Madrid QCI: a QKD network infrastructure

Presenting Author (Daniel Gómez)
Co-Authors (Vicente Martin, Juan P. Brito, Laura Ortiz, Alberto Sebastian, Rafel J. Vicente, Ruben. B Méndez, Jaime Sáez de Buruaga, Marta I. García Cid, Rafael Artiñano, José Luis Rosales). *UPM, Quantum Information Group, Campus de Montegancedo, 28660 Boadilla del Monte Madrid, Spain*

JoseLuis.Rosales@upm.es

Feynman's contributions to the foundation of Quantum Information Technologies were numerous and significant. His ideas and insights helped to inspire and guide many of the developments in this field over the past decades, which leads, among many others, to the concept of Quantum Key Distribution (QKD) in cryptographic networks. This technology is used to create and distribute a secure encryption key. QKD takes advantages of the quantum nature of single photons (in discrete variables or and equivalent in continuous variables) to generate keys Information Theoretically Secure (ITS), ensuring the secrecy of the key, up to a certain threshold.

The technological challenge is inserting this novel cryptographic scenario in current optical networks. Optical networks are used to transmit large volumes of data over long distances with high speed and efficiency and quantum technologies could be disruptive in this environment.

On this basis, our testbed, Mad QCI (Madrid Quantum Communication Infrastructure), have integrated QKD with optical networks to endorse security against future quantum computers to the transmission of information. Thus QKD can be used as an additional layer of security to ensure the confidentiality of communications that are made over the optical network. Moreover, well-known protocols in classical domain were turned into quantum-secure, substituting by QKD the present key-negotiation step.

The Spanish Quantum Communications project is now being developed in Mad QCI, one of the main Hubs in EUROQCI. In the near future, Mad QCI will include QKD fiber networks including QKD and conventional optical communications as well as satellite connections to reach long-distance communications.

References

[1] Martin et al. "Quantum Technologies in the Telecommunications industry". EPJ Quantum Technology (2021) doi.org/10.1140/epjqt/s40507-021-00108-9

[2] Miralem Mehic et al. "Quantum Key Distribution: A Networking Perspective". ACM Computing Surveys, 55-5, Article 96 (2020)

[3] Alejandro Aguado et al. " VNF deployment and service automation to provide End-to-End quantum Encryption". Opt. Commun. Netw. Vol 10-4 (2018), 421-430

[4] Marta I. García Cid et al., "Madrid Quantum Network: a first step to Quantum Internet". Proc. ARES 2021, ACM, ISBN 978-1-4503-9051-4/21/08, doi.org/10.1145/3465481.3470056 (2021).

Figures

Figure 1: The UPM leads the Spanish project on Quantum Communications of the Integral Plan for Recovery, Resilience and Transformation, with the participation of the autonomous communities of Castilla y León, Catalonia, Galicia, Madrid, the Basque Country and the CSIC