# Quantum Key Distribution in Commercial Optical Networks*

D.Lancho (1), J.Martínez (1), D.Menéndez (2), M.Soto (2), J.A.Pozas (2) and V.Martín (1)**
(1) DLSIIS, Fac. Informática, Universidad Politécnica de Madrid.
Campus de Montegancedo, Boadilla del Monte. 28660 Madrid (Spain)
(2) Seguridad en Redes y Servicios, Telefónica Investigación y Desarrollo.
C/ Emilio Vargas 6. 28043 Madrid (Spain)

## Abstract

Quantum Key Distribution is possibly the best positioned technology to build extremely secure communications networks, however, the weakness of the signals in the quantum channel poses some constraints that for the moment hinder its widespread adoption. One of the problems is the use of a separate physical channel for the quantum channel. In optical fiber communications this usually implies the need of an extra separate fiber as a carrier of the quantum channel, which is both expensive and unconvenient since it is not straightforwardly integrated in a commonly managed infrastructure. The purpose of this contribution is to present our current effort in searching the integration of QKD in real testbeds built out of standard modules in a way as close as possible to a production system.

## Introduction

From a telecommunications company perspective, a technology is useful if it satisfies needs, either from a customer or from the company itself, at a reasonable cost. The definition of “reasonable cost" is quite varied, since it could address the needs of a small but high profit market or a big, although small margins, one.

QKD [1] as it is today essentially offers very high security at a high cost. Lowering its cost would increase the user base and also appeal to network operators themselves, since the benefits of a low maintenance continuous supply of high quality symmetric keys in a network are not to be overlooked.

To share logical and physical infrastructures with the already installed networks is the most straightforward way to reduce implementation and maintenance costs. In order to explore the integration of QKD with standard telecommunications networks, we have defined scenarios that span the whole of a metropolitan area network, including the backbone and access networks. All are based on current passive optical networks and use standard equipment. Our aim is to clearly delineate the limits and technological modifications required to achieve this compatibility and the expected throughputs.

## Testbeds.

The first scenario is devoted to the backbone and is depicted in Fig.1. We use standard Reconfigurable Optical Add and Drop Modules (ROADM) in a Coarse Wavelength Division Multiplexing (CWDM) environment. The testbed can use several ITU 100 GHz channels. A modified QKD device able to emit photons at several frequencies is used to address different nodes in the ring. If Bob wishes to communicate with Alice at ROADM node 2 it can instruct node 1 not to drop the quantum channel, or simply configure node 0 to use the up pathway to go directly to node 2. Also, a wavelength addressing could be used, but that would imply to use the more expensive D(ense) WDM variant of the ROADM.

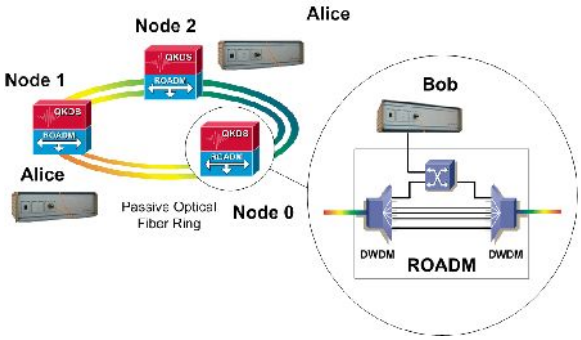


*Figure 1: The backbone testbed. Standard module ROADM are configured , using a ring topology, in a way such that the quantum channel can be injected and extracted in/from the shared fiber at every node.*

Presently we use two classical channels at 1470 nm and 1510 nm to assess the survival of the quantum channel in presence of classical signals within the same environment. As expected, when these channels are populated the QBER rises considerably. However, the quantum channel can be made compatible with the classical equipment, hence quantum and classical channels can be used at the same time. The price to pay is an increased QBER that lowers noticeably the key throughput. Also, the attenuation induced when crossing an intermediate node makes very difficult to jump more than one node with present day commercial QKD equipment, that have its practical limits set around 20 dB losses.

*Supported by CDTI, Ministry of Trade and Industry of Spain under project Segur@, CENIT-2007 2004 and by the Comunidad Autónoma de Madrid, project CCG07-UPM/TIC-2051

**vicente@fi.upm.es

Planned devices able to overcome ~40 dB[2] would be a major improvement for this purposes.

