


Brief Report

Demonstration of Software Defined Network Services Utilizing Quantum Key Distribution Fully Integrated with Standard Telecommunication Network

Diego R. Lopez ^{1,*}, Vicente Martin ^{2,*}, Victor Lopez ¹, Fernando de la Iglesia ¹, Antonio Pastor ¹, Hans Brunner ³, Alejandro Aguado ², Stefano Bettelli ³, Fred Fung ³, David Hillerkuss ³, Lucian Comandar ³, Dawei Wang ⁴, Andreas Poppe ³, Juan P. Brito ², Pedro J. Salas ² and Momtchil Peev ³

¹ Telefónica Investigación y Desarrollo, Ronda de la Comunicacion s/n, 28050 Madrid, Spain; victor.lopezalvarez@telefonica.com (V.L.); fernando.delaiglesiamedina@telefonica.com (F.d.I.I.); antonio.pastorperales@telefonica.com (A.P.)

² Center for Computational Simulation and ETSI Informáticos, Universidad Politécnica de Madrid (UPM), 28660 Madrid, Spain; a.aguado@fi.upm.es (A.A.); juanpedro.brito@upm.es (J.P.B.); psalas@etsit.upm.es (P.J.S.)

³ European Research Center, Huawei Technologies Duesseldorf GmbH (HWDU), MRC, Riesstrasse 25, 80992 München, Germany; hans.brunner@huawei.com (H.B.); stefano.bettelli@huawei.com (S.B.); fred.fung@huawei.com (F.F.); david.hillerkuss@huawei.com (D.H.); lucian.comandar@huawei.com (L.C.); Andreas.Poppe@ait.ac.at (A.P.); momtchil.peev@huawei.com (M.P.)

⁴ School of Electronics and Information Technology, Sun Yat-sen University, Guangzhou 510275, China; dw.wang@huawei.com

* Correspondence: diego.r.lopez@telefonica.com (D.R.L.); Vicente.Martin@upm.es (V.M.); Tel.: +34-682-051-091 (D.R.L.)

Academic Editors: Michel Planat and Antonio Manzalini

Received: 4 July 2020; Accepted: 19 August 2020; Published: 3 September 2020



Abstract: We present a demonstration of software defined networking (SDN) services utilizing quantum key distribution (QKD) technology, fully integrated with standard telecommunication network connecting production facilities of Telefonica in Madrid. All communications “co-propagate” over the same fiber infrastructure.

Keywords: quantum optics; quantum communications; quantum cryptography

1. Introduction

Quantum key distribution (QKD) [1,2] is a method for distant key generation employing quantum principles. The latter allow the unprecedented security of the generated key material. This is certainly quantum safe (i.e., the key generation method cannot be broken by prospective quantum computers) [3] in contrast to the presently used computational methods to this end. Its security is independent of the computational power of the attacker and can in principle reach the level of Information Theoretic Security (ITS) [2]. It is, however, theoretically impossible that due to exponential decay with distance, QKD cannot generate a reasonable amount of key material if channel losses exceed 25 to 30 dB (something like 120 to 150 km with state-of-the-art optical fibers and non-forbiddingly demanding technology).

In principle, it is possible to build quantum repeaters [4]: devices that can transmit quantum states over long distances without actually measuring them, and thus preserve the no-cloning principle on which the security of QKD is based [2]. Although proofs of concept for these quantum repeaters performed, these devices are still far away in the future. For this reason, since a long time, there

have been attempts to eliminate the distance restriction by designing and implementing so called “QKD networks” [5,6]. In the absence of quantum repeaters, the developers of QKD networks have resorted to hops over trusted stations, known as trusted repeater QKD networks, where the key is revealed and forwarded at each trusted station. The initial interpretation of QKD networks was that of infrastructures for ITS key delivery, (at least logically) decoupled from the telecommunication network. This leads to the idea of parallel communication infrastructures that have to be developed just to enhance the security of communication. A major objective, with a potentially broad economic impact, is to enable QKD utilization without building parallel physical infrastructures by finding ways to integrate QKD in communication networks, increasing their security without the absolute requirement of delivering end-to-end ITS key, as long as trust on the intermediary nodes is assumed.

