Quantum Technologies for future Quantum Optical Networks

Alberto Gatto
Dipartimento di Elettronica, Informazione e Bioingegneria
Politecnico di Milano
Milano, Italy
alberto.gatto@polimi.it

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

Marco Brunero
Cohaerentia S.r.L.
Milano, Italy
marco.brunero@cohaerentia.com

Dileepsai Bodanapu
Institute of Electronics, Information Engineering and Telecommunications
Consiglio Nazionale delle Ricerche
Torino, Italy
https://orcid.org/0000-0003-4822-7186

Ruben B. Mendez
Center for Computational Simulation
Universidad Politécnica de Madrid
Madrid, Spain
ruben.bmendez@upm.es

Rafael J. Vicente
Center for Computational Simulation
Universidad Politécnica de Madrid
Madrid, Spain
rafaelj.vicente@upm.es

Paolo Comi
Innovation Lab and Research
Italtel S.p.A
Milano, Italy
paolomaria.comi@italtel.com

Vicente Martin
Center for Computational Simulation and Dept LSIIS
Universidad Politécnica de Madrid
Madrid, Spain
vicente@fi.upm.es

Paolo Martelli
Dipartimento di Elettronica, Informazione e Bioingegneria
Politecnico di Milano
Milano, Italy
paolo.martelli@polimi.it

***Abstract*— The recent evolutions in the convergence of QKD and classical communication systems are described, together with the relevance of SDN as a suitable approach for a real integration between QKD and WDM networks. Preliminary experimental results on a discrete-variable QKD prototype working in the O-band co-propagating with 40 50-GHz C-band information channels are reported, showing the capabilities of QKD in short/medium reach optical networks.**

Keywords—QKD, Quantum optical networks, SDN

I. INTRODUCTION

In recent years, photonic quantum technology has created unknown opportunities thanks to the counterintuitive concepts of quantum physics. Quantum Optical Communication (QOC) exploits photons as Qubits to convey information between two entities through the optical network; its well-known application is Quantum Key Distribution (QKD) [1], in which, to generate a shared key, the exchange of information between two parties is done with the aid of quantum states. Up to now, the security of public-key cryptosystems (e.g., Rivest–Shamir–Adleman (RSA) [2]) has been based on the high computational complexity needed to resolve them, suffering from the advances in computational power and algorithm evolution (e.g., quantum computing [3]). On the other hand, QKD holds the potential of sharing information-theoretic secure (ITS) symmetric keys, thanks to the fundamental principles of quantum physics. Unlike digital bits, in fact, quantum states cannot be perfectly copied due to the Heisenberg uncertainty principle, leading to an unconditionally secure information exchange totally immune to any algorithmic cryptoanalysis.

Quantum Optical Networks (QON) [4] extend the concept of QOC, since they will interconnect quantum nodes and devices to transport, elaborate and store quantum information (Qubits), facing new challenging phenomena with no counterpart in classical networks to obtain new networking and computing capabilities. In the next future, Quantum networks have to face several challenges before their full implementation: the main requirement is their integration with existing and future classical optical communication networks [5]. As wavelength-division multiplexing (WDM) networks are pervasive in current backbone network infrastructure, incorporating QKD into existing WDM networks provides a practical way to reduce the complexity and cost of QKD networking [6].

Recently, the introduction of software defined networking (SDN) technologies, through the development of standard protocols and interfaces, has allowed to integrate new services and systems in telecommunications networks. Thanks to SDN, the management and optimization of the entire infrastructure is accessible from a central controller, directly acting on several agents located in different network sections. The flexibility of SDNs could allow an easier integration of quantum communications in the classical network without requiring a one-to-one replacement of network devices to create a Quantum Channel, avoiding large deployment costs [7].

In this work, recent advances in the QKD/classical communications convergence are described, together with an overview of SDN approach for future quantum networks. Moreover, preliminary results on a discrete-variable QKD system working in the O-band with classical information channels propagating in the C-band are reported.

