Enabling Quantum Key Distribution Networks via Software-Defined Networking

Alejandro Aguado
Center for Computational Simulation
Universidad Politécnica de Madrid
Madrid, Spain
a.aguadom@fi.upm.es

Victor López
Telefónica I+D/GCTIO
Madrid, Spain
victor.lopezalvarez@telefonica.com

Juan Pedro Brito
Center for Computational Simulation
Universidad Politécnica de Madrid
Madrid, Spain
juanpedro.brito@upm.es

Antonio Pastor
Telefónica I+D/GCTIO
Madrid, Spain
antonio.pastorperales@telefonica.com

Diego R. López
Telefónica I+D/GCTIO
Madrid, Spain
diego.r.lopez@telefonica.com

Vicente Martin
Center for Computational Simulation
and DLSIIS ETSI Informáticos
Universidad Politécnica de Madrid
Madrid, Spain
vicente@fi.upm.es

***Abstract*—Quantum Key Distribution (QKD) is one of the major cryptographic solutions to tackle the security threats associated to future computational advances, in particular those coming from quantum computing. At the most simple level, QKD can be seen as a highly secure source of symmetric secret keys in two separated places. Nonetheless, the lack of standardization and the strong requirements from the physical layer makes this technology very difficult to integrate in existing infrastructure.**

However, the success of QKD networks radically depends on the degree in which they can be adopted in the existing infrastructure, and it is a must that it happens via standard protocols and interfaces. The flexibility of novel network paradigms, like Software-Defined Networking (SDN), allows for a faster adoption of new concepts, hardware and services in telecommunications networks. This paradigm can be used for quantum communications, allowing for a fast and scalable deployment of quantum technologies and services in the telecommunications network to a degree that was simply impossible in previous schemes, where the different network devices and their connections should be modified, one by one, to create a quantum communications channel.

This tutorial provides an introduction to existing QKD technologies and networks, followed by a descriptive explanation on how SDN principles can be utilized to abstract and integrate QKD systems as part of the network management. This will help to reduce the time-to-market for quantum technologies, and also will make quantum cryptography available as a service to be capitalized by the network operators.

***Index Terms*—Quantum Key Distribution, Software-Defined Networking**

I. Introduction

Quantum cryptography [1] most prominent and mature result is Quantum Key Distribution [2] (QKD). QKD can be viewed as two synchronized sources of random bit streams located in two separated places with the additional property that no information about the bit stream is leaked outside of the two participants. This is actually a way to solve the problem of secret key distribution. This is independent of any computational process, as it relies on the laws of physics rather than in any computational complexity assumption. Thus, it allows to tackle the security threats associated to any type of computational advances, like those coming from quantum computing developments. Therefore, QKD is considered an Information-Theoretic Secure (ITS) cryptographic primitive: it is immune to any attack, independently of the computational power that the eavesdropper might have, thus QKD can be regarded as a base for a quantum-safe communications infrastructure.

This advantage comes at a price, since QKD is a physical layer technology that depends on the ability to produce, manipulate, transmit and detect signals at the quantum level. QKD systems are designed as black-boxes that require a separate ad-hoc network. This is the easier route to transmit the quantum signals and avoid any interference from the many orders of magnitude stronger classical signals ($\sim 10^8$). Such interferences would kill the delicate correlations encoded in the quantum signals that make possible the creation of secret keys in two remote locations. The longer distances achieved for QKD transmission are usually obtained in laboratory experiments, with technologies and components that are difficult to build, deploy and maintain in an operational environment. Quantum channels have been demonstrated in distances of around 300 kms [3] while full QKD links in distances slightly below (between 250 and 300 kms) [4]. Newer schemes allow for even larger distances [5], [6] that even surpasses previous limits [7]. The current commercial readiness of such deployments is close to null, commonly using very low-loss components and other unusual devices (as, for example superconducting detectors), although this is expected to improve with time. Measured in attenuations, systems can work in a reasonable manner (generating, at least few kbps) with losses up to 30dB for the close to commercial systems, with promises of doubling this figure for the new experimental ones mentioned above. Obviously any type of active component in the quantum signals path, such as optical

978-3-903176-21-8 (c) 2020 IFIP

amplifiers, must be avoided, since this would kill the quantum correlations on which this technology is based.

