Deployed QKD Networks in Europe

Hannes Hübel[(1)], Florian Kutschera[(1)], Christoph Pacher[(1,2)], Martin Achleitner[(1)], Werner Strasser[(2)], Francesco Vedovato[(3)], Edoardo Rossi[(3)], Francesco Picciariello[(3)], Giuseppe Vallone[(3)], Paolo Villoresi[(3)], Luca Calderaro[(4)], Vicente Martín[(5)], Juan Pedro Brito[(5)], Laura Ortíz[(5)], Diego Lopez[(6)], Antonio Pastor-Perales[(6)], Marc Geitz[(7)], Ralf-Peter Braun[(7)] and Piotr Rydlichowski[(8)]

[1)]AIT Austrian Institute of Technology, Center for Digital Safety&Security / Security & Communication Technologies, 1210 Vienna, Austria.
[2)] fragmentiX Storage Solutions GmbH, IST Austria Technologiepark, Plöcking 1, 3400 Klosterneuburg, Austria.
[3)] Dipartimento di Ingegneria dell'Informazione, Universita degli Studi di Padova, via Gradenigo 6B, 35131 Padova, Italy
[4)] ThinkQuantum srl, via della Tecnica 85, 36030 Sarcedo, Italy.
[5)] Center for Computational Simulation and ETSI Informáticos, Univ. Politécnica de Madrid, Boadilla del Monte, Madrid, Spain.
[6)] Telefonica I+D, Ronda de la Comunicación s/n, Madrid, Spain.
[7)] T-Labs, Winterfeldtstrasse 21, 10781 Berlin, Germany.
[8)] Poznan Supercomputing and Networking Center, ul. Jana Pawła II 10, 61-139 Poznan, Poland
Author e-mail address: hannes.huebel@ait.ac.at

Abstract: We report several use-case demonstrations for quantum key distribution in deployed fiber networks. The tests were carried out under real world conditions at the end-user premises using commercial QKD systems.

1. Introduction

Quantum key distribution (QKD) offers information-theoretically secure communications, even in a post-quantum world where powerful quantum computers are a reality. Since most of our current public key infrastructure would be rendered obsolete in such a scenario, the shift to quantum-safe encryption must start now. The technological development of QKD has made extensive progress in the last two decades, culminating in technologically mature systems, that are offered commercially by an ever-increasing eco system. The evolution of single point-to-point links to large QKD networks has mirrored this trend, starting form the first proof-of-principle QKD networks [1] to impressive technology demonstrations that span over large countries and even offer intercontinental QKD links via satellite [2]. Despite this tremendous technological advance, QKD has failed so far to secure a foothold in the communications market. It is therefore paramount to showcase the technology to potential end-users, highlight its security advantages and demonstrate its ease of use when it comes to actual deployments and operations. We report here recent developments of QKD test networks in Europe. The focus of those demonstrations was to implement real-world use-cases and work as closely as possible with the end-users of the technology to understand better the user expectations as well as identify potential roadblocks for larger QKD rollouts.

