ΕΘΝΙΚΟ ΚΑΙ ΚΑΠΟΔΙΣΤΡΙΑΚΟ
ΠΑΝΕΠΙΣΤΗΜΙΟ ΑΘΗΝΩΝ ΣΧΟΛΗ ΘΕΤΙΚΩΝ
ΕΠΙΣΤΗΜΩΝ ΤΜΗΜΑ ΦΥΣΙΚΗΣ

MSc in Control and Computing, UoA

Nikolaos Makris - 7110132100209

Master Thesis

Quantum and classical optical channels Coexistence in optical Access Networks

Members of the Tripartite Committee:

1) Κανέλλος Γεώργιος – Επικ. Καθηγητής Ε.Κ.Π.Α. (Supervisor)

2) Τζανακάκη Άννα – Αν. Καθηγήτρια Ε.Κ.Π.Α.

3) Ρείσης Διονύσιος – Καθηγητής Ε.Κ.Π.Α.

July 18, 2023

Contents

Abstract

This master thesis explores the coexistence of Quantum Key Distribution (QKD) with classical channels in optical access networks. The introduction provides an overview of the topic, followed by an overview of the principles of quantum mechanics and QKD procedures. Various QKD protocols, including BB84and BB84 Decoy State are discussed. The thesis also investigates the impact of nonlinear effects such as Raman scattering and four-wave mixing, as well as linear effects like Rayleigh back-scattering and chromatic dispersion on the coexistence of QKD with classical channels. After having discussed the theoretical background the thesis provides a synopsis of prior research on the coexistence of QKD with classical channels. Furthermore there is an experimental procedure which consists of two parts. The first part involves an investigation of counter-propagating interactions in quantum communications using two pairs of Toshiba machines which implement the BB84 protocol with decoy states and also the coexistence of counter-propagating interactions with classical channels . Finally the second part presents the practical deployment of QKD coexistence over GPON replica located at OTE Academy.

Keywords: Quantum Key Distribution, Coexistence, Optical Access Networks, BB84 with Decoy States .

Περίληψη

Η διατριβή αυτή ερευνά τη συνύπαρξη της Διανομής Κβαντικών Κλειδιών (QKD) με κλασικά κανάλια σε οπτικά δίκτυα πρόσβασης. Η εισαγωγή παρέχει μια επισκόπηση του θέματος και στη συνέχεια ακολουθεί μια σύνοψη των αρχών της κβαντικής μηχανικής και των διαδικασιών που εφαρμόζονται στην κβαντική διανομή κλειδιών. Συζητούνται κάποια πρωτόκολλα QKD, συμπεριλαμβανομένων των BB84 και BB84 με decoy καταστάσεις. Η διατριβή εξετάζει επίσης την επίδραση μη γραμμικών φαινομένων, όπως η σκέδαση Raman, ο θόρυβος που προκαλείται απο την παρουσία πολλαπλών κυμάτων , καθώς και γραμμικών φαινομένων, όπως η ανάκλαση Rayleigh και η χρωματική διάσπορά. Μετά την ανάλυση των θεωρητικών προαπαιτούμενων, παρέχεται μια σύνοψη των προηγούμενων ερευνών για τη συνύπαρξη του QKD με κλασικά κανάλια. Επιπλέον, περιλαμβάνεται η πειραματική διαδικασία που αποτελείται από δύο μέρη. Το πρώτο μέρος περιλαμβάνει μια έρευνα που γίνεται στο εργαστήριο οπτικής. Πιο συγκεκριμένα μελετώνται οι αλληλεπιδράσεων όταν δύο ζεύγη μηχανημάτων Toshiba που υλοποιούν το πρωτόκολλο BB84 με decoy states τοπόθετούνται σε φορά αντίθετης διάδοσης καθώς και η συνύπαρξη αυτής της τοπολογίας με κλασσικά κανάλια. Τέλος, το δεύτερο μέρος παρουσιάζει την πρακτική εφαρμογή της συνύπαρξης των κβαντικών καναλιών θέτοντας σε λειτουργία τον εξοπλισμό της Toshiba στην προσομοίωση του GPON δικτύου της COSMOTE που βρίσκεται στο OTE Academy.

Λέξεις Κλειδιά: Διανομή Κβαντικών Κλεδιών, Συνύπαρξη Κβαντικών και κλασσικών καναλιών, Οπτικά Δίκτυα Πρόσβασης, BB84 με decoy καταστάσεις.

1 Introduction

The increasing need for network security in today's digital landscape arises from a multitude of factors. Firstly, the exponential growth of internet connectivity has expanded the attack surface, offering cybercriminals more opportunities to exploit vulnerabilities. Additionally, the proliferation of interconnected devices and the rise of the Internet of Things (IoT) have created a complex web of interconnected systems, amplifying the potential impact of security breaches. Moreover, the escalating sophistication of cyber threats demands robust security measures to safeguard sensitive information and critical infrastructure. The reliance on cloud computing, remote work, and digital transactions further heightens the urgency for network security to protect privacy, data integrity, and maintain business continuity. Consequently, organizations and individuals must prioritize network security to mitigate risks and safeguard their digital assets in an increasingly interconnected world [2, 22].

The vulnerability of traditional networking to a variety of attacks has made classical data encryption unable to provide unconditional security and has prompted the exploration of innovative solutions, such as quantum key distribution (QKD). As traditional encryption methods face the growing threat not only of common cybercriminal techniques but also that of quantum computers, which can potentially decrypt sensitive data, QKD emerges as a promising alternative [2]. QKD utilizes the principles of quantum mechanics to establish secure encryption keys, leveraging the unique properties of quantum particles to detect any unauthorized interception and also be resistant to unlimited computational power. By employing quantum principles QKD provides a theoretically secure method for exchanging cryptographic keys over long distances [12, 19]. This emerging technology offers the potential to revolutionize network security by ensuring confidentiality and integrity in the face of quantum computing advancements and sophisticated cyber threats.

2 Quantum Key Distribution

Quantum Key Distribution is a method that uses quantum mechanics rather than simple numerical algorithms to generate a secret key and distribute it across a network [2, 12, 19]. Numerous protocols have been proposed and implemented by researchers to facilitate Quantum Key Distribution (QKD) and enhance its security and efficiency.

In order to fully understand how QKD works and why it is theoretically impossible to Eavesdrop a quantum generated encryption key we should first analyze some basic quantum principles which are key for understanding the implementation of every protocol.

2.1 Quantum Mechanics Principles

Quantum State

A quantum state represents the fundamental description of a quantum system. It describes the state of a particle, atom, or any quantum entity, and contains all the information necessary to predict the outcomes of measurements performed on that system. It is denoted by the symbol $|\Psi_N\rangle$ [18] . The quantum states refer to specific properties of a quantum system, such as spin, polarization, phase, or a combination of them. In classical information theory, a bit can exist in two distinct states, 0 or 1, representing the levels of charge. Similarly, in quantum mechanics, the state of a system can be represented as 'up' $|0\rangle$ or 'down' $|1\rangle$ when describing the spin of a particle. However, quantum states are more complex and possess distinct properties compared to classical states.By exploiting quantum states, qubits serve as the fundamental unit of measurement in quantum information theory.

Basis

Measurement plays a fundamental role in Quantum Key Distribution (QKD) protocols, particularly in the context of polarization-based schemes. In QKD, the bits of the secret key are encoded onto individual photons using different polarization bases [18]. Polarization refers to the orientation of the electric field associated with a photon. The measurement of photons' polarization states allows for the extraction of the key. However, as shown in 1 the basis in which the photons will be encoded is not standard. Different polarization basis (linear and rectangular are generated by using Polarizing beam splitters (PBS) and wave plates. PBS splits incoming light based on its polarization, while wave plates introduce controlled phase differences to manipulate the polarization states [21]. By adjusting the angles of wave plates in conjunction with PBS, various polarization bases, such as linear and diagonal, can be generated. The basis in which photons are encoded every time is chosen randomly.

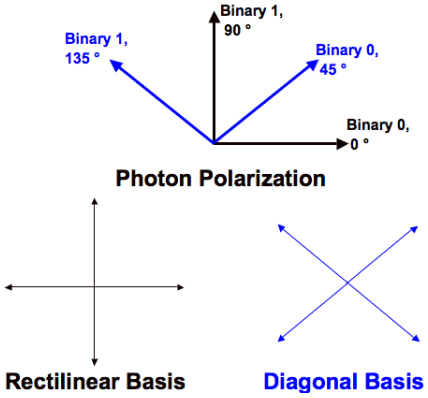

Figure 1: Basis and bit encoding [13]

The No-Cloning Theorem

The no-cloning theorem, a cornerstone of quantum mechanics, is mathematically formalized through the linearity of quantum operations. It can be expressed by the equation:

$$\Psi_1 \otimes \Psi_2 \neq \Psi_1 \otimes \Psi_1$$

where Ψ_1 and Ψ_2 represent two arbitrary quantum states. This equation shows that it is impossible to create an exact copy of an unknown quantum state, highlighting the fundamental limitation on cloning quantum states [18]. This theorem plays a very important role in most of the QKD Protocols because it ensures that there can be no intermediate between two nodes without being detected.

The Collapse of the Wavefunction

The collapse of the wavefunction, a consequence of quantum measurement, is mathematically described by the projection postulate. It can be expressed as:

$$|\Psi\rangle = \sum c_i |\Psi_i\rangle$$

where $|\Psi\rangle$ represents the initial quantum state, c_i are complex coefficients, and $|\Psi_i\rangle$ are the eigenstates of the measured observable. This equation shows how the quantum state collapses into one of the eigenstates upon measurement, capturing the probabilistic nature of the collapse [18]. When we perform a measurement on a quantum system, we choose a specific basis to observe its properties. The choice of basis affects which eigenstates are accessible and influences the probabilities of different outcomes. This principle is vital in Quantum Key Distribution (QKD) systems, as the random selection of measurement basis ensures that any potential eavesdropper, Eve, will receive noise instead of useful information, enhancing the security of the communication.

The Uncertainty Principle

The uncertainty principle, formulated as an inequality between the variances of non-commuting observables, is mathematically expressed as:

$$\Delta A \Delta B \geq \frac{1}{2} |\langle [A, B] \rangle|$$

where ΔA and ΔB represent the standard deviations of the observables A and B, respectively, and $[A, B]$ denotes the commutator of A and B. This equation demonstrates the fundamental trade-off between the precision of measurements for non-commuting observables, emphasizing the inherent uncertainty in quantum systems [14, 18].

