the transmission of critical data.

The pilot development

Within the framework of the project and as a second step, a team of researchers from **ICFO**, **Cellnex Telecom** -manager of the Xarxa Oberta de Catalunya-, and the recently created ICFO spin-off company **LuxQuanta**, carried out a pilot test deploying hardware and software for the fiber optic network of the **Generalitat de Catalunya**. The pilot test consisted in establishing a 30 km point-to-point quantum communication link between ICFO headquarters (Castelldefels) and the CTTI Telecommunications and Information Technology Center (L'Hospitalet del Llobregat).

The main objective has been to test on the ground the implementation of a secure, point-to-point communication system that uses the secure communication technique or protocol called "Quantum Key Distribution" (QKD). This protocol is an encryption method based on the laws of quantum physics, which uses quantum phenomena to create a completely secure key. The key is created by encoding the random bits into photons and is transmitted over today's fiber optic networks or even through space.

Birth of a new company

As a result of this joint project, ICFO founded the spin-off **LuxQuanta**, a company born with the mission of facilitating ultra-secure communications through the use of quantum technologies. The company provided the necessary know-how for the implementation of the technology, the manufacturing of the transmitting and receiving devices and their integration into the current fiber optic telecommunications network. It also made possible the development of QKD protocols that guarantee a secure connection.

Companies such as LuxQuanta reaffirm the enormous potential that this technology can offer to protect all types of data in the future, expanding the impact to other areas of great importance for society in general, beyond the telecommunications sector, such as critical infrastructures, the public administration or the health sector, among others.

It is, therefore, a successful example of the 'mission driven' research and innovation model promoted by the Government -where the Administration poses its own challenges-, and of 'dual-use', where the results of the research are used by the public sector and transferred to the private sector for the generation of economic growth, the creation of jobs and the achievement of technological sovereignty and global leadership.

Validating the technology

To test and validate the equipment, LuxQuanta carried out several communication tests between ICFO and CTTI, using chats and video conferences as test beds. It did so using components from **Quside**, another ICFO spin-off, which designs and manufactures innovative quantum technologies based on quantum random number generators. Thus, the quantum keys were generated and each message was encrypted. Through a control screen, it was possible to monitor the performance of the communication channel and see how the system alerted users of the presence of a hacker who could be listening to the call.

Contrary to what happens with traditional encryption methods, based on mathematical algorithms, with this method it is possible to detect when someone intercepts the exchange of the key. When a hacker tries to retrieve the information encoded in the photons, th properties of these same photons change irreversibly, because quantum states cannot b cloned or copied

In other words, when trying to observe the photons that make up the key, the informatio that is encoded is modified, and this alerts the parties that someone has intercepted the ke

exchange and that the communication is compromised. The key is then discarded and a ne key is generated and sent back to each party to continue with the secure communication

The Quantum Internet in Barcelona

This successful link is the first step towards the deployment of the **quantum ring in Barcelona** , traced through the fiber optic network of the Government of Catalonia and Cellnex Telecom, which will ultimately form part of the deployment of the quantum Internet in Europe. The physical ring will surround the city of Barcelona, and will aim to connect various infrastructures and key facilities, demonstrating, on one hand, the scalability of this technology to larger areas, and on the other, that the transmission of critical information can be carried out in an ultra-secure way. In future phases of the deployment, it is planned that the Barcelona ring will be connected via land and satellite with other national and international locations.

This ring represents the first materialization of an initiative that places Barcelona on the European map as an important hub for innovation in quantum technologies, positioning it among the leading players in the field and leaders in the development and deployment of these technologies in Europe, such as Germany, France or the Netherlands.?

It is a strategic project for the country that will be one of the lines of action of 'Quantica - t e Mediterranean Valley of Science and Quantum Technologies initiative promoted by t e Government and which seeks funding from state funds and NextGenerationEU Europe n funds, in order to accelerate its implementation

The embryo of the EuroQCI

Additionally, the execution of the quantum ring in Barcelona will mean a further step toward the development of the future pan-European quantum communications infrastructure, th so-called**EuroQCI**, which will be developed soon within the framework of the Complementary Program for Quantum Communications, funded by the Generalitat of Catalonia and by the Ministry of Science and Innovation within the framework of the Recovery, Transformation and Resilience Plan, and the Quantum Flagship and Digital Europe programs of the European Commission.

This initiative of the European Commission will provide Europe with a quantum communications network that will be deployed over the next ten years. Certified point-to-point, it will allow the transmission and storage of data and information in a totally secure manner through terrestrial and satellite connections and links between the different key infrastructures within the European Union.

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)