This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/LPT.2014.2308921, IEEE Photonics Technology Letters



# Quantum Key Distribution Based on Selective Post-Processing in Passive Optical Networks

Jesus Martinez-Mateo, Alex Ciurana, and Vicente Martin

***Abstract*—One of the main obstacles to the widespread adoption of quantum cryptography has been the difficulty of integration into standard optical networks, largely due to the tremendous difference in power of classical signals compared to the single quantum used for quantum key distribution. This makes the technology expensive and hard to deploy. In this paper we show an easy and straightforward integration method of quantum cryptography into optical access networks. In particular, we analyze how a quantum key distribution system can be seamlessly integrated in a standard access network based on the passive optical and time division multiplexing paradigms. The novelty of this proposal is based on the selective post-processing that allows for the distillation of secret keys avoiding the noise produced by other network users. Importantly, the proposal does not require the modification of the quantum or classical hardware specifications neither the use of any synchronization mechanism between the network and quantum cryptography devices.**

***Index Terms*—quantum key distribution, passive optical network, time division multiplexing**

## I. Introduction

Quantum key distribution (QKD) allows two legitimate parties to exchange a secret key. Its secrecy is founded on the laws of nature [1], as opposed to the computational complexity assumptions used in conventional cryptography. Although this technology has advanced much in the past years, it requires the communication of signals at the quantum level, making it extremely sensitive to noise and losses. QKD security relies in the ability to detect the modification on the quantum information carrier, or qubit, that is imposed by nature when measuring it. However, this modification can also be produced by the environment and cannot be distinguished from the modification caused by an eavesdropper. Thus, any disturbance of the quantum signal produced in the communication channel impairs the performance of a QKD system. Given the delicate nature of the quantum signals, it is easy to completely destroy its functionality. The traditional solution to this problem has been to use a dedicated fiber for the quantum channel: the part of a QKD system that carries the single quantum signals. However, to have a separate communications infrastructure is a very costly approach and this has triggered many studies focusing on the integration of quantum and classical channels in a single optical link [2], [3] and multiplexing technologies to share the media among multiple QKD systems [4], [5], with their unavoidable trade-offs and limitations on power, number of channels, scheduling, etc.

On the positive side, the passive optical network paradigm, widely used in standard telecom networks, provides the opportunity to establish a uninterrupted optical path between any two points connected to the network. This path can also be used as a quantum channel to support QKD. Therefore, these passive optical networks (PONs), mainly located in the *last mile* [6], are possibly a good setting for the future commercialization of this technology. Many research papers deal with the integration of QKD in such networks [7]–[11].

In this paper we show how the integration of QKD in commercial optical networks is, sometimes, an easy exercise if one is ready to accept some loss in efficiency. In particular, we demonstrate hassle free QKD communications among users in an standard access network based on time division multiplexing (TDM). The integration is direct, and does not require any modification of the devices attached to the network, neither the classical ones nor the QKD devices themselves. Furthermore, in contrast to other schemes [11], [12], our proposal enables direct communications between QKD devices, without any trust in a central node. The scheme described here allows only for the key exchange between network subscribers (users) in a limited distance scenario. However, it does not need any synchronization with the subscribers neither requests TDM slots, and does not impose modifications to the PON standards, such as power limitation, etc. The novel proposal is based on a modification of the classical QKD post-processing step used to discard the detections that with high probability are errors, i.e. those caused by the classical strong signals propagating in the network.

In section II we summarize TDM-based PON and describe how QKD can be used in these networks. In Section III, we estimate the expected performance for the proposed scheme. Finally, conclusions are presented in Section IV.

## II. TDM-based Passive Optical Networks

The standards Gigabit-capable and Ethernet PON (GPON [13] and EPON [14], respectively) are point-to-multipoint networks that connect subscribers using a tree like topology. Subscribers (called optical network units, ONU) are connected to an splitter that links to the root node (called optical line terminal, OLT), usually located at the telecommunications company's premises. Occasionally, ONUs can be grouped in network branches, using a second splitter that is connected to the first one as shown in Fig. 1. Between ONUs and OLT, upstream (from ONU to OLT) and downstream communications are performed simultaneously. This is typically accomplished using (in GPON and EPON standards) two different wavelengths[1]: 1310 nm and 1490 nm, respectively.