Entanglement

Entanglement is an aspect of Non-locality which refers to the property that entangled particles can exhibit instantaneous correlations, regardless of the distance between them.

This means that measurements made on one particle can instantaneously affect the state of the other particle, regardless of the spatial separation [18]. Entanglement is mathematically described using the tensor product of quantum states. For two entangled particles, the mathematical representation is:

$$|\Psi\rangle = \sum c_{ij} |\Psi_i\rangle \otimes |\Phi_j\rangle$$

where c_{ij} are complex coefficients and $|\Psi_i\rangle$ and $|\Phi_j\rangle$ represent the quantum states of the respective particles. This equation illustrates the entanglement between the particles, indicating that the overall state cannot be described independently of the individual states.

Superposition

Superposition, another mathematical concept in quantum mechanics, is represented by the linear combination of quantum states. For example, in the BB84 protocol - which we are going to discuss thoroughly, the polarization states can be expressed as:

$$|0\rangle = |H\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)$$

$$|1\rangle = |V\rangle = \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)$$

where $|H\rangle$ and $|V\rangle$ represent the horizontal and vertical polarizations, and $|0\rangle$ and $|1\rangle$ represent the qubit states. These equations show how superposition allows the encoding of information in different quantum states [18]. If the basis used to measure the received photons is the same as the one used to transmit photons the probability of measuring the correct state is 100%. However if the basis is different the outcome will be random and the probability of measuring the correct state is 50% [12].

Quantum Measurement and Post-Selection

Quantum measurement and post-selection are mathematically described through the use of Hermitian operators and projection operators. The measurement operator for an observable A can be represented as:

$$M_A = \sum_{a_i} |a_i\rangle\langle a_i|$$

where $|a_i\rangle$ represents the eigenstates of observable A [18].

In this thesis, we will not delve further into the mathematical part of these principles. However it is important to note that these equations express in theory what we shall see in practice afterwards by examining the most commonly known and implemented protocols.

2.2 QKD Procedures

In 2 the QKD system is depicted. There are two channels, the quantum channel and the public channel. The Quantum Channel is used to transmit and share the information of

secret key in the form of polarized photons, called as quantum bit (qubit). Meanwhile the public channel is used to discuss the process of qubits transmission and make a deal about the shared secret key. Generally, there are two medium types of quantum channel which are implemented on QKD system, optical fiber and free space.

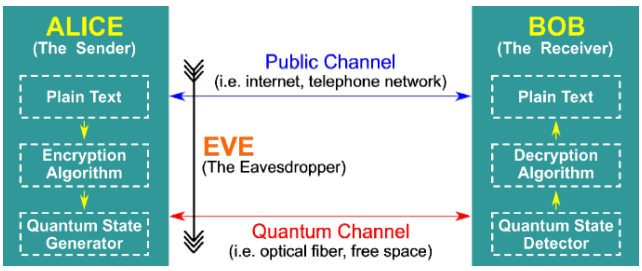

Figure 2: Basic Block Diagram of a QKD System [19]

However 2 is a plain overview of QKD.In reality more complex procedures take place, which are necessary for almost all protocols that we are going to discuss later. So, before surveying these protocols we should first examine the basic procedures as shown in 3.

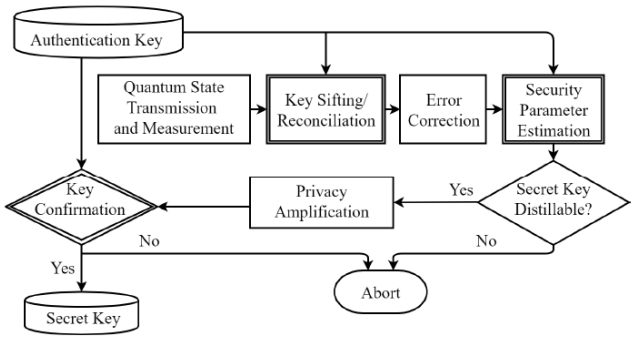

Figure 3: Basic Block Diagram of QKD System [19]

Quantum State Preparation

Alice prepares individual photons in specific quantum states, typically using a polarization or phase encoding scheme. This can involve manipulating the quantum properties of photons, such as their polarization angle or phase, to encode information [12]. One common method involves using specialized optical elements, such as wave plates or beam splitters, to control the polarization or phase of individual photons (depending on the protocol), enabling their encoding for quantum information processing. The bits encoding procedure in known as modulation [21].

Quantum Transmission

Alice sends the prepared photons to Bob over a quantum communication channel, which could be an optical fiber or free space. The transmission of quantum states is subject to various noise sources, such as attenuation and channel-induced errors [19, 13].

Measurement

Upon receiving the photons, Bob performs measurements on each photon to extract information about their quantum states. This involves applying appropriate measurement operators, such as projective measurements, to determine the properties of the received photons [19, 13]. Bob utilizes measurement devices, such as polarizers or interferometers, to perform specific measurements on the received photons, extracting information about their polarization angle or phase [21].

Basis Announcement

Alice and Bob publicly communicate their chosen measurement bases for a subset of the transmitted photons. This information is used later for error estimation and correction. The measurement bases can be represented by random variables, denoted as A (for Alice's basis choice) and B (for Bob's basis choice) [12, 19].

Key Sifting

Key sifting, also known as information reconciliation, is the process of reconciling discrepancies in the raw key generated by the sender and receiver. Due to the fact that Bob chooses randomly the measurement Basis also due to factors like channel noise and loss, the raw key may contain errors or discrepancies. For example, if Alice sends to Bob a photon polarized in Rectilinear Basis and Bobs measures it in the Diagonal Basis, this bit will be discarded from the raw data after the public basis announcement, since the outcome is probabilistic. Key sifting allows the sender and receiver to generate sifted agreed-upon key by removing these discrepancies and aligning their respective keys [12, 19, 16].

Error Estimation

By comparing their measurement bases during the sifting procedure, Alice and Bob identify the subset of photons used for error estimation. They calculate the error rate, indicating the discrepancy between their measurement outcomes for the subset of photons. The error rate can be quantified using mathematical formulas, such as the bit error rate (BER) or the quantum bit error rate (QBER) [12, 19, 16].

Error Correction

During the transmission of quantum states over a noisy channel, errors can occur due to various factors such as noise, interference, and imperfections in the hardware. Error correction techniques are employed to detect and correct these errors, ensuring that the final shared key is free from transmission-induced errors. Error correction codes, such as the Cascade or LDPC codes, are commonly used to achieve error correction in QKD protocols [12, 19, 16].

Privacy Amplification

Privacy amplification is the process of distilling a secure and uniform secret key from a raw key that may contain information about the initial quantum states and measurement outcomes. It ensures that any potential information leaked during the key generation process is reduced to an insignificant level, thus enhancing the privacy and security of the final key. Privacy amplification typically involves the use of cryptographic hash functions or information-theoretic techniques to extract a shorter, secure key. For example, if Alice and Bob have a sifted key of length 100 bits they can use a hash function that will reduce the key size to 50 bits. The new set of 50 bits becomes the final shared secret key between Alice and Bob, and any potential information an eavesdropper may have had about the original sifted key is now significantly reduced.[12, 19, 27].

Final Key Generation

After applying all necessary procedures, Alice and Bob obtain a final secure key that can be used for cryptographic purposes. The length of the final key depends on the error rates, the privacy amplification scheme used, and the desired level of security [12, 19].

2.3 QKD Protocols

For the discussion of QKD protocols there is going to be a brief but comprehensive review of the protocols that have been researched until now. However, the experiment that is conducted for this thesis includes QKD pairs which use Efficient BB84 protocol with decoy states and phase encoding, so more thorough analysis will be conducted for the BB84 protocol and the BB84 decoy states.

2.3.1 BB84

In 1984, researchers Bennett and Brassard proposed the BB84 protocol, which revolutionized the field of quantum cryptography. The protocol leverages the principles of quantum mechanics, specifically Heisenberg's uncertainty principle, to securely share a secret key between two parties. The BB84 protocol is a prepare-and-measure-based quantum key distribution (QKD) protocol and is presented below [12, 19, 13, 18].

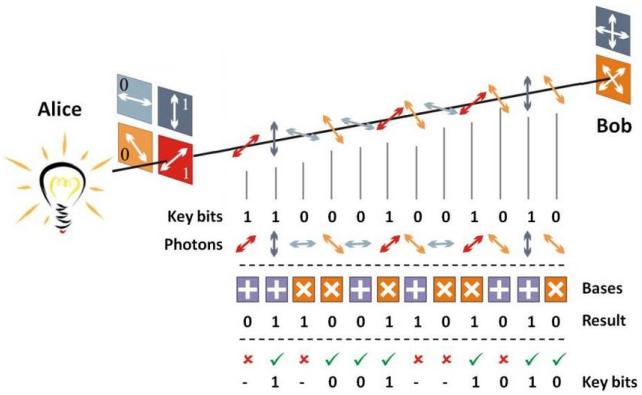

Figure 4: Alice prepares the Photons by modulating the bits (usually with polarization encoding) and send them through a quantum channel to Bob. Then Bob measures the photons using random basis as explained before. After measurement Alice and Bob proceed to the reconciliation process. Firstly, Alice and Bob publicly announce the used Basis for every bit and sift all the bits measured in different basis. Then they continue with Error Correction and Privacy Amplification in order to distill the final key. [7]

The essence of the BB84 protocol lies in the use of photon polarization states to transmit the information of the secret key through a quantum communication channel. It employs single photons, each polarized in one of four possible polarization states. These states are selected from two conjugate bases: the rectilinear basis, consisting of vertical and horizontal polarizations, and the diagonal basis, consisting of diagonal and anti-diagonal polarizations as shown below [12, 19, 13, 18, 7].

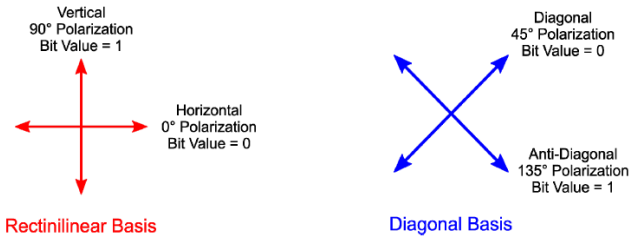

Figure 5: Polarization Basis of BB84 Protocol [19]

More analytically the exact stages of the BB84 are shown below:

1. **Quantum State Preparation:**

   Alice prepares individual photons in one of four polarization states: vertical ($|0\rangle$), horizontal ($|1\rangle$), diagonal ($|+\rangle$), and anti-diagonal ($|-\rangle$). These polarization states can be mathematically represented using the basis states of the rectilinear basis ($|0\rangle, |1\rangle$) and the diagonal basis ($|+\rangle, |-\rangle$).

