Distribution of Quantum Keys in Optically Transparent Networks: Perspectives, Limitations and Challenges

Slavisa Aleksic[(1)], Senior Member, IEEE, Dominic Winkler[(1)], Andreas Poppe[(2)], Member, IEEE, Gerald Franzl[(1)], Bernhard Schrenk[(2)], Member, IEEE, and Florian Hipp[(2)]

[(1)]Institute of Telecommunications, Vienna University of Technology,
Favoritenstrasse 9/388, A-1040 Vienna, Austria
{slavisa.aleksic, gerald.franzl}@tuwien.ac.at, e0426151@student.tuwien.ac.at
[(2)] Safety & Security Department, AIT Austrian Institute of Technology GmbH
Donau-City-Strasse 1, 1220 Vienna, Austria
{andreas.poppe, bernhard.schrenk, florian.hipp.fl}@ait.ac.at

ABSTRACT

Transparent optical networks are capable of providing a flexible and dynamic data transport via transparency regarding both data rate and format of transmitted signals achieved by implementing data transmission and forwarding in the optical domain. While supporting all-optical end-to-end paths, transparent optical networks are in principle suitable to integrate end-to-end quantum cryptography. However, quantum signals are extremely sensitive to loss and noise, which is a particular issue because of the cascaded passive and active components along signal paths, common with transparent optical networks. In this paper we analyze different options for integrating quantum key distribution (QKD) in wavelength-division multiplexed (WDM) transparent optical networks where QKD signals are transmitted along with conventional WDM signals. We discuss potentials, challenges and limitations in order to assess the practicability of such systems.

1. INTRODUCTION

Quantum cryptography, in particular quantum key distribution (QKD), promises a high level of communication privacy and security through utilizing quantum physical properties of optical signals in combination with conventional cryptography methods and algorithms. QKD relies on the principles of quantum physics and does not depend on mathematical or computational assumptions. The main benefit of using QKD is that eavesdropping is unavoidably detected since any attempt to yield information about the key disturbs the quantum bits (called qubits) carried by single photons. Especially the no-cloning theorem [1] forbids an identical copy of any arbitrary qubit, because the needed superposition of the states would be destroyed and subsequently the quantum bit error rate (QBER) is increased.

Although the idea to utilize the quantum nature of optical phenomena to encrypt transmitted data is not substantially new - it was already introduced in early 1980's [2] - practical QKD systems that can be smoothly and economically integrated in conventional optical networks are still not available. First attempts to realize practical QKD systems were concentrated on transmitting QKD channels over dedicated fibers [3] -[5], which is economically impractical because of the high costs of installing (or leasing) additional dark fibers. Therefore, the options to transmit weak QKD signals together with strong conventional optical channels while sharing the same fiber has been of particular interest in recent years [6] -[11]. However, most studies consider systems with limited launch powers, network reach and spectral occupancy (i.e., number of wavelength channels). An overall characterization of possibilities and limitations upon the integration of QKD systems in conventional networks, considering typical and worst case conditions, is to the best knowledge of the authors missing. Especially the integration of QKD systems in transparent optical networks has not yet been adequately addressed.

In this paper, we focus on different options to integrate QKD systems in transparent optical networks and analyze the impairments that result from strong classical signals and cascaded optical components. The paper is structured as follows. In the next section, we outline different methods to implement QKD systems. Following that we discuss different options for integrating QKD systems in transparent optical networks and indicate the factors that primarily limit the achievable reach and key rate. In Section 4 we discuss limitations and perspectives for the evaluated QKD integration options. Finally, in Section 5 we draw our conclusions.

