QKD in Optical Networks

Slavisa Aleksic, Dominik Winkler, Gerald Franzl,
Andreas Poppe, Bernhard Schrenk and **Florian Hipp**

FFG

TU WIEN

AIT AUSTRIAN INSTITUTE OF TECHNOLOGY

Florian.hipp.fl@ait.ac.at

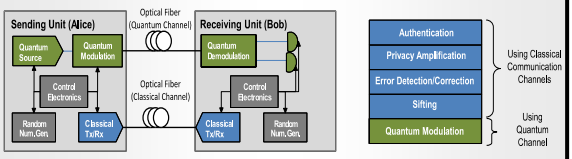
The Situation Today / Motivation

State of the art cryptographic protocols for public networks like TLS or IPsec employ methods like RSA, Diffie Hellman or Elliptic Curve Cryptography to ensure the secure creation of a key pair. These methods are based on trap door functions that can only be inverted by solving a computational hard problem. Assuming further developments in classical as well as in quantum computations these methods can no longer guarantee for safe communication.

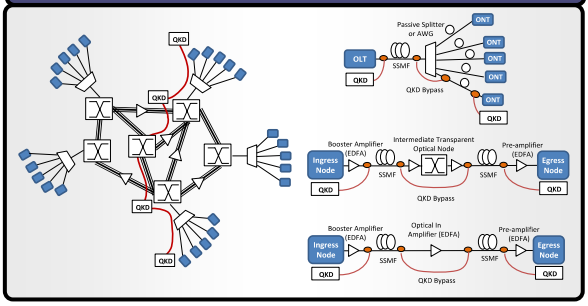
Abstract

We investigate the possibility to include QKD models like BB84 and SARG in actual optical networks alongside with classical signals. Our simulations include standard networks like 1G and 10G active optical Ethernet, Gigabit Passive Optical Network (GPON), Ethernet PON (EPON) as well as high capacity networks such as 10G-PON, XG-PON, WDM PON and WDM/TDM PON. The noise generation due to spontaneous Raman or Rayleigh scattering of all important telecom bands (1240nm to 1660nm) has been considered to establish guidelines for a possible integration of QKD signals.

QKD Scheme

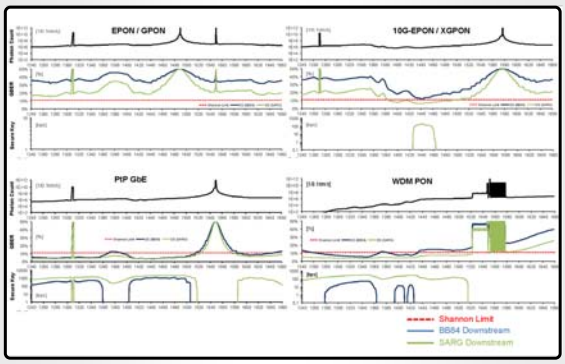


Bypass Scheme



Access Network

•QBER, Noise Rate and Key Rate



QBER Rate:

$$QBER = QBER_{Opt} + QBER_{Darks} + QBER_{Scatter}$$

$$QBER = \frac{1}{2}\,\frac{p_\mu(1-V)+2p_{dc}+p_{AP}+p_{ram}+p_{ct}}{\beta\ p_\mu+2p_{dc}+p_{AP}+p_{ram}+p_{ct}}$$

Secure Key Rate:

$$R_{sec} = R_{sift}\,(I_{AB} - I_{AE})$$

$$R_{sift} = \tfrac{1}{2}(\beta\ p_\mu+2p_{dc}+p_{AP}+p_{ram}+p_{ct})\ f_{rep}\eta_{duty}\eta_{dead}$$

$$I_{AB} = 1-\eta_{ec}H(QBER) \text{ with } H(p)=-\,p\log_2(p) - (1-p)\log_2(1-p)$$