2. **Basis Selection:** Alice randomly chooses a basis (rectilinear or diagonal) for each photon she prepares . The basis selection can be represented by random variables, denoted as A (for Alice's basis choice) and B (for Bob's basis choice)

3. **Quantum Transmission:** Alice sends the prepared photons to Bob over the quantum channel, while keeping track of the basis used for each photon.

4. **Measurement:** Upon receiving the photons, Bob randomly selects a measurement basis (rectilinear or diagonal) for each photon using random variable B. Bob performs a measurement on each photon, extracting information about its polarization state.

5. **Public Announcement:** After the transmission, Alice and Bob publicly communicate their basis choices (random variables A and B) for a subset of the transmitted photons. They do not reveal the measurement results, only the basis choices.

6. **Error Estimation:** By comparing their basis choices, Alice and Bob can identify the subset of photons used for error estimation. They calculate the error rate, which indicates the discrepancy between their measurement outcomes for the subset of photons.

7. **Key Generation:** Alice and Bob discard the subset of photons used for error estimation. They extract a secure key from the remaining subset of photons, using the agreed-upon basis choices where their measurement outcomes match.

8. **Privacy Amplification:** To further enhance security, Alice and Bob apply privacy amplification techniques, such as error correction codes and hashing algorithms, to distill a shorter but secure final key.

Throughout the BB84 protocol, the security is rooted in the fundamental principles of quantum mechanics, such as the no-cloning theorem and the uncertainty principle. The randomness in basis selection and the inherent uncertainty in quantum measurements ensure the security of the key distribution process [16, 12, 19].

The BB84 protocol serves as a cornerstone for quantum cryptography, demonstrating the practical implementation of quantum principles for secure communication.

However,in the original BB84 protocol, the encoding of information relies on single photons. But generating and manipulating single photons reliably can be challenging in practical implementations. Generating exactly one photon per pulse is not practically achievable in reality due to various factors like the probabilistic nature of photons emission or the devices imperfections. Thus, the process of photon generation follows a statistical distribution, often approximated by a Gaussian distribution. This means that the number of photons generated in each pulse can vary, and there is a non-zero probability of generating more than one photon. Therefore, instead of using single photon pulses, weak laser pulses are often employed, where the number of photons in each pulse follows a Poisson distribution with an adjustable mean value, known as the intensity of the source. In QKD, it is preferable to have a mean photon value per pulse, often denoted as the average photon number, less than 0.5. This requirement is aimed at reducing the likelihood of generating more than one photon per pulse, which is important for maintaining the security and integrity of the QKD process.

The presence of multiple photons in these laser pulses introduces a vulnerability known as the photon-number-splitting (PNS) attack. In a PNS attack, an eavesdropper can intercept a pulse containing multiple photons, split it into separate paths, and measure individual photons without being detected. This allows the eavesdropper to gain information about the key without introducing significant errors or disturbing the state of the remaining photons [22].

To address this vulnerability, it is crucial to assume that any key material derived from multi-photon pulses is compromised. In other words, it is necessary to consider that an eavesdropper might have obtained partial information about the key.

So the researchers were compelled to explore the development of new protocols due to the challenges and limitations of the BB84 [16].

2.3.2 BB84 Decoy State

The BB84 decoy state has some important differences with the simple BB84 including the key generation techniques, modulation and overall security against photon number splitting attacks.

BB84: In the original BB84 protocol, the key is generated by comparing the measurement outcomes of Alice and Bob for the subset of photons where they publicly announced matching basis choices. The secure key is extracted from these matching outcomes.

Decoy State BB84: In the decoy state BB84 protocol, in addition to the single-photon states, Alice sends additional intensity-modulated weak coherent states (decoy states) or vacuum pulses. These decoy states are used to enhance the security of the protocol, particularly against attacks such as photon number splitting (PNS) attacks.

After Bob receives the pulses from Alice, he announces to Alice which pulses generated photon counts (meaning they were detected) and which did not (meaning they were not detected). The order of the pulses is known only by Alice.

Based on the information received from Bob, Alice can compare the expected number of photon counts for the different types of pulses (decoy states and single-photon states) with the actual counts observed. If the discrepancy between the expected and observed counts exceeds certain thresholds, indicating a deviation from the expected behavior, it suggests a potential eavesdropping attempt. In such cases, the protocol is stopped as there is a high risk of eavesdropping or other security vulnerabilities.

By monitoring and analyzing the photon counts, the protocol can detect deviations caused by eavesdropping or other forms of interference. This allows Alice and Bob to take appropriate measures to ensure the security and integrity of the key distribution process.

An example of a practical approach to the BB84 with decoy states has been shown in [26] in which they used two normal pulses for signal and key distillation and one decoy state with mean photons values μ1 and μ2 ranging from 0.2 to 0.5 . A second experiment shown by [16] used one normal pulse and two decoy states with mean photons values μ = 0.425, v = (decoy state 1) = 0.044 , w = (decoy state 2) 0.001.

2.3.3 E91

In 1991, Artur Ekert introduced a groundbreaking quantum key distribution (QKD) protocol known as the Ekert or E91 protocol, which harnessed the remarkable phenomenon of photon entanglement. Entanglement is a unique property of quantum mechanics that allows two or more particles to become intricately connected, even when physically separated.

In the Ekert protocol, Alice and Bob share entangled pairs of photons, which can be created through various methods such as spontaneous parametric down-conversion. These entangled photons exhibit a special correlation known as quantum entanglement, where the state of one photon is instantly determined by the state of its entangled partner, regardless of the spatial separation between them. Entanglement-based QKD model can be illustrated by 6.

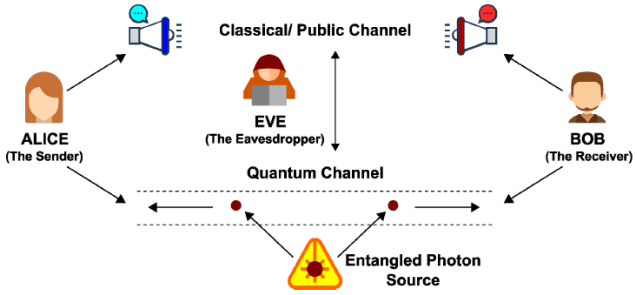

Figure 6: Basic Concept of Entanglement-Based QKD Protocol [19]

By exploiting this entanglement, Alice and Bob can perform a series of measurements on their respective photons, comparing the outcomes to establish a secret key. The key generation process relies on the fact that any attempt by an eavesdropper, commonly referred to as Eve, to gain information about the key through measurement or interception would introduce detectable disturbances to the entangled state.

The Ekert protocol leverages the violation of Bell's inequality, a fundamental concept in quantum mechanics, to detect the presence of eavesdropping. Bell's inequality sets bounds on the correlations that can be observed in classical systems, while quantum entanglement allows for correlations that surpass these bounds. By performing specific measurements on their entangled photons, Alice and Bob can test for the violation of Bell's inequality and detect any potential eavesdropping attempts.

The use of entangled photons in the Ekert protocol offers several advantages. First, it ensures the security of the key distribution process by exploiting the fundamental principles of quantum mechanics. Second, entanglement-based protocols can achieve higher key generation rates compared to protocols based on single-photon states. This is because entangled states allow for the detection of eavesdropping with higher probability, enabling the rejection of compromised key material.

Overall, the Ekert protocol revolutionized the field of quantum key distribution by harnessing the power of entanglement. It demonstrated the potential of entangled photon pairs as a resource for secure key distribution, paving the way for further advancements in quantum cryptography and quantum communication [19].

2.3.4 BBM92

The BBM92 protocol, proposed by Bennett, Brassard, and Mermin in 1992, is an entanglement-based quantum key distribution (QKD) protocol that shares similarities with the BB84 protocol. The fundamental concepts of raw key exchange, key sifting, and privacy amplification are essentially the same in BBM92 as in BB84. However, the key distinction is that BBM92 utilizes the principles of entanglement to establish a secure key.

In BBM92, entangled pairs of photons are used for key generation. The entanglement property ensures that the measurement outcomes of these pairs are correlated, allowing for secure key distribution. The entanglement-based nature of BBM92 distinguishes it from other QKD protocols that rely on single-photon states.

The BBM92 protocol emerged shortly after Ekert proposed his E91 protocol, and both

protocols fall under the category of entanglement-based QKD. While BB84 is widely recognized as a pioneering QKD protocol, BBM92 expands upon its principles by leveraging the power of entanglement to achieve secure key distribution [19].

2.3.5 B92

The B92 protocol, proposed by Bennett in 1992, is a simplified version of the BB84 protocol with some key differences. In B92, only two polarization states are used, compared to the four polarization states in BB84. This reduction in the number of states is a notable distinction between the two protocols.

In the B92 protocol, the encoding of information is done using a single non-orthogonal basis. The 0-bit value is encoded as 0 degrees in the rectilinear basis, while the 1-bit value is encoded as 45 degrees in the diagonal basis. Bennett realized that utilizing a single non-orthogonal basis for encoding and decoding the QKD protocol does not compromise the ability to detect the presence of an eavesdropper.

Another significant difference is that in the B92 protocol, if the receiver (Bob) selects the wrong basis, he will not measure anything. This condition, known as an erasure in quantum mechanics, occurs when Bob's measurement does not provide any conclusive information. This erasure condition adds a unique aspect to the B92 protocol compared to BB84.

Overall, the B92 protocol is classified as a prepare-and-measure-based QKD protocol, similar to BB84. However, its utilization of a reduced set of polarization states and the erasure condition sets it apart as a distinct protocol in quantum key distribution [19].

2.3.6 SSP

The Six-State Protocol (SSP), proposed by Pasquinucci and Gisin, introduces an extension to the BB84 scheme by incorporating an additional basis and increasing the number of polarization states. The SSP utilizes six polarization states and three measurement bases, compared to the four polarization states and two measurement bases in BB84.

In the SSP, the six polarization states correspond to $\pm$x, $\pm$y, and $\pm$z on the Poincaré sphere, offering a higher degree of symmetry compared to the BB84 protocol. This increased symmetry is advantageous for certain applications and analysis.

