Is there Room for Quantum Photons in my Access Network?

Annachiara Pagano[(1)], Antonio Manzalini[(1)], Maurizio Valvo[(1)]

[(1)] TIM Access Innovation, annachiara.pagano@telecomitalia.it

Abstract *Quantum Key Distribution is gaining momentum as an ultimate solution for network security. The paper provides the network operator's point of view about the deployment of a quantum key distribution optical layer in metro-access, discussing resource sharing and constraints related to the coexistence of heterogeneous optical technologies.*

Introduction

Cryptography provides methods to support data confidentiality and authentication; some cryptographic methods require the use of a key and protocols to securely distribute it. With the introduction of Quantum Key Distribution (QKD), where the security of the transmission of the generated key is guaranteed by the laws of quantum physics, the vulnerability of conventional cryptography, as a consequence of the advent of powerful quantum computers, has been surpassed, opening the way to a variety of new services and business opportunities [1] [2].

For telco operators, the benefits obtained by enabling a QKD network layer are twofold. Internally, it allows to render quantum-safe some critical parts of the network and infrastructure and to support time-critical applications by a quantum distribution of valuable synchronization signals. Towards the customers, the QKD layer offers secure communication as a service for mission-critical applications of governmental and military institutions, of the Industry 4.0 sector, or in a medium-term scenario, of cyber-physical IoT systems (eg, robots, drones). The Quantum Communication network layer can be provided by: 1) a new stand-alone infrastructure, including equipment, transmission medium, and management network; 2) a hybrid architecture, including dedicated transmission fiber for the quantum channel but with management and control integrated and carried over the legacy infrastructure; 3) a fully integrated solution sharing part of the equipment, transmission medium, management, control, and design rules of the legacy infrastructure. In this work, we will focus on the challenges imposed by the third scenario, and we will concentrate on the access network segment, mainly the end point of QKD services use cases.

Scope of the work is to provide: a) an overview of the access network infrastructure with the aim of introducing a QKD transmission layer b) some examples of noise-induced degradation on inserted QKD layer c) some design rules for both classical data signals and quantum key carriers.

Access network

Originated at the access termination points, a continuously growing bandwidth demand due to new emerging applications and a lifestyle change after the pandemic period is pushing technological evolution [3]. Fixed Access networks scream for an upgrade in data rate to residential users, for instance, by increasing the capacity of current Passive Optical Networks (PONs) towards 25G and 50G. To fully support 5G enhancements, the mobile Radio Access Network (RAN) asks for decentralizing computing and processing functions and site coordination and radio layer aggregation, generating high throughput to be carried with low latency.

Finally, looking at edge nodes and back-end and demarcation points located into suburbs at customer premises, there is a need for point-to-point fiber links with strong requirements in terms of security and latency to support backhauling Industry 4.0 private networks or traffic generated by cloudification and virtualization of many flavours of manufacturing processes.

IEEE and dedicated MSAs efforts are promoting standardization of <20 km hundreds of Gigabit/s

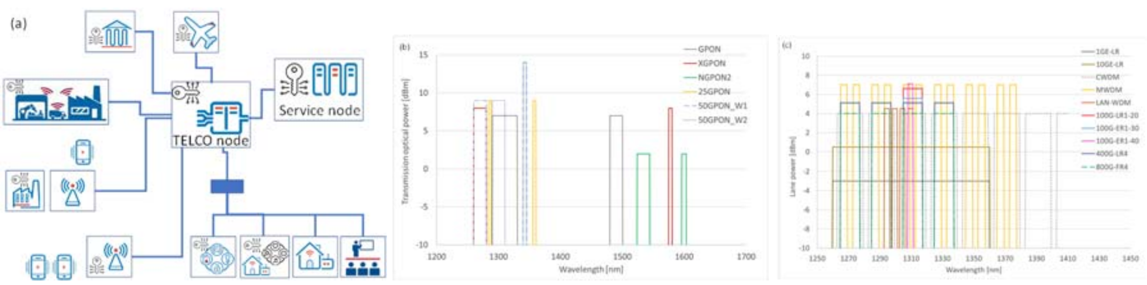

Fig. 1: a) pictorial view of access network, **b)** PON wavelengths, **c)** O band single and WDM carriers' allocation.

optical ports to address the use cases just mentioned. Figure 1a illustrates this access network scenario, while Figure 1b and 1c show wavelengths allocation (PON and Ethernet carriers) supporting all the services described above. It's difficult to find a spectral interval where to allocate a new type of optical carrier such as the one required for quantum communication, which is heavily affected by any type of noise and crosstalk [4][5].