The authors are with the Facultad de Informática, Universidad Politécnica de Madrid, Madrid, Spain (e-mail: {jmartinez, aciurana, vicente}@fi.upm.es).

[1] A third channel at 1550 nm is reserved for overlay services, e.g. video or two-fibers configurations, but the same filtering scheme than for the 1490 nm signal applies, hence it has not been considered here.

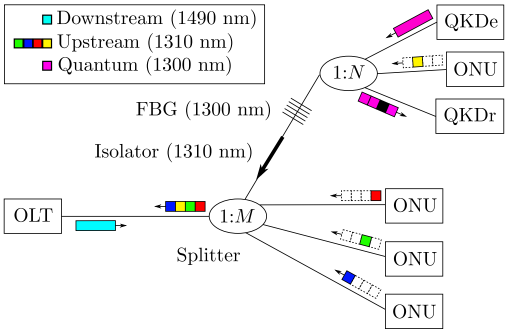


Fig. 1. TDM-based PON, as defined in the standards, with QKD integration. An optical line terminal (OLT) is connected to several optical network units (ONUs) via a 1:M splitter. QKD devices (emitter and receiver) are connected as if they were standard ONUs in a secondary 1:N branch. In order to enable a direct optical path between them, a fiber Bragg grating (FBG) is used at the input of the 1:N splitter, which reflects back the quantum signal. Communication frames are depicted as colored rectangles. Squares of different colors are used for TDM slots assigned to different ONUs. The QKD pair has not an assigned slot, since it works outside of the TDM scheme. To avoid noise in the quantum channel from the strong broadcast downstream classical signals, a wavelength separated by 190 nm is used for the quantum channel.

Note that while downstream communications are broadcast among all the subscribers using the splitters, the upstream frames are divided into variable time slots. These slots are dynamically assigned to the ONUs depending on their needs, and thus only one ONU is emitting at a time.

### A. QKD in TDM-based PON

In the standardized network schemes, signals can be only transmitted from ONUs to OLT and vice versa. Our goal is to connect a pair of QKD devices, emitter and receiver, as subscribers in the network and to enable a direct path between them without disturbing the network. Both systems are assumed to be connected to a branch, thus isolating them from subscribers in the rest of the network. Note that a branch can be always created without hindering the network's performance whenever the maximum loss budget allowed by the standard is not exceeded. The network requires a passive optical component capable of reflecting back the quantum signals while not affecting the rest. An easy solution is to use a fiber Bragg grating (FBG) connected between the first and second splitter as shown in Fig. 1. FBGs are readily available in-fiber filters with low losses (below $0.1$ dB) and configurable passband ($0.4$-$70$ nm) [15]. Since only the narrow passband around the quantum channel is reflected, the rest of signals remain unaltered and the setup does not impose any kind of modification on the subscribers and other network devices.

Now, along with the powerful classical signals (typically $10^7$ photons per pulse) we transmit signals at the quantum level, i.e. single photon pulses. Unfortunately, these can be easily spoiled by the noise generated by the classical ones—e.g. due to Rayleigh and Raman scattering. In order to reduce these effects, we allocate the quantum channel just beside the upstream, at 1300 nm. The almost 200 nm spectrum distance between quantum and downstream channel is large enough to minimize the signal and noise contribution of the latter [16] by filtering. Other optical effects, such as the crosstalk of WDM devices or four wave mixing, are negligible in these networks. The penalty to be paid is just a increased absorption of $0.1$ dB per km with respect to the 1550 nm window. A minimal amount considering that the expected distances in an access network are not very large and that most absorptions take place in the network components themselves.

We have measured the backward noise produced by the upstream signal for different scenarios in terms of the fiber length and number of ONUs (i.e. number of output ports in the first and second splitter). Our results show that if the ONU is located outside the branch with the QKD devices, the backward noise is weak enough such that, adding a 1310 nm isolator [17] (40 dB of isolation and $0.4$ dB of insertion loss) between both splitters, as shown in Fig. 1, it is reduced below the dark count rate ($\approx 10^{-5}$ ns$^{-1}$) of current single photon detectors (SPDs). However, when an emitting ONU and the QKD devices coincide in the same branch, the backward noise saturates[2] the SPD at the QKD receiver ($\approx 10^{-2}$ ns$^{-1}$), mainly due to Rayleigh scattering.

