The Madrid Quantum Network: A Quantum-Classical Integrated Infrastructure

V. Martin[1], A. Aguado[1], P. Salas[1], A.L. Sanz[1], J.P. Brito[1], D. R. Lopez[2], V. Lopez[2], A. Pastor[2], J. Folgueira[2], H.H. Brunner[3], S. Bettelli[3], F. Fung[3], D. Hillerkuss[3], L. C. Comandar[3], D. Wang[3], A. Poppe[3] and M. Peev[3]

[1]*Center for Computational Simulation and ETSI Informáticos, Universidad Politécnica de Madrid 28660 Madrid, Spain*
[2]*Telefónica Investigación y Desarrollo, Ronda de la Comunicación s/n 28050 Madrid. Spain*
[3]*Huawei Technologies Duesseldorf GmbH, European Research Institute, Riesstrasse 25-C3, 80992 München. Germany*
email: vicente@fi.upm.es

Abstract: We report on the Madrid Quantum Network, designed to demonstrate that a telecommunications network can also host quantum communications in a unified, logical and physical infrastructure. Using new Quantum Key Distribution systems paired with modern networking paradigms, we demonstrate a high technology readiness level of QKD installing the network in production facilities and running relevant use cases.
OCIS codes: 060.4250, 060.5565, 270.5568

1. Introduction and statement of the problem.

Telecommunications networks are, arguably, one of the cornerstones of our modern information society. They are one of the main drivers of our economy and provide the basis on which many of our day to day activities rely. This central position renders these to be a critical infrastructure; a general failure would produce catastrophic effects. This situation is exacerbated with each new technology: IoT, Artificial Intelligence, self-driving cars, e-health… all of these being interconnected and not reaching their full potential unless an underlying communications network meets their requirements. Security, for the infrastructure and its services, is increasingly demanded but, at the same time, it is undergoing major changes. The advent of quantum computing challenges the security community to rethink their basic algorithms. Current public key algorithms used in fundamental tasks, such as signatures or key agreement, are in danger because they rely on questionable computational security arguments and need replacement. One of the candidates is Quantum Key Distribution. QKD allows the generation of identical key strings at two remote locations, whereby these are known only to the legitimate users of the channel connecting them. This channel has to be able to transport signals at the quantum level. The secrecy is then guaranteed by the laws of quantum mechanics. This is quite a different proposition compared to the typical security algorithms, which rely on assumptions on the complexity of some mathematical problem and thus are bound to change if these turn out not to be true, as has happened with the advent of quantum computing -and could have happened even due to advances in classical computing or mathematics.

It is also fair to say that QKD is not a perfect technology. The current state of the art makes it practical only within limited distances, of the order of a few hundred km., and it only provides symmetric keys. To perform QKD it is necessary to have access to a communication link able to transmit signals at the quantum level. This is difficult and, up to now, it is standard to recourse to physically separate quantum and classical channels to avoid any interference. If we want to go beyond the point-to-point link, a standalone, separate, network has been proposed to provide QKD services. This is an extremely expensive proposition that has hindered the field up to now. The objective of this talk is to sketch the solutions to this problem implemented in Madrid. A long write-up will be published elsewhere.

2. The Madrid Quantum Network. Description and Results.

The main objective in designing and building the Madrid Quantum Network [1] can be summarized as reducing the barriers for a broad adoption of quantum communications technologies. To achieve this goal we set several strategies:

- Avoid the need of a separated, quantum only, physical infrastructure. Demonstrate production readiness.
- Use network technologies compatible with carrier grade technologies for a unified logical infrastructure.
- Use quantum technologies that are as much as possible compatible with communications technologies and have a clear industrialization path. The quantum communications devices have to be network-aware.
- Integrate QKD in the existing security ecosystem rather than as an alternative; demonstrate practical use cases.

As mentioned in the introduction, the first point is mandatory to bring the costs to a reasonable level, but also to reduce up-front costs allowing a staged deployment and enhancing existing links with quantum capabilities only when and where necessary. The second point is related, because the deployment, management and control of an infrastructure using new, untested or not production-ready software is an obvious no-go for telcos. We addressed these two issues by using the Software Defined Networking paradigm. The main point here is the fact that a centralized entity (the SDN controller) oversees the whole network, controls programmable devices in the lower -physical- layer (including