II. QKD IMPLEMENTATION IN OPTICAL NETWORK

The deployment of QKD over classical WDM networks is a promising and feasible solution for future QKD networking. Lately, several implementations of QKD systems have demonstrated their feasibility exploiting several technologies [8,9]. Nevertheless, multiple factors are limiting the global

978-3-903176-33-1

deployment of the QKD approach, as the low transfer rate, the modest transmission distance and its hard compatibility with the existing network infrastructure: QKD is a technology intrinsically distance-limited, since an interaction of the Qubit with the transport medium cannot be avoided. The exponential attenuation typical of optical fibers leads to a reduction of the achievable secret-key rate, limiting the exploitation of QKD technology to metro-haul links. Moreover, the interaction with the environment can shade the presence of an eavesdropper, leading to error correction strategies that penalize the secret-key throughput to strongly increase security.

The first QKD protocol proposed by Bennett and Brassard in 1984 (BB84) [10] relied on the polarization encoding of single photons, but since then new protocols and encoding schemes have emerged. QKD communications realized so far require a separate infrastructure, e.g. dark fibers, to shade Qubit transmission from high-power classical information channels. This option protects the QKD channel from undesired crosstalk from the information channels; however, building such a parallel infrastructure is very expensive, requiring large investments by Telco operators. Another solution could be the exploitation of different wavelength bands for QKD and telecommunication signals [11]. In this case, a convergence between QKD and WDM networks can be achieved, relaxing the financial efforts needed but reducing the QKD power/distance budget and performance. Recent demonstrations show practical systems tolerating attenuations of around 30 dB (corresponding at most to 150 km) still maintaining a feasible key rate [12].

A realistic approach to increase the QKD distance limit relies on trusted-node architecture [13]: by cascading several links, and trusting all intermediate nodes, in principle it is possible to achieve the exchange of secret keys at longer distances. Firstly, secret keys between neighboring nodes are generated; then, the initial key is relayed, in an encrypted way, to the other remote user. This scheme is based on the strong assumption that all the nodes on the path connecting the two remote users can be trusted, which can be acceptable just for the first generation of quantum networks or in case of nodes inside a security perimeter. In the future this requirement will be removed by relying on quantum repeater [14], even though this technology is not yet available and ready to be employed.

III. SDN APPROACH FOR QUANTUM NETWORKS

QKD can be mathematically proven to be secure, independently of the resources of the adversary: It is an information theoretic secure primitive [15]. The physical layer restrictions and the point-to-point nature of QKD has led this technology to be implemented in ad-hoc, usually point-to-point and highly experimental scenarios. Nevertheless, new initiatives are emerging all around the world in the last years to ease the integration of the QKD technology as a service into real production networks, such as OpenQKD [16], CiViQ [17] or Q-Secure Net [18] trying to mitigate the highly experimental state of QKD devices and increase Technological Readiness Level (TRL), more suitable to the current status of real production networks.

In parallel, telecommunication networks are experiencing a transformation process, moving their traditional monolithic architectures towards novel networking trends, like software-defined networking. This novel paradigm is based in one fundamental concept: the separation between the Control Plane and the Data Plane. In a very simplified definition, the Control Plane is the set of elements (hardware or software) that create a local dataset for configuring the device. The Data Plane is in charge of handling the incoming traffic and forward it toward the correct destination. The fundamentals behind this paradigm are network configurability and programmability. The first feature means to take network automation to a next level, where capacity and services are allocated on demand from a centralized SDN Controller that orchestrates all the resources of the network. On the other hand, programmability refers to network elements that evolved from traditional routing or switching to boxes that are fully programmable, being capable of behaving in different ways, as defined by the centralized controller

We apply this high degree of configurability and programmability in our prototype, easing the degree of adaptability in which the QKD devices could be managed. The SDN paradigm could be used not only over high-end and mature devices but also low and more experimental ones, making possible the adaptation of the software to fit perfectly well with the requirements and limitations of any QKD device, including the experimental ones.

The use of well-known standards, high level abstraction models and open interfaces are crucial elements not only to ease the integration of the QKD communication layers but also the future integration of the devices into real production networks: the success of QKD technology, in fact, will be probably based in the use of tools, schemes, standards and protocols that are familiar to the telecommunication industry.