2. QUANTUM KEY DISTRIBUTION SYSTEMS

Quantum-encrypted communication systems comprise a sending unit (Alice) and a receiving unit (Bob) (see Fig. 1a). The main difference to classical communication systems resides in the properties of the optical signals exchanged, particularly the extremely low signal powers at single-photon level and the methods used to establish a reliable exchange of secret keys. Depending on the QKD system, a co-existing time-stable classical channel for synchronization may be needed besides a necessary communication between the different layers of the QKD protocol stack (see Fig 1b). The foundation of any QKD protocol is a quantum channel that allows encoding

quantum information by transmitting photon states (e.g. qubits) and eventually measuring them in one of at least two unbiased, non-orthogonal bases. Quantum mechanics and mathematical statistics dictate that an eavesdropper cannot gain full information without prior knowledge about the encoding bases. Any attempt to eavesdrop, i.e. to measure the transmitted photon projects the quantum state to a certain result. The attacker will be noticed either by the lack or the incorrect state (only guessing is possible) of the transmitted photon. The eavesdropper thus leaves its mark in the form of an increased error rate of QBER $\geq$ 11 %, if the best possible attack is assumed and all photons are successfully attacked. A lower error rate indicates quantum information protected by physical laws to any third party. In that a case, a secret key can be extracted with confidence.

QKD protocols either belong to the family of "prepare and measure" protocols (e.g. BB84, BB92, SARG), i.e., Alice prepares a photon by measuring it in a certain basis and then transmits it to Bob together with the information gained, or are "entanglement based" protocols (E91, BBM92), where Alice and Bob both receive entangled photons and perform measurements on an individual basis. In the sifting phase (Fig. 1b) all transmitted keys are discarded for which no photon was measured due to absorption or limited quantum efficiency of the detector and in case the receiver selected a different basis than the sender. Next an error detection/correction phase is executed to compensate for wrong measurements due to intrinsic detector or channel noise and potential quantum attacks. Finally, the key length is reduced according to the evaluated QBER level in order to decrease the potential for leaked key bits (privacy amplification). The remaining key bits form the secret key used to securely exchange data utilizing classical data encryption methods. In order to prevent a man-in-the-middle attack some sort of authentication needs to be established on top.

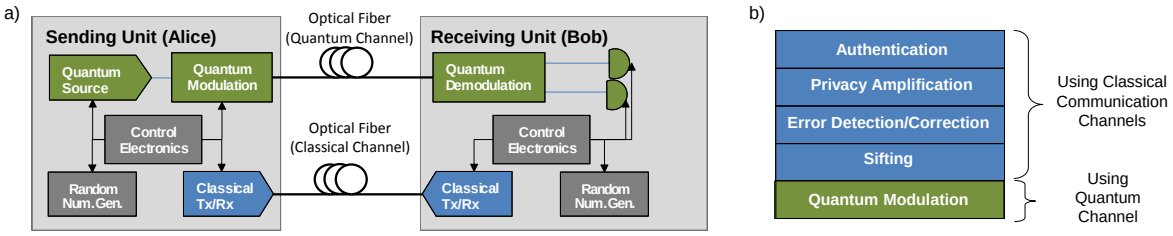

Fig. 1. Generic structure of a) QKD system and b) QKD protocol stack.

The recent research literature presents a variety of QKD schemes that can be distinguished by the type of quantum encoding (phase or polarization of photons) and the used photon sources. The quantum information is encoded on quantum signals with a resolution of only one photon corresponding to pulse energy of 1.28×10^{-19} J at 1550 nm. Each signal with two or more photons is a security risk, because a second photon may carry the same quantum information and could subsequently be eavesdropped by an adversary without being noticed.

Since the technology to generate single photons on demand with quantum dots is not mature enough, many QKD schemes use weak laser pulse sources. The laser pulse is attenuated by approximately 70 dB to the level of 1 photon/pulse in average. According to the Poisson statistics, there still exist quite many pulses with more than 1 photon/pulse; and thus techniques such as decoy state protocols were proposed to minimize the impact of photon-number-splitting (PNS) attacks on the secure key rate. Asymmetric Mach-Zehnder Interferometers (AMZI) and phase modulators can be used to realize the fast weak laser pulse scheme with the disadvantage of on-going phase-stabilization [3]. Further, the commercially available Mach-Zehnder implementation called plug&play scheme from the Swiss company idQuantique [4] can be used to phase-encode quantum bits. Here, the signal is generated at Bob's site and attenuated, measured (prepared) and reflected by a Faraday mirror at Alice's site to compensate for polarization and phase fluctuations along the quantum channel.