QKD devices can exchange keys whenever no subscriber's ONU is emitting within their branch (i.e. when a time slot was assigned to a subscriber outside of the branch with the QKD devices). In this setup it could be possible to transmit single photons under the assumption that TDM slots are assigned to the QKD devices, hence synchronized to emit and detect single photon pulses only when there is no upstream traffic in their branch. This synchronization can be, however, avoided by performing what is essentially a collision detection based solely on the QKD post-processing steps, as described below. The technique is general enough to be applied in networks that by design have a chance of low noise periods.

Note that only the quantum channel was considered here. Several possibilities can be used to include the classical QKD post-processing. If a TDM-PON channel is used, the performance would be reduced, since quantum and classical channels cannot operate simultaneously in the same device. On the other hand, using a wavelength separated well enough to avoid disturbing the quantum channel and outside of the classical channel plan, there would be no performance loss.

### B. Selective QKD post-processing

Let us assume that single photon pulses are emitted simultaneously with strong upstream and downstream signals in the network, i.e. QKD systems operating continuously without any TDM synchronization. The impossibility to extract a secret key in a noisy environment is due to the inability to distinguish among noise and legitimate signals, assuming that there are any. However, in the current scenario, legitimate signals can be identified and discriminated in noise free periods (time slots) due to the particular construction of upstream frames.

Fig. 2 illustrates an upstream frame ($U$) divided into time slots ($T$) of variable length. Grayed out time slots represent noisy, saturated periods of time, while the white ones represent the non-saturated periods where a secret key can be exchanged and distilled. After a saturated time slot, a detection deadtime

[2]It is considered to be saturated when a detection occurs with a probability higher than expected.

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/LPT.2014.2308921, IEEE Photonics Technology Letters



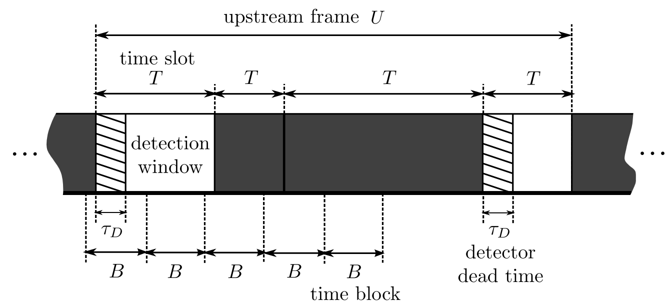


Fig. 2. Upstream frame ($U$) divided into time slots ($T$) of variable length. Each $T$ is assigned to a given ONU, and they are colored depending on whether the emitting ONU is located in the same branch than the QKD systems (gray) or not (white). Two QKD users may distill a secret key using the signals exchanged during the time slots marked white, which correspond to low noise, non-saturated, slots.