We have followed this approximation and we have used well known standards. This is essential for ensuring the interoperability of equipment and protocols in complex systems. This is the reason why the definition of standards is gaining importance in the last years for QKD technology. Some international organizations like European Telecommunications Standards Institute (ETSI) [19] and International Telecommunication Union (ITU) [20] are generating QKD related standards, covering the important aspects of the QKD technology. In this regard, one crucial step from the QKD point of view is the key material delivery to the application layer (final services that will use the key). One of the most relevant standards that we have implemented is the ETSI ISG 004: Application Interface [21]. This standard defines the API to deliver keys to the final application. One important characteristic of these interfaces is that is implementation agnostic, and as a consequence, the implementation of this interfaces can be adapted to the specific requirements of each QKD devices in a transparent way.

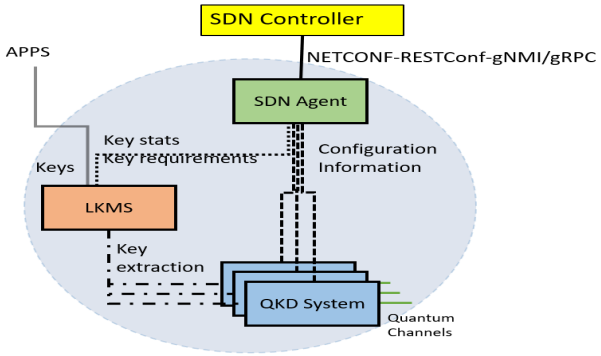

Figure 1. Logical view of a SD-QKD node [22].

From the point of view of SDN, another important standard that we have integrated in our prototype is the ETSI ISG 015: Control Interface for Software Defined Networks [22]. This standard defines an interface between the SDN Central Controller and a high-level abstraction of a QKD node, shown on Figure 1. This interface uses YANG language, which is protocol independent and message structure independent. We also have included in our prototype additional interfaces to interact with the QKD hardware. In our implementation, we decided to use the QuAM/QuAI interfaces [23]. These interfaces are also implementation agnostic and model oriented, which means that, from the high abstraction models defined for the devices, specific commands could be implemented based on the models to interact and configure the device at low level.

The relation between SDN and QKD technologies shall be seen as a symbiosis, where each of them brings benefits to the other. The flexibility of SDN allows a high degree of adaptability to different QKD devices, network setups and restrictions etc. This degree of adaptability was simply impossible in previous schemes, where the different network devices should be modified, one by one, to create a Quantum Channel.

IV. Discrete-Variable QKD Prototype

QKD capabilities have been tested in case of a WDM link with several co-propagating classical channels by developing a discrete-variable QKD prototype, based on the exploitation of the BB84 protocol with polarization encoding. The complete protocol procedure is illustrated in Fig. 2 and summarized as follows [10].

- *Qubit exchange*: after a first phase of hardware update (concerning key length, the key generation rate, etc.) and after the generation of random Qubits to be sent, the transmitter (Alice) starts the QKD transmission on the Quantum channel, while the receiver (Bob) detects the Qubits after having chosen a random state of polarization to be measured. In this work, we exploit one single-photon avalanche detector (SPAD) at the receiver end, in a scheme similar to [24]. This choice leads to cost limitation, even though it increases the complexity of the Quantum system and halves the effective transfer rate of the keys.
- *Key sifting*: after the QKD transfer on the Quantum channel, Bob and Alice determine, by public exchange of messages, which photons were successfully received with the correct basis. Alice and Bob can therefore test for eavesdropping by publicly comparing some of the bits on which they think they should agree, though of course this sacrifices the secrecy of these bits.