The result of such restrictive requirements and lack of flexibility is that current QKD systems cannot be easily integrated into telecommunications networks, being these networks the only way to push forward QKD technologies for common communication services. Software-Defined Networking (SDN) [8] allows new services and systems to be seamlessly integrated in telecommunications networks by using common practices and standard protocols and interfaces from the networking field. The success of QKD networks radically depends on the extent to which they can be adopted in the existing infrastructure, so it is a must that it happens via standard procedures. The flexibility brought by SDN allows the integration of quantum communications in the telecommunications network to a degree that was simply impossible in previous schemes, where the different network devices should be modified, one by one, to create a quantum channel.

This tutorial is distributed as follows: first we describe the main concepts of QKD networking; secondly, we ellaborate on the different logical layers that compose a QKD network; then, we provide an overview of a QKD network that is being deployed in the city of Madrid; after that, we go through the main use cases that are an added value for operators to deploy QKD networks. We finalize the work with conclusions and future work.

II. QKD Networks

The first QKD Networks date back to 2004, when the DARPA network [9] was built. It was a proof of concept network using dark fibre to link several laboratories in Boston, where QKD devices were being developed. It later was upgraded to include a free space link. In 2008 the SECOQC [10] network was built in Vienna, somewhat larger, it already included several companies among the equipment manufacturers. Here a full protocol stack was developed [11]. The Tokyo network [12], linking several universities, companies and national laboratories started in 2010 and it has been maintained over time till today. A large network was built in China in 2017 [17], linking Shanghai with Pekin through about 50 intermediate trusted nodes spanning a distance of 2000 Km. Other network prototypes, with different objectives have been also built over time. In 2009 a network was built in Switzerland [16] to demonstrate technological maturity by running non-stop during 9 months. At the same time, a metopolitan area network prototype was built in Madrid to demonstrate integration in core and PON access networks [13]. It later evolved to demonstrate a pure quantum services network without trusted nodes in a metro area [14] and also to distribute entanglement [15] –the quantum resource par excellence–. More recently, we have demonstrated the first QKD network linking production facilities and based on SDN principles [20]. A much enlarged version has become the Madrid Quantum Network, one of the four large nodes in the recently EU project OpenQKD devoted to the creation of a European-wide quantum network infrastructure, that we will speak about later. Other relevant efforts include the Quantum Communications Hub in UK [18] and an attemp to a wide-area commercial QKD network in the USA [19].

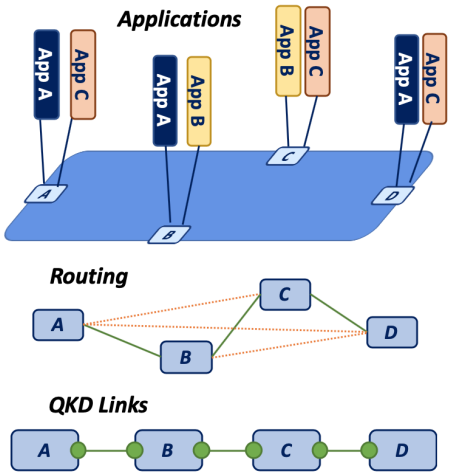

Fig. 1. High level representation of a QKD network using three planes, including physical links (quantum forwarding plane), routing (embedded in the control and management plane) and applications (Application plane).

III. QKD Network Planes

Despite of the various approaches followed for their implementation, we can broadly describe a QKD network using several planes, as depicted in Fig. 1, where we have depicted those more important for the topic of this tutorial (it is typical in other representation to show a key management plane, that here we embed as part of the Application plane for simplicity). Note that some authors refer to these planes as layers, in similitude to IP or OSI layers, although here they obviously do not follow the original ideas, lacking the proccess of adding and stripping headers as the packets travel the hierarchy. We prefer here to follow the typical SDN approach using planes, which better reflects the QKD network structure. The first one is composed by the physical QKD links. This is the quantum forwarding plane, where the actual implementation of a QKD protocol is realized, including the quantum channel and the classical (public and authenticated) channel needed for secure key distribution. When keys are generated at both ends, they are stored, and will then be made available for different purposes: end user applications, QKD link authentication, key forwarding, etc. Note that this plane is also where general quantum communications would take place, albeit using different protocols and capabilities (i.e. when quantum memories are available) and the purpose is different than to extract secret keys.

