Journal of Applied Science and Innovation Studies
ISSN 2998-3606
Vol. 2, No. 4, 2025
Published by STSL Press

Original Paper

Performance of a Quantum Key Distribution (QKD) protocol in a High-Speed Passive Optical Network

Héctor L. Núñez-Ramırez[1,2], Luis A. Santos-Avendaño[1], Gloria G. Carvalho-Kassar[1], Freddy C. Brito-Maestre[2]

[1] Laboratorio de Fotónica, Fundación Centro Nacional de Desarrollo e Investigación en Telecomunicaciones, 1060A, Caracas, Venezuela.

[2] Departamento de Comunicaciones, Universidad Central de Venezuela, 1050, Caracas, Venezuela.

Correspondence: hnunez@cendit.gob.ve

Abstract

The access network portion of a telecommunications system in the last years demands ever-increasing bandwidth to serve not only residential and commercial customers but also other telecommunications operators, as is the case with back-haul in mobile infrastructure. To achieve this, technologies using fiber optics as a transmission medium are being developed. Passive Optical Network (PON) protocols such as ITU-T G.9804.1 provides new schemes of multiplexing that improve higher speed offered both in the downstream channel (operator to user) and in the upstream channel (user to operator). In some cases a symmetrical optical link is required to support new services, applications and terminals from users side because their profiles and demands has changed in the last decade with new challenges to maintain network parameters within the established contracted values. On the other hand, information security has also been a topic of interest in recent years, so quantum cryptography offers an alternative to increase robustness compared to the mechanisms available in electronic systems that could be vulnerable to the development of quantum computing. Although quantum cryptography protocols were defined in the last century, their application is of interest today, as they can exploit the properties of photons to make it more difficult for an intruder to obtain the private key of an information system that uses optical fiber as a transmission medium. This work shows the computational application of the BB84 quantum key distribution (QKD) protocol on an operating model of a 50G passive optical network, demonstrating both the cryptography performance and network quality parameters such as the bit error rate (BER) and the eye diagram.

Keywords: PON, QKD, BB84, ITU-T G.9804, BER, eye diagram

1. Introduction

The evolution of the optical access network has occurred due to the technological development of devices to facilitate the generation of content available to any user (not just businesses or commercial users also mobile providers), which requires greater bandwidth, highlighting arguments about planned obsolescence. However, Internet service providers must consider this evolution and demand in their business models, as well as in their planning regarding network scalability and compatibility. By the end of the first decade of the 2000s, devices had already begun to be deployed in the optical access network to achieve asymmetric speeds of up to 2.5 Gbps in the down-link and 1.25 Gbps in the up-link, which could be shared by up to 64 or 128 users, in what is known as the GPON protocol (gigabit-capable passive optical network) under the recommendation of the International Telecommunication Union (ITU) G.984, which results from the evolution of APON (passive optical network under ATM transmission) and BPON (broadband passive optical network) developed in the last century.

Even the Institute of Electrical and Electronics Engineers (IEEE) proposed a version within its well-known IEEE 802.3 series, known as EPON (Ethernet-based Passive Optical Network) or IEEE

802.3ah, with obvious limitations compared to GPON in terms of speed and shared bandwidth. Even so, both ITU and IEEE protocols have evolved, reaching speeds of 10 Gbps and 40 Gbps, asymmetric and symmetric: XG and XGS-PON. Even in the case of ITU, there is a version that allows a connection of up to 50 Gbps (ITU-T G.9804). To implement these increases, advanced modulation and multiplexing techniques have been used. From conventional time division multiplexing (TDM) as well as optical wavelength multiplexing (WDM) in the case of G-PON.