2. The Vienna QKD Network

The QKD network in Vienna aimed at securely linking governmental buildings and other public institutions. The network itself consisted of 10 locations: 5 public institution, 2 internet exchanges, the University of Vienna, AIT, and another office building, as shown in Fig. 1a. A total of 23 fiber pairs, ranging from 4 to 28 km, were deployed by a commercial optical-fiber supplier. Losses in the optical fibers amounted to between 1.5 and 8.5 dB (0.3 dB/km on average). For the demonstrations a total of 7 QKD links from IDQ and ThinkQuantum were installed in the network. Each link was complemented by a 10-Gbit AES encryptor from ADVA, which was provisioned with keys via a standardized interface by the corresponding QKD system. The QKD systems were each connected via a dark fiber, while the second fiber carried the QKD-management channel, the AES encrypted data and all other classical traffic needed for monitoring and managing the network. The secure key rate achieved in the various links was on average between 1800 bit/s and 650 bit/s during the continuous 4-month long operation. Besides the standard AES data encryption between federal ministries, which was secured by QKD, a secret-sharing demonstration was also performed in the Vienna QKD network. For this, three locations were linked via QKD, AES encryption and Secret-Sharing appliances (provided by fragmentiX). While QKD was securing the data between the ministries during the transit, the secret-sharing application, providing information-theoretic security, securely stored the data by splitting it into fragments. Retrieval of the data is also permitted for other parties in the network as long as they are running the same Secret-Sharing appliances. To demonstrate the possible inclusion of locations that cannot be connected directly to an inner-city fiber network, we demonstrated an intermodal QKD transmission combining a 200 m long free-space channel (10 dB) with a 4 km long fiber channel (5 dB loss). The transmitter part of the ThinkQuantum QKD system operating at 1550nm was deployed together with a transmitter telescope by UniPD in an office building across the street from AIT. The QKD signal was transmitted in free-space to AIT where the receiver telescope, also by UniPD, was installed and then coupled into a single mode fiber which was connected to a different location in the Vienna QKD network where the ThinkQuantum QKD receiver was located. A secure key rate of 600 bit/s was achieved over the intermodal channel under daylight conditions and also under the rain. The QKD key was then used as an input for an AES encrypted video link between the transmitter and receiver locations.

3. The Madrid QKD Network

The Madrid QKD network is the last development in a line of testbeds started in 2009. During these years several technologies have been demonstrated, all of them pivoting around the integration of QKD in telecommunications networks. Starting from pilots to use QKD in PON access networks and CWDM metropolitan core networks, the development of QKD-only multiplexed networks (Quantum channels and classical key distillation sharing the same infrastructure) and field demonstration of Software Defined networking [3], SDN-QKD quantum and classical integrated optical network using production facilities of Telefónica, the current network is built out of the OpenQKD project [4 The network is fully deployed in the field (Fig. 1b) sharing infrastructure with two production networks: 3 production sites of Telefónica and 6 production sites of RedIMadrid, hosting up to 4 QKD devices per node. This network is fully operational, providing commercial-level classical services to its customers with very strict Service Level Agreements. A border node is set to connect both networks. Nodes distances range from 1.5km -in the border node- up to about 33km and secret key rate varies from 3kbps to over 1Mbps. The emphasis is to demonstrate a tight operational integration of a QKD network and a conventional telecommunications network at both, the optical and security levels. 24 systems (emitters and receivers) from three different manufacturers using a variety of technologies (discrete variables (DV) and continuous variables (CV) systems using several quantum protocols) are integrated using standard optical transport systems, programmable optical switches, and optical add and drop modules, with the classical communications. This is done using a mixture of techniques, CV for classical and quantum communications in the same band (C-band) or using the O-band for the quantum channel and the C for the classical in other segments. Other possibilities have been also used, since only a pair of fiber strands is available to connect the whole infrastructure and the emphasis was in researching how to add quantum capabilities to a running optical network. Several systems have been running for three years (the CV ones), while others were installed just during the last three months. The whole infrastructure is controlled using SDN technology, that can also manage the optical switches, so that the network is dynamical, with the capability to by-pass some nodes without dropping the quantum channel. The SDN controller keeps a global view of the network, managing the optical paths (switching allows for over 60 possible direct quantum paths) and controlling the keys that are stored at each node, providing this information to the Key Management System so that a key can be shared between any two nodes in the network, independently of the QKD system installed. The keys can be fed to a variety of encryptors working at Level 1, 2 and 3, so that a large variety of use-cases can be executed. These range from critical infrastructure protection to 5G applications and cover about 50 different metrics: latencies, number of concurrent applications, throughput, etc.