Scarcity of fiber and span length could be discriminating factors in the choice between stand-alone/hybrid or fully integrated quantum layer. If fiber is a valuable asset and the optical power budget is enough to compensate for integration penalties, a fully integrated quantum layer will be preferable to a stand-alone solution. On the other hand, the stand-alone option is mandatory in case of high losses or strong coexistence penalties and is always preferrable if fiber is available and its cost is not an issue.

If we consider the statistical distribution of connection lengths in a typical access network, PON branches in urban/semi-urban environments are within 2-5 km, more than half of point-to-point dedicated pairs to customer sites are below 6 km, 50% of mobile xhauling links are below 10 km; microwave radio is exploited for specific geographic longer spans (up to 30 km, but with residual numbers and at lower rates). All these distances are fully compliant with state-of-the-art QKD fiber solutions [6][7], while a free space QKD link in parallel to a microwave radio link seems hardly feasible over longest reaches.

Looking at the numbers of available pairs into the buried cable, the scenario is twofold: in case of a high numerology cable deployed up to the site, the fiber is most probably available; conversely, in a small cable with few pairs, probably all of them are occupied with running signals, and deployment of a new quantum optical layer should be done according to a fully integrated scenario.

Quantum Key Distribution link design

A QKD system consists of two units exchanging one-way qubit/s; the transmitter consists of a signal source and an encoder, the receiver contains a selector for the measurement basis and one or more signal detectors. In weak laser pulse QKD systems, the qubit values are encoded upon laser pulses attenuated to the single-photon level. In the following, we'll refer only to this kind of equipment, despite other interesting alternatives such as CV-QKD that are out of the scope of this work.

Single-photon detectors are employed in the receiver section; dark count and noise could affect the detection process and be detrimental for the key recovery process from qubit measurements. In addition to back-to-back dark count and after-pulse effect, main noise sources are related to the transmission medium and system architecture. Poor Side Mode Suppression Ratio (SMSR) in classical data laser sources, low isolation in filtering elements, back-reflections, and nonlinear effects (mainly Raman) produce spurious signals and wrong detections.

If we consider coexistence on the same fiber through WDM muxing of O band quantum signals and C band classical data (or vice-versa), crosstalk by poor isolation of band mux/demux components could ask for many cascaded filtering layers to avoid detector saturation. Figure 2a reports an example of Out of Band (OoB) isolation of O/C band splitter. Depending on filter isolation and SMSR of data channels, crosstalk level could be higher than maximum tolerated Signal to Noise ratio (SNR) for Quantum channel. Figure 2b shows how many cascaded filters are needed to guarantee 20 dB of SNR on the quantum channel as a function of filter OoB isolation and SMSR of classical data carriers (in the 55-70 dB range).

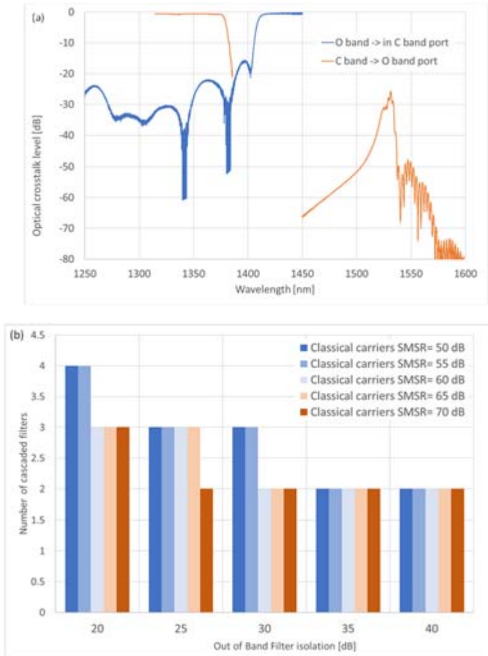

Fig.2: (a) Optical Out of Band extinction for O/C band splitters/combiners**, (b)** Estimation of the number of filters to be cascaded to guarantee spectral extinction.