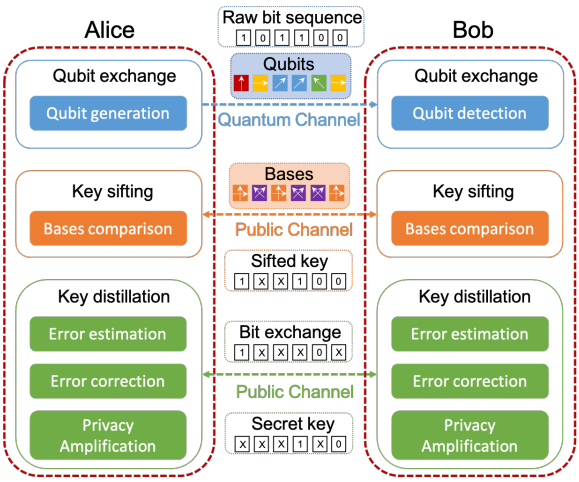

Figure 2. BB84 key generation procedure.

- *Key distillation*: if the comparison leads to an estimated Quantum Bit Error Rate (QBER) lower than a threshold level, Alice and Bob can conclude that the quantum transmission has been free of significant eavesdropping, and those of the remaining bits that were sent and received with the same basis can safely be used as a one-time pad for subsequent secure communications over the public channel. The error correcting code is based on an efficient version of the standard Cascade protocol [25], which needs the exchange of several parity bits on the Public Channel in order to correct all the bit errors in Bob's key. Finally, the privacy amplification [26] is performed, during which a hashed version of the corrected key is computed through a universal$_2$ random hash function that guarantees a null residual information for an eavesdropper performing a partial intercept-and-resend attack.

Quantum signals transmitted on the Quantum Channel are faint and easily experience the presence of interference from co-propagating information channels. To underline the impact of crosstalk, the experimental setup shown in Fig. 3 has been used. In particular, Alice exploits two different distributed-feedback (DFB) lasers with identical nominal wavelength as sources for the QKD channel and the auxiliary channel needed to synchronize the acquisition and to fully recover the

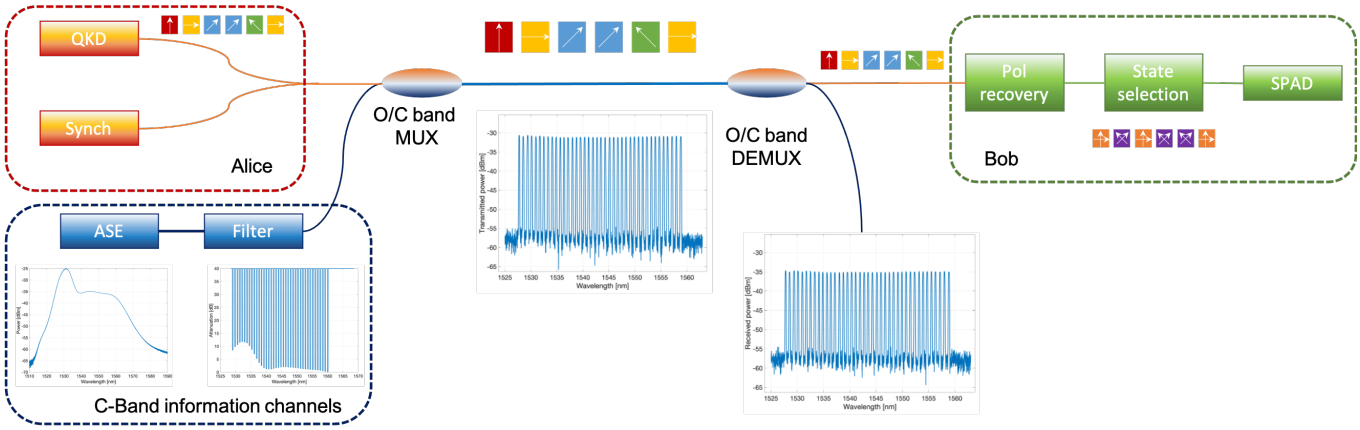

Figure 3. Experimental setup.