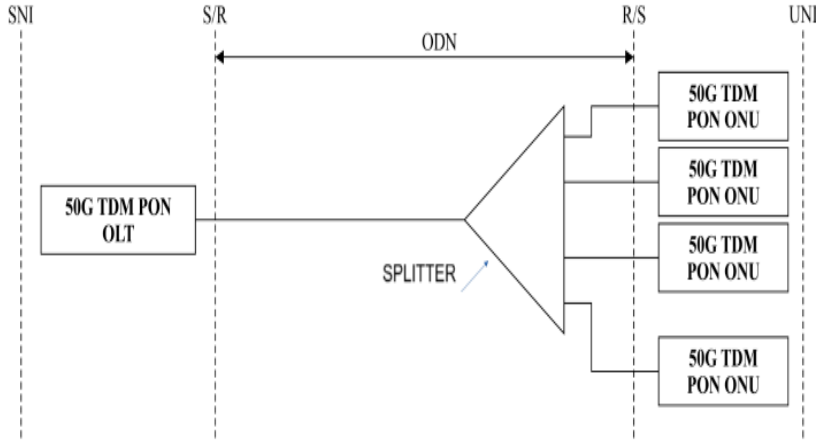


Figure 1. Model of Passive Optical Network based in ITU-T G.9804

To achieve speeds of 10, 40 or 50 Gbps, WDM combines with TDM in the multiplexing technique known as TWDM, which allows combining up to 4 wavelengths in the same port, allowing to multiply the capacities. Even the optimization in the manufacture of optical fiber has allowed a better use of the available bandwidth in the second window (1310 nm) and third window (1550 nm). It is possible to measure the quality of the link through the bit error rate (BER) or through the eye diagram, the extinction radius using expression (1), the lower this value, the more deteriorated the signal quality (ITU G.9804.1 and G.9804.3, 2021).

$$ER = 10\log\left(\frac{P_1}{P_0}\right) \quad (1)$$

Where: ER is the extinction radius, P_1 is the average value of a high level at the center of the pulse and P_0 is the average value of a high level also at the center of the pulse, measured on the eye diagram.

On the other hand, information security is important in any telecommunications system, particularly the robustness of the cryptography mechanism implemented in electronic systems, due to the distribution and storage of the private key. It has been demonstrated that if a random key of the same length as the message to be encrypted is used only once and kept secret, the message encryption is secure. However, the use of long, single-use keys imposes storage restrictions on systems.

Even so, public-key systems allow for reducing storage and usability issues, but they cannot be proven to be completely secure. In fact, quantum computing could pose a challenge to such systems, since quantum mechanics, from which it is derived, proposes computational tools to find the keys. In turn, quantum mechanics provides alternatives to solve the problem of securely distributing a private key, since for this purpose, the sender and recipient use a quantum channel to share the key, such as the one implemented in this work using optical fiber, encoding the message using photon polarization states. Therefore, an interception of the message and the channel is detectable, since measuring quantum states in the system will result in these states being modified, generating an alert.

There are quantum cryptography protocols that allow for the generation of one-time private keys, known as Quantum Key Distribution (QKD) protocols. These protocols implement a channel for sharing the quantum key and a classical channel for recovering the original information. The polarization states of a photon can be used to design a one-time quantum cryptography system. In quantum key generation protocols, the principle is to send a string of qu-bits, using photons to encode them. Qu-bits or quantum bits are the basic unit of quantum computing, they are quantum systems obtained from two states $|0\rangle$ and $|1\rangle$, or a combination of them. Quantum systems of n qubits are described by vectors of a complex Hilbert space of dimension 2^n. Therefore, it is possible to encode an exponential amount of information in the state of a quantum system of n qu-bits.

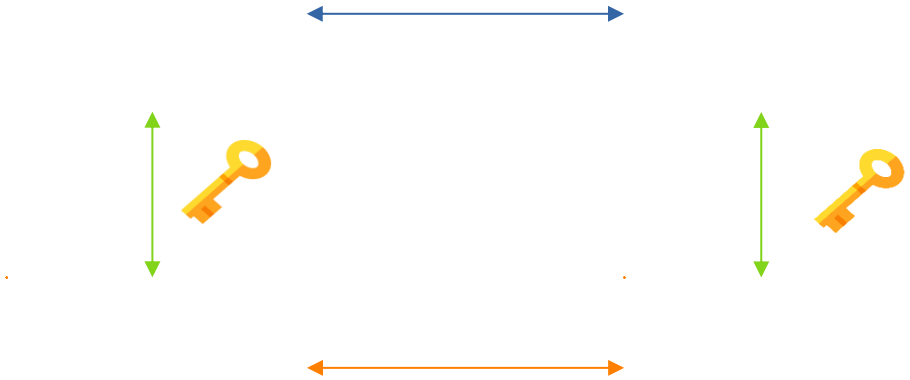


Figure 2. Model of QKD

Additionally, any change in the state of the system leads to the simultaneous modification of all stored information. Therefore, quantum computing capacity, in storage and calculation grows exponentially. Measurements of a quantum state are of interest because they are not deterministic; they depend on the state of the system. Among the best-known quantum cryptography protocols is BB84, proposed by Bennett and Brassard in 1984, based on the encoding of the information carried by the photon through polarization (Martinez, 2013).