If some noise can be filtered, In Band noise such as the one induced by Raman effect cannot be canceled. Raman gain extends over a large frequency range (up to 40 THz): both Stokes and anti-Stokes scattering, could generate spontaneous scattered noise levels that are low but significant relative to the average QKD channel power. Figure 3 shows a spectral measurement of Raman scattering induced by two laser sources at 1320 nm and 1600 nm.

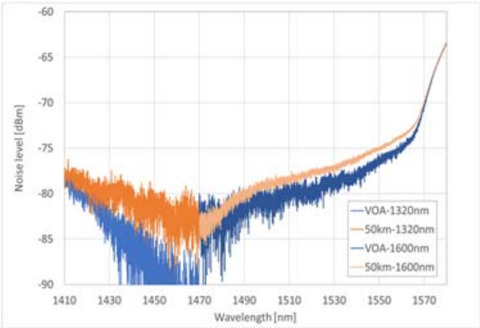

Fig. 3: Raman noise after 50 km of fiber (orange trace) compared to no fiber transmission (blue curve).

Design of a quantum compliant classical link

If classical and quantum channels coexist on the same fiber by means of O/C band separation, a careful design of the overall system budget has to be performed, considering penalties on both systems and defining a common operating range. As shown in Figure 4, extra attenuation imposed on the classical channel (orange curve) to minimize Raman crosstalk penalties could generate BER penalties going beyond receiver specifications. Increasing span length and maintaining optical classical to quantum ratio reduces the operating range up to few dBs for few extra kms, mainly for the system operating in O band with higher fiber loss and hard possibility of optical amplification.

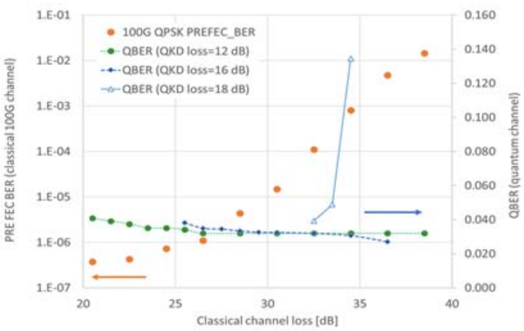

Fig. 4: BER against loss for classical and quantum carriers over 20 km of G.652 fiber (blue and green curve for QKD carrier, orange for classical one).

Management and Control of QKD layer

Looking at standard specifications for interoperability, both at the physical and upper layers (e.g., for management and control functions), growing efforts in the direction of defining and adopting a Software Defined Networks (SDN) architectural paradigm also for managing and control QKD resources and services are ongoing, aiming at a smooth and simpler integration of QKD nodes in current telco infrastructures. SDN allows the management, control and orchestration of an entire infrastructure using a hierarchy of logically centralized elements, usually called controllers, and this applies also for QKD nodes, with their own specific controllers and interfaces. Programmability and flexibility brought by SDN architectural paradigm reduce integration times and efforts. QKD nodes require data models to be properly configured and monitored to operate and support interworking with traditional network nodes effectively. In this perspective, standard YANG data models can also be used for QKD nodes. This is expected to bring full interoperability and plug-and-play capabilities to quantum systems.

Standardization and Certification

Several Standardization Bodies are currently working on defining roadmaps, architectures, and specifications on quantum networks (e.g., ETSI, ITU-T, ISO, IETF/IRTF, CEN/CENELEC, GSMA). ETSI, for instance, has already produced over twenty specifications [8] on QKD, covering very specific tasks (e.g., API for exchanging the keys, SDN control and orchestration, YANG data modelling, etc). ITU activities are ongoing in SG 11 (Protocols and Test Specifications), SG 13 (Future Networks), SG 17 (Security) and in the Focus Group on Quantum Information Technology for Networks (FG QIT4N) [9].
Recently GSMA [10, 11] is working on the Quantum-Hardware Abstraction Layer (HAL) for both Quantum Computing and Quantum Networks systems and nodes. The main motivation is that, today, one major obstacle hindering the exploitation of quantum technologies is that the industry has not yet consolidated around hardware technologies and architectures. The specification of a Quantum-HAL would allow decoupling quantum hardware from software so that Applications and Services Developers can start using the abstractions of the underneath quantum hardware, even if not consolidated.

