oesia grupo

QUANTUM CRYPTOGRAPHY AND ITS IMPACT ON OUR CYBERSECURITY

Introducción

As an introduction to quantum cryptography, we begin by defining cryptography in security applied to **protect information**, both of users, their personal and private information, as well as that of companies and governments. To do so, we rely on ensuring confidentiality, integrity and authenticity.

Confidentiality is ensured by **encrypting communications from one point to another**, protecting the information against possible threats from third parties in the transmission medium. This should be coupled with **authenticity and integrity** to identify who generates the information and that they have not been modified.

A good encryption service prevents such cyber-attacks or deceptions and, therefore, allows us to live more securely.

A present threat

The concept of quantum cryptography has been gaining more and more weight within the field of cybersecurity. This new concept is linked to the **emergence of quantum computers and the problems they can bring to our security**.

The emergence of **quantum computing makes it possible** to solve mathematical problems in a shorter time (current classical cryptography) with the possibility of breaking all our secure communications as they are currently conceived.

At present, all our communications could be being stored, saved for when we have that quantum computing capability to exploit and open them. Therefore, **we must start now to protect ourselves against these future threats**.

How can we protect ourselves?

Two alternatives have been developed to protect us against the increase in computational capacity by quantum computers :

Algorithms

Change the current mathematical algorithms to stronger ones that are not threatened by quantum computation. These algorithms have already been selected by international organizations, are available and are being implemented and deployed.

Technology

Change the technology, **the way we do things**. And that's where the new concept of quantum cryptography comes in, **applying quantum mechanics to make our transmissions secure**. The term quantum cryptography is **used to identify QKD (Quantum Key Distribution) technology**.

What is quantum cryptography?

Quantum cryptography or QKD is the distribution of keys based on quantum mechanics. **Between sender and receiver we send photons to each other.** This makes the medium secure, because **if someone tries to get in the middle to listen to that communication, the photons are altered** and the result I get in the receiver is different, allowing us to perceive that the communication has been compromised.

Until now we were familiar with the concept of bits, 0 and 1. In the case of photons what we are talking about is **qubits**, putting them in relation to the emitter and the receiver. Where before it could receive a zero or a one **I can now receive multiple combinations. The result of this transmission is used as a key**, which is also injected into the traditional encryptors that protect all communications, converting that key into a **secret and secure key**.

Challenges of quantum cryptography

Quantum cryptography is under development and brings many challenges to our current means. On the one hand, **we need to be able to industrialize it**, as well as to ensure the interoperability of equipment from different manufacturers. In addition, it requires security standards to apply the technology correctly and to transfer keys to encryptors securely. It even has challenges of reaching further distances with better functional characteristics, providing more keys regardless of the physical environment.

There are already **initiatives in Spain and other countries to cover different segments (terrestrial and satellite)**, but we still need to work on how to improve the technology so that we can turn it into a real solution.

Part of the success will depend on having **the necessary talent** to enable us to implement this technology.

We are facing a new technology that **must place universities and study centers as the main drivers of the development of these tools**. But this research should not remain academic papers to be shared at specialized conferences, but should make **the leap to companies** in order to be converted into products that allow their practical application as soon as possible.

Its **priority application must be in the public secto**r, the Administration or Defense of the States. But, there are other types of **private organizations that must place as soon as possible** on their radar with plans to implement quantum cryptography, as is the case with the companies in the **financial sector the companies that manage critical facilities** for society (such as energy), **private clinics** for the information they store on their patients or insurers who handle sensitive customer information.

In Tecnobit-Oesia Group we are already working on this technology in order to contribute with our experience to the challenges: training professionals, standardizing and industrializing.

By

Lourdes Velasco

Cifra Director
Cipherbit-Grupo Oesía

oesia grupo

tecnobit grupo oesia cipherbit grupo oesia UAV Navigation grupo oesia inster grupo oesia

Creating a better, more efficient, safer and sustainable world

grupooesia.com