Simultaneously, until recently the traditional telecommunications network realizations have not been very inviting to integrate QKD within them. Highly specialized and essentially autonomous devices, proprietary to the level of interfaces and not easy to reconfigure, these devices were not designed to extend their functionality beyond what was originally foreseen. For this reason, in analogy to modern computing trends, the software defined networking (SDN) paradigm has emerged to intrinsically increase the flexibility of communication networks. The SDN approach, in contrast to the traditional one, introduces a centralized network controller, which creates on demand a dedicated virtual infrastructure out of general purpose but programmable resources. Using standard interfaces, optical paths are established, wavelength planning is carried out and in general, any networking functionality is realized on a flexible, programmable environment, allowing a quick adaptation to new requirements. SDN is now a major trend in telecommunication, deployed by many operators. Here, we address the adoption of SDN methods also in practical QKD networking.

2. Materials and Methods

We put together continuous variable QKD (CV-QKD) devices by Huawei Technologies Duesseldorf GmbH (HWDU), Munich Research Center, and SDN implementations by UPM and Telefonica on a production-level optical fiber infrastructure of Telefonica to demonstrate, for the first time, an operational software defined QKD network (SDQKDN) realization. The first demonstration took place between May and September 2018 in downtown Madrid, using three production sites of Telefonica Spain, forming a triangle of roughly 15 Km perimeter. Figure 1 illustrates the location of the different nodes, including distances and measured attenuations, over a satellite image of the Madrid area where they were located.



Figure 1. Physical topology of the three nodes used in the reported demonstrator.

The deployment included several innovations on the software front, using standard interfaces, creating a system to automatize the integration of QKD devices in the network and creating the SDQKDN control mechanisms needed to manage the classical and quantum parts of the network as a single entity. On the hardware front, the QKD systems were made more compact, with increased performance and flexibility, to allow further characteristics (like the directional switching of the quantum channel) to be managed from the controller. Resiliency to the noise of copropagating classical channels was also improved.

3. Results

The advantage of the SDN approach for QKD is that QKD equipment can in principle be seamlessly integrated into an SDN by appropriate extensions, into a SDQKDN. Naturally, QKD devices need to exhibit a certain degree of flexibility in order to allow for such an integration. They must: (i) be equipped with interfaces that can interpret and respond to the network controller commands, and (ii) be able to react correspondingly to these controller commands, at least in a minimal way. An optimal flexibility would be reached if the devices would be able to: start and stop key generation with minimal latency, after receiving a corresponding command; if different senders and receivers could seamlessly couple/decouple one with the other also after minimal transition periods; if data communication and QKD optical transmission could coexist in parallel over the same optical fiber, and; finally if QKD senders/receivers could change their transmission/reception wavelength on demand. It is worth noting that all these QKD properties are not strictly necessary, their absence implying only a restricted degree of overall flexibility and an increased cost of creating a QKD service in existing networks. Currently, a particular type of the QKD technology, the CV-QKD approach, is the most flexible in the sense discussed above and therefore most appropriate for SDQKDN realizations.

3.1. The QKD Devices Developed by HWDU

The CV-QKD development by HWDU (shown in Figure 2) is a particularly advanced CV-QKD prototype, being both robust and flexible by design, in the sense mentioned above. HWDU provided three devices—one sender and two receivers. Each device is equipped with a 3U QKD optical box (the units with a screen on the photo below), a 1U server (Supermicro Super Server 1028R), with 2 Intel(R) Xeon(R) CPU E5-2650 v4 @ 2.20GHz—processors 12-core hyperthreading (middle) and standard telecom equipment (Huawei OptiX OSN1800 Optical Transport Network platform), each housing an AES encryption/decryption card (TNF1LTX) with modified firmware to accept the external keying from QKD devices in addition to the default internal Diffie–Hellman based mechanism.