Conclusions

Coexistence of quantum photons with legacy classical data is a challenge for both systems and for the overall architecture of the access network. Results show that a joint classical/quantum system design is essential in all cases where a stand-alone configuration with a dedicated fiber is not possible.

Acknowledgements

The research has received funding from the European Community through the H2020 B5G-OPEN (G.A. 101016663) project. Experimental results have been obtained in the CEQUAM project testbed in TIM within the framework of the EU funded Open-QKD Open Call programme.

References

[1] P. W. Shor, "Algorithms for quantum computation: discrete logarithms and factoring," Proceedings 35th Annual Symposium on Foundations of Computer Science, 1994, pp. 124-134, doi: 10.1109/SFCS.1994.365700

[2] . A. Mink, S. Frankel and R. Perlner "Quantum Key Distribution (QKD) and Commodity Security Protocols: Introduction and Integration, National Institute of Standards and Technology (NIST)" , 100 Bureau Dr., Gaithersburg, MD 20899 International Journal of Network Security & Its Applications (IJNSA), Vol 1, No 2, July 2009 101, (http://airccse.org/journal/nsa/0709s9.pdf).

[3] Anja Feldmann, Oliver Gasser, Franziska Lichtblau, Enric Pujol, Ingmar Poese, Christoph Dietzel, Daniel Wagner, Matthias Wichtlhuber, Juan Tapiador, Narseo Vallina-Rodriguez, Oliver Hohlfeld, Georgios Smaragdakis, “A Year in Lockdown: How the Waves of COVID-19 Impact Internet Traffic” Communications of the ACM, July 2021, Vol. 64 No. 7, Pages 101-108, doi: 10.1145/3465212

[4] R. Gaudino, V. Curri and S. Capriata, "Propagation impairments due to Raman effect on the coexistence of GPON, XG-PON, RF-video and TWDM-PON," 39th European Conference and Exhibition on Optical Communication (ECOC 2013), 2013, pp. 1-3, doi: 10.1049/cp.2013.1675.

[5] N. Vokic, D. Milovančev, B. Schrenk, M. Hentschel and H. Hübel, "Deployment Opportunities for DPS-QKD in the Co-Existence Regime of Lit GPON / NG-PON2 Access Networks," 2020 Optical Fiber Communications Conference and Exhibition (OFC), 2020, pp. 1-3.

[6] Domenico Ribezzo, Mujtaba Zahidy, Ilaria Vagniluca, Nicola Biagi, Saverio Francesconi, Tommaso Occhipinti, Leif K. Oxenløwe, Martin Lončarić, Ivan Cvitić, Mario Stipčević, Žiga Pušavec, Rainer Kaltenbaek, Anton Ramšak, Francesco Cesa, Giorgio Giorgetti, Francesco Scazza, Angelo Bassi, Paolo De Natale, Francesco Saverio Cataliotti, Massimo Inguscio, Davide Bacco, Alessandro Zavatta, “”https://doi.org/10.48550/arXiv.2203.11359

[7] Alessia Scriminich, Giulio Foletto, Francesco Picciariello, Andrea Stanco, Giuseppe Vallone, Paolo Villoresi, Francesco Vedovato, “Optimal design and performance evaluation of free-space Quantum Key Distribution systems”, https://doi.org/10.48550/arXiv.2109.13886

[8] ETSI Industry Specification Group - https://www.etsi.org/committee/1430-qkd

[9] ITU FG QIT4N - https://www.itu.int/en/ITU-T/focusgroups/qit4n/Pages/default.aspx B. D. Cullity and C. D. Graham, *Introduction to Magnetic Materials,* 2nd ed. Hoboken, NJ: John Wiley & Sons, Inc., 1972. DOI: 10.1002/9780470386323

[10] GSMA, IG.11 – Quantum Computing Networking and Security, July 2021

[11] GSMA, IG.12 – Quantum Networking and Service, December 2021