the QKD devices) and can thus manage and optimize the whole quantum-classical infrastructure. It can make room for quantum channels at the physical level when needed and when the boundary conditions allow for it (e.g. managing the total power in a fiber to allow a quantum channel share the same fiber). To afford this level of flexibility, the QKD devices have to communicate with the network. We structured the SDN system in three stages. First is the advertising/discovery capability step that allows a local SDN agent to identify the QKD system, its characteristics and how to manage it from the network that communicates with the central SDN controller. This is done using the tools and concepts familiar to the Telecommunications companies and their engineers, so that the installation and management procedures are essentially identical to those for an installation of a classical communications device in production level facilities such as the ones used in the Madrid Quantum Network. The implementation meets several of the standards that are being developed in the quantum communications community in ETSI. The systems used [2], developed by Huawei Research Germany, can be driven from the network. They are built using Continuous Variables technology that uses detection systems akin to the ones used in classical communications. This opens an easier path to full-scale industrialization compared to technologies based on bulky and super-cooled single photon detectors used in other schemes. Finally, the network security protocols were modified so that they can use QKD together with existing algorithms (or even post-quantum ones) [3]. This means that the existing security methods do not need to be changed now, and that QKD can be used as an additional security layer -based on a very different technology- before new algorithms are certified and replace the old ones. This is a compelling argument that would allow the deployment of QKD now, without the need to wait for long certification processes.

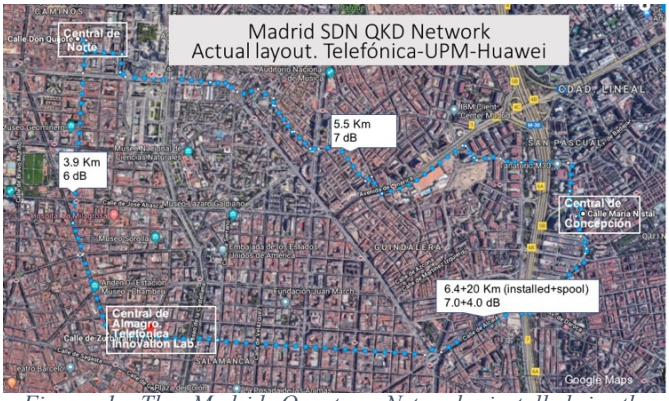

Figure 1: The Madrid Quantum Network, installed in the production facilities of Telefonica Spain. Distances and losses among the three main nodes are given in the white boxes.

The overall system was integrated in a production level network, owned by Telefonica of Spain, in downtown Madrid (see Fig. 1). In this network we implemented several use cases, demonstrating real world applications and also tested some critical aspects of QKD performance such as quantum-classical co-propagation or architecture integration. It is to be noted that the SDN paradigm, as all paradigms based on softwarization, brings new security challenges that can be mitigated by QKD. This means that securing the network itself as a critical infrastructure is also a valuable use case for this technology. In the particular case of an SDN network, current QKD technology fits particularly well since one of its shortcomings -the limited reach- is less of a problem since SDN nodes are in secure locations that are usually relatively nearby. The use cases tested fit in the following families of applications [3-5]:

- Data plane security: End to end data encryption of the data flow in the network.
- Control plane security: Security protocols for the control and management of the network.
- Network Function Virtualization: Securing the creation and operation of virtualized services.
- Novel Services: Ordered Proof of Transit, to check the packet flows for security and attestation.

Moreover, the functionality of the physical layer operation was also tested. The quantum-classical channel co-propagation with up to seventeen co-propagating mixed (1 – 100G and 16 – 10G) channels was demonstrated in the same communications band without preventing adequate QKD operation. Switching capabilities (the ability to use one transmitter with two receivers in different locations) and a useful key generation rate (that would reach between 40 and 70 kbps with highly optimized but realistic post-processing) have been shown.

The main result of this demonstration was to show that a quantum-classical network, with a unified logical and physical infrastructure is a real possibility when the integration technologies are chosen carefully and appropriately adapted. This network shows that a broad implementation of quantum communications to enhance current telecommunications networks with real world applications is possible already with current technologies.

Supported by FET QT-Flagship, EU H2020 grant agreement 820466 CiViQ: Continuous Variable Quantum Communications, and the Spanish Ministry of Economy MINECO/FEDER, CVQuCo, TEC2015-70406-R

[1] V. Martin et al. "The Madrid SDN-QKD Network" presented at Qcrypt 2018. A long write up will be published elsewhere.
[2] H. H. Brunner et al. "A low-complexity heterodyne CV-QKD architecture," in ICTON 2017. IEEE, Jul. 2017.
[3] A. Aguado, et al. "Hybrid Conventional and Quantum Security for Software Defined and Virtualized Networks", in JOCN 9, 819-825 (2017).
[4] A. Aguado, et al., "Quantum Technologies in Support for 5G services: Ordered Proof-of-Transit", submitted to ECOC 2019.
[5] A. Aguado, et al. "VNF Deployment and Service Automation to Provide End-to-End Quantum Encryption," JOCN 10, 421 (2018)