The CV-QKD systems operate using the traditional Gaussian modulation, single polarization, at a relatively low clock rate of 12.5 MHz. The advanced local–local oscillator (LLO) approach, using a pilot tone [7], was implemented. The devices allow the co-propagation of light in the same optical band (the C-Band) of 8 to 10 dBm. The operation is extremely stable (during long periods of time), as the system assesses online all noise sources and thus reduces noise-fluctuation vulnerabilities. All transmitted signals are successfully processed online using the server for DSP and post-processing. The key generation rate reaches of 2 to 3 kb/s at 12 dB channel attenuation. Moreover, using an optical switch, the sender can redirect operation from one receiver to the other with a pretty low switching time of only 10–15 s after disconnecting of the first link. All devices were mounted on flight boxes and operated straight after delivery and later in the harsh and restricted environment of the production facilities.

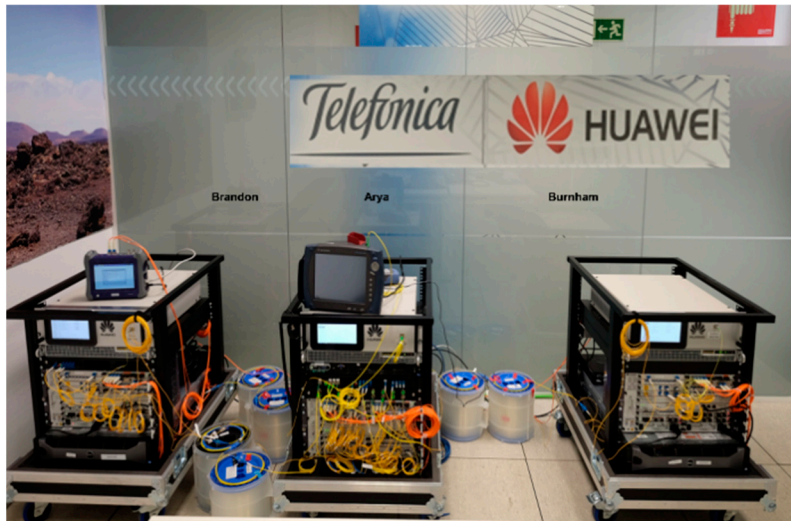


Figure 2. Three quantum key distribution (QKD) devices by HWDU in the Telefonica Lab in Madrid, one sender (“Arya”) and two receivers (“Burnham” and “Brandon”).

3.2. SDN Implementation

A rough sketch of the SDN topology (following the approach of [8]) of the three nodes is given in Figure 3 below.

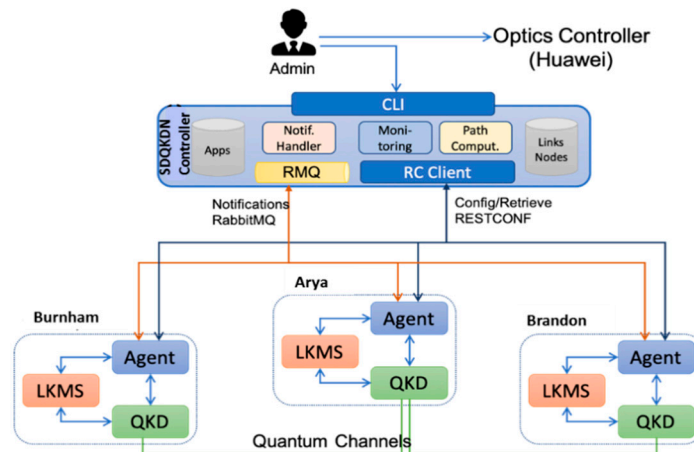


Figure 3. Basic software defined networking (SDN) topology of the software defined QKD network (SDQKDN) using the 3 QKD devices collocated with SDN nodes, controlled by a SDQKDN controller.

