QKD in Classic Optical Networks: Two different worlds forever?

Andreas Poppe,[1] Bernhard Schrenk,[1] Vicente Martin,[2] Slavisa Aleksic[3]

[1]*AIT Austrian Institute of Technology GmbH, Optical Quantum Technology, Safety & Security Department, Donau-City-Strasse 1, Austria*

[2]*Research Group on Quantum Information and Computation, Universidad Politécnica de Madrid, Spain*

[3]*Institute of Telecommunications, Vienna University of Technology, Favoritenstrasse 9/388, A-1040 Vienna, Austria*

Quantum Key Distribution (QKD) is maturing quickly. However, the current approach as a collection of dedicated point-to-point connections over dark fibers specially assigned to the QKD-link turn it to an expensive technology. Thereby the cost of ownership will be determined by the cost of fiber infrastructure. To cut costs a straightforward strategy is to combine QKD-links to QKD-networks or to multiplex communication lines. Different possibilities are feasible:

Firstly, a single connection from each user to the overall QKD-network is possible. In a trusted node the key is combined on demand in such a way that the user can share a secure key with every other user in the network. This kind of QKD-network was shown in recent demonstrations [1, 2]. The disadvantage is that the nodes in between need to be trusted.

Secondly, with a switched network it is possible to connect each user with its communication partner in a direct way. The routing through the network is done by a combination of optical switches and a selection of the wavelength used in the QKD-devices. A solution proposed recently even shares the communication line on the backbone network between many different users [3] and multiplexes the needed classical channel with the quantum channel by the periodic behavior of AWGs (Arrayed-Waveguide Gratings).

Thirdly, the reuse of fiber based telecom access and backbone networks for quantum communication is highly desirable [4]. However, a heterogeneous variety of telecom standards in the access network using passive optical splitters hinders the design of a typical QKD-link suitable for broad usage. Additionally, effects like Raman radiation and Rayleigh backscattering narrows down the possible bands usable for the transmission of single photons without being flooded by uncorrelated noise photons. In the case of the emerging standard NG-PON2 all communication lines in the access network are operated around the S, C and L-Band and so the O-band seems to be free for QKD signals. A suggestion of a possible overall network is shown in fig. 1.

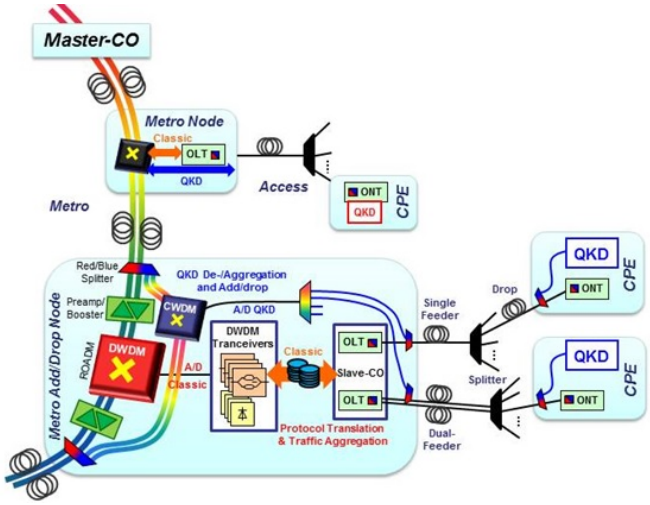

Fig. 1 Schematics of a possible solution to integrate QKD-links in a classic optical network. The QKD-devices located at the CPE (customer premises equipment) are operated at the O-band and the quantum signals are wavelength-multiplexed with the communication channel.

Conclusion: With a new generation of QKD-devices with higher tolerance to losses and more resistant to noise compared with nowadays typical QKD schemes it will be possible to cross access and metro networks.

References

[1] M. Peev et al., "The SECOQC quantum key distribution network in Vienna," New J. Phys.**11**, 075001 (2009).

[2] M. Sasaki, et al., "Field test of quantum key distribution in the Tokyo QKD Network," Opt. Express **19**, 10387 (2011).

[3] A. Ciurana et al., "Quantum metropolitan optical network based on wavelength division multiplexing," Opt. Express 22, 1576 (2014).

[4] P. Townsend, "Quantum cryptography on multiuser optical fibre networks," Nature385, 47–49 (1997).