2. Method

For the development of this work, the physical and mathematical model of the passive optical network and the BB84 protocol were defined, as well as the software implementation of the passive optical network at 50 Gbps using two channels, one conventional and one quantum based on the operating principle of the BB84 protocol.

2.1 Physical and mathematical model

The description of the 50G-PON protocol is established in the ITU-T recommendation G.9804.1, which allows symmetrical access network speeds of 50 Gbps for both the downlink and the uplink and asymmetrical speeds of up to 50 Gbps in the downlink and 25 Gbps in the uplink, based on the multiplexing mechanisms defined above: TDM, WDM and TWDM, with speeds of 10 Gbps and 12.5 Gbps as its basis, making it fully compatible with previous and currently used versions such as GPON, XG-PON and XGS-PON. These bandwidth capacities can be shared by up to 256 users connected to the same OLT optical port through optical splitters.

Additionally, it offers latencies of less than 20 ms on content servers, less than 8 ms on real-time playback services, and less than 2 ms for interactive services that require it, such as virtual reality. This protocol operates on separate wavelengths: between 1260 and 1310 nm for the uplink and between 1340 and 1344 nm for the downlink, which allows for this increase in bandwidth compared to other

versions. It has maximum transmission power levels of around +9 dBm and minimum receiver sensitivity of around +29 dBm, which translates into a much greater range in kilometers compared to other protocols (20–40 km).

The 50G-PON protocol has a well-known security mechanism such as the Advanced Cryptography Standard (AES), however, this work proposes an alternative, by sharing the quantum channel with the QKD protocol with an Internet access service on the same optical fiber strand.

The BB84 protocol is a QKD protocol that can encode information through the polarization of photons traveling, for example, in an optical fiber. This property describes how the polarization of the electromagnetic field behaves according to the direction of propagation, through its variation in degrees or radians. If a photon with polarization is passed through α through a polarization filter with orientation β, the photon passes changing its polarization to β with a probability $\cos^2(\alpha-\beta)$ or can be absorbed with probability $1-\cos^2(\alpha-\beta)=\sin^2(\alpha-\beta)$. If $\alpha-\beta=\pi/2$ the photon never passes, and if $\alpha-\beta=0$ it always passes without being affected by polarization. If $\alpha-\beta=\pi/4$, half of the time it passes with a polarization β, and the other half of the time it is absorbed.

Generally, two polarization bases are used: horizontal-vertical (B_{+}), and an oblique one (B_x). In the basis B_{+} we take the qu-bit with vertical polarization state as logical 1, and the horizontal one as 0. Similarly, in the case of the oblique basis, with 1 at $\pi/4$ and 0 at $3\pi/4$. If you have a photon in horizontal and you measure it in the oblique basis, half the time you get 1 and the other half 0. If you have a photon as 1 in the basis B_x that is measured in the basis B_{+}, half the time you get the correct result and the other half the time you get the incorrect result. To know the original state with certainty it is necessary to know in which basis it was prepared and make the measurement in the same (Moret, 2008).

$$|\varphi_{x0}\rangle=\cos\frac{\pi}{4}|\varphi_{+0}\rangle+\sin\frac{\pi}{4}|\varphi_{+1}\rangle$$

$$|\varphi_{x1}\rangle=\cos\frac{\pi}{4}|\varphi_{+0}\rangle-\sin\frac{\pi}{4}|\varphi_{+1}\rangle \quad (2)$$

Where: B_{+} is the basis of the horizontal or vertical polarization state, B_x is the basis of the oblique polarization state, the arrows indicate the polarization: vertical, horizontal, $\pi/4$ and $3\pi/4$, 0 indicates horizontal and right-oblique polarization states, 1 indicates vertical and left-oblique polarization states.

This protocol is based on the principle of two channels, one quantum where what is indicated in the previous paragraph occurs, which is summarized in table 1 and can be modeled with expression (2), and a classical channel, which allows information to be recovered.