The second plane is the routing of QKD keys across the network. This has many implications, starting from the security perspective. The main purpose of a QKD link is to provide quantum-safe keys at both ends. When extending this concept to the network, the same level of security must apply. This requires that the security protocols at each hop

of a virtual association must also be ITS (e.g. Wegman-Carter authentication, One Time PAD -OTP- encryption), with a subsequent penalty of using QKD-derived keys for transporting key material end-to-end. As an example, a single key transported across N nodes shall use N-1 keys only for encryption. If OTP is used, this means that making available n bits of key at both ends of a path with N nodes, will require Nn QKD generated bits of key. Note that this is different of requiring the same amount of classical communications, since the amount of quantum communications required to obtaing them is much larger and expensive in terms of resources.

Another implication is the way the routing decisions are made in a QKD network: distributed control plane vs. centralized. In a distributed scenario, QKD nodes (a set of QKD systems in a secure area) collects information of other nodes and link states to take the optimal decision on which path use to forward a key material to a remote end. An example of such scenario is the SECOQC network [10] deployed in Vienna in 2008. The nodes exchanged link state information using a protocol similar to OSPF, so each node hosted an updated routing database. The centralized approach follows the same networking principles as SDN, with a first implementation in the Madrid network, in 2018 [20]. This architectural principle allows a central entity, called SDN controller, to gather information about every node and link of the network, having an end-to-end view. This allows to have a single entity taking routing decisions based on the load (key requests) on each link and the available resources.

The third plane is composed by the applications of the QKD network. Applications can be internal processes of the QKD network that reutilize keys for maintaining the security of the network (e.g. key managers), or external entities that require QKD-derived keys to secure their communications. The load caused by these applications, the priorities of each of them and other parameters are to be taken into acount by the routing layer to optimize the resource utilization.

IV. The OpenQKD Madrid Network

In late 2019 the OpenQKD: European Open QKD network project started. It aims to show practical applications of quantum cryptography in networks using several demonstrators and testbeds. The project has much industrial participation and also intends to increase the Technology Readiness Level in QKD devices, networks and applications in order to bring a QKD related industry to maturity. It defines several demonstrators in many places of Europe and four larger testbeds in Berlin, Madrid, Poznan and Vienna.

The OpenQKD Madrid Quantum Network builds on top of the previous quantum network built in the Telefnica production premises, where we did our SDN experiments. It has been enlarged with sites of the RedIMadrid network, which is the network provider that links all research centers and Universities in the Madrid region, to a total of 13 links. The distances range from a couple to slightly over 40 km (60 km in new links under comissioning) and losses from a few dB to about 12-14 dB (counting additional connectors, filters, multiplexers, switches and add/drop devices). The network has amplifiers at several places that need to be bypassed. Fortunately, they are at the entry points in some nodes, and are easy to bypass. A Map of the network is presented in Fig. 2.

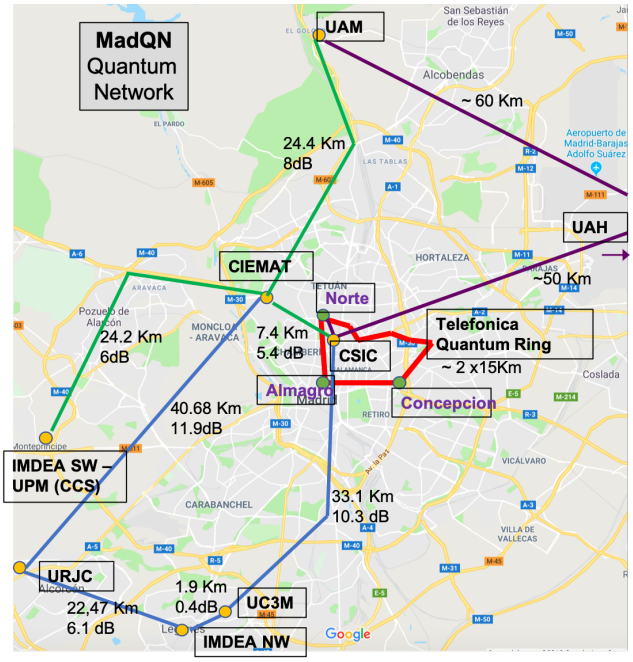

Fig. 2. The Madrid Quantum Network has currently 13 links. The network is a real world one in the sense that all the network is in production facilities and that most of the nodes are being used simultanously for classical communications, including the fiber. This is not an ad hoc network builf for quantum purposes. As a result, this presents the same challenges that a commercial deployment of QKD technologies would need to overcome, making for a realistic testbed. Distances and losses are also representative of a typical metropolitan area network, ranging from 2 to about 40 km and from 3 to 14 dB, respectively (when all losses, not only the fibre is taken into account). Distances and losses (only fiber) are quoted in the figure. The purple lines (connecting to UAH) are under comissioning. The red ring in the center is the old Madrid Quantum Network installed in Telefónica premises [20]. It is interesting to note that some nodes host special installations that are of particular interest, like IMDEA Networks (IMDEA-NW) which hosts a Telefónica 5G lab.