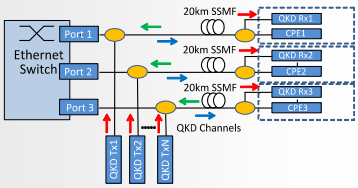
$$I_{AE,BB84} = \frac{(1-\frac{\mu}{2t})(1-H(P))+\frac{\mu}{2t}}{1+\frac{1p_{dc}}{\mu t\eta}} \qquad I_{AE,SARG} = I_{pns}(1)+\frac{1}{12}\frac{\mu^2}{t}e^{-\mu}(1-I_{pns}(1))$$

$$P=\frac{1}{2}+\sqrt{D(1-D)}, \quad D=\frac{(1-V)}{2-\mu/t} \qquad I_{pns}(k)=1-H\left(\frac{1}{2}+\frac{1}{2}\sqrt{1-\frac{1}{2^k}}\right)$$

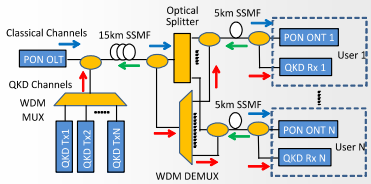
Classical Network Scheme

Network Standarts (IEEE and ITU-T) operate in the C and O Band using AWG, WDM and TDM for routing and asigning two dedicated wavelengths to each user (DS and US)
For integration of QKD a third quantum channel for each user is assumed.

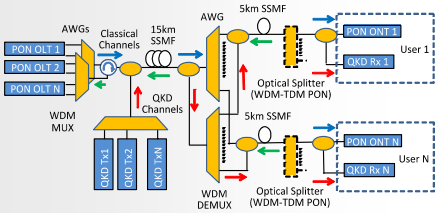
• PTP Active Optical Ethernet (1G/ 10 G Ethernet)



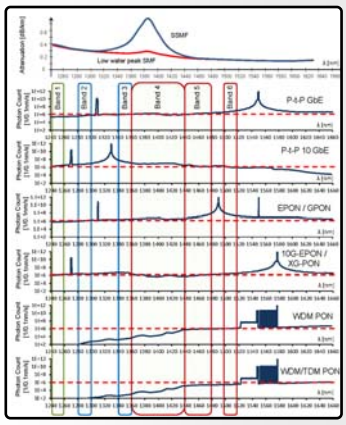
• EPON / GPON / XG-PON 10G-EPON



•WDM PON /WDM-TDM PON



Bandselection

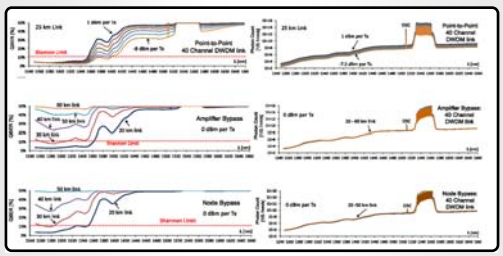


Raman, FWM, Rayleigth scattering have been simulated when classical signals are applied to a 40 channel network. The tolerable backround for a possible QKD signal is assumed to be 600000 Photons

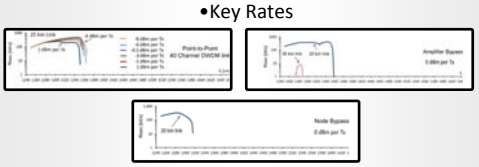
As simulations show only WDM and WDM-TDM networks are prospects for a QKD channel in the O band

Metropolitan Network

•QBER and Noise Rate



•Key Rates



Conclusion

To make an integration of currently available QKD systems in in optical networks possible, the transmitters for data channels must be operated at low power levels and narrow band optical filters should be used in front of QKD receivers to efficiently suppress the background noise. The results favour a wavelength in the range of 1290nm to 1310nm

The simulations will be followed by experimental measurements with suitable free running InGaAs detectors to confirm the results.

REFERENCES

[1] S. Aleksic, D. Winkler, A. Poppe, G. Franzl, B. Schrenk and F. Hipp,"Distribution of Quantum Keys in Optically Transparent Networks: Perspectives, Limitations and Challenges", invited, 15th International Conference on Transparent Optical Networks (ICTON 2013), Cartagena, Spain, July 2013, pp. 1-6

[2] 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

[3] S. Aleksic, D. Winkler, A. Poppe, G. Franzl, B. Schrenk and F. Hipp," Quantum Key Distribution Over Optical Access Networks", invited, 18th European Conference on Network and Optical Communications (NOC 2013), Graz, Austria, July 2013, p. 4