The additional basis in the SSP introduces an extra level of complexity and flexibility in the measurement process. Instead of performing measurements solely in the rectilinear and diagonal bases, as in BB84, the SSP incorporates an additional measurement basis. This additional basis enhances the robustness and security of the protocol by increasing the available information for key generation and error estimation.

Essentially, the Six-State Protocol can be seen as an extension of the BB84 scheme, building upon its principles and adding an extra measurement basis to accommodate the use of six polarization states. By expanding the measurement options and introducing additional symmetry, the SSP offers an alternative approach to quantum key distribution with potential advantages in certain scenarios [19].

2.3.7 DPS

The Differential-Phase-Shift QKD (DPS-QKD) protocol, proposed by K. Inoue et al. in 2003, is a quantum key distribution protocol that utilizes the principles of quantum entanglement. This protocol offers several advantages, including robustness against photon number splitting (PNS) attacks, a simple configuration, and efficient use of time resources.

One notable feature of the DPS-QKD protocol is its resilience against PNS attacks. Photon number splitting is a potential attack in which an eavesdropper could intercept a photon from the transmitted states, store it, and later measure it to extract information without being detected. The DPS-QKD protocol employs techniques that make it more secure against such attacks, enhancing the overall security of the key distribution process.

Another advantage of the DPS-QKD protocol is its simplicity in terms of configuration. The protocol can be implemented using relatively straightforward setups, making it easier to deploy and operate in practical scenarios [19].

2.3.8 COW

The Coherent One-Way (COW) protocol, proposed by Nicolas Gisin et al. in 2004, is a quantum key distribution protocol that utilizes the principle of photon entanglement. The COW protocol offers several advantages, including high efficiency in terms of distilled secret bits per qubit, robustness against photon number splitting (PNS) attacks, and tolerance to reduced interference visibility.

In the COW protocol, the information is encoded in the time function of the photons. This means that the temporal characteristics of the photons, such as their arrival times, are used to encode the quantum states representing the secret key. This approach allows for efficient encoding and decoding of the key information.

One of the advantages of the COW protocol is its high efficiency in extracting secret bits per qubit. This means that a higher number of secret bits can be generated per individual qubit used in the protocol, resulting in a more efficient key distribution process.

The COW protocol is also robust against PNS attacks, where an eavesdropper attempts to split the incoming photons to extract information. By utilizing the entanglement properties of the photons, the COW protocol offers enhanced security against such attacks.

Additionally, the COW protocol is tolerant to reduced interference visibility. Interference visibility refers to the quality of the interference pattern observed when combining two or more photons at a beam splitter. The COW protocol can still function effectively even in scenarios where the interference visibility is not ideal, allowing for practical implementations in real-world conditions.

The COW protocol is classified as an entanglement-based QKD protocol, as it relies on the generation and manipulation of entangled photon pairs to establish the secret key. This protocol provides an alternative approach to quantum key distribution, offering advantages in terms of efficiency, security, and tolerance to various conditions [19].

2.3.9 SARG04

The SARG04 protocol, proposed by Scarani et al. in 2004, is a quantum key distribution protocol that utilizes attenuated laser pulses as the source of photons instead of single-photon sources. This protocol shares a similar initial phase with the BB84 protocol. However, it differs in the second phase, where Alice, the sender, uses one of her pairs of non-orthogonal states to encode her bit instead of directly announcing her bases.

In the SARG04 protocol, if Bob, the receiver, uses the appropriate basis, he will measure the exact state and obtain the bit accurately. However, if he chooses the wrong basis, he will not obtain the bit. This approach helps in detecting the presence of an eavesdropper, as any attempt to intercept and measure the photon will result in a high probability of obtaining an incorrect bit value.

Under the assumption of no errors in measurement, the length of the key remaining after the sifting stage is 0.25 of the raw key sent. This indicates that, on average, only a quarter of the raw key remains after the sifting process, resulting in a reduced key length but increased security.

The SARG04 protocol belongs to the category of prepare-and-measure-based QKD protocols, where Alice prepares the photon states and Bob measures them. By using attenuated laser pulses and non-orthogonal states for encoding, this protocol offers an alternative approach to quantum key distribution, providing certain advantages and considerations compared to the BB84 protocol [19].

2.3.10 S13

The S13 protocol, proposed by Eduin H. Serna, is a quantum key distribution protocol that shares similarities with the BB84 protocol in terms of the underlying quantum mechanisms. However, the S13 protocol introduces differences in the key reconciliation process and the use of asymmetric cryptography.

In the BB84 protocol, the key reconciliation process involves public communication between Alice and Bob to compare their measurement outcomes and establish a common subset of matching bits for the key. This process is susceptible to potential eavesdropping and may require additional error correction and privacy amplification steps to ensure the security of the final key.

In contrast, the S13 protocol utilizes a private reconciliation approach. Instead of exchanging information publicly, Alice and Bob use a random seed to independently generate their reconciliation data. This private reconciliation process reduces the potential for eavesdropping and enhances the overall security of the key distribution.

Additionally, the S13 protocol incorporates asymmetric cryptography techniques. Asymmetric cryptography involves the use of different cryptographic keys for encryption and decryption. In the context of the S13 protocol, asymmetric cryptography is utilized to secure the communication of reconciliation data between Alice and Bob. This adds an extra layer of security to the key distribution process, protecting against potential attacks on the reconciliation stage.

By employing private reconciliation and asymmetric cryptography, the S13 protocol en-

hances the security and privacy of the key distribution process compared to the traditional BB84 protocol. These modifications aim to mitigate vulnerabilities and provide a more robust framework for secure key exchange in quantum communication systems [19].

A list of the QKD protocols is shown below in the Table 1.

No.	Year	Name of Protocol	Principle Base
1	1984	BB84	Heisenberg's Uncertainty Principles
2	1991	E91	Quantum Entanglement
3	1992	BBM92	Quantum Entanglement
4	1992	B92	Heisenberg's Uncertainty Principles
5	1999	SSP	Heisenberg's Uncertainty Principles
6	2003	DPS	Quantum Entanglement
7	2004	SARG04	Heisenberg's Uncertainty Principles
8	2004	COW	Quantum Entanglement
9	2013	S13	Heisenberg's Uncertainty Principles

Table 1: List of QKD Protocols [19]

2.4 Metrics

In order to measure the performance and the effectiveness of a QKD protocol we use some metrics that allow us to characterize the systems which are used to implement every protocol.

Quantum Bit Error Rate (QBER): QBER measures the error rate in the transmission of quantum bits (qubits) between the sender (Alice) and the receiver (Bob). A low QBER indicates a higher fidelity of transmission and better resistance to eavesdropping.

Key Generation Rate: This metric quantifies the speed at which Alice and Bob can generate a shared secret key. It is usually measured in bits per second (bps) or key bits per second (kbps). A higher key generation rate indicates a more efficient protocol.

Secure Key Rate: The secure key rate represents the rate at which Alice and Bob can generate a secure key after applying error correction and privacy amplification techniques. It takes into account factors such as QBER, reconciliation efficiency, and information leakage.

2.5 Losses

One of the main limitations of Quantum Key Distribution (QKD) is the losses that occur during the propagation of quantum signals. As quantum signals are transmitted over long distances through optical fibers or free space, various sources of loss can degrade the signal quality. These losses can be due to factors such as absorption, scattering, and imperfections in the transmission medium. Losses during propagation reduce the signal-to-noise ratio, making it challenging to reliably detect and decode quantum states at the receiving end. High losses also limit the achievable communication distance, as the signal strength diminishes over longer transmission spans. Mitigating losses in QKD systems requires advanced

techniques such as efficient error correction codes, amplification schemes, and optimized fiber optic links. Addressing the issue of losses is crucial to improve the overall performance and practicality of QKD for secure quantum communication. An example of how losses affect the achievable communication distance in shown below.

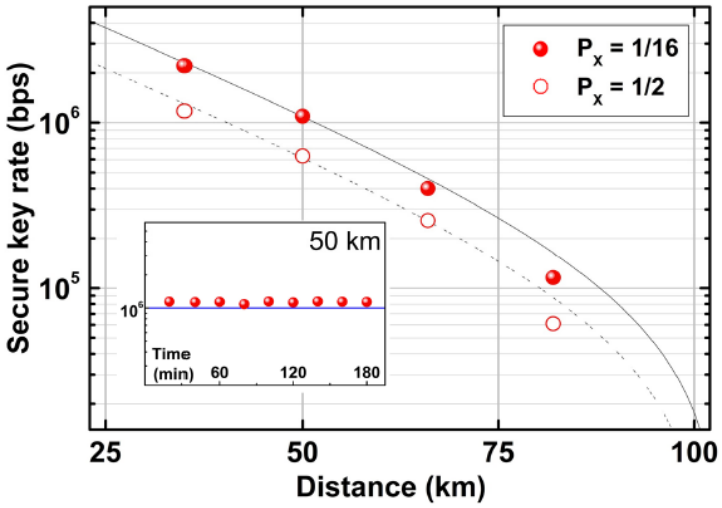

Figure 7: SKR in respect with distance for an implementation of BB84 with Decoy-States [16]

3 Coexistence of QKD with Classical Channels

Quantum communication networks represent a significant advancement in the field, moving from simple point-to-point quantum links to complex multi user networks with real-life connectivity. The ultimate goal is to establish a Quantum Internet, where nodes are seamlessly interconnected, enabling applications beyond Quantum Key Distribution (QKD) like distributed quantum computing. Achieving this requires a medium that allows the coexistence of high-power classical optical channels and quantum channels, integrating quantum technologies into existing optical infrastructure [2, 23].

Incorporating Quantum Key Distribution (QKD) into the existing infrastructure is of utmost importance for several reasons. Firstly, it allows for a seamless integration of quantum technologies with the current optical network, enabling widespread deployment and utilization of quantum communication protocols. By leveraging the existing infrastructure, the cost and complexity associated with building a separate dedicated network solely for quantum communication can be significantly reduced. This practical approach ensures that QKD becomes more accessible and feasible for real-world applications.

Secondly, integrating QKD with the existing infrastructure provides a smooth transition from classical to quantum communication. It allows for the coexistence of high-power classical optical channels and delicate quantum channels, which is essential for practical implementation. Rather than relying on separate optical fibers dedicated solely to quantum communication, integrating quantum channels within the same infrastructure allows for efficient use of resources and facilitates interoperability between classical and quantum systems.