In contrast to the weak laser pulse approaches it is also possible to exploit the entanglement of two photons. In order to get entangled, information about all possible observables that could be measured to distinguish two photons has to be erased. Spontaneous parametric down-conversion (SPDC) in non-linear crystals can be used to generate such pairs of photons that can be distributed to Alice and Bob. Two different approaches can be used to measure the correlation. The rather impracticable Ekert scheme (E91) [12] uses on-going tests based on Bell's inequality to detect eavesdropping. Today, most entanglement based QKD schemes implement an adaptation of the conventional BB84 protocol called BBM92 [13]. Instead of Alice preparing the photon before Bob measures it, both can measure their received photons independently and negotiate jointly a secret key based on the unique quantum mechanical correlations they independently detect.

Instead of using the phase or polarization of single photons to encode qubits coherent detection of stronger optical pulses can be used as in Continuous-Variable (CV) QKD protocols [14]. For example, the two quadratures of a coherent state can be used as conjugate variables.

Many systems mentioned above have been integrated in a dark fiber network [3], [4], [13] and [14]. The sender and receiver have been allocated at trusted nodes and the systems could deliver their keys to key-stores.

Key distribution has been achieved by XOR-combinations of secret keys from different systems, such that a quantum key received by a QKD link was encrypted by a second key in order to deliver it over a classical channel. Only the corresponding partner that knows the second key could decrypt the original in order to use it.

Despite the attractiveness of QKD to enable novel, secured services in a trusted network infrastructure, the integration of quantum-enabled concepts in modern optical telecommunication architectures is by no means straightforward. The susceptibility of quantum channels to even weak crosstalk from classical channels in the same, shared fiber medium demands spectral-occupancy conscious planning. The requirements on the maximally allowed background noise in QKD systems become clearer when we consider the following example. If we assume a weak laser pulse system operated with a pulse repetition rate of 10MHz (limited by detector opening frequency) with a typical number of photons/pulse of 1/10, which is operated on a quantum channel (a transparent all-optical path) with a transmission loss of 15 dB, one can expect that approximately 30.000 photons per second arrive at the receiver. For the sake of simplicity, we do not consider the effect of the detector dead time here, so we can assume an overall receiver opening time of 50 ms in each second (10 million gate openings of 5 ns duration). Within this time any in-band background noise photons generate detector signals, which are not distinguishable from the original quantum signals. In order to achieve reliable quantum keys, the ratio between signal and background photon counts needs to be greater than 10, such that within this 50 ms only 3,000 background photons may at maximum be received, which corresponds to an accepted background noise rate of 600,000 photons per second. These numbers are rough estimations taking the basic operation of a QKD-system into account only; practical tests are required to evaluate the precise limits for different QKD systems.

3. INTEGRATION OF QKD SYSTEMS IN TRANSPARENT OPTICAL NETWORKS

Successful exchange of quantum keys has been demonstrated recently up to about 144 km in a free-space terrestrial link [15] and 250 km over optical fibers [17]. However, the latter experiment has been carried out using a dedicated special low-loss fiber for the quantum channel. Theoretical and experimental investigations concerning the co-existing of quantum and conventional channels have shown that when using the current QKD technology, limiting the number of WDM channels (e.g. to four channels) and reducing the signal power far below the standardized levels, a reach up to 50 km is achievable [6]. This is too short for long-haul links, but suitable for implementing QKD in the metropolitan area. More recently, co-existence of QKD with a classical channel in a shared fiber has been demonstrated by reducing the launch power for classical communication to its limits [18]. The work presented here, however, considers options for implementing QKD in optically transparent metro and access networks as depicted in Fig. 2a that are operated according to typical standards.