Table 1. States of QKD protocol

Base	Value	State	Meaning
B+	0	$\|\varphi_{+0}\rangle$	qubit in B+ value=0
B+	90°	$\|\varphi_{+1}\rangle$	qubit in B+ value=1
Bx	45°	$\|\varphi_{x0}\rangle$	qubit in Bx value=0
B+	-45°	$\|\varphi_{x1}\rangle$	qubit in Bx value=1

2.2 Computational model

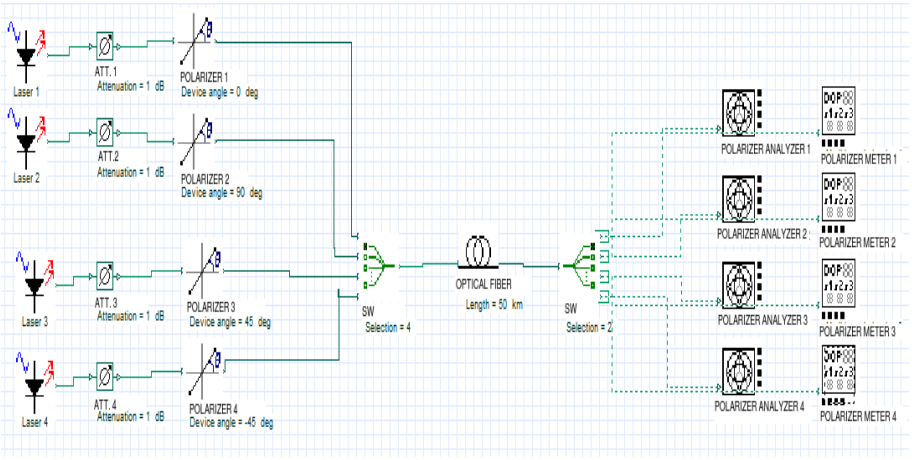
The simulation of the operation of the BB84 QKD protocol (Buhari, 2012, Luo, 2017) is developed in the Optisystem software, as shown in Figure 4. Random bit generators and pulse generators modulated by continuous wave lasers and attenuators have been used at the transmission end to establish the generation of photons, while the linear and oblique polarization bases have been implemented using polarizers, whose outputs are connected to a four-state selector with which the randomness in the sending of photons over an optical fiber can be represented.

At the other end, there is another four-state random selector. The photon's polarization angle is measured to extract the corresponding bit value. Ports one and two at the receiving end measure linear polarization angles. i.e.. 0 and $\pi/2$, while the remaining ports measure oblique polarization angles, i.e., $\pi/4$ and $3\pi/4$. When transmitting the encryption key, only when the transmitter and receiver selectors match is the correct reception of a photon confirmed; if there are discrepancies, the information is discarded.

Figure 5 describes the implementation of a 50 Gbps passive optical network model in Optisystem, which shares the optical channel with an encrypted channel using the BB84 protocol (Fröhlich, 2016; Mallick, 2024; Rahmanpour, 2025). For this purpose, wavelength multiplexing (WDM) was used between the classical channel and the quantum channel (for encryption), operating at wavelengths of 1340 and 1345 nm, respectively.

The simulation of the 50 Gbps passive optical network model was performed, obtaining the following performance in terms of bit error rate (BER) and eye diagram.

The simulation results of the classical channel of the 50G-PON model and the BB84-based quantum channel are shown in the next section.



