Integration of QKD in WDM networks

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

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

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

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

Mariangela Rapisarda
Politecnico di Milano, Dipartimento di Elettronica, Informazione e Bioingegneria,
Milano, Italy
mariangela.rapisarda@polimi.it

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

Mario Martinelli
Politecnico di Milano, Dipartimento di Elettronica, Informazione e Bioingegneria,
Milano, Italy
mario.martinelli@polimi.it

***Abstract*— The theme of the integration of Quantum Key Distribution (QKD) in existing WDM optical networks will be discussed. Some evaluations about a reduced-cost implementation of BB84 protocol for QKD will be presented, where a QKD channel in O band is added to classical C-band WDM channels in the same fiber.**

Keywords—Quantum Key Distribution (QKD), Wavelength Division Multiplexing (WDM), Optical Communications

I. Introduction

Nowadays encryption is exploited for protecting information exchange in several applications. Nevertheless, the security of commonly used algorithms of encryption is based on the extremely high computational cost required for message decryption. On the other hand, quantum key distribution (QKD) allows for exchanging between two users (Alice and Bob) a secret key in a way which has been proved as unconditional secure, thanks to the fundamental principles of quantum physics, as the no-cloning theorem, which is an application to qubits of the intrinsic quantum indeterminacy in the measurement of a pair of complementary observables. However, to make the QKD a reliable and effective widespread solution, it is essential to reduce the cost and expand the scalability.

In the present work we investigate the feasibility of a reduced-cost solution for the QKD, based on a novel implementation of the BB84 protocol, the first example of QKD proposed in 1984 by C. H. Bennett and G. Brassard [1] and still adopted today [2-3]. In order to reduce the cost, a polarization-based QKD BB84 protocol has been implemented exploiting only one expensive single-photon detector, placed after the cascade of a controllable polarization rotator (giving one among four possible rotation angles) and a polarization analyzer for the measurement of the quantum state of the photon [4], differently from the standard BB84 implementation that employs a pair of single-photon detectors.

Furthermore, for avoiding the use of dedicated fiber for QKD, in order to reduce the installation and maintenance costs of the communication infrastructure, it is required the integration of QKD in already deployed wavelength-division multiplexing (WDM) fiber-optic communication networks [5-13]. The requirements for the copresence in the same fiber of a QKD channel in O band with classical communication channels in C band will be discussed.

II. Single-detector QKD implementation in WDM optical networks

The common implementation of polarization-based BB84 protocol for QKD is based on the transmission by Alice of a sequence of single photons with controlled states of polarization. For each single photon Alice chooses one of two non-orthogonal polarization basis (either "rectilinear" or "diagonal") and then one of the two states in the given basis. Bob can choose the basis for the single-photon polarization measure by means of a variable polarization rotator with polarization rotation set to either 0° (rectilinear basis) or 45° (diagonal basis). Then Bob perform the quantum measure of the photon polarization by means of two single-photon detectors at the different output ports of a polarization beam splitter. Finally, a sifted key bit either 1 or 0 is obtained when Alice and Bob choose the same basis and there is correspondingly a photon detection either in the first detector or in the second one.

For cost reduction we use a modified version [4] of the polarization-encoded BB84 protocol, where Bob uses a polarization rotator variable over four states and only one single-photon detector. Alice transmits to Bob a stream of polarized single photons, obtained by a strongly attenuated laser followed by a polarization controller. The polarization of each photon is set by Alice in one state of polarization among four possible states (horizontal, vertical, diagonal, anti-diagonal). A key bit is exchanged in a secure way through the

978-3-903176-33-1

quantum channel when Alice and Bob choose the same basis (either "rectilinear" or "diagonal") and a photon is detected after a polarizer set in a fixed state (e.g., vertical). Bob chooses the rotation angle among four possible values (0°, 45°, 90°, 135°), making two binary choices. The first one (i.e., a rotation of either 0° or 45°) represents the choice of the measurement basis and is communicated to Alice through the public channel, while the second one (i.e., an additional rotation of either 0° or 90°) is maintained secret and allows Bob for determining the key bit.

