Coexistence scheme for entanglement based QKD in a wavelength multiplexed PON

Florian Hipp[a], Michael Hentschel[a], Slavisa Aleksic[b], Andreas Poppe[a] and Hannes Hübel[*,a]
[a]Safety & Security Department, AIT Austrian Institute of Technology GmbH, Donau-City-Strasse 1,1220 Vienna, Austria; [b]Institute of Telecommunications, Vienna University of Technology, Favoritenstrasse 9/388, 1040 Vienna, Austria
Corresponding author: hannes.huebel@ait.ac.at

1. COEXISTANCE SCHEME AND ENTANGLED PHOTON SOURCE

Distributing quantum mechanically secured key over optical fiber networks, will substantially enhance the security of digital communication. Current QKD systems however require a dedicated point-to-point fiber between sender (Alice) and receiver (Bob) to act solely as the quantum channel. This is needed because additional signals, in particular classical telecommunication signals, on the same fiber lead to high levels of noise and in most cases the weak quantum signal cannot be recovered afterwards. The high cost of a dark fiber which is exclusively used for the quantum data transfer is likely to prohibit a large scale roll-out of QKD over metropolitan area networks (MAN) and passive optical networks (PON). It is therefore essential for the further growth of QKD in telecommunication networks when the quantum signal and classical data are transmitted over the same fiber. Integrating a quantum signal and classical channel on the same fiber, also referred to as *coexistence scheme*, has recently been demonstrated in a number of QKD implementations. The theoretical scheme how a QKD system is implemented into a telecom system is shown on the left side of Figure 1. In contrast to these approaches that use attenuated laser pulses our coexistence scheme exploits polarization entanglement of two photons. The right hand side of Figure 1 shows the experimental setup that was used to determine the performance of such integration. Photon pairs of 1310nm (O-Band) and attenuated classical signals are hereby transmitted on a shared fiber and separated afterwards with the help of Far Wave Division Multiplexers (FWDM) and suitable filters. The corresponding 590nm photon is measured locally in two non-orthogonal bases.

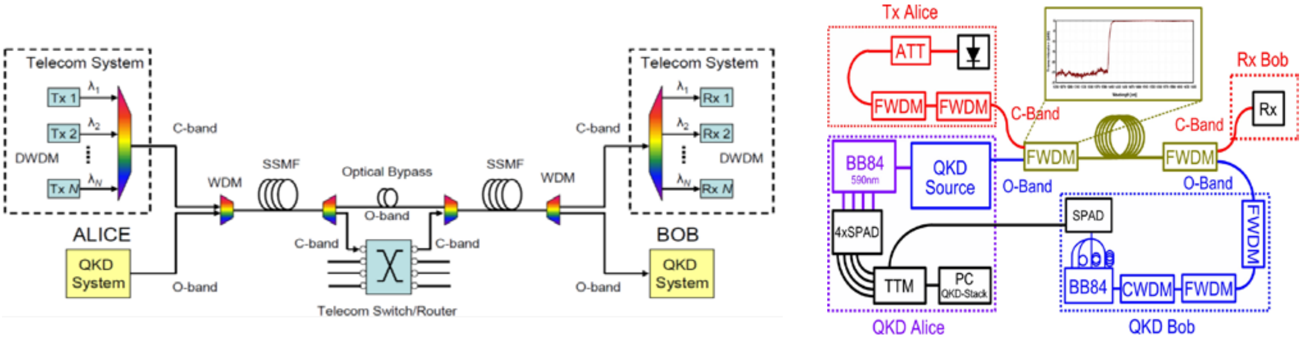

Figure 1: Left: Coexistence scheme of a classical telecommunication link in the C-band with a multiplexed quantum channel in the O-band. Right: Experimental setup of an entanglement based QKD system integrated in a classical link for performance evaluation .