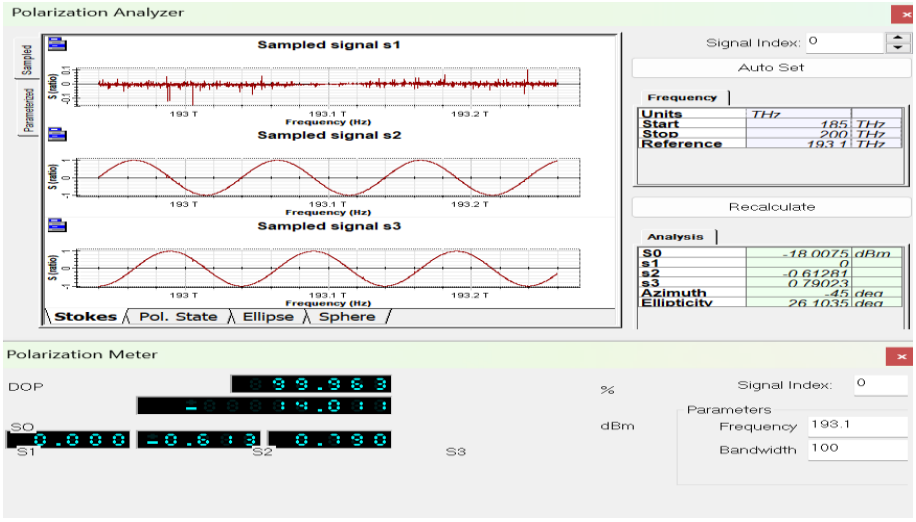


Figure 3. Simulation of model of QKD: BB84

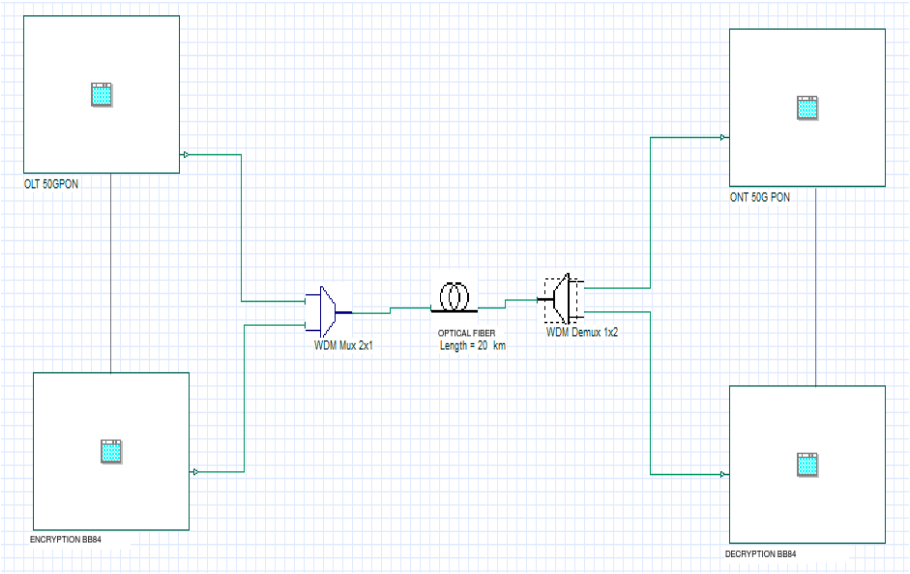


Figure 4. Simulation of BB84 over ITU-T G.9804.1 optical network model

3. Result

The performance of the BB84 protocol on the 50G – PON passive optical network model, simulated in Optisystem, is shown in Figure 7, representing the behavior for polarization at 0 (6a) and $\pi/2$ (6b) respectively, while the remaining ports measure the oblique polarization angles, that is, $\pi/4$ (6c) and $3\pi/4$ (6d). Additionally, the behavior of the BER and the eye diagram are shown for each polarization proposed in Figure 7.

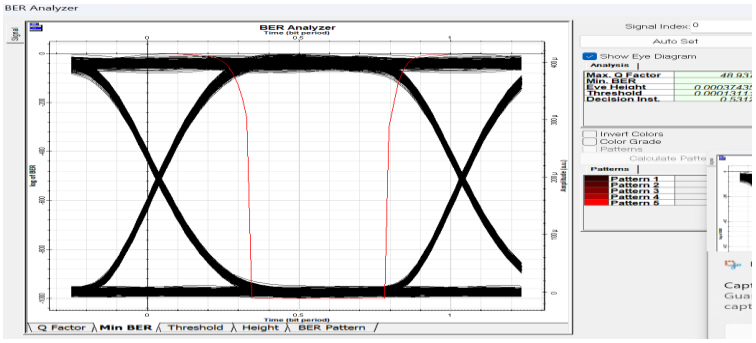
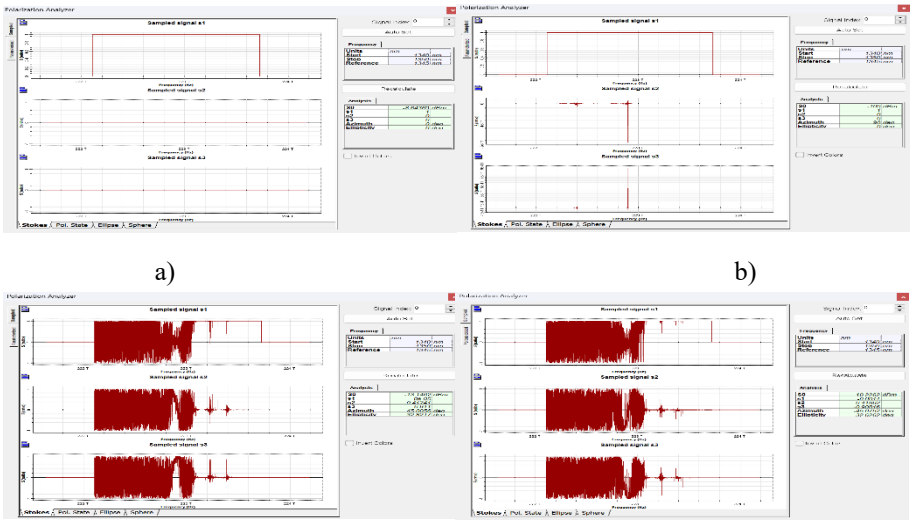