The feasibility of the integration of the proposed scheme of QKD in a WDM optical network has been tested according to the scheme depicted in Fig. 1. The QKD channel is in O band at the wavelength of 1310 nm, while the classical WDM channels, used for carrying the conventional data traffic, are in C band in the wavelength range from 1528 to 1559 nm. The choice of moving the QKD in O band is motivated by the reduction of the crosstalk on QKD channel from classical channels. In our lab experimentation the classical WDM channels are emulated by filtering the amplified spontaneous emission (ASE) of an Erbium-doped fiber amplifier (EDFA) through a programmable optical filter, in order to reproduce the same optical spectrum of a typical WDM signal consisting of 80 channels with 50-GHz spacing and 28-GBaud symbol rate. The QKD channel is multiplexed/demultiplexed in the WDM network by exploiting commercially available O/C WDM couplers. After the demultiplexing of QKD channel, an optical filter centered at 1310 nm and with full-width half-maximum of about 0.8 nm is inserted in the QKD receiver for cancelling the out-of-band crosstalk. The detection of the single photons is carried out through an InGaAs/InP SPAD in gated mode [14]. The experimental results confirm the feasibility of the proposed cost-effective QKD implementation in WDM optical networks, achieving a quantum bit-error rate (QBER) below the accepted limit (11%) for secure QKD [15], in typical operating conditions emulated in laboratory. In view of an in-field deployment of the fiber-optic QKD system, there is the need of an automatic polarization stabilizer at the receiver to compensate for the polarization fluctuations introduced by the standard fiber (i.e., not preserving the polarization) of the optical link [16]. To this aim we have used a device provided by Novoptel and were able to recover the polarization alignment between Alice and Bob over the whole Poincaré sphere [17].

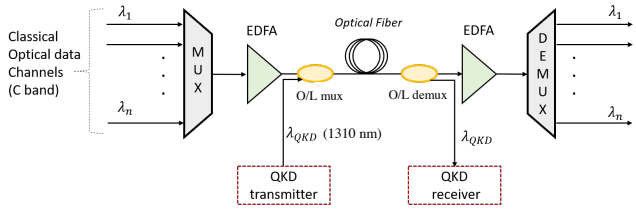

Figure 1. Scheme of the integration of QKD at 1310 nm in a WDM optical communication system.

III. EVALUATION OF QKD SYSTEM PERFORMANCE

The key parameter for evaluating the performance of the QKD system is the quantum bit error rate (QBER) of the sifted key obtained through BB84 protocol. The QBER can be calculated as

$$\mathrm{QBER} = p_{ext} + \frac{p_{dark} + p_{XT}}{p_{photon}}, \tag{1}$$

where p_{ext} represents the polarization extinction ratio of the polarization-based QKD system (i.e. the probability to detect a photon encoded on a state of polarization nominally orthogonal to the state selected by the polarization analyzer), p_{dark} is the probability of having a dark count due to the SPAD, p_{XT} is the probability of having a photon count due to the crosstalk on the QKD signal from the classical C-band signal and p_{photon} represents the probability of a signal photon count.

Assuming a polarization extinction ratio higher than 20 dB, and hence a value of p_{ext} less than 1%, the condition for guaranteeing a QBER in the range for secure QKD, that is QBER ≤ 11%, can be equivalently written as

$$\frac{p_{dark} + p_{XT}}{p_{photon}} \leq 0.1. \tag{2}$$

We can evaluate the above probabilities of counting in a time interval of duration equal to the width T_{gate} of the detection gate in the following way:

$$p_{photon} = \frac{\eta}{A_{link} \cdot A_r} \xi_t \tag{3}$$

$$p_{dark} = r_{dark} \cdot T_{gate} \tag{4}$$

$$p_{XT} = \frac{\eta}{h\nu} \frac{P_{\mathrm{xt}}}{A_r} T_{gate}\,, \tag{5}$$

where η is the quantum efficiency and r_{dark} is the dark count rate of the single-photon detector, while ξ_t is the average number of transmitted QKD photons per gate, A_{link} is the optical attenuation of the fiber link, A_r is the optical loss of the receiver, $h\nu$ is the single-photon energy at 1310 nm and P_{xt} is the average received optical power due to the crosstalk.

Combining Eq. (2), considering the limit condition represented by the equality, with Eqs. (3-5), it is possible to derive the expression of the maximum tolerable crosstalk power at the receiver

$$P_{\mathrm{xt}}^{(max)} = 0.1 \frac{h\nu\, \xi_t}{A_{link}\, T_{gate}} - \frac{h\nu}{\eta} A_r\, r_{dark}\,. \tag{6}$$

Substituting in (6) the values used in lab experimentation $\eta = 0.2$, $r_{dark} = 800$ counts/s, $\xi_t = 0.1$, $T_{gate} = 20$ ns and $A_r = 5$ dB, we can obtain the curve of maximum crosstalk power as a function of the optical link attenuation shown in Fig. 2. In case of optical networks in urban area, with typical links of maximum length of 20 km and link attenuation not higher than 14 dB, we obtain that a crosstalk power of -120 dBm is sufficient for guaranteeing a secure QKD. From preliminary measurements in typical conditions of deployed fiber-optic links in the range of length 5-20 km, in presence of data traffic in C band wavelength channels, the actual

measured crosstalk power at the receiver (after the filter centered at 1310 nm) remains below -120 dBm, allowing for secure QKD over optical links with attenuation up to 14 dB.
The QBER calculated according to (1) and assuming an average crosstalk power at the receiver of -120 dBm, in addition to the previously considered values of parameters for QKD is plotted in Fig. 3 as function of the fiber-optic link attenuation. It is possible to see that the QBER remains below the threshold limit of 11%, guaranteeing the possibility of extracting an unconditionally secure key, when the link attenuation is not higher than 14 dB.