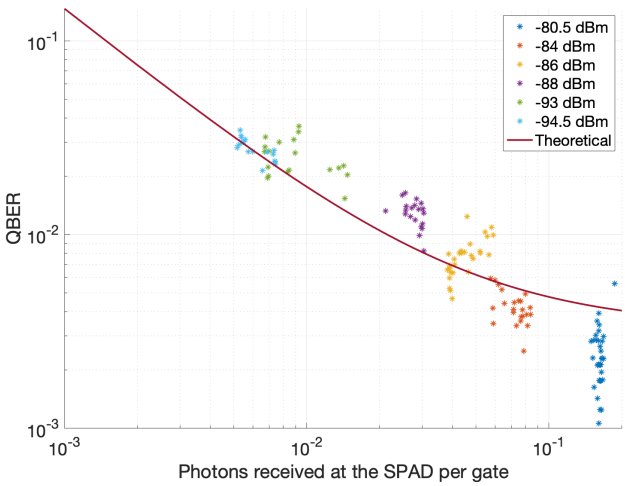

Figure 4. QBER vs photon count rate at SPAD input.

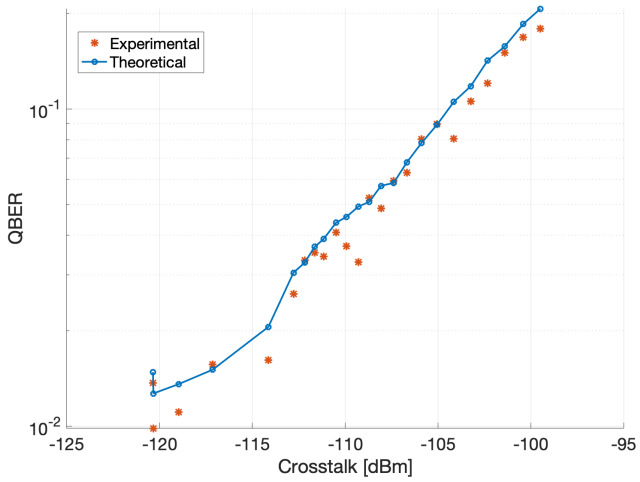

Figure 5. QBER vs C-Band crosstalk.

transmitted polarization state at the receiver side. The QKD signal is composed by 20-ns optical pulses with a 1-kHz repetition rate. To reduce the presence of unavoidable crosstalk, the QKD wavelength is fixed at 1310 nm, located very far from the classic information channels at 1550 nm. The amplified spontaneous emission (ASE) of an Erbium-doped fiber amplifier (EDFA) filtered by a programmable Finisar Waveshaper is used to mimic the presence of 40 50-GHz C-band information channels. QKD and C-band channels are multiplexed by a standard WDM coupler in order to limit the losses. At the receiver end, a cascade of WDM couplers is used as demultiplexer, in order to reach the desired crosstalk extinction. At Bob's side, several algorithms for polarization recovery can be exploited [27]. In the proposed solution, an automatic polarization stabilizer [28] is used to recover the polarization reference both for the rectilinear and diagonal bases. Then, a specific state of polarization to be measured is selected at each gate time and the QKD signal is detected by a single SPAD [29]. Finally, the secret key is distilled by following the procedure reported previously.

In Fig. 4, the performance of the QKD system in terms of QBER in function of the photon count rate at the SPAD input is reported. The measurements have been performed for several input power conditions in case of sifted key length of 4096 bits. The results are in good agreement with the expected theoretical curve, described by

$$QBER = p_{ext} + \frac{p_{dark}+p_{XT}}{p_{photon}} \qquad (1)$$

where p_{ext} represents the extinction ratio of the receiver (i.e. the probability to detect a photon encoded on a state of polarization orthogonal to the specific polarizer angle), p_{dark} is the probability of having a dark count in the gate window, p_{XT} is the probability of detecting a photon from the residual C-band signal and p_{photon} represents the total counting ratio. In particular, the performance strongly depends on p_{dark} and p_{XT} in case of very low incident power, while the extinction ratio degrades the QBER only for very high photon count rate (i.e. close to 0.1 photons/gate and above). The several measurements shown in Fig. 4 are obtained in case of null crosstalk signal with an extinction ratio of 27 dB and dark count rate of 800 counts/s. A QBER of about 3% can be achieved with a total attenuation of 13 dB, while the 11% QBER limit is estimated for a total attenuation around 20 dB, which roughly corresponds to a maximum transmission distance of about 60 km at 1310 nm.