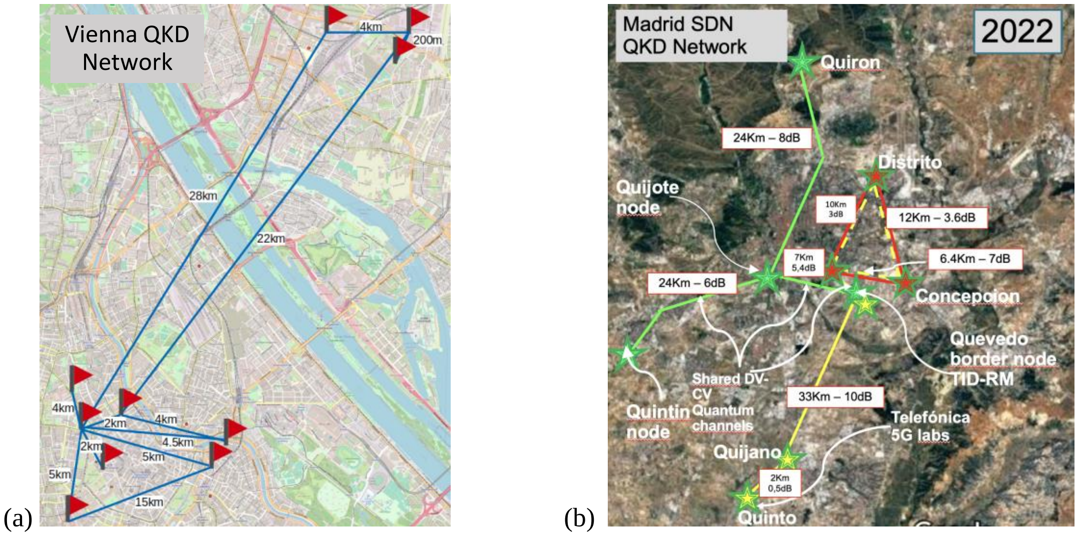

Fig. 1. (a) Layout of the Vienna QKD network, the free-space link is in the right upper corner. (b) Madrid SDN QKD network. A Metropolitan quantum infrastructure deployed together with a classical optical network from two providers (Telefónica -red- and RedIMadrid green and yellow) in production, providing commercial connectivity services to customers.

4. The QKD Testbed in Berlin

The Berlin Testbed is operated by Deutsche Telekom and is built upon a metropolitan research network in the city of Berlin. The interest of DT was to prove the integrability of QKD technology into fiber networks of a telecom's provider, comprising the physical quantum layer based on glass fiber, a key management layer including a Key Management System (KMS) and Secure Key Storage (SKS) and finally an application layer with hardware and software encryptors (see Fig. 2a). Exchanged QKD keys were exported into the SKS for secure storage and single point of truth for cryptographic artifacts. Applications and encryptors retrieved the encryption keys from the SKS using the ETSI QKD 0014 API and thus could establish a secure communication channel. The secure transmission of data (movies or files) as well as a quantum secure "voice, video & chat" application has been demonstrated.