There are several salient features of this network. In the first place, this is a production network, where in many nodes classical commercial communications are taking place. This does not only shares the classical optical equipment, but also the fibre is shared in many cases. This makes this testbed a real world one, that will present to QKD deployment the same challenges than a commercial one. This is much more realistic than any other previous QKD network built. To solve these challenges, the degree of control of the network must be large which is where the flexibility of the SDN approach shines. Note that in order to cope with internal restrictions in several of the links, quantum communications are allowed only when there is a backup link where no quantum transmissions are taken place, so that classical communications are always safeguarded. This means that the control must route the quantum signals accordingly in order to comply with this requirement. Other interesting feature is the fact that

the network is owned by two providers, which makes for a demonstration of a multitenant quantum network. Finally, the network connects nodes from the Telefnica metro core network (e.g. Norte node in the map) to their 5G lab (IMDEA-NW node) which makes also for a realistic use case in blending QKD and 5G technologies.

Along with this use case, the network will run many others, from more generic cases like critical infrastructure protection or secure data transmission for e-health services to other more specific, like network attestation or ordered proof of transit. The network is also open for testing from external users and offers a means for it through a schem of Open Calls, where resources, support and even funding is made available to non OpenQKD partners. Some of these use cases are described in the next section.

V. Security Scenarios

This section provides a high-level overview of use cases position as an added-value for operators to capitalize a QKD network. Any of this use cases can be considered as applications that sit at the Application plane (as per described in section III) making use of the outcome from the QKD network resources: symmetric keys. Three cases are presented: reinforcing security measures at the network's control plane, providing quantum safe connectivity services for end users and service chain flow validation in virtualized environments.

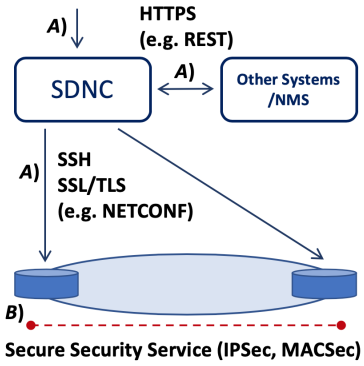

Fig. 3. Logical view on the applicability of QKD for securing control and data planes.

A. Quantum-Safe Network's Control Plane

Providing quantum-safe security for end user services or applications seems meaningless if the infrastructure supporting those services is not secured via quantum-safe means. Currently, network controllers, management systems and devices communicate with each other using transport protocols, such as HTTPS, SSH, SCFTP, SCP, etc. These protocols at its time use traditional key exchange methods (e.g. Diffie-Hellman) to generate master keys that are not quantum-safe.

Contributions in [22] shows a method to integrate QKD systems in modern network infrastructures and cryptographic protocols to tackle this issue (Fig. 3 case A). The presented method reutilizes existing protocols (SSH, TLS), augmenting their implementation to incorporate QKD-derived keys in combination with the ones derived from classical key echange, in a hybrid fashion that could also be extended for other cryptographic methos (e.g. post-quantum). This also allows to leverage existing certifications: the augmented system is never worse than the certified one. The net result is an increased security level and a network much more resilient to side channel attacks. In addition, the proposed scheme works in an incremental, flexible and non-disruptive manner, so the systems could (if needed) shift to old schemes, whenever QKD-derived keys or others are not available.

B. Secure Connectivity Services

Once network management is considered quantum-safe, a first step for start capitalizing quantum cryptography would be to offer it as an additional feature into business-to-business (B2B) commercial agreements, providing secure connectivity services for overlay networks. This secure connetivity can be then implemented at different layer: e.g. layer 2 (MACSec), layer 3 (IPSec), etc.

A good example of this integration for IPSec using the internet key exchange (IKE) protocol was implemented in [23] (Fig. 3 case B). Beyond data plane realization of this services, there is also a lack of standardization from network management's perspective for the automatic creation of these services. The authors of this work also contributed in this area by defining protocol extensions to provision quantum encryption in end-to-end services [24]. This automation can be achieved not only by using existing control plane protocols, but using instead common DevOps practices and tools (e.g. Jenkins, Ansible) that again rely on protocols such as SSH for sending out configuration commands. This channels, as stated above, can also be secured using QKD.