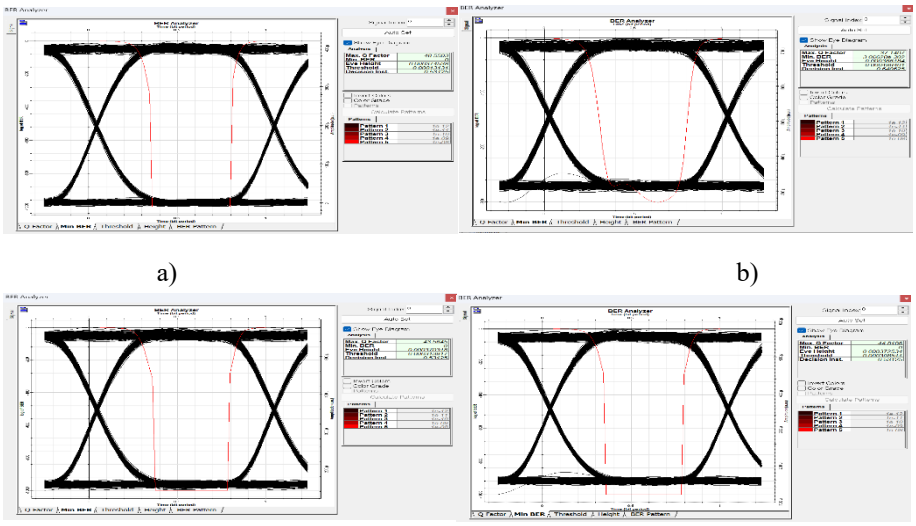
Figure 5. Performance of BB84 over ITU-T G.9804.1 optical network model



a) b)

c) d)

Figure 6. Performance of the link for different polarizations in BB84 over ITU-T G.9804.1 optical network model



a) b)

c) d)

Figure 7. Results of BER and eye diagram for different polarizations in BB84 over ITU-T G.9804.1 optical network model

4. Conclusion

A passive optical network model has been proposed under the ITU G.9804 protocol, coexisting with the BB84 protocol, at speeds of up to 50 Gbps, using Optisystem software.

Good performance is obtained at the link speed, both in terms of bit error rate and eye diagram, specifically the extinction radius, demonstrating the computational feasibility of this security mechanism in high-speed passive optical networks.

Acknowledgements

Authors would like to thank the Ministry of Science and Technology and the National Fund for Science, Technology and Innovation for the resources that allowed the results of this work to be presented.

References

Buhari, A. et al. (2012). *An efficient modeling and simulation of quantum key distribution protocols using OptiSystem™*. 2012 IEEE Symposium on Industrial Electronics and Applications, Bandung, Indonesia, pp. 84-89.

Fibre to the Home Council Europe. (2018). *FTTH Handbook*.

Fröhlich, B. et al. (2016). Quantum secured gigabit optical access networks. Nature Sci Rep 5, 18121.

Luo, J. et al. (2017). *Changes of quantum state of polarization in coexistence scheme of quantum-classical signal*. Proceedings Volume 10464, AOPC 2017: Fiber Optic Sensing and Optical Communications; 104640G.

Mallick, B. et al. (2024). Long distance QKD propagation using optical single sideband scheme. *Optics Continuum, 3*(3), 427.

Martínez, J. et al. (2008). *Criptografía Cuántica Aplicada*. Universidad Politécnica de Madrid.

Moret, V. (2013). *Principios Fundamentales de Computación Cuántica*. Universidad de Coruña.

Rahmanpour, M. et al. (2025). *Reducing the afterpulse effect in QKD systems using detector doubling in the BB84 protocol.* Optica Open, version 3.

International Telecommunication Union (ITU). Higher speed passive optical networks – Requirements G.9804.1

International Telecommunication Union (ITU). 50-Gigabit-capable passive optical networks (50G-PON): Physical media dependent (PMD) layer specification G.9804.3