However, the theoretical approach of using separate optical fibers for the quantum channel is often considered due to the stringent requirements of quantum communication. Quantum signals are extremely sensitive to noise and interference, and any disruptions can compromise the security and integrity of the transmitted information. By employing separate fibers, the risk of crosstalk, signal degradation, and unintended interactions between classical and quantum channels is minimized. This approach ensures a higher level of isolation and enhances the overall performance and security of the quantum communication system.

While a separate fiber approach provides enhanced isolation, it introduces challenges in terms of scalability, cost, and infrastructure complexity. The deployment of dedicated fiber networks across large distances can be logistically challenging and financially demanding. Moreover, maintaining and managing separate networks for quantum communication alongside existing infrastructure can be operationally burdensome.

Therefore, integrating QKD into the already existing infrastructure presents a more practical and cost-effective approach, enabling the widespread adoption of quantum communication technologies. It strikes a balance between the need for security and the constraints of real-world implementation, making quantum communication more accessible, efficient, and seamlessly integrated with existing optical networks.

3.1 Non Linear Effects

The key challenge coexistence has to overcome is the introduction of Non- Linear effects that occur during the propagation of the optical signals in the fibers. The non linear effects that will be presented, result in excessive noise and therefore influence the Quantum Channel. The quantum channel operates at very low power levels, typically involving single photons or a few photons per pulse. This low power is necessary to preserve the delicate quantum properties of the transmitted information. However, the presence of high-power classical optical signals can induce unwanted interactions and disturbances on the quantum channel. The nonlinear effects in the fiber, such as Raman scattering and four-wave mixing, can generate noise and interfere with the quantum signals, leading to errors and degraded performance that will be shown as higher QBER and lower secure key rate.

The investigation and analysis of nonlinear effects and their impact on the coexistence of quantum and classical channels will indeed be a critical component of this thesis work. By conducting experiments and obtaining empirical results, valuable insights into the behavior of nonlinear effects in practical scenarios will be gained.

3.1.1 Raman Scattering

Raman scattering, a nonlinear optical effect, is caused by Phonons which are lattice vibrations in a material. This phenomenon involves the interaction of photons with molecular vibrations in the optical fiber, resulting in the transfer of energy from the signal photons to scattered photons of different frequencies . Raman scattering can produce scattered photons in two spatial region. When energy is transferred from incident light to the the molecular vibration is losses energy and a lower energy and thus lower frequency photon is produced in the Anti-Stokes Region. On the other hand if energy is transferred from the phonon to

the incident photon, a scattered photon with higher energy and frequency is generated in the Stokes Region [1]. The presence of Raman scattering introduces additional noise and fluctuations in the quantum channel, degrading the signal quality and reducing the fidelity of quantum states. Raman scattering is a broadband effect that can cover 200 nm of spatial range, thus it can affect quantum channels that are operating in different spectral regions if the power of the noise originating from the Raman scattering in greater than that of the quantum channel. In QKD this is the case since the photons of the quantum channel are propagating with low power in order to keep their quantum properties. In order to have reliable quantum communication and preserve the confidentiality of the transmitted quantum information include various techniques, such as fiber design optimization, power management, endpoints synchronization and noise filtering, are employed to minimize the detrimental effects of Raman scattering and enhance the performance of quantum communication systems [11].

Below is a graphic example of how noise from classical channels can totally obscure the quantum channels.

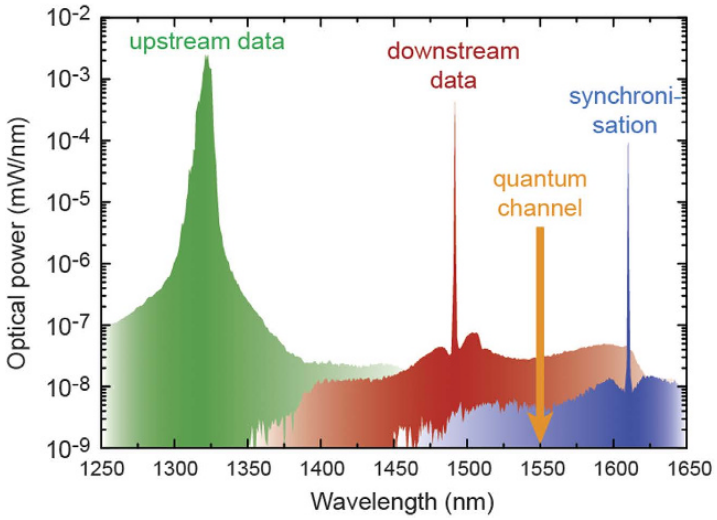

Figure 8: Spectrum measured in upstream direction by inserting a 50:50 beam splitter in front of the OLT in an 8-user network. The spectrum shows peaks at 1310 nm and 1490 nm from data signals and a peak at 1610 nm from the synchronisation signal. The quantum signal at 1550 nm is completely obscured by the broad Raman scattering background.[11]

3.1.2 Four-wave mixing

When a high-power optical signal is launched into a fiber, the linearity of the optical response is lost. One such nonlinear effect, which is due to the third-order electric susceptibility is called the optical Kerr effect . In the equations below the third order non linearity is shown firstly in the refractive index change in response to an external electrical field which in our case can be the light itself and secondly as the polarization induced in a material by the applied electric field [6, 15].

$$n = n_0 + \frac{3\chi^{(3)}}{4}(|E_\omega|)^2$$

$$P = \varepsilon_0 \left(\chi^{(1)} E + \chi^{(2)} E^2 + \chi^{(3)} E^3 + \ldots \right)$$

Four-wave mixing (FWM) is a type nonlinear optical Kerr effect that can occur when multiple optical signals interact within an optical fiber. It involves the mixing of different optical frequencies, resulting in the generation of new frequencies and interfering with the desired quantum signals. The FMW phenomenon is observed when in a fiber there is an already existing wave which is called the signal wave or probe light. If in addition to this one or more pumping waves are launched into the fiber then there is a generation of another wave which is called the idler wave. This generated wave has a new frequency calculated by the equation:

$$f_{\text{idler}} = f_{p1} + f_{p2} - f_{\text{probe}}$$

for the case with two pumping waves and by the equation

$$f_{\text{idler}} = 2f_p - f_{\text{probe}}$$

which is the case with pumping waves at the same frequency and is called degenerated FWM. [3, 6]

FWM can introduce crosstalk and impair the performance of quantum communication systems, leading to information leakage or errors in the transmitted quantum bits. To mitigate the impact of FWM, techniques such as wavelength management, signal power optimization, and careful system design are employed to minimize the interactions among different optical frequencies and maintain the integrity of quantum information [6].

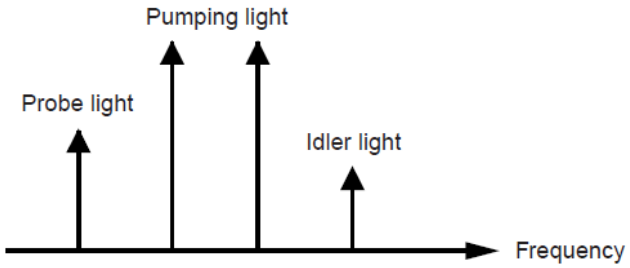

Figure 9: Four-wave mixing with two pumping channels [6]

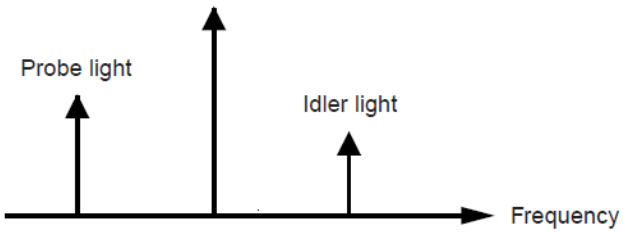

Figure 10: Four-wave mixing with one pumping channel [6]

3.2 Linear Effects

Linear effects in optical communication, such as chromatic dispersion and Rayleigh scattering, can impact the performance of Quantum Key Distribution (QKD) systems. Chromatic dispersion can cause pulse broadening and overlapping, leading to errors in the time resolution of photon detection, affecting the accuracy of key generation. Rayleigh scattering introduces background noise that can degrade the signal-to-noise ratio of the quantum channel, reducing the secure key rate. Understanding and mitigating these linear effects is essential to ensure reliable and secure QKD operation in the presence of optical impairments.

3.2.1 Rayleigh back-scattering

Rayleigh backscattering is another important aspect to consider in quantum communication systems. It refers to the scattering of light that occurs when the incident photons interact with inhomogeneities or imperfections in the fiber. This backscattered light can interfere with the desired quantum signals, leading to signal degradation and increased noise levels. In the context of Quantum Key Distribution (QKD), Rayleigh backscattering can introduce information leakage, compromise the security of transmitted quantum bits, and limit the achievable communication distance. To mitigate the effects of Rayleigh backscattering, techniques such as forward error correction, signal encoding, and advanced signal processing algorithms are employed. By effectively managing and reducing the impact of Rayleigh backscattering, quantum communication systems can achieve improved signal quality, enhanced security, and longer communication distances, enabling the reliable and secure transmission of quantum information [1, 20].

3.2.2 Chromatic dispersion

Chromatic dispersion and four-wave mixing are additional factors that need to be addressed in quantum communication systems. Chromatic dispersion refers to the phenomenon where different wavelengths of light propagate at different speeds in an optical fiber, causing the spreading of optical pulses over long distances. This dispersion can distort the temporal characteristics of quantum signals, leading to errors in the detection and decoding of quantum information. To mitigate chromatic dispersion, dispersion compensation techniques such as dispersion-compensating fibers or dispersion compensation modules are utilized to ensure accurate transmission of quantum signals [1, 20].

For this thesis, the experimental setup involves running the experiments over relatively short distances, typically within a few kilometers, with a maximum distance of 10 kilometers. Given the limited span of the transmission, the primary nonlinear effect that becomes prominent in this scenario is Raman scattering. As the experiments focus on shorter distances, the significance of Raman scattering becomes more pronounced, making it a crucial phenomenon to understand and mitigate in order to achieve reliable and efficient quantum communication.

3.3 Optimal Wavelength for QKD Channel

There are two key reasons why the wavelength range around 1310 nm is often considered optimal for the quantum channel in certain quantum communication systems.

Firstly, at 1310 nm, there is a lower occurrence of Raman scattering compared to other wavelength ranges. Raman scattering is a nonlinear effect in optical fibers that causes the conversion of some of the signal's energy into unwanted noise. By operating at 1310 nm, the impact of Raman scattering on the quantum channel is reduced, resulting in a cleaner and more reliable transmission of quantum information. This is crucial for maintaining the integrity and security of the quantum communication system [24].