In the following, we assume typical distances (20 km to 60 km), signal power levels (-8 dBm to 1 dBm) and channel count (40 channels) in metro and access networks. Across a transparent optical network the weak quantum signals may have to traverse optical amplifiers and optical switches, in addition to traversing the fiber links along their path. Both, active and passive components within an optically transparent node contribute to a disadvantageous increase in either background noise or attenuation, which can severely impair the quantum signal. To reduce the influence of amplified spontaneous emission (ASE) noise, attenuation, crosstalk and nonlinear effects such as inelastic scattering and four-wave mixing, the appropriate selection of the emission wavelength for QKD channels must be performed carefully. Optical components such as splitters, amplifiers and even whole network nodes often need to be bypassed, using separation of QKD and classical channels by wavelength or waveband filters (WDM couplers) with a relatively low loss of 0.4-0.6 dB. Fig. 2b shows bypassing of passive splitters or arrayed waveguide gratings (AWGs) in case of passive optical networks (PONs). In this figure, we show only one QKD channel reaching a single user of the PON for the sake of simplicity. In general, all users can be connected by separate QKD channels at different wavelengths transmitted in a WDM manner [11]. Fig. 2 c,d show bypassing of in-line amplifiers and entire optical nodes respectively for metropolitan area networks. Having bypassed the network components that a QKD signal cannot pass well, the signal degradation that accumulates along the traversed fiber sections still needs to be considered.

Since all QKD systems are extremely sensitive to losses and noise, the effects that mainly influence the transmission of the weak QKD signals determine if sharing the same fiber is possible or not. Depending on the fiber type used for transmission, an attenuation curve describes the wavelength dependent attenuation of optical signals being transmitted along the fiber. ITU-T G.652-compatible Standard Single-Mode Fibers (SSMF) exhibit a broad water peak around 1383 nm, making this wavelength range impractical for efficient transmission. The "conventional" band about 1.5 μm (C-band) is most widely used for modern long-range optical communications due to the low attenuation down to 0.2 dB/km. The low attenuation makes this band also attractive for QKD systems, but the co-existing classical signals within the same band likely cause serious impairments. The "original" band around 1.3 μm (O-band) has a higher attenuation of about 0.3 dB/km. It is often used for short- and middle-range transmission and may be appropriate for accommodating a quantum channel in some cases because of the large spectral offset to signals in the typically highly occupied C-band.

Scattering effects in the fiber medium poses one of the major sources for signal degradation in QKD

channels. Inelastic photon scattering causes frequency shifts of incident photons. The scattering related to acoustic vibrations (Brillouin scattering) can be mostly neglected because of its low bandwidth (1-10 GHz) that does not influence neighboring channels in the 100 GHz ITU-T grid. In contrast, Raman scattering, where optical phonons are involved, introduces large spectral shifts with a maximum offset of 13 THz from the incident (pump) wavelength. In case of Stokes scattering, part of the photons energy is absorbed by the fiber resulting in the generation of scattered waves at lower frequencies. When a photon is scattered off, exited phonon energy is transferred to the photon in an anti-Stokes process resulting in a higher frequency. The anti-Stokes scattering is less effective as it requires the pre-existence of vibrational modes. Thus, the QKD wavelength should preferably be chosen below the wavelength of crosstalk-inducing data channels in order to minimize Raman scattering effects.

