NAME : Miguel Á. Sánchez	GROUP REF. : SC D2
COUNTRY : Spain	PREF. SUBJECT : PS2
REGISTRATION NUMBER : 219711391	QUESTION N° : Q2.10

Rather than emerging technologies, we would like to talk about the evolution and innovation in cryptography that will need to be deployed in the future power grids.

In our Paper, 11051 Analysis of the impact of cryptography in the GOOSE communications, we analyzed cryptography applied to the most restrictive communications, and we see that it is already possible to apply cryptographic solutions to obtain segmentation, confidentiality, and integrity. However, the evolution of quantum computing in recent years, the large investments being made in their development and their increasingly widespread use, make a scenario increasingly possible in which in the short to medium term many of the cryptographic algorithms we use will be invalidated (asymmetric cryptography), and in others we will have to modify parameters, such as duplicating key sizes. The time it usually takes for the selection, standardization and widespread adoption of algorithms ranges from 5 to 10 years, and in OT these times can generally be doubled, so, although there are very different positions as to the time needed for a real attack to be possible (some say it is already possible, others say it is several decades away), it is possible that we are lagging behind. NIST, the world reference body for the standardization of cryptographic algorithms, initiated in 2016 the Post-Quantum Cryptography project, which is already in the process of selecting post-quantum algorithms (algorithms resistant to attacks with quantum technology), and last July 5 the finalists were announced, which are being tested by cryptanalysts and interested parties from all over the world. The chosen ones should be evaluated and gradually incorporated into the industry, in order to protect the most critical assets from attacks with quantum computers.

We may think that quantum cryptography, that is, using principles of quantum mechanics to transmit and store information securely, is still a long way off, although there have already been successful tests of transmitting information using quantum interlacing, which eliminates the transmission medium, so MiTM attacks are not possible. For example, in the implementation of Quantum Key Distribution (QKD), it is possible to use interlacing, or to establish a communication system that detects an eavesdropper. If a third party tries to obtain the key, the system is disrupted and detected, so there is a mechanism to ensure that the medium is secure and no one is listening in, and only then can the key be extracted. If someone is detected trying to listen in, the key is not extracted and the communication is cut off.

Is it time to start testing post-quantum algorithms in the electrical sector devices?

What other surprises will quantum technology show us?