The design logically positions each QKD device in a SDQKDN node, which comprises a SDQKDN agent and a local key management store (LKMS). The LKMS stores key material, as pushed by QKD. The agent interacts with the central SDQKDN controller and both ensure key routing over the full network and key availability announcement and subsequent retrieval to applications. Secure applications are collocated with the respective secure nodes and directly interact with the LKMS. Hop-by-hop key forwarding can also be performed, if required, by the LKMS and the QKD device (set in a relay mode), acting as a trusted station. In general, the nodes must be trusted, in contrast to the controller, accessed by the system administrator through a Command Line Interface (CLI). It is important to stress that the controller never gets hold of any key material, private or critical data. Thus, a failure or malicious operation cannot contribute to a security breach but at most to a Denial of Service (DoS) attack. Trusting the node SDQKDN agent is a security design choice. Not including the controller in the QKD security perimeter ensures the scalability in spite of the relatively short range of QKD: trusting the controller and some of its communications with the agents might be sometimes desirable, but then a mechanism

alternative to QKD, such as e.g., post-quantum crypto [8], well suited for non-regular and short-term secure communication, might be considered.

For demonstration of simplicity, all the SDN software was deployed on isolated virtual machines on the mentioned HWDU device servers. A classical communication networks was established seamlessly using the intrinsic functionalities of the OSN 1800 Optical Transport Network (OTN) platform. Moreover, whenever block-cipher encryption for secure data transport is being used, the built-in Advanced Encryption Standard (AES) encryption/decryption cards are employed.

4. Discussion

The QKD devices were first installed in the Future Technologies laboratory in Telefonica Research premises, where the testing and installation of the mentioned SDN software implementation in the device servers took place. Subsequently the devices were distributed to three production facilities used by Telefonica of Spain for the commercial service provision in the Madrid metropolitan area [9]. To be more precise, dedicated dark fibers were provided, connecting these facilities, operating a full-scale network over these. Due to standard security procedures for the operators, neither the HWDU team nor the collaborating UPM and Telefonica teams were allowed to deploy the devices, and certified subcontractors of Telefonica with no experience in QKD did the installation following the same procedures as that used for the standard network equipment. This is important to demonstrate the maturity of the development. The deployment was carried out in a single day, the control over the QKD devices and SDQKDN nodes configured, and the full-scale operation of the network initiated. The network was running continuously during three months without experiencing any major issue. Only a single instance of a power outage took the network down, but functionality was automatically restored. The QKD devices resumed normal operation after a standard recalibration procedure, like the ones used to keep the performance of the systems at an optimal level. Actually, recalibration is run periodically as part of automatic maintenance procedures.

The SDQKDN was used to demonstrate Network Function Virtualization (NFV) and data-center-based protection of the SDN and NFV control and data planes [7], and novel (ordered) proof of transit (OPoT/PoT) service provision protocols [10]. It will be used on a set of new use-cases, mainly devoted to secure the control and data planes of the network as a critical infrastructure, in an enlarged testbed starting in the fourth quarter of 2020. The testbed is now composed not only of the existing quantum ring, but also part of the RediMadrid network. This network is a production network providing connectivity to the universities and research centers in the Madrid region, under strict service level agreements (SLA) for the classical communications. The limited resources of the network, with only two strands of fiber connecting the nodes, forced the quantum and classical channels to share the same fiber adding complexity to the deployment and run-time. With the experience gained in this first deployment, we plan to demonstrate a new generation of QKD devices and new integration patterns supporting more complex use-cases on the enlarged testbed, such as the ones designed to increase the security in 5G B2B networks, showcasing the maturity of the technology in the real-world.

Moreover, the functionality of the physical layer operation was also tested. The quantum-classical channel co-propagation with up to seventeen co-propagating mixed (1–100 G and 16–10 G) channels was demonstrated in the same communications band without preventing adequate QKD operation. Switching capabilities, with the ability to use one transmitter with two receivers in different locations at a useful key generation rate (see above) were verified as well.

5. Conclusions

The Madrid SDQKDN network has demonstrated for the first time a full-scale integration of QKD technology in SDN environments in real-world production environments. It paves the way for future product-level implementations of SDQKDN as an emerging technology.