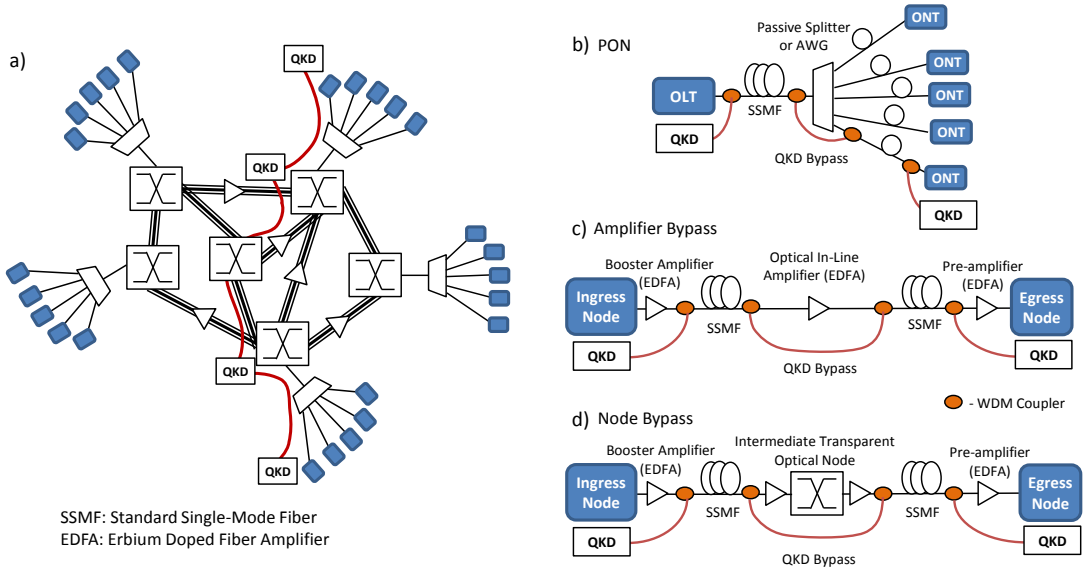

Fig. 2. Integration of QKD in transparent optical networks: a) generic representation of a QKD path in metro-access networks, b) QKD in PONs, and QKD bypass for c) an in-line amplifier and d) a transparent node.

Finally, when dealing with multiple signals at different wavelengths or frequencies f_1, f_2, .. f_n, as it is the case in WDM transmission systems, the effect of four-wave mixing has to be considered as well. Here, no energy is transferred to or from the fiber matter, but the scattering of incident photons produces another photon at a different wavelength. The efficiency of four-wave mixing depends on the coherence of the incident photons and commonly decreases quickly due to the chromatic dispersion. Thus, the quantum channel should not be placed at frequencies corresponding to $f_{ijk} = f_i + f_j - f_k$, where $i, j, k = 1, 2, \ldots, n$ and $i, j \neq k$.

4. WAVELENGTH SELECTION FOR QKD IN TRANSPARENT OPTICAL NETWORKS

Since both attenuation and accumulated background noise depend on the chosen wavelength and are influenced by system parameters such as the path length, power levels of transmitters, wavelength plan and network architecture, it is crucial to determine noise levels and achievable QBER for the systems presented in Fig. 2 taking into account typical system parameters. Fig. 3 presents the background noise spectra obtained by numerical simulations in terms of photon numbers per second and 12.5 GHz resolution bandwidth. In order to allow a reliable exchange of quantum keys, the number of background photons should be in the order of or preferably below 10^5 (< 600,000 photons as stated in Section 2). Thus, it seems that the O-band is potentially best suited to accommodate QKD channels. It is evident from Fig. 3a that the background noise in 1 Gbit/s and 10 Gbit/s PONs such as EPON, GPON, 10G-EPON and XG-PON is above 10^5 across the entire considered wavelength range. This is mainly due to the fact that these standards specify spectrally widely separated upstream and downstream channels. In contrast, the upstream and downstream channels of PON options employing wavelength-division multiplexing (WDM PON and WDM/TDM PON) can be all accommodated within the C-band, such that background noise in the O-band remains below 10^5. Similarly, metropolitan area networks commonly make use of the ITU-T grid within the C-band. Optionally, an optical supervisory channel (OSC) can be placed around 1510 nm. Hence, for 40-channel point-to-point DWDM metro networks, the background photon count remains below 600,000 per second within the whole O-band for launch powers up to 1 dBm per channel (see Fig. 3b). A similar noise spectrum with 10^4 to 10^6 background photons per second within the O-band has been obtained for optically transparent paths with bypassed in-line amplifiers and optical nodes.

In addition to the background noise, the path loss and the QKD scheme and protocol applied influence the achievable QBER and, thereby, the achievable secret key rate (R_{sec}) of the QKD system. To illustrate the effect of

combined impairments, we estimate the achievable QBER and R_{sec} for an exemplary QKD system [6] that uses the BB84 protocol. A detailed description of the method and the parameters to calculate QBER and R_{sec} can be found in [6]. The obtained results are presented in Fig. 4. The QBER and R_{sec} values shown in Fig 4a indicate that for WDM and WDM/TDM PONs, a QBER < 11 % and secret key rates in the order of tens of bit/s are achievable within a portion of the O-band, while for10G-EPON and XG-PON the QBER values are above the Shannon limit all over the considered spectrum.