Finally, the impact of C-Band crosstalk on QKD performance has been evaluated. Fig. 5 shows the QBER for different crosstalk residual powers at the SPAD input in case of a photon count rate of 0.03 photons/gate. Such photon count has been chosen considering the total losses of the multiplexer, demultiplexer and polarization recovery stage, which are about 5 dB. The theoretical curve is calculated using Eq.(1). As expected, low crosstalk signals (e.g. about -120 dBm) don't induce any significant variation with respect to the reference QBER, which is close to 1% in absence of crosstalk. The increase in the residual C-band channels power leads to a strong degradation of the performance, reaching the 11% QBER limit value in case of -103 dBm. To avoid the insurgence of crosstalk penalties, therefore, it could be useful to increase the number of cascaded WDM couplers used as demultiplexer, but at the expense of total losses that impact on the secret key bit rate.

V. Conclusions

The recent evolutions in the integration of QKD and classical communication systems have been addressed, underlining the impact of SDN approach for obtaining a complete and fast convergence between QKD and already deployed WDM networks. Preliminary experimental results on a discrete-variable QKD prototype working in the O-band with 40 50-GHz classical information channels propagating in the C-band have been reported, demonstrating the capabilities of QKD in short/medium reach optical networks.

Acknowledgment

This work has been supported by the EIT Digital Q-Secure Net innovation activity and by MIUR PRIN2017 FIRST Project (GA 2017HP5KH7_002).

References

[1] H.-K. Lo, M. Curty, and K. Tamaki, "Secure Quantum Key Distribution," Nat. Photonics, vol. 8, no. 8, pp. 595–604, Aug. 2014.

[2] R. L. Rivest, A. Shamir, and L. Adleman, "A Method for Obtaining Digital Signatures and Public-Key Cryptosystems," Commun. ACM, vol. 21, no. 2, pp. 120–126, Feb. 1978.

[3] L. R. Schreiber and H. Bluhm, "Toward a Silicon-Based Quantum Computer," Science, vol. 359, no. 6374, pp. 393–394, Jan. 2018.

[4] M. Sasaki, et al., "Quantum Photonic Network: Concept, Basic Tools, and Future Issues," IEEE J. Sel. Top. Quantum Electron., vol. 21, no. 3, pp. 49–61, May–June 2015.

[5] A. Ciurana, et al., "Quantum Metropolitan Optical Network Based on Wavelength Division Multiplexing," Opt. Exp., vol. 22, no. 2, pp. 1576– 1593, 2014.

[6] Y. Cao, Y. Zhao, J. Wang, X. Yu, Z. Ma, and J. Zhang, "Cost-Efficient Quantum Key Distribution (QKD) Over WDM Networks," J. Opt. Commun. Netw. 11, 285-298 (2019)

[7] A. Aguado et al., "Hybrid Conventional and Quantum Security for Software Defined and Virtualized Networks," in IEEE/OSA Journal of Optical Communications and Networking, vol. 9, no. 10, pp. 819-825, Oct. 2017, doi: 10.1364/JOCN.9.000819.

[8] Y. Ding, D. Bacco, K. Dalgaard, et al. "High-Dimensional Quantum Key Distribution Based on Multicore Fiber Using Silicon Photonic Integrated Circuits." npj Quantum Inf **3,** 25 (2017).

[9] D. Bacco, I. Vagniluca, B. Da Lio, et al. "Field Trial of a Three-State Quantum Key Distribution Scheme in the Florence Metropolitan Area." EPJ Quantum Technol. **6,** 5 (2019).

[10] C. H. Bennett and G. Brassard, "Quantum Cryptography: Public Key Distribution and Coin Tossing," in *Proc. IEEE Int. Conf. Comput. Syst. Signal Process.*, Bangalore, India, 1984, pp. 175–179.

