Integration of a Cost-Effective QKD Implementation in WDM Optical Networks

P. Martelli, M. Brunero, P. Parolari, F. Rossi, A. Tosi, and M. Martinelli

Politecnico di Milano, Dipartimento di Elettronica Informazione e Bioingegneria, Via G. Ponzio 34/5, 20133 Milano, Italy

Nowadays encryption is exploited for protecting information exchange in several applications. Nevertheless the security of commonly used encryption algorithms is based on the extremely high computational costs required for message decryption. On the other hand, quantum key distribution (QKD) allows the key exchange between two users (Alice and Bob) in a way which has been proved as unconditionally secure, thanks to the fundamental principles of quantum physics [1,2]. However to make the QKD a reliable and effective widespread solution, it is essential to reduce the cost and enhance the scalability.

In the present work we experimentally demonstrate the integration of a cost-effective QKD implementation in a typical WDM optical network. The considered QKD system is based on a modified version [3] of the polarization-encoded BB84 protocol [1], where Bob uses a Faraday rotator (FR) variable over four states and only one single-photon avalanche detector (SPAD), as shown in Fig. 1(a). 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 quantum channel when Alice and Bob choose the same basis (either "rectilinear" or "diagonal") and a photon is detected by the SPAD after a polarizer set in a fixed state (e.g., vertical). Bob chooses the FR 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 integration of the proposed scheme of QKD in a WDM optical network has been tested according to the scheme depicted in Fig. 1(b). The QKD channel is in L band at the wavelength of 1583 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. In our 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 L/C WDM couplers. The detection of the single photons is carried out through an InGaAs/InP SPAD, as described in [4]. 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 [2], in typical operating conditions.

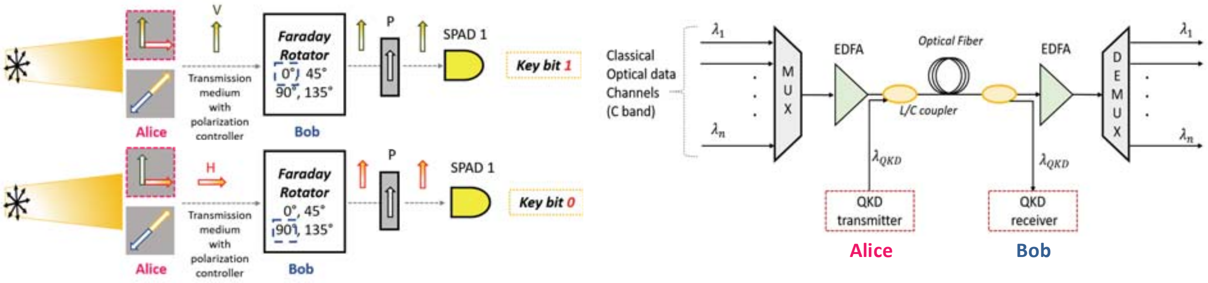

Fig. 1 Scheme of the single-SPAD implementation of BB84 (a); integration of QKD in WDM optical network (b).

References

[1] C.H. Bennett and G. Brassard, “Quantum cryptography: public key distribution and coin tossing,” in Proc. IEEE Internat. Conf. on Computers, Systems and Signal Processing 1984, Bangalore, 175.

[2] P.W. Shor and J. Preskill, “Simple proof of the security of the BB84 quantum key distribution protocol,” Phys. Rev. Lett. **85**, 441 (2000).

[3] P. Martelli et al., “Single-SPAD implementation of quantum key distribution,” in Proc. ICTON 2019, We.C5.1.

[4] A. Tosi et al., “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).