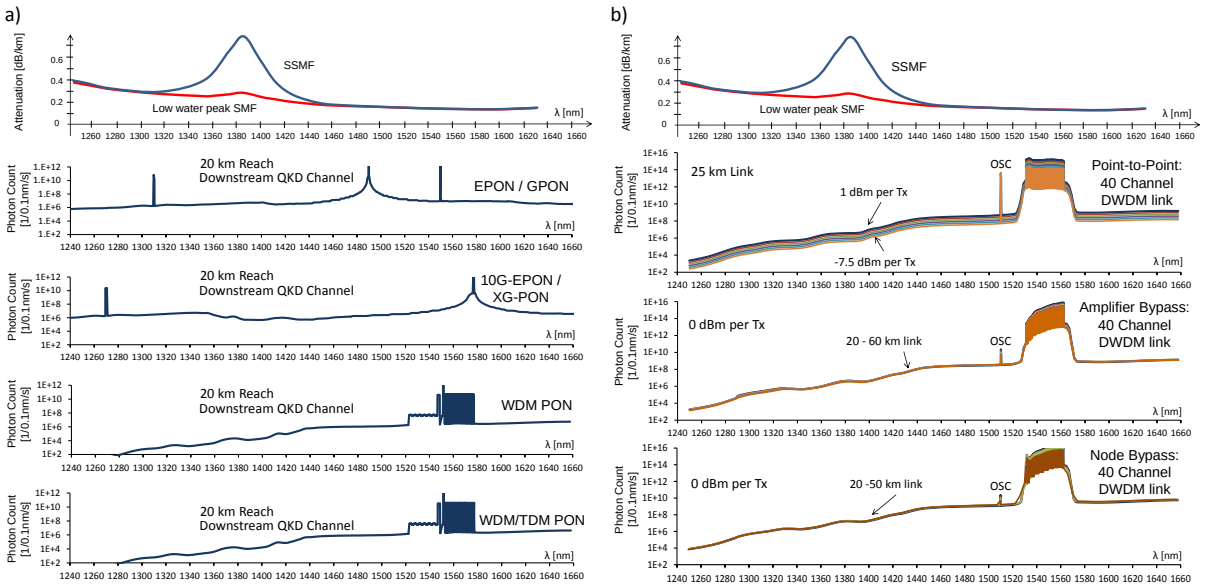

Fig. 3. Intensity of background noise given in photons/s and 12.5 GHz resolution bandwidth in a) passive optical networks and b) metropolitan area networks with 40 DWDM channels (100 GHz ITU-T grid).

