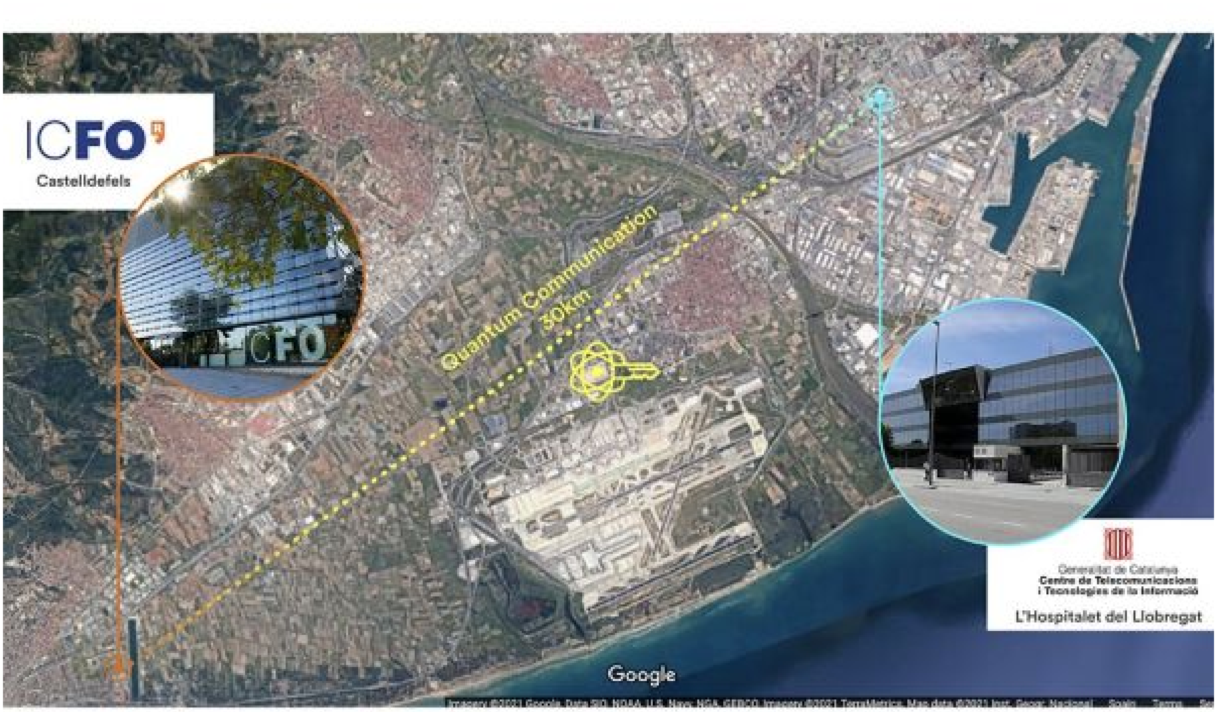
ICFO
Castelldefels
Quantum Communication
30km
Generalitat de Catalunya
Centre de Telecomunicacions i Tecnologies de la Informació
L'Hospitalet del Llobregat
Google

First steps towards the implementation of the ?EuroQCI?, the European Quantum Communication Infrastructure

The Government of Catalonia, ICFO and Cellnex launch the project 'Quantum Cryptography in Critical Communications' to develop and validate a system of quantum keys for ultra-secure encryption and transmission of information.

March 04, 2021

The project 'Quantum Cryptography in Critical Communications' will develop and validate a quantum distribution system of cryptographic keys that will be implemented through a pilot test, done via a point-to-point link between the ICFO - Institute of Photonic Sciences, located in Castelldefels, and the Center of Telecommunications and Information Technologies (CTTI), located in Hospitalet del Llobregat, Barcelona.

The project is part of the Research and Innovation Program in Advanced Digital Technologies promoted by the Government of Catalonia through the Department of Digital Policies and Public Administration, and is coordinated by ICFO, together with the collaboration of the company Cellnex, manager of the Open Network of Catalonia, and the Foundation i2CAT, provider of part of the software needed to carry out the test.

The main objective of the pilot is to carry out a field test for the implementation of a secure communication system, point-to-point, that includes quantum communication technology, which will use the secure communication method called "Quantum Key Distribution" (QKD). This test implies the materialization of concepts in real implementations for the industry and the general public, while seeking to validate the true advantages of this technology with respect to current systems thanks to its easy integrability and cost but, above all, its significant market potential.

This project is part of several initiatives to be implemented for the development of the future pan-European quantum communications infrastructure EuroQCI. EuroQCI is an initiative of the European Commission that will provide Europe with a quantum communications network and which will be deployed in the next 10 years.

This future infrastructure, which is certified point-to-point, will allow the transmission and storage of data and information in a completely secure manner, through connections between the different key infrastructures within the European Union, achieved through terrestrial and satellite links.

EuroQCI will seek to demonstrate different use cases in which this initiative is a first step to have, in the future, a relevant role in areas such as cybersecurity for data centers, communication between satellites and Earth, as well as protection of electrical distribution networks and governmental communications, among others.

For the Minister of Digital Policies, Jordi Puignero, "the push for quantum technologies is a priority for the Government and especially in the field of cryptography for quantum communications, which will allow us to improve the security and privacy of our communication networks and, at the same time, generate a new industry based on cutting-edge technology and knowledge ".

On the other hand, Professor Lluis Torner, director of ICFO, assures that "the information technologies that will appear from the second quantum revolution, which has already begun and of which EuroQCI is just one example, will create tremendous opportunities in the COVID-19 post-modern era. Catalonia has great assets in order to create companies and jobs in this area and we must take advantage of them".

Finally, the Global Director of Business and Innovation at Cellnex, Oscar Pallarols, highlights "the role that a resilient network of telecommunications infrastructures must play in developing the necessary conditions to enable an ecosystem favorable to secure communications based on quantum protocols".

About Quantum Cryptography

The Internet been a major game changer in the way we do and interact in our day-to-day lives: every minute we send millions of messages around the world, which has allowed us to be connected a global level instantaneously. Mobile phones have become an extension of our hands, enabling us an easier interaction with the environment around us, but, although we use them to carry out all kinds of operations, we often do not stop to think that our financial transactions, our electronic emails, our private data or even our pictures can be compromised or breached.

To avoid the hacking of information and keep the network secure, current encryption systems are based on conceptually very simple mathematical operations, but extremely difficult to solve in practice: with the algorithms known and used today, we would need computers of unfathomable capabilities to decipher them.

However, throughout history we have seen that secret codes have been deciphered long before those affected were even aware of it. Furthermore, the computational and algorithmic advances that will take place over the next few years will make decryption tasks much easier, and therefore, may compromise security, communications networks, critical infrastructures as well as sensitive/ personal, health, financial, security or defense data, among others.

Bearing this vulnerability issue in mind, quantum technologies provide encryption systems, based on the fundamental laws of quantum physics and classical computational operations, and thus become more secure for new computational techniques. Quantum cryptographic keys also have two key advantages: they are compatible with current technologies, easily integrated into systems as an ï¿½add-onï¿½ element, and remain secure in the long term.