The second testbed concerns the access network. The increased use of optical fiber to cover all of the segments in a network, including the last mile, opens a real opportunity to carry the quantum channel to the final user. The preferred use of passive optical network (PON) technology further support this. Current access networks being installed or planned are usually GPON (Gigabit) or WDM-PON. The GPON testbed scheme is presented in Fig. 2. Its main ingredients are an Optical Line Terminator (OLT) at the provider's premises and an Optical Network Terminator (ONT) on the user side. Both are communicated using a fiber shared for up to 64 users till a splitter. From the splitter to the user, non shared fiber is used. The ITU defines three wavelengths in this standard: 1550 nm for video broadcast. 1490 nm for IP downstream traffic and 1310 for upstream. In our tests we have consistently obtained QBER values of 3-4% using lines of ~4Km length and with the classical channels populated while the OLT was kept synchronized with all the ONTs. It is to be noted that the hardware needs to inject the quantum channel in the GPON network are quite small, since the same filters used to isolate it can be used for that purpose. This is specially important since one of the design criteria for the ONTs are low cost and low maintenance. With present day QKD equipment, a splitter 1:4 is the most that can be reasonably used. It induces a ~7dB loss that reduces very much the key throughput. QBER values of ~6-8% (Fig. 3) can be obtained but at the cost of increasing the per pulse photon mean number to values as high as 0.8, which means that a decoy state protocol should be used.

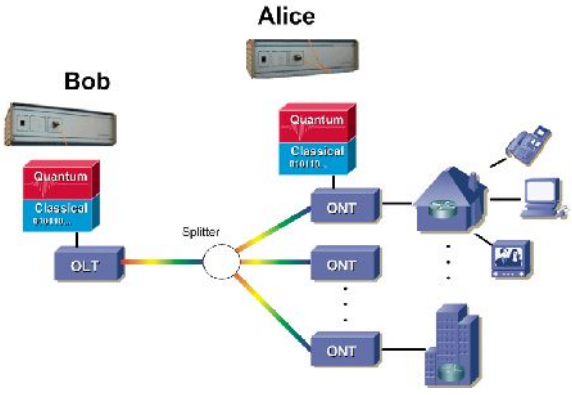


*Figure 2: GPON testbed.*

It is to be noted that although the splitter heavily penalises GPON, it also provides one of the reasons why QKD would be a highly welcome addition. The splitter sends downstream everything that the OLT emits to all the ONTs. Hence, it can be heard by all of the users that share the splitter. QKD would add a nice and low maintenance physical security layer. Also, worth to be noticed is that GPON final limitation is only the optical loss: it works using Time Division Multiplexing, which means that the quantum channel can be decoupled from the classical, thus effectively eliminating interference. The modifications needed would amount to an OLT firmware update.

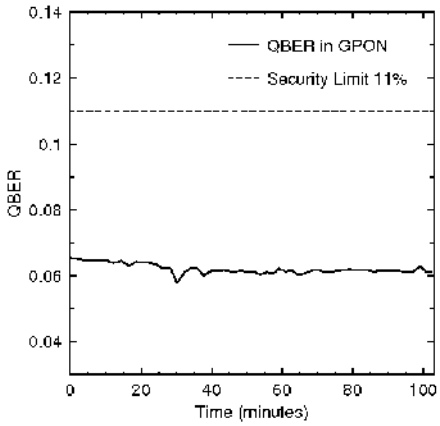


*Figure 3: QBER in GPON with 1:4 splitter.*

The WDM-PON testbed is still under construction. Physically is quite similar to GPON, only differing in that the splitter is substituted by an Arrayed Waveguide Grating (AWG). This assigns a wavelength to each ONT and logically converts WDM-PON in a wavelength addressable network. This scheme would be in principle more benign for QKD, but in practise it does not uses only one wavelength at a time in the shared part of the fiber, which would be the case in an implementation using a tunable laser: a broadband light source[3] is used instead, which is much more noisy.

## Conclusions

The widespread use of optical fiber and passive equipment in today's communications networks opens a window of opportunity for QKD. For its widespread use, it is necessary to integrate it in current standard infrastructure, sharing as much as possible. We have built testbeds that explore this integration using current network commercial technology with off the shelf components. As expected, there are limitations, but they are not as stringent as one could imagine. Several techniques can be used to share with reasonable success many of the components of a Metropolitan area network. In order to spread QKD, interfaces able to manage together the quantum and classical channel requirements must be agreed an implemented. QKD devices able to overcome optical losses of around 40 dB would be highly welcome.

## References

1. N. Gisin et al, Rev. Mod. Phys. vol. 74 (2002) 145
2. Various authors, see presentations in this SECOQC Conference!!
3. K-M. Choi et al, IEEE Photonics Technology Letters, vol. 18 (2006) 1167.