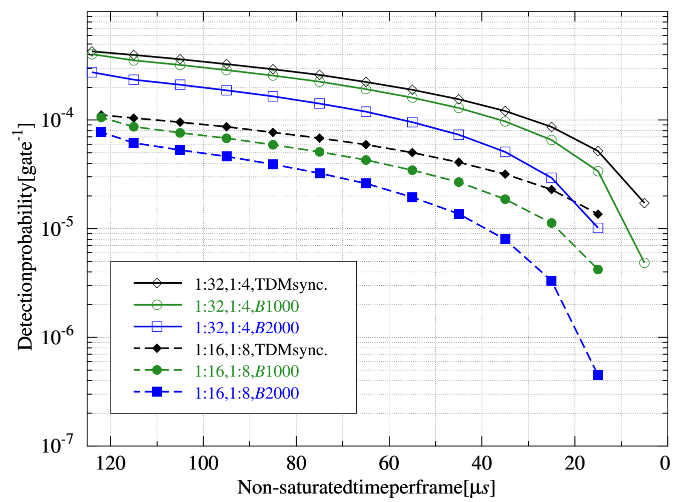


Fig. 3. Effective detection probability $p^*_{\text{exp}}$ as a function of the non-saturated time per frame; the available time for quantum transmissions. The total frame length in GPON is 125 $\mu$s. Results are compared for two network configurations allowing up to 128 users, a 1:4 (1:8) splitter connected to a 1:32 (1:16) splitter, and two block lengths in the post-processing, $B = 1000$ and 2000. A threshold of 2 detections per block was used to rule out saturate blocks in the 1:32 1:4 network, while in the 1:16 1:8 case it was set to 3. The detection probability for the ideal case is also shown, i.e. assuming perfect post-processing or TDM synchronization.

of length $\tau_D$ is shown. This is a parameter in SPDs, set to avoid false counts, that stands for the time during which the detector is not operational after a detection event. This limits the number of detections that can be obtained during a time slot, being a crucial parameter for the success of the scheme. Note that a saturated slot can then be distinguished from a non-saturated one when the number of detections is significantly higher. Therefore, for the scheme to perform efficiently, the deadtime must be significantly shorter than the shortest time slot assigned by the network protocol in use.

Most erroneous detections due to excess noise can then be ruled out by simply discarding *time blocks* with a number of detections above a threshold. We have implemented this method for post-processing as a proof of concept and analyzed the performance for different block's time lengths ($B$, of constant length). In order to avoid any detection corresponding to a saturated slot (i.e. an error with probability one half), whenever we find one or several saturated blocks, we also discard those detections obtained in the neighboring (last and next) non-saturated blocks. This helps to keep the QBER low. Simulation results are shown below in Section III.

The behavior described above is confirmed experimentally. We have tested that SPDs in a QKD receiver are driven into saturation only when ONUs within their network branch are emitting. Likewise, there also exist low noise periods that can be used to correctly detect emitted single photon pulses.

## III. Results

The secret key rate of a QKD system using the original BB84 protocol is roughly estimated as a function of the photon detection probability $p_{\text{exp}}$ and the quantum bit error rate $\epsilon$, $S = p_{\text{exp}}(1 - 2h(\epsilon))$ [1]. In the absence of noise in the quantum channel, a detection can be considered the result of two independent events: pulses coming from the source of single photons or dark counts. Both events occur with probability $p_q$ and $p_d$, respectively. Thus, $p_{\text{exp}} = p_q + p_d - p_q p_d$ and $\epsilon = p_d/2p_{\text{exp}}$. Assuming that the dark count probability is constant, the error rate and hence the secret key rate directly depends on the probability at which the emitted single photon pulses reach the receiver.

In practical devices, the source is usually implemented using attenuated laser pulses with an average number of photons per emitted pulse $\mu$. The detection of an emitted pulse is then output by the receiver with probability $p_q = 1 - \exp(-\mu \cdot \eta \cdot t_{\text{line}})$, where $\eta$ is the detector efficiency, and $t_{\text{line}}$ is the transmittance in the fiber, such that $t_{\text{line}} = 10^{-\alpha L/10}$ given the attenuation constant $\alpha$ ($\approx$ 0.3 at 1300 nm) and the distance $L$ in km. Typical values for current gated avalanche SPDs used in QKD were considered, $\eta = 0.1$, $\mu_{\text{opt}} = \eta \cdot t_{\text{line}}$, $p_d = 10^{-5}$ ns$^{-1}$, $\tau_D = 50$ ns, and 100 ps of gate width [11], [18]. Emitted single photon pulses and detection gates are assumed to be synchronized at a clock frequency of 1 GHz.

Simulation results were computed using the values given above for the QKD devices. The rest of them, frame time and bandwidth, are from the GPON standard. The fiber length within the QKD branch is 1 km (i.e. 2 km between a QKD pair), while the whole network ranges from 5 to 15 km. Network traffic using an upstream frame of 125 $\mu$s divided into variable time slots (with a minimum time of 410 ns, corresponding to an Ethernet frame with the shortest payload) was simulated. The loss budget of a network with 128 subscribers was considered ($\approx$ 28 dB), where a single 1:128 splitter is replaced by two in a cascade configuration as in Fig. 1. Two network configurations were compared: one of the outputs of a first level splitter with 16 or 32 output ports ($M$ in Fig. 1) is connected to a second level splitter (QKD branch) with 8 or 4 output ports ($N$ in Fig. 1). Ports in the QKD branch not used by the QKD devices are assumed to be assigned to ONUs, hence there will be two or six classical subscribers contending for resources in the QKD branch.