At 11 the count rate of Raman noise generated from a continuous-wave laser source is shown. The source is tuned from 1530 to 1570 nm and launched with a power level of 6 dBm.

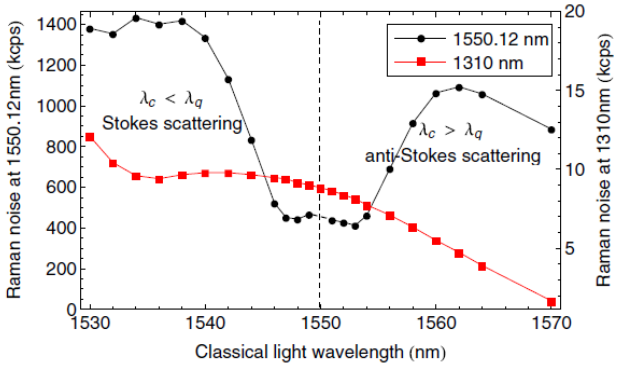

Figure 11: Raman noise at 1550.12 nm (black circles) and 1310 nm (red squares). The forward Raman noises are measured in kilocounts per second (kcps) [24]

Secondly, the wavelength range around 1310 nm also exhibits lower levels of Four-Wave Mixing (FWM). FWM as explained above, results in unwanted signal mixing and degradation. By operating in the 1310 nm range, the influence of FWM on the quantum channel is minimized. This ensures that the quantum signals remain distinct and unaffected by the presence of other optical signals, maintaining the quality and reliability of the quantum communication link.

These advantages of lower Raman scattering and reduced FWM make the wavelength range around 1310 nm an attractive choice for the quantum channel. It provides a favorable environment for the transmission of quantum information with minimal interference and signal degradation. However, it is important to note that the optimal wavelength choice may vary depending on the specific characteristics and requirements of the quantum communication system [24].

3.4 Coexistence Procedure

3.4.1 QKD in Laboratory

The first step towards demonstrating the coexistence of quantum key distribution (QKD) with existing communication systems is typically conducted in laboratory conditions. In this

controlled environment, researchers aim to establish the feasibility and functionality of QKD protocols, validate their security measures, and optimize their performance parameters. Laboratory experiments allow for comprehensive testing and evaluation of QKD systems under controlled settings, enabling the identification and resolution of potential technical challenges and limitations.

3.4.2 QKD over PON

Once the laboratory experiments are successful, the next crucial step is to integrate QKD technology into real-world communication networks, such as a Passive Optical Network (PON). Passive Optical Networks (PONs) are a type of telecommunications network that use fiber optic cables. They are widely used in broadband access networks, such as Fiber to the Home (FTTH) or Fiber to the Curb (FTTC) networks to provide high-speed data, voice, and video services to subscribers. However, the presence of passive components (splitters, couplers) in the commonly used passive network architecture makes successful transmission of weak quantum signals challenging. This is especially true if QKD (Quantum key distribution) and data signals are multiplexed in the passive network. The splitter introduces an imbalance between quantum signal and Raman noise, which can prevent the recovery of the quantum signal completely.

A PON typically consists of the following components:

OTN (Optical Transport Network): Backbone network infrastructure that carries high-speed optical signals between the OLT and ODN, providing efficient and reliable transmission of data.

ODF (Optical Distribution Frame): Central distribution point where optical fibers from multiple subscribers are terminated and connected to the PON infrastructure.

ODP (Optical Distribution Point): Intermediate distribution point in the PON that connects multiple ODNs and serves as a branching point for the optical fibers.

OTO (Optical Termination Outlet): Physical termination point at the subscriber's premises where the optical signal is received and converted into electrical signals for connection to the subscriber's devices.

OLT (Optical Line Terminal): Centralized equipment in the service provider's network that controls and manages the PON, transmitting and receiving data between the ODN and subscriber ONTs.

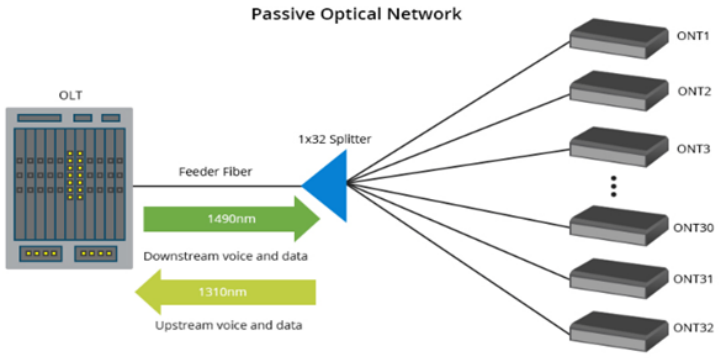

Figure 12: Passive Optical Network (PON) [1]

GPON (Gigabit Passive Optical Network) is a specific type of PON that utilizes the ITU-T G.984 standard, designed to provide higher data rates and increased efficiency over optical fibers, GPON operates at higher data rates, typically up to 2.5 Gbps downstream and 1.25 Gbps upstream.

3.4.3 QKD Procedure for this Diploma Thesis

The procedure that will be followed for this master thesis includes three sections. Firstly an overview of the already existing works. Secondly, experimental procedure in the laboratory for the Quantum Key distribution will be shown including two experiments, one showing communication of two pairs of nodes distributing the quantum key, with them positioned in such a way that the signal propagates in the opposite direction and one showing coexistence of the quantum channels with CW lasers. In the final section, the objective is to implement Quantum Key Distribution (QKD) over the PON (Passive Optical Network) systems of OTE (Hellenic Telecommunications Organization) and demonstrating its applicability in the existing network. So, to achieve this, we will conduct measurements and test the feasibility of QKD on the existing PON replica at the OTE Academy Lab.

[1] Source: https://community.fs.com/blog/passiveoptical-network-tutorial.html

4 Synopsis of prior research on the coexistence of Quantum Key Distribution (QKD)

4.1 Ultra-high bandwidth quantum secured data transmission [9]

The report discusses the challenge of integrating quantum key distribution (QKD) with high-bandwidth optical networking infrastructure. Traditionally, QKD systems have used separate dedicated links for quantum signals and conventional data, which can be expensive and not always available. The goal is to enable QKD signals to share the same fiber as conventional data, allowing for cost-effective deployment [9].

The researchers conducted an experiment to demonstrate the compatibility of quantum communication with high-bandwidth optical networking. They combined QKD with dual-polarization quadrature phase shift keying (DP-QPSK) for data channels, achieving a quantum encryption system with QKD key rates in the megabits per second (Mb/s) range and encrypted data transport at a bandwidth of 200 gigabits per second (Gb/s) on the same fiber [9].

The system operated over fiber lengths of up to 101 kilometers (km), which covers most metropolitan area networks.The researchers also explored the feasibility of multiplexing QKD with up to 10 terabits per second (Tb/s) of data for fiber lengths up to 50 km [9].

To mitigate the challenges posed by the stronger and broadband data signals, the researchers implemented spectral, temporal, and optical power control techniques. They used spectral and temporal filtering to minimize Raman scattering into the quantum channel, and optical power control to reduce the launch power of data signals [9].

The results showed that QKD could coexist with high-volume data traffic. The secure bit rate was dependent on the fiber distance and the width of the spectral filter used in the quantum receiver. With a 100 gigahertz (GHz) filter, secure bit rates of up to 1.9 Mbps were achieved for fiber distances of 35.5 km, and secure bit rates of up to 10 kbps were achieved for a distance of 101 km using a 25 GHz filter [9].

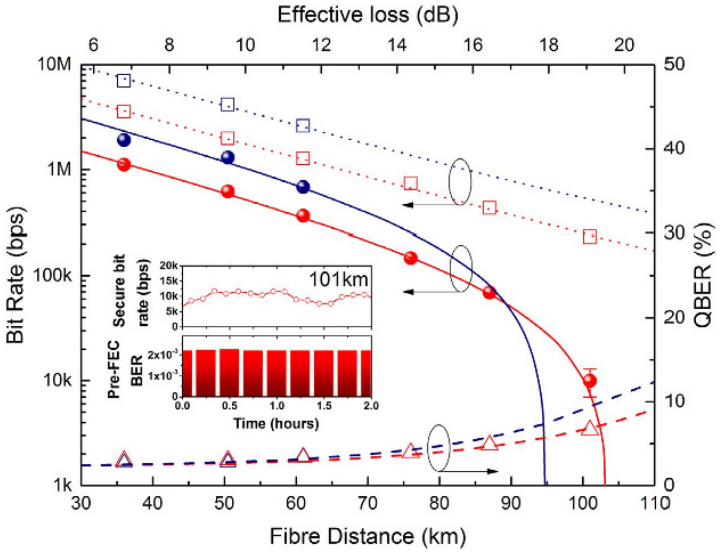

Figure 13: Experimental secure bit rate as a function of fibre distance in the presence of 2 × 100 G forward directed classical data traffic over the same fibre [9]

The researchers also conducted an experimental simulation to investigate the maximum data bandwidth that could coexist with QKD signals. They demonstrated that QKD could coexist with 10 × 100 Gb/s data channels, corresponding to an aggregate bandwidth of 1 terabit per second (Tbps) over a duration of 18 hours. Furthermore, the simulation showed that QKD with a finite bit rate was possible for data bandwidths up to 6 Tb/s with a 100 GHz filter and up to 10 Tb/s with a 25 GHz filter [9].

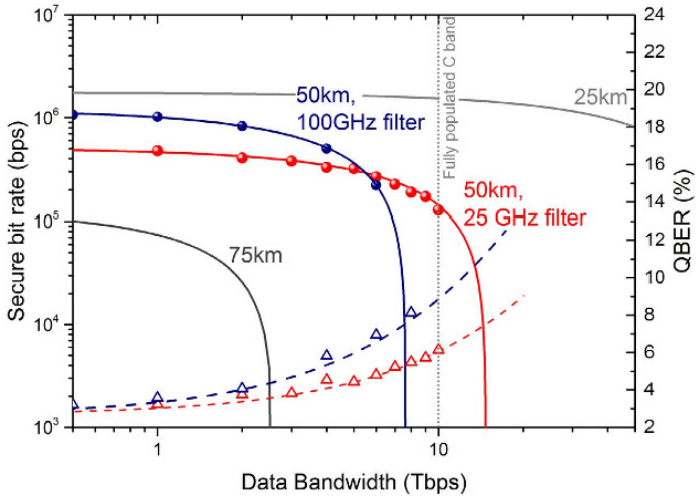

Figure 14: Experimental secure bit rate as a function of data bandwidth simulated by increasing the launch power of 10 data lasers. [9]

The results of the experiment and simulation indicate that QKD can be integrated with high-bandwidth optical networking, supporting data rates exceeding 10 Tb/s for fiber lengths up to 50 km. This represents a significant advancement in terms of data bandwidth and secure bit rates compared to previous studies.

