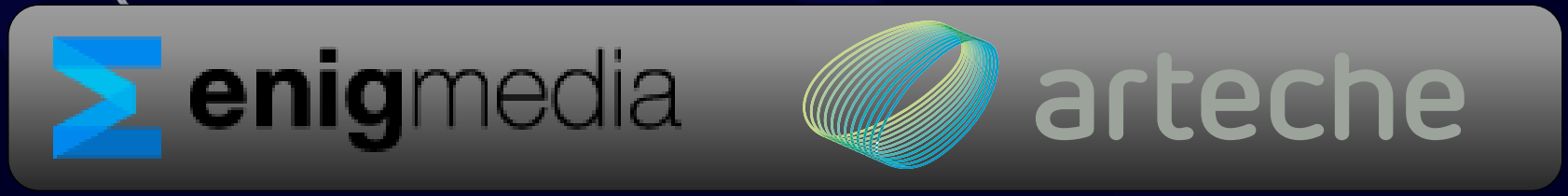
Paris Session 2022

Post-Quantum cryptography

SC D2: Information Systems and Telecommunication
PS2 Question 2.10: What emerging cybersecurity technologies are important for the future power grids?

Gerard Vidal (Spain) / Miguel Á. Sánchez (Spain)



Post-Quantum cryptography

- 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
- With the evolution of quantum computing, large investments in this technology and algorithms and their increasingly widespread use, current cryptographic algorithms will be broken (asymmetric crypto), or we will have to modify parameters, such as duplicating key sizes.
- Selection, standarization and widespread adoption usually takes from 5 to 10 years, may be the double in OT.
- In 2016 NIST started the Post-Quantum Cryptography project. Last July 5th the finalists were announced.

Post-Quantum cryptography

- In other hand, quantum cryptography, that is, using principles of quantum mechanics to transmit and store information securely, is closer than many people think. There have already been successful tests of transmitting information using quantum interlacing, which eliminates the transmission medium, so MiTM attacks are no longer possible.
- There are some algorithms for Quantum Key Distribution (QKD), to establish a communication system that detects an eavesdropper. If someone is trying to listen in, the key is not extracted in the remote endpoint, and the communication is cut off.
- Is it time to integrate some of them in electrical sector?
- What other surprises will quantum technology show us?