Fig. 3 and Fig. 4 show the effective detection probability $p^*_{\text{exp}}$ and quantum bit error rate $\epsilon$, respectively, of a QKD system in the previous scenario using the proposed post-processing scheme. $p^*_{\text{exp}}$ is calculated as the number of detections, after the post-processing, over the total number of

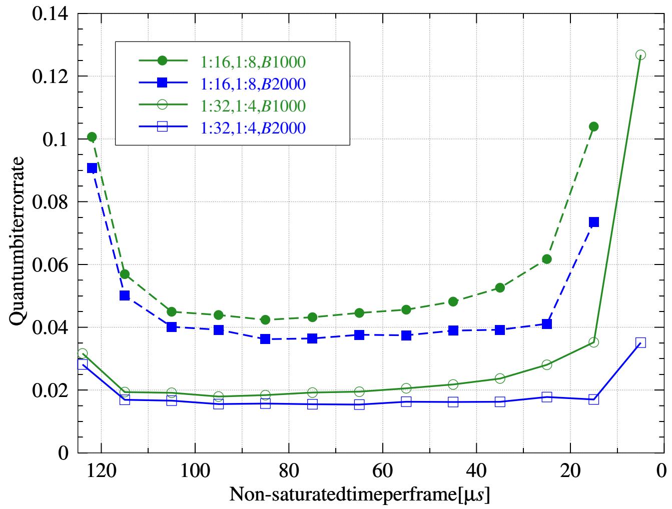


Fig. 4. Quantum bit error rate $\epsilon$ as a function of the non-saturated time per frame. Results for two network configurations and different block lengths, as in Fig. 3, are compared. Saturation thresholds are also chosen as in Fig. 3. Note that the QBER for low non-saturated times increases due to the detection probability $p^*_{\text{exp}}$. When the non-saturated time decreases, the number of single photon detections also decreases, while the dark count probability remains constant, thus $\epsilon$, as defined in Section III, increases. The high QBER for large non-saturated times is due to an increase of the number of detections marked wrong by the protocol.

opened gates. Configurations for the first splitter and second splitter are described in the legend of both figures. Since the post-processing method used to discriminate wrong detections significantly influences the final outcome, the results are also shown for two block lengths $B$: 1000 and 2000 detection gates.

Results are compared for different non-saturated time per frame. This is the available time that might be used for a quantum transmission. Since the length of an upstream frame is 125 $\mu$s, this is the maximum effective time for QKD in the ideal case. The minimum saturated time per frame is set to 1 $\mu$s for the 1:32 1:4 network, and 3 $\mu$s for the 1:16 1:8 network; these cases approximately correspond to assigning 1 slot of minimum duration to each subscriber of the branch.

Fig. 4 shows how the QBER is well below the threshold allowed for secret key distillation under the assumption of BB84 and one-way key distillation (11%). In the case of a secondary 1:4 splitter, $\epsilon$ is below 2% while $p^*_{\text{exp}}$ is above $10^{-4}$ over a wide range of available time. This demonstrates that it is possible to extract good performance by direct integration of modern QKD systems in these networks. Final secret key rate will be heavily dependent on the QKD system itself, the security assumptions and the actual load of the network.

## IV. Conclusions

Passive optical networks are, in essence, an ideal scenario for the QKD integration whenever we can control the side effects caused by the transmission of strong signals. Here we have shown how up-to-date QKD devices can be directly integrated in some standard access network, in particular in the widely used TDM-based PONs. The main advantage is that the integration is straightforward and does not require any modification, neither of the QKD devices nor of the network standard, including network devices and protocols. An additional QKD post-processing step substitutes any synchronization by ruling out noisy time slots. This performs essentially a similar task than the collision detection mechanisms in classical networks by detecting time slots where a successful QKD transmission can take place. The only physical modification required is to simply install an isolator, that reduces the noise issues, and a standard filter to reflect back the quantum signals to the branch in which the QKD devices are placed. The price to pay is a reduced efficiency when compared to an explicit TDM case, but in order to use TDM the QKD devices and network protocols would need to be modified in order to create clean time slots to cater to quantum transmissions, a much more difficult and costly task to accomplish.