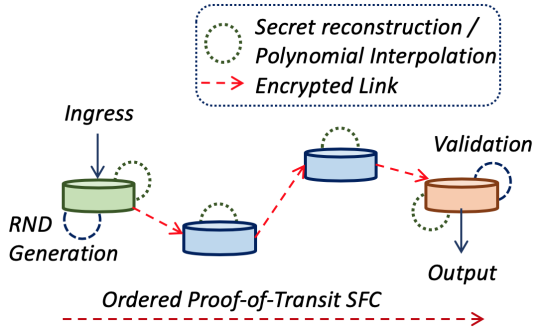

Fig. 4. Ordered Proof-of-Transit Scheme (example with four nodes).

C. Service Chain Service Verification

The final presented scenario is related to the implementation of service function chains (SFC), in the context of network virtualization for 5G. The connectivity between network functions is implemented across virtual instances (e.g. OpenVSwitches), data center networks and overlay transport networks. The appropriate verification of the traffic forwarding

across SFC nodes is a problem that has been address by the IETF SFC working group in the Proof-of-Transit draft [25].

The contributions in [26] show that the original approach of the internet draft had associated security vulnerabilities, so a possible attacker of the service chain could tamper a node, learn the scheme and bypass it. If the node implements any time of security function for the service chain (e.g. firewall, gateway), this could mean a security breach for the service. The solution presented (see Fig. 4) required masking of the packet's metadata using randomly generated keys between every two nodes in the path, provisioned via QKD. This not just mitigates the security issue presented, but also allows to verify the correct forwarding order of the traffic across the chain.

VI. Conclusions

Quantum Key Distribution, as any other technology in the applied research phase, needs to undergo serveral phases of standardization and subsequent certification for it to achieve the required level of maturity for market-ready mass production. In addition, the current implementations of QKD links and networks lack the necessary flexibility to be adopted into telecommunications networks.

Software Defined Networking has demonstrated to be the paradigm to follow for the adoption of any new solution in the telecommunications environment. The examples presented in this tutorial not only allow to understand the Software Defined QKD Networking approach, but also provide examples of existing and future implementations of the solution, together with use cases that can be applied for operators to capitalize QKD and get a return on investment.

Acknowledgment

Authors would like to thank the Madrid's regional government, Comunidad Autonoma de Madrid, for the project Quantum Information Technologies Madrid, QUITEMAD+ S2013/ICE-2801, the FET Flagship on Quantum Technologies, European Unions Horizon 2020 research and innovation programme under grant agreement No 820466: Continuous Variable Quantum Communications (CiViQ) and ICT grant agreement No 857156: Open European Quantum Key Distribution Testbed (OpenQKD) and the team of Transport and IP Connectivity in Telefónica Spain for their support to this activity.

References

[1] N. Gisin et al. "Quantum cryptography". In: Rev. Mod. Phys. 74.1 (2002), pp. 145195.

[2] V. Martin, J. Martinez-Mateo, and M. Peev. "Introduction to Quantum Key Distribution". In: Wiley Encyclopedia of Electrical and Electronics Engineering. 2017, pp. 117. ISBN: 9780471346081. DOI: 10.1002/047134608X. W8354.

[3] T. Inagaki, N. Matsuda, O. Tadanaga, M. Asobe, and H. Takesue,"Entanglement distribution over 300 km of fiber," Opt. Express 21, 23241-23249 (2013)

[4] Stucki, D. et al. "High rate, long-distance quantum key distribution over 250km of ultra low loss fibres." New J. Phys. 11 (2009) 10.1088/1367-2630/11/7/075003.

[5] Zhong, X. Hu, J. Curty, M. Qian, L. and Lo, H-K. "Proof-of-Principle Experimental Demonstration of Twin-Field Type Quantum Key Distribution", Phys. Rev. Lett. 123, 100506 (2019) DOI: 10.1103/PhysRevLett.123.100506

[6] Liu, Y. et al. "Experimental Twin-Field Quantum Key Distribution Through Sending-or-Not-Sending." in Phys. Rev. Lett 123, 100505 (2019) DOI: 10.1103/PhysRevLett.123.100505

[7] Pirandola, S., Laurenza, R., Ottaviani, C. et al. "Fundamental limits of repeaterless quantum communications." Nat Commun 8, 15043 (2017). https://doi.org/10.1038/ncomms15043

[8] "SDN Architecture Overview" Opennetworking.org. Retrieved 22 November 2014.