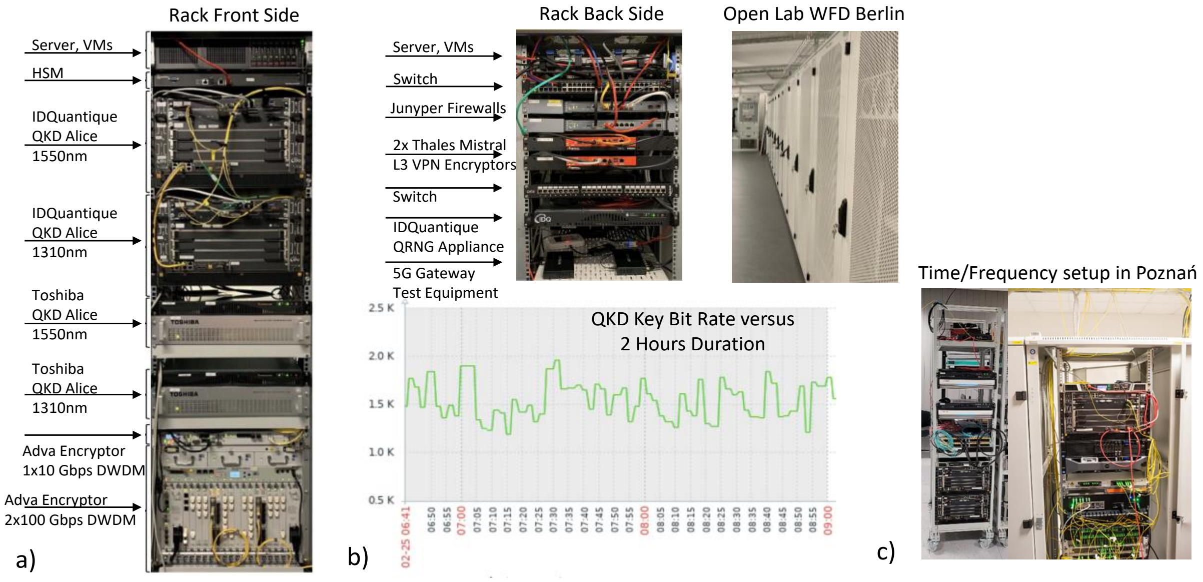

Fig.2: (a) the Berlin QKD Testbed with QKD equipment by IDQ and Toshiba in the 1310nm and 1550nm band, a KMS server, a Hardware Security Module by Gemalto and hardware encryptors by Adva Optical and Thales. (b) the QKD Key Rate of 1.5kBit/s, Quantum Bit Error Rate (QBER) of 3% and QKD Visibility of an IDQ QKD channel of 97%. (c) Setup for cross-border QKD tests, including T&F services.

Next to QKD, the testbed implemented a key exchange mechanism secured by Post Quantum Cryptography (PQC) and extended the key exchange platform to 5G networks and mobile clients. The rate of the PQC key exchange proved to be compatible to the QKD key exchange rate. Wherever possible, the protocols implemented by the stack, for example the ETSI QKD 0014 API or the QKD key forwarding process, have been strengthened by PQC to add another layer of security and harden the key exchange installation.

5. The QKD testbed in Poznań

The PSNC testbed was built based on the POZMAN and PIONIER network infrastructure. PSNC as owner and operator of Polish Research and Education Network – PIONIER used this infrastructure and also its own local Metro Area Network in Poznań – POZMAN to implement a QKD testbed and associated use-cases. The long distance QDK link use-cases were implemented in the PIONIER backbone and metro area QKD links were implemented in POZMAN network. Long distance QKD use-cases were related to inter data center links (cross-border QKD link to VSB in Ostrava, Czech Republic) and coexistence trials with reference time and frequency (T&F) distribution infrastructure achieving secure key rates of 1600 bit/s. Fig. 2c presents the scheme for these activities. Use-cases related to local metro links in Poznań and POZMAN network are focused mainly on collaboration with partners and City Hall services. These use-cases present how the QKD infrastructure can be integrated with HPC and public services in existing infrastructures.

Acknowledgement: This work was supported by the ERC under the EU Horizon-2020 programme (grant agreement No 857156).

6. References

[1] M. Peev et al., "The SECOQC quantum key distribution network in Vienna", New J. Phys. Vol. 11, p. 075001, 2009.
[2] Y.A. Chen et al., "An integrated space-to-ground quantum communication network over 4,600 kilometres," Nature vol. 589, p. 214, 2021.
[3] A. Aguado et al., "The Engineering of Software-Defined Quantum Key Distribution Networks," IEEE/Communications Magazine, vol. 57, no. 7, pp. 20-26, 2019.
[4] Open European Quantum Key Distribution Testbed, see: https://openqkd.eu/