## Acknowledgment

This work has been partially supported by the projects Quantum Information Technologies Madrid (QUITEMAD), P2009/ESP-1594, funded by *Comunidad Autónoma de Madrid*, and Hybrid Quantum Networks, TEC2012-35673, funded by *Ministerio de Economía y Competitividad*, Spain.

## References

[1] N. Gisin, G. Ribordy, W. Tittel, and H. Zbinden, "Quantum cryptography," *Rev. Mod. Phys*, vol. 74, pp. 145–195, 2002.
[2] P. Eraerds, N. Walenta, M. Legré, 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] K. Patel *et al.*, "Coexistence of High-Bit-Rate Quantum Key Distribution and Data on Optical Fiber," *Phys. Rev. X*, vol. 2, p. 041010, 2012.
[4] W. Chen *et al.*, "Field Experiment on a Metropolitan Quantum Key Distribution Network," *IEEE Photonics Technol. Lett.*, vol. 21, pp. 575–577, 2009.
[5] I. Choi, R. J. Young, and P. D. Townsend, "Quantum key distribution on a 10gb/s wdm-pon," *Opt. Express*, vol. 18, no. 9, pp. 9600–9612, 2010.
[6] C.-H. Lee, W. V. Sorin, and B. Y. Kim, "Fiber to the Home Using a PON Infrastructure," *J. Lightwave Technol.*, vol. 24, pp. 4568–4583, 2006.
[7] P. Townsend, S. Phoenix, K. Blow, and S. Barnett, "Design of quantum cryptography systems for passive optical networks," *Electron. Lett.*, vol. 30, no. 22, pp. 1875–1877, 1994.
[8] W. Maeda, A. Tanaka, S. Takahashi, A. Tajima, and A. Tomita, "Technologies for Quantum Key Distribution Networks Integrated With Optical Communication Networks," *IEEE J. Sel. Top. Quantum Electron.*, vol. 15, no. 6, pp. 1591–1601, 2009.
[9] D. Lancho, J. Martínez, D. Elkouss, M. Soto, and V. Martín, "QKD in Standard Optical Telecommunications Networks," in *Conf. on Quantum Communication and Quantum Networking*, vol. 36, 2010, pp. 142–149.
[10] J. Capmany and C. R. Fernandez-Pousa, "Optimum design for BB84 quantum key distribution in tree-type passive optical networks," *J. Opt. Soc. Am. B*, vol. 27, no. 6, pp. A146–A151, 2010.
[11] B. Frohlich, J. F. Dynes, M. Lucamarini, A. W. Sharpe, Z. Yuan, and A. J. Shields, "A quantum access network," *Nature*, vol. 501, no. 7465, pp. 69–72, 2013.
[12] I. Choi, R. J. Young, and P. D. Townsend, "Quantum information to the home," *New J. Phys.*, vol. 13, no. 6, p. 063039, 2011.
[13] *Gigabit-capable passive optical networks (GPON): General characteristics*, ITU-T Std. G.984.1, 2008.
[14] *Ethernet in the first mile*, IEEE Std. 802.3ah, 2004.
[15] Advanced Optics Solutions (AOS), "Fiber Bragg gratings," Available at http://www.aos-fiber.com/eng/Products.html.
[16] T. E. Chapuran *et al.*, "Optical networking for quantum key distribution and quantum communications," *New J. Phys.*, vol. 11, p. 105001, 2009.
[17] Flyin Optronics Co.,Ltd., "Isolator at 1310 nm," Available at http://www.flyinoptronics.com/polarization-maintainning-optical-isolator-p436.html.
[18] A. R. Dixon, Z. L. Yuan, J. F. Dynes, A. W. Sharpe, and A. J. Shields, "Gigahertz decoy quantum key distribution with 1 Mbit/s secure key rate," *Opt. Express*, vol. 16, no. 23, pp. 18 790–18 979, 2008.