[9] Elliot, C. Colvin, A. Pearson, D. Pikalo, O. Schlafer, J. Yeh, H. "Current Status of the DARPA Quantum Network" in Quantum Information and Computation III, Proc. SPIE 2005 v. 5815, pp.138-149, doi 10.1117/12.606489

[10] Peev, M. et al. The SECOQC quantum key distribution network in Vienna. New J. Phys. 2009, v. 11, pp. 075001, doi 10.1088/1367-2630/11/7/075001

[11] Maurhart, O. (2010) "QKD Networks based on Q3P." in C. Kollmitzer and M. Pivk (ed.) "Applied Quantum Cryptography" Springer, pp. 151-172.

[12] Sasaki, M. et al. Field test of quantum key distribution in the Tokyo QKD Network, Opt. Express, 2011, v. 19, pp. 10387-10409, doi 10.1364/OE.19.010387

[13] Lancho, D. Martinez, J. Elkouss, D. Soto, M. and Martin, V. QKD in Standard Optical Telecommunications Networks, in QuantumComm 2009, LNICS, vol. 36, pp. 142-149, 2009 (arXiv:1006.1858)

[14] Ciurana, A. Martinez-Mateo, J. Peev, M. Poppe, A. Walenta, H. Zbiden, H. Martin, V., "Quantum metropolitan optical network based on wavelength division multiplexing", Opt. Express, 2014, v. 22, pp.1576-1593, doi 10.1364/OE.22.001576

[15] Ciurana, A. Martin, V. Martinez-Mateo, J. Schrenk, B. Peev, M. Poppe, A., "Entanglement Distribution in Optical Networks", IEEE J. Sel. Top. Quantum Electron. 2015, v. 21, pp. 6400212, doi 10.1109/JSTQE.2014.2367241

[16] Stucki, D. et al. "Long-term performance of the SwissQuantum quantum key distribution network in a field environment", New J. Phys. 2011, v. 13, pp.123001, doi 10.1088/1367-2630/13/12/123001

[17] Xiang, Hong and Han, Zheng-Fu, "The Chinese QKD networks", 2015, 3rd ETSI Quantum Safe Cryptography Workshop.

[18] [Online] UK Quantum Technology Hub for Quantum Communications Technologies: http://quantumcommshub.net

[19] A. Morrow, D. Hayford and M. Legr, "Battelle QKD test bed". 2012 IEEE Conference on Technologies for Homeland Security (HST), Waltham, MA, 2012, pp. 162-166.

[20] A. Aguado et al., "The Engineering of Software-Defined Quantum Key Distribution Networks," in IEEE Communications Magazine, vol. 57, no. 7, pp. 20-26, July 2019.

[21] Quantum Key Distribution (QKD); Application Interface. In: ETSI GS QKD 004 V1.1.1. 2010-12.

[22] A. Aguado et al. "Hybrid Conventional and Quantum Security for Software Defined and Virtualized Networks." In: J. Opt. Commun. Netw. 9.10 (2017), pp. 819825. DOI: 10.1364/JOCN.9.000819.

[23] Stefan Marksteiner and Oliver Maurhart (2015). "A Protocol for Synchronizing Quantum-Derived Keys in IPsec and its Implementation." 10.13140/RG.2.1.4756.4001.

[24] A. Aguado et al. "Virtual Network Function Deployment and Service Automation to Provide End-to-End Quantum Encryption." In: J. Opt. Commun. Netw. 10.4 (2018), pp. 421430. DOI: 10.1364/JOCN.10.000421.

[25] F. Brockners et al. "Proof of Transit." IETF Internet Draft draft-ietf-sfc-proof-of-transit-04. 2019.

[26] A. Aguado, D. R. Lpez, A. Pastor, V. Lpez, J. P. Brito, M. Peev, A. Poppe, and V. Martn, "Quantum cryptography networks in support of path verification in service function chains," J. Opt. Commun. Netw. 12, B9-B19 (2020)

[27] Y. Yorozu, M. Hirano, K. Oka, and Y. Tagawa, "Electron spectroscopy studies on magneto-optical media and plastic substrate interface," IEEE Transl. J. Magn. Japan, vol. 2, pp. 740–741, August 1987 [Digests 9th Annual Conf. Magnetics Japan, p. 301, 1982].

[28] M. Young, The Technical Writer's Handbook. Mill Valley, CA: University Science, 1989.