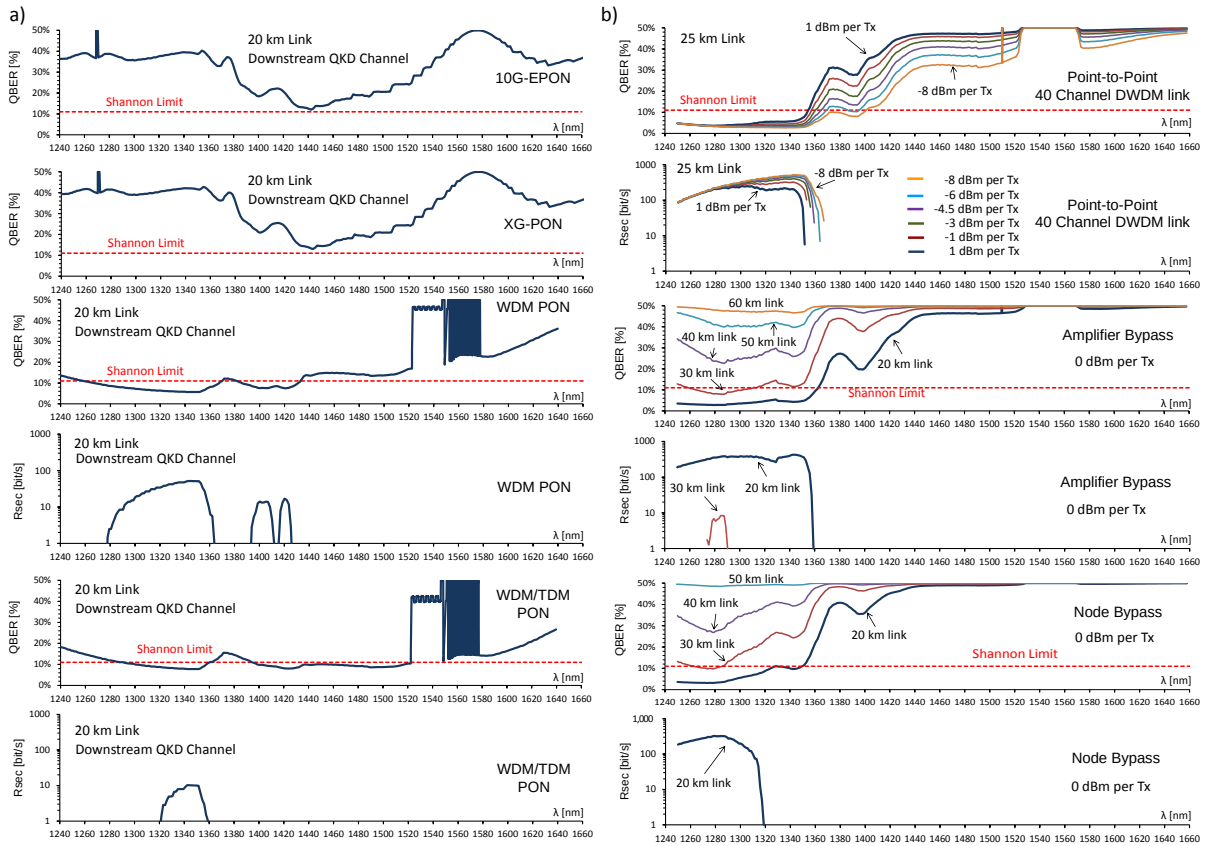

Fig. 4. Estimated quantum bit error rates (QBER) and secret key rates of a QKD system using the BB84 protocol in a) passive optical networks and b) metropolitan area networks with 40 DWDM channels.

Fig. 4b shows that for a point-to-point 20 km DWDM link, the QBER remains below 5 % in the whole O-band, promising achievable secret key rates of several hundreds of bit/s. Bypassing amplifiers or nodes the R_{sec} reduces to a maximum of 10 bit/s for 30 km long transparent optical paths. For wavelengths above 1360 nm and paths longer than 30 km the QBER increases above the Shannon limit (11 %) in any bypassing case.

5. CONCLUSIONS

Although the idea to utilize the quantum optical properties for the encryption of data transmitted over optical links is about 30 years old, the implementation of quantum cryptography has not yet reached acceptance by users, also caused by the current need of a dark fiber for each quantum key distribution (QKD) system. The integration in conventional optical networks presumes a robust and economical embodiment of QKD systems.

In this paper, we discussed perspectives, limitations and challenges for implementing QKD systems in transparent optical networks. We evaluated the expected impairments deriving from coexisting data channels and network subsystems conforming to conventional standards. The main impairments result from optical losses and noise accumulation along paths. Even following the selection of the preferred wavelength for QKD systems (according to the outcome of our simulations) the QKD performance is limited by optical excess losses and noise accumulation along the lightpath. Optical components and network nodes that heavily affect the QKD channel need to be bypassed at the cost of additional coupling losses. In particular, for QKD channels placed within the preferred O-band we observed low-enough background noise levels for a reliable quantum key exchange in WDM PON, WDM/TDM PON and 40-channel DWDM metro networks. A forbiddingly high background noise level across the entire considered spectrum was observed for EPON, GPON, 10G-EPON and XG-PON. Acceptable QBER and sufficient secret bit rates seem possible if classical data channels are restricted to the C-band and the QKD channel is allocated in the O-band, at least for transparent optical paths not exceeding 20 to 30 km of standard single-mode fibers, provided that optical amplifiers, splitters and any intermediate active nodes are bypassed.