Overall, the findings of the report suggest that quantum communication can be effectively combined with high-speed data transmission, enabling secure encryption in high-bandwidth optical networks.

4.2 Quantum secured gigabit optical access networks [11]

The article discusses the integration of quantum key distribution (QKD) into existing telecommunication infrastructure, specifically in GPON (Gigabit Passive Optical Network) networks. The integration of QKD with classical data signals is important for seamless integration into the existing infrastructure. However, the presence of classical data signals in a live fiber can introduce excess noise, particularly from inelastic Raman scattering, which makes the retrieval of quantum information challenging as discussed above [11].

The article presents a method for integrating multi-user QKD into a GPON network using a dual feeder architecture as shown in **??** below. In this architecture, secure quantum keys can be transmitted alongside full-power GPON data signals without the need for post-processing or time alignment. The method allows for the operation of QKD with up to 128

users in realistic network layouts while maintaining the advantage of single fiber links in the main part of the network [11].

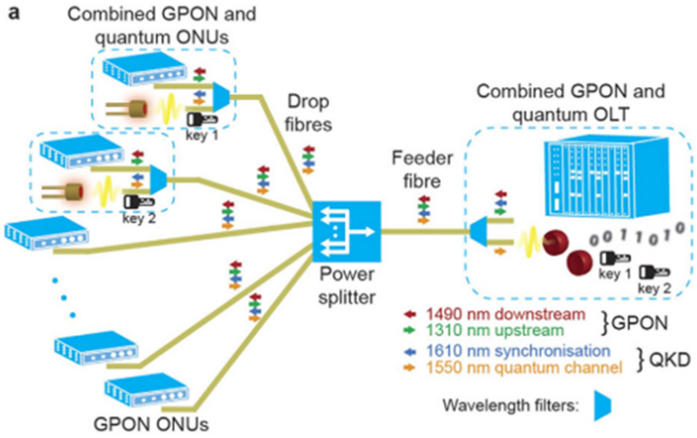

Figure 15: In a passive optical network multiple users (ONU: optical network unit) are connected via drop fibres, an optical power splitter, and a feeder fibre to a network node (OLT: optical line terminal). [11]

The results show that in single feeder networks, the achievable network capacity is strongly restricted due to Raman noise. However, in dual feeder networks, where a second feeder fiber is added, the limitation imposed by Raman noise is overcome. The article provides experimental and simulation data to demonstrate the effectiveness of the dual feeder architecture in increasing the secure key rate and supporting larger network capacities [11].

The simulation results also show that the secure key rate remains positive even when more users are added to the quantum access network. Additionally, the article discusses the influence of the total drop fiber length on the secure key rate in a dual feeder network [11].

Results are shown below

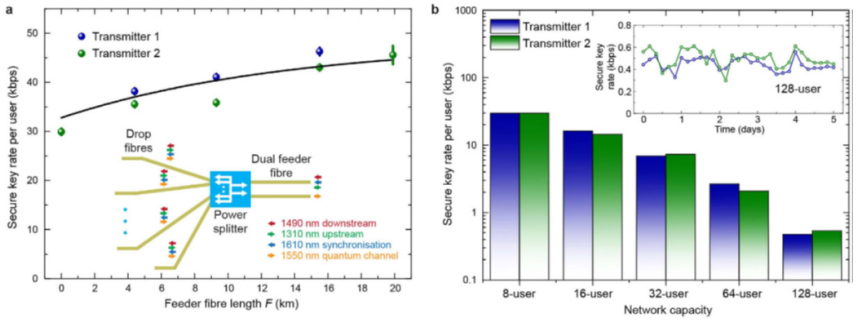

Figure 16: Secure key rate per quantum transmitter as a function of feeder fibre distance F in a dual feeder network. The total distance F + D is kept equal to 20 km. Error bars correspond to 1 standard deviation of 3 consecutive measurements. The solid line is calculated using the numerical simulation described in the methods section. Inset: Schematic of the dual feeder network. The power splitter is replaced with a 2 × N splitter connected to two separate feeder fibres. The downstream GPON and synchronisation signal are launched into one feeder fibre, whereas the quantum signals is extracted from the second feeder fibre. (b) Secure key rate per transmitter for varying network capacity with two feeder fibres. Secure transmission is demonstrated up to a splitting ratio of 2 × 128. Inset: Secure key rate over several days in a 128-user network. [11]

Overall, the article presents a method for integrating QKD into GPON networks, overcoming the challenges posed by Raman noise and enabling the secure transmission of quantum keys alongside classical data signals. The dual feeder architecture allows for the operation of QKD with multiple users in large-scale networks.

4.3 DV-QKD Coexistence With 1.6 Tbps Classical Channels Over Hollow Core Fibre [4]

The feasibility of coexisting a quantum channel with carrier-grade classical optical channels over Hollow Core Nested Antiresonant Nodeless Fibre (HC-NANF) is experimentally explored for the first time in terms of achievable quantum bit error rate (QBER), secret key rate (SKR) as well as classical signal bit error rates (BER). A coexistence transmission of 1.6 Tbps is achieved for the classical channels simultaneously with a quantum channel over a 2 km-long HC-NANF with a total coexistence power of 0 dBm. To find the best and worst wavelength position for the classical channels, the researchers simulated different classical channels bands with different spacing between the quantum and classical channels considering the crosstalk generated from both Raman scattering and four-wave-mixing (FWM) on the quantum channel. Following their simulation, they numerically estimate the best (Raman spectrum dip) and worst locations (Raman spectrum peak) of the classical channel with respect to its impact on the performance on the quantum channel in terms of SKR and QBER.They further implemented a testbed to experimentally test both single-mode fibre (SMF) and HC-NANF in the best and worst-case scenarios. In the best-case scenario, the spacing between quantum and classical is 200 GHz (1.6 nm) with 50 GHz (0.4 nm) spacing between each classical channel. The SKR was preserved without any noticeable changes when coexisting the quantum channel with eight classical channels at 0 dBm total coexistence power in HC-NANF compared to a significant drop of 73% when using SMF at -24 dBm total coexistence power which is 250 times lower than the power used in HC-NANF. In the worst-case scenario using the same powers, and with 1 THz (8 nm) spacing between quantum and classical channels, the SKR dropped 10% using the HC-NANF, whereas in the SMF the SKR plummeted to zero [4].

The experimental setup is shown below

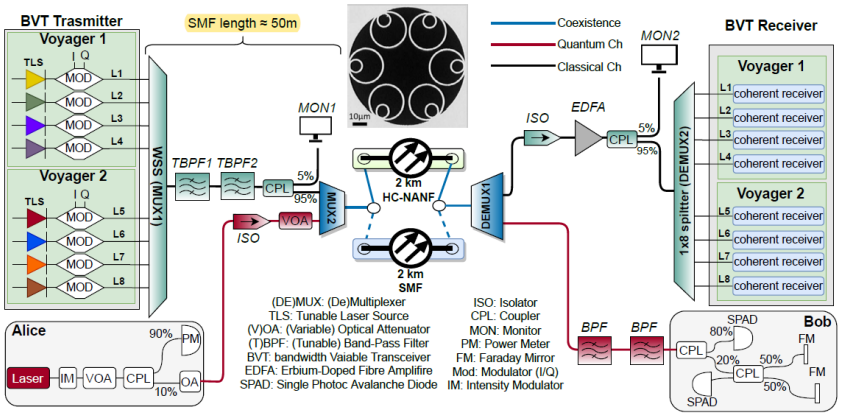

Figure 17: Experimental Testbed for the Coexistence of 1.6 Tbps classical channels and DV-QKD channel over 2km HC-NANF and SMF. Inset: scanning electron micrograph (SEM) of the HC-NANF cross section. [4]

5 Laboratory Experimental Procedure

The experimental procedure consists of two parts. The first part of the experiment takes place in the Optics Laboratory of the Informatics and Technology department of the National and Kapodistrian University of Athens.

Two experiments are presented in the lab:

a) "Investigation of Counter-Propagating Interactions in Quantum Communications using efficient BB84 protocol with decoy states"

b) "Investigation of Coexistence of quantum channels with classical optical signals generated by CW lasers again with counter propagating layout"

5.1 Experimental setup

QKD transmitter and receiver

The QKD pairs we use for our experiments both in lab and on the access network are manufactured by Toshiba and implement the Efficient BB84 protocol with decoy states and phase encoding. They consist of two parts, the main part which implements the protocol with all the optical components including lasers, photodetectors, isolators etc. and the Control Server for user interaction with the system. The server runs a Linux based operating system and is preconfigured with all the required control software which includes a graphical interface that we are going to use for our experimental procedure and results. The layout is shown below.

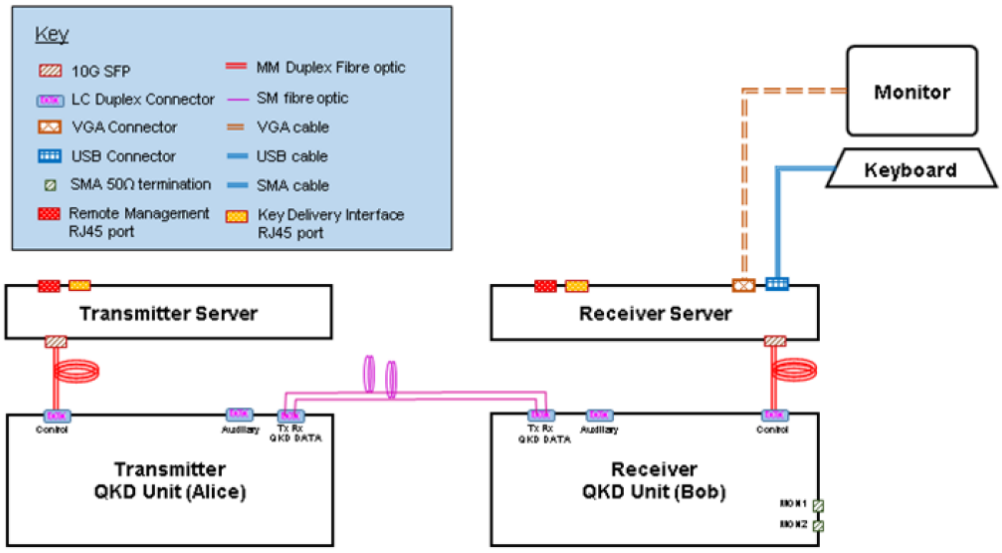

Figure 18: Connection diagram for QKD configuration

Every QKD consists of 3 dublex LC fibers connectors. Connector with label "Control" is to connect to its QKD control server using a duplex multimode LC cable.
the connector, labelled as "QKD Data", is to connect QKD Transmitter and Receiver using a simplex single mode fibre cable with LC connectors.