In our setup we make use of a periodically poled Potassium Titanyl Phosphate (KTP) crystal with a poling period of $\Lambda = 3.875\ \mu m$ embedded in a Sagnac interferometer. Figure 2 shows the setup of the complete source. The pump laser is a 405 nm single frequency laser with an elliptical beam profile, which needs to be reshaped by means of cylindrical lenses and is focused with a spherical lens to a spot size of 40 µm. The polarization is set to diagonal and the phase can be adjusted with a pair of birefringent wedges. Inside the Sagnac loop the two polarization components (horizontal and vertical) are split with a polarizer and sent into the loop with counter-propagating directions. The vertical polarization (clockwise) is flipped to horizontal with a half wave retarder set to 45°. As, to our knowledge, half-wave-plates operating at three arbitrary wavelengths are not readily available, we employ the phase shift of total internal reflection in Fresnel-rhombs to obtain the desired wave retardation. The actual implementation can be seen in middle of Figure 2. In order to provide a complete indistinguishability of the two round trip modes, we placed an identical wave retarder at the according position in the other arm, only set to zero degree. Moreover, a piece of Calcite is placed before the interferometer with its optical axis rotated by 90° with respect to the polarizer, in order to exactly compensate the birefringent effect of the latter. The respective pump beams are then steered by two silver mirrors into the nonlinear crystal where the type-0 down-conversion takes place. Thus, signal and idler photons are generated with $\lambda_s = 586$ nm and $\lambda_i = 1310$ nm, respectively. Again, the counter-clockwise mode gets flipped in polarization and is superimposed on the clockwise mode at the polarizer, thus creating the entangled state $|\phi^+\rangle = |H_{586}\rangle\,|H_{1310}\rangle + |V_{586}\rangle\,|V_{1310}\rangle$. The photons are then separated from the pump beam with a specially designed trichroic mirror and further split into signal and idler with a dichroic mirror. Finally the photons are bandpass filtered and coupled into the optical fibers. The 1310nm are multiplexed with classical signals and eventually measured in a time multiplexed BB84 module that requires only a single free running InGaAs-APD to reduce cost on the detection side of the Bob, the user. The arrival time of each photon is recorded by a time tagging module (TTM) and via post processing assigned to its 590nm counterpart measured by Alice. After sifting, error correction and privacy amplification a secure key is generated.

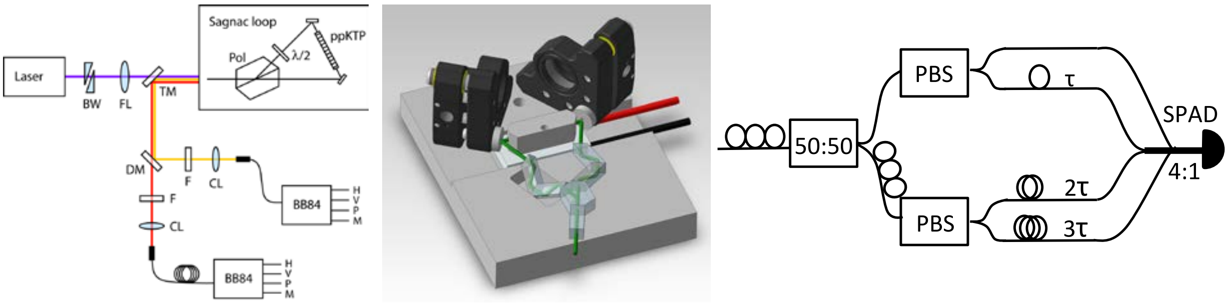

Figure 2: Left: Schematic of the entangled source with birefringent wedges BW, focusing lens FL, trichroic mirror TM, Glan-Thomson polarizer Pol, half wave retarder, KTP crystal, dichroic mirror DM, filters F and coupling lenses CL. Middle: A detailed 3 dimensional model of the Sagnac loop. Right: Time multiplexed BB84 module with polarization control PC, 50:50 splitter, polarizing beam splitters PBS, delay fibers and 4:1 coupler.