ACKNOWLEDGEMENTS

This work was supported in part by the project “QKD-Telco: Practical Quantum Key Distribution over Telecom Infrastructures” (contract No. 835926), within the FIT-IT programme funded by the Austrian Federal Ministry for Transport, Innovation and Technology (BMVIT) in coordination with the Austrian Research Promotion Agency (FFG).

REFERENCES

[1] W. Wootters, W. Zurek, "A Single Quantum Cannot be Cloned". Nature 299, pp. 802–803, 1982.
[2] C. Bennett and G. Brassard, “Quantum cryptography: public key distribution and coin tossing,” in Proc. of *IEEE Intern. Conf. on Comp. Syst. and Sign. Process*., Bangalore. IEEE, 1984, pp. 1291–1293.
[3] A. J. Shields, C. Gobby, and Z. L. Yuan, “Quantum key distribution over 122 km of standard telecom fiber,” in *Applied Physics Letters*, vol. 84, 2004.
[4] D. Stucki, N. Gisin, O. Guinnard, G. Ribordy, and H. Zbinden, “Quantum key distribution over 67 km with a plug&play system,” New Journal of Physics, vol. 4, pp. 41–1, 2002.
[5] A. Treiber, A. Poppe, M. Hentschel, D. Ferrini, T. Lornser, E. Querasser, T. Matyus, H. Hbel and A. Zeilinger, “A fully automated quantum cryptography system based on entanglement for optical fibre networks,” in *New J. Phys.*, 11, 2009.
[6] P. Eraerds, N. Walenta, M. Legre, N. Gisin, and H. Zbinden, “Quantum key distribution and 1 Gbps data encryption over a single fibre,” *New J. Phys*, vol. 12, no. 6, p. 063027, 2010.
[7] R. J. Runser, et al., “Demonstration of 1.3 μm quantum key distribution (QKD) compatibility with 1.5 μm metropolitan WDM,” in Proc. of *OFC’05*, Anaheim, 2005, paper OWI2.
[8] T. Chapuran, et al., “Optical networking for quantum key distribution and quantum communications,” *New J. Phys.*, vol. 11, no. 10, p. 105001, 2009.
[9] P. Townsend, “Simultaneous quantum cryptographic key distribution and conventional data transmission over installed fibre using wavelength-division multiplexing,” in *Electronics Letters*, vol. 33, no. 3, 1996.
[10] R. J. Runser, et al., “Progress toward quantum communications networks: opportunities and challenges,” *Optoelectronic Integrated Circuits IX*, vol. 6476, p. 6476OI, 2007.
[11] S. Aleksic, D. Winkler, A. Poppe, B. Schrenk and F. Hipp, “Quantum key distribution over optical access networks”, to be published in Proc. of *NOC/OC&I 2013*, Graz, Austria, July 2013.
[12] A. K. Ekert, Phys. Rev. Lett. 67, 661, 1991.
[13] C. H. Bennett, G. Brassard, and N. D. Mermin, *Phys. Rev. Lett*. 68, 557, 1992.
[14] S. Fossier et al., 2009 *New J. Phys.* 11, 045023 doi:10.1088/1367-2630/11/4/045023.
[15] T. Schmitt-Manderbach et al., “Experimental Demonstration of Free-Space Decoy-State Quantum Key Distribution over 144 km,” Phys. Rev. Lett. 98, pp. 010-504-1 - 010-504-14, 2007.
[16] M. Peev et al., 2009 *New J. Phys.*, 11, 075001 doi:10.1088/1367-2630/11/7/075001.
[17] D. Stucki, et al., 2009 *New J. Phys*., vol. 11, 075003, doi:10.1088/1367-2630/11/7/075003.
[18] K. A. Patel, J. F. Dynes, I. Choi, A.W. Sharpe, A. R. Dixon, Z. L. Yuan, R.V. Penty, and A. J. Shields “Coexistence of High-Bit-Rate Quantum Key Distribution and Data on Optical Fiber,” *Physical Review X*, vol. 2, p.041010, 2012.