The QKD wavelengths are:

On the forward direction:

Quantum channel 1310 nm : 1 GHz gain switched laser diode with 50 ps pulses. Average power under normal operating conditions exiting Alice: < 10 nW.

Synchronisation channel 1530.33 nm (DWDM): DWDM SFP emitting 250 MHz with a 50:50 duty cycle, shortest pulse 1 ns or greater. Average output power under normal operating conditions < 2 mW.

Synchronisation QKD Classical channel 1529.55 nm (DWDM): SFP+ emitting 10Gb/s NRZ data stream, shortest pulse 40 ps or greater. Average output power under normal operating conditions < 2 mW.

On the backward direction:

Synchronisation QKD Classical channel 1528.77 nm (DWDM): SFP+ emitting 10Gb/s NRZ data stream, shortest pulse 40 ps or greater. Average output power under normal operating conditions < 2 mW.

We have two (2) pairs of QKD units in the lab, so this enables us to conduct the first experiment which includes both pairs.

CW Lasers

We also use CW lasers in order to simulate the classical channels and multiplex them into the network in order to implement the coexistence.

Continuous wave (CW) lasers have a nominally constant output over a set interval. This means that key beam parameters (power output, intensity, etc.) remain constant throughout the beam's duration. The phrase continuous-wave refers to the coherent beam of monochromatic light emitted by the gain medium, which also determines the laser wavelength.

To ensure precise and stable operation of CW lasers, a dedicated controller is utilized. The controller acts as the interface between the laser and the operator, allowing for fine-tuned control over various parameters such as precise current control, temperature regulation. It provides the necessary electrical current and voltage regulation to drive the laser diode each laser diode.

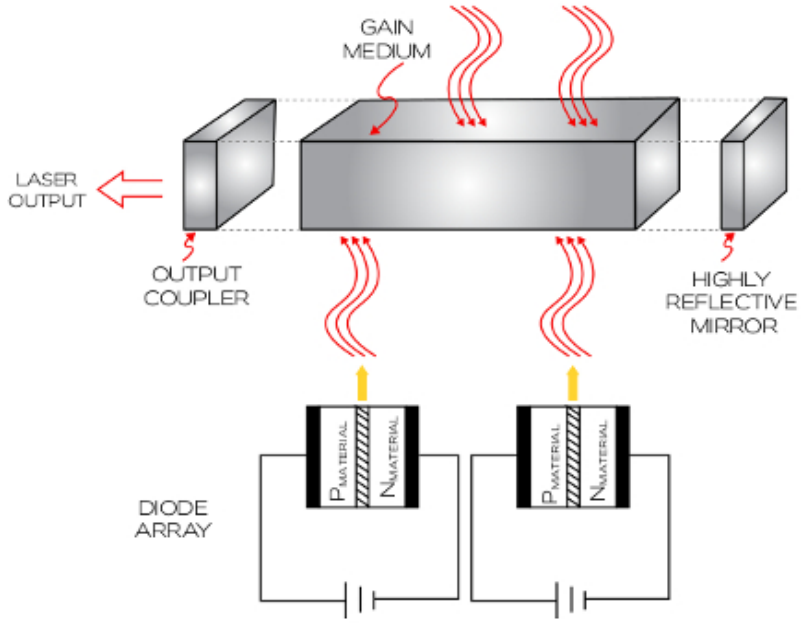

Figure 19: DFB laser [2]

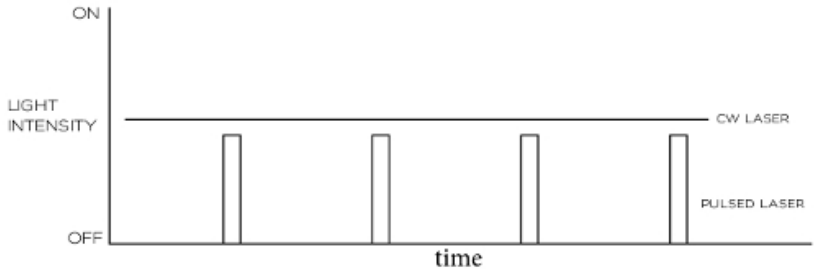

Figure 20: Difference between CW and pulsed laser in light intensity [2]

5.1.1 Optical Spectrum Analyzer (OSA)

An Optical Spectrum Analyzer (OSA) is a device used in optical communications and fiber optics to analyze and measure the power and wavelength distribution of an optical signal over a specific range of wavelengths. It is a crucial tool for characterizing and troubleshooting optical systems.

The main features for which the OSA is going to be utilized:

Measurement Range: An OSA can measure optical signals over a wide range of wavelengths, typically from the visible to the infrared spectrum, covering several hundred nanometers or more. The one we one in the laboratory has a spectral range

Wavelength Resolution: OSAs provide high-resolution measurements, allowing precise analysis of individual spectral components. They can resolve small wavelength differences, typically in the range of picometers or better.

Power Measurement: OSAs can measure the power or intensity of optical signals at different wavelengths. This information helps determine the power distribution across the

[2]Source: https://www.laserlabsource.com/Solid-State-Lasers/cw-laser-basics

spectrum.

Spectral Analysis: OSAs display the spectral power distribution graphically, usually in the form of a wavelength versus power plot. This graphical representation helps identify peaks, notches, and other spectral characteristics.

Signal Analysis: OSAs provide various analysis functions such as peak search, sideband analysis, channel power measurements, signal-to-noise ratio (SNR) calculations, and more. These features aid in signal characterization and performance evaluation.

5.2 Investigation of Counter-Propagating Interactions in Quantum Communications using efficient BB84 protocol with decoy states

This experiment focuses on evaluating the interference effects that arise when two QKD Toshiba machines are connected in a counter-propagating configuration. The setup involves two pairs of Alices and Bobs, where their respective quantum channels are multiplexed over a shared optical fiber using 1:4 couplers. Specifically, the transmitter of Alice 1 and the receiver of Bob 2 are connected to the first coupler, while the transmitter of Alice 2 and the receiver of Bob 1 are connected to the second coupler. Furthermore there is a direct connection between QRx of Alice1 and Alice 2 with QTx of Bob1 and Bob2 respectively. On this fiber, the backward direction is implemented. This arrangement allows for bidirectional signal transmission and enables the examination of interference phenomena in the QKD system.

The topology is shown below.

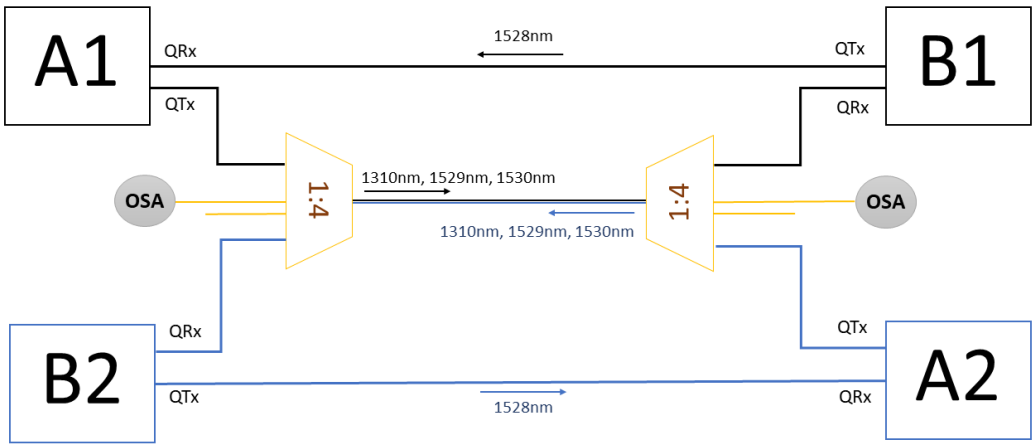

Figure 21: Experimental Testbed for two QKD setups with counter propagation

Results

After we put the system into operation we are going to determine the system's behavior by looking at the SKR and the QBER of both pairs. To start with, both pairs are connected and generate key, so they work properly. The SKR and QBER are shown below.

Figure 22: SKR and QBER for A1-B1

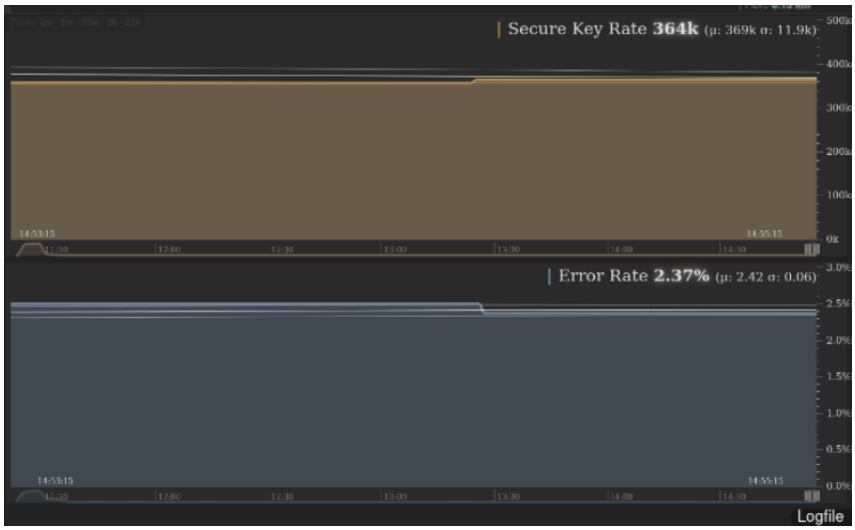

Figure 23: SKR and QBER for A2-B2

After conducting the experiment for a duration of approximately 4 hours, it can be inferred that the counter propagation configuration had negligible effects on the Secret Key Rate (SKR) and Quantum Bit Error Rate (QBER) of both QKD