Author Contributions: D.R.L., V.L., F.d.I.I. and A.P. (Antonio Pastor); SDN elements and integration with fiber infrastructure, V.M., A.A., J.P.B. and P.J.S.; SDN elements and crypto interfaces. H.B., S.B., F.F., D.H., L.C., D.W.,

A.P. (Andreas Poppe) and M.P.; CV-QKD device concept and development. All authors have read and agreed to the published version of the manuscript.

Funding: This research was partially supported by EU's Horizon 2020. Flagship on Quantum Technologies, Grant Agr. No 820466: "Continuous Variable Quantum Communications" (CiViQ).

Conflicts of Interest: The authors declare no conflict of interest.

References

1. Scarani, V.; Bechmann-Pasquinucci, H.; Cerf, N.J.; Dušek, M.; Lütkenhaus, N.; Peev, M. The security of practical quantum key distribution. *Rev. Mod. Phys.* **2009**, *81*, 1301. [[CrossRef](#)]
2. Pirandola, S.; Andersen, U.; Banchi, L.; Berta, M.; Bunandar, D.; Colbeck, R.; Englund, D.; Gehring, T.; Lupo, C.; Ottaviani, C.; et al. Advances in Quantum Cryptography. Available online: <https://www.osapublishing.org/aop/abstract.cfm?doi=10.1364/AOP.361502> (accessed on 18 July 2020).
3. See e.g., QSC Workshops by ETSI. Available online: <https://www.etsi.org/technologies/quantum-safe-cryptography> (accessed on 18 July 2020).
4. Briegel, H.-J.; Dür, W.; Cirac, J.I.; Zoller, P. Quantum Repeaters: The Role of Imperfect Local Operations in Quantum Communication. *Phys. Rev. Lett.* **1998**, *81*, 5932. [[CrossRef](#)]
5. Peev, M.; Pacher, C.; Alléaume, R.; Barreiro, C. The SECOQC quantum key distribution network in Vienna. *New J. Phys.* **2009**, *11*, 075001. [[CrossRef](#)]
6. Sasaki, M.; Fujiwara, M.; Ishizuka, H.; Klaus, W.; Wakui, K.; Takeoka, M.; Tanaka, A.; Yoshino, K.; Nambu, Y.; Takahashi, S.; et al. Field test of quantum key distribution in the Tokyo QKD Network. *Opt. Express* **2011**, *19*, 10387. [[CrossRef](#)] [[PubMed](#)]
7. Wang, T.; Huang, P.; Zhou, Y.M.; Liu, W.Q.; Ma, H.X.; Wang, S.Y.; Zeng, G.H. High key rate continuous-variable quantum key distribution with a real local oscillator. *Opt. Express* **2018**, *26*, 2794. [[CrossRef](#)] [[PubMed](#)]
8. Aguado, A.; Lopez, V.; Martinez-Mateo, J.; Szyrkowiec, T.; Autenrieth, A.; Peev, M.; Lopez, D.; Martin, V. Hybrid Conventional and Quantum Security for Software Defined and Virtualized Networks. *JOCN* **2017**, *9*, 819. [[CrossRef](#)]
9. Aguado, A.; Lopez, V.; Lopez, D.; Peev, M.; Poppe, A.; Pastor, A.; Folgue, J.; Martin, V. The Engineering of a SDN Quantum Key Distribution Network. *IEEE Commun. Mag.* **2019**, *57*, 20–26. [[CrossRef](#)]
10. Aguado, A.; López, V.; Brito, J.P.; Pastor, A.; López, D.R.; Martin, V. Quantum cryptography networks in support of path verification in service function chains. *IEEE/OSA J. Opt. Commun. Netw.* **2020**, *12*, B9–B19. [[CrossRef](#)]



© 2020 by the authors. Licensee MDPI, Basel, Switzerland. This article is an open access article distributed under the terms and conditions of the Creative Commons Attribution (CC BY) license (<http://creativecommons.org/licenses/by/4.0/>).