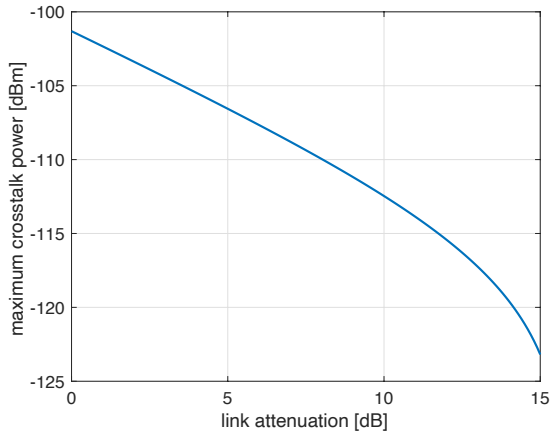

Figure 2. Maximum tolerable crosstalk power as a function of the fiber-optic link attenuation.

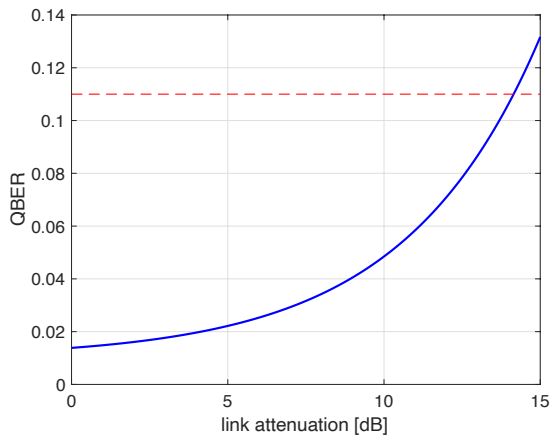

Figure 3. QBER as a function of the fiber-optic link attenuation in case of average crosstalk power of -120 dBm at the receiver.

IV. Conclusions

The feasibility of the integration of a reduced-complexity QKD, based on polarization-encoded BB84 protocol, in WDM optical networks for urban areas has been experimentally verified by laboratory tests, considering a QKD channel in O band, centered at 1310 nm, in presence of an emulated 80-channel WDM classical signal in the commonly used C band. The measured crosstalk level guarantees a QBER less than the threshold value of 11%, guaranteeing an unconditionally secure QKD after the application of information reconciliation and privacy amplification to the BB84 sifted key, for a link attenuation up to 14 dB.

Acknowledgment

This work has been supported by the EIT Digital 2020 “Q-Secure Net” innovation activity.

References

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

[2] H.-K. Lo, M. Curty, and K. Tamaki, “Secure Quantum Key Distribution,” *Nature Photonics* 8, pp. 595–604, 2014.

[3] S.-K. Liao et al., "Long-distance free-space quantum key distribution in daylight towards inter-satellite communications," *Nature Photonics* 11, pp. 509-513, 2017.

[4] P. Martelli, M. Brunero, A. Fasiello, F. Rossi, A. Tosi, M. Martinelli, “Single-SPAD Implementation of Quantum Key Distribution” in *Proc. of Internat. Conf. Transparent Optical Networks (ICTON)*, Angers, France, 2019, paper We.C5.1.

[5] J. Morosi, et al., “25 Gbit/s per user coherent all-optical OFDM for tbit/s-capable PONs,” *J. Opt. Communic. Network.* 8, n. 7452817, pp. 190-195, 2016.

[6] 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.

[7] A. Ciurana, et al., “Quantum Metropolitan Optical Network Based on Wavelength Division Multiplexing,” *Opt. Express* 22, pp. 1576– 1593, 2014.

[8] 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, pp. 285-298, 2019.

[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, 2019.

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

[11] N. Walenta, et al., “A Fast and Versatile Quantum Key Distribution System with Hardware Key Distillation and Wavelength Multiplexing,” *New J. Phys.* 16, 013047, 2014.

[12] M. Sasaki, et al., “Field Test of Quantum Key Distribution in the Tokyo QKD Network,” *Opt. Express,* 19, pp. 10387–10409, 2011.

[13] N. Lo Piparo and M. Razavi,“Long-Distance Trust-Free Quantum Key Distribution,” *IEEE J. Sel. Topics Quantum Electron.* 21, 6600508, 2015.

[14] 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.* 83, 013104, 2012

[15] P.W. Shor and J. Preskill, "Simple proof of the security of the BB84 quantum key distribution protocol," *Phys. Rev. Lett.* 85, pp. 441-444, 2000.

[16] P. Martelli, et al., “Polarization stabilizer for polarization-division multiplexed optical systems,” *in Proc. ECOC 2007 - 33rd European Conference and Exhibition of Optical Communication*, 2007, paper 57584682007.

[17] 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.