[11] T E Chapuran et al., "Optical Networking for Quantum Key Distribution and Quantum Communications", New J. Phys. 11, 105001, 2009

[12] N. Walenta, et al., "A Fast and Versatile Quantum Key Distribution System with Hardware Key Distillation and Wavelength Multiplexing," New J. Phys., vol. 16, no. 1, 013047, 2014.

[13] M. Sasaki, et al., "Field Test of Quantum Key Distribution in the Tokyo QKD Network," Opt. Express, vol. 19, no. 11, pp. 10387–10409, May 2011.

[14] N. Lo Piparo and M. Razavi,"Long-Distance Trust-Free Quantum Key Distribution," IEEE J. Sel. Topics Quantum Electron., vol. 21, no. 3, p. 6600508, May 2015.

[15] V. Scarani et al. "The Security of Practical Quantum Key Distribution". In: Rev. Mod. Phys. Vol. 81. 2009, 10.1103/RevModPhys.81.1301. DOI: 10.1103/RevModPhys.81.1301

[16] [Online]. Open Quantum Key Distribution - OpenQKD. Available: https://www.openqkd.eu/ (Accessed May 12, 2021).

[17] [Online]. Continuous Variables in Quantum Communications - CiViQ. Available: https://civiquantum.eu/ (Accessed May 12, 2021).

[18] [Online]. EIT Digital: Q-Secure Net - Available: https://www.eitdigital.eu/fileadmin/files/2020/factsheets/digital-tech/EIT-Digital-Factsheet-Q-Secure-net.pdf (Accessed May 12, 2021).

[19] [Online]. European Telecommunications Standards Institute - ETSI. Available: https://www.etsi.org/ (Accessed May 12, 2021).

[20] [Online]. Internation Telecommunication Union - Telecommunication Standardization Sector. Available: https://www.itu.int (Accessed May 12, 2021).

[21] "Quantum Key Distribution (QKD); Application Interface," ETSI GS QKD 004 V2.1.1, 2020-08

[22] "Quantum Key Distribution (QKD); Control Interface for Software Defined Networks," ETSI GS QKD 012 V1.1.1, 2021-03

[23] R. B. Mendez, et al. "Quantum Abstraction Interface: Facilitating Integration of QKD Devices in SDN Networks." 2020 22nd International Conference on Transparent Optical Networks (ICTON). IEEE, 2020.

[24] P. Martelli, M. Brunero, A. Fasiello, F. Rossi, A. Tosi, M. Martinelli, "Single-SPAD Implementation of Quantum Key Distribution" in Proc. of International Conference on Transparent Optical Networks, ICTON, 2019. doi:10.1109/ICTON.2019.8840199

[25] G. Brassard, L. Salvail, "Secret-Key Reconciliation by Public Discussion" in Advances in Cryptology – EUROCRYPT '93, Workshop on the Theory and Application of Cryptographic Techniques, volume 765 of Lecture Notes in Computer Science Springer, Berlin Heidelberg, 1994, pp. 410–423.

[26] Bennet et al, "Generalized Privacy Amplification", IEEE Trans. on Inf. Th., Vol. 41 No. 6, Nov. 1995 pp. 1915-1923.

[27] P. Martelli, P. Boffi, M. Ferrario, L. Marazzi, P. Parolari, S.M. Pietralunga, R. Siano, A. Righetti, M. Martinelli, "Polarization Stabilizer for Polarization-Division Multiplexed Optical Systems", in Proc. ECOC 2007 - 33rd European Conference and Exhibition of Optical Communication, Article number 57584682007 (2007)

[28] B. Koch and R. Noe, "PMD-Tolerant 20 krad/s Endless Polarization and Phase Control for BB84-Based QKD with TDM Pilot Signals," Photonic Networks; 21th ITG-Symposium, 2020, pp. 1-3.

[29] A. Tosi, A. Della Frera, A. Bahgat Shehata, and C. Scarcella, "Fully Programmable Single-Photon Detection Module for InGaAs/InP Single-Photon Avalanche Diodes with Clean and Sub-Nanosecond Gating Transitions," Rev. Sci. Instrum., vol. 83, p. 013104, 2012.