2. RESULTS

When measured locally, i.e. without a long fiber between Alice and Bob and without multiplexed classical signal the source produces a raw key rate of around 3000 bit/s with an QBER of 5.6%. Using a fully operational QKD post-processing stack a secure key with a rate of 220 bit/s can be extracted with this setup. The low overall rate and rather high QBER is attributed to a faulty wedge (BW), which produces spatial beam distortions and phase distortions. Nevertheless the performance of the setup alone can be seen as a benchmark against which the influence of Raman scattering is evaluated. For the first measurement a cw tunable laser source at 1550.12nm was used to simulate the classical channel. The blue curve in this case indicated the 15.3km fiber, the red line 2x4.3km and black 4.3km.

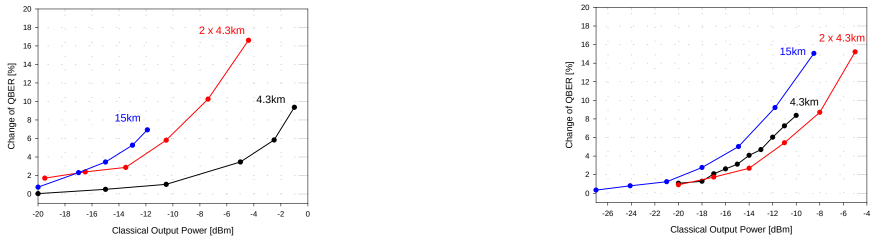

Figure 3: Left: Change of QBER with increasing Output power of a single classical channel for 4.3km (black) 2x4.3km (red) and 15.3km (blue). Right: Change of QBER with increasing Output power of 6 classical channels for 4.3km (black) 2x4.3km (red) and 15.3km (blue).

With a cascade of CWDM and 1310nm Add/Drop filter, as displayed on the left picture of Figure 4, we were able to improve the robustness of the QKD system with respect to noise photons by a factor of 10. This is shown on the right picture of Figure 4, where the two lines represent the received noise photon at Bob's detector (blue for DWDM, red for CWDM filter). This results in a slower raise of QBER (shown in the two graphs in the middle of Figure 4, again red for CWDM filter and blue for DWDM) such that data channels can be operated at output powers close to -4 dBm.

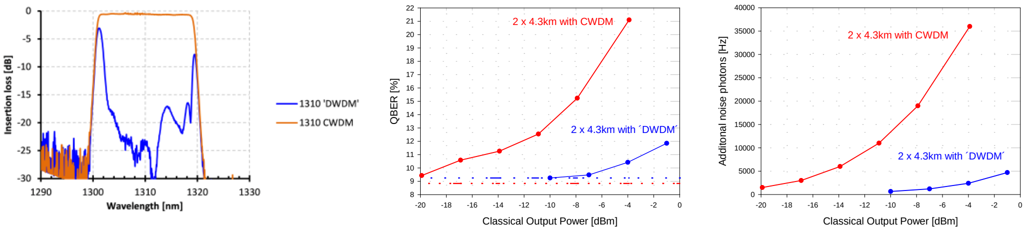

Figure 4: Left: Transmission curve of the "DWDM" filter. Middle: QBER over output power for CWDM (red) and DWDM filter. Right: Noise photons over output power for CWDM (red) and DWDM filter (blue)

Furthermore a quantum and an attenuated classical channel could be demonstrated to operate in the same band when time multiplexing is applied. The results showed that the QBER can be reduced by over 30% when Alice detector and data signal are gated in disjunct time windows.

Finally we were able to setup a point-to-point link with two encrypter boxes for Alice and Bob. Both operated the AIT Stack software in such a way that classical communication, such as sifting and privacy amplification, was sent via the same fiber as the single photons. A secure key was hereby established over 8.4km and 13.2km.

ACKNOWLEDGMENTS

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 program funded by the Austrian Federal Ministry for Transport, Innovation and Technology (BMVIT) in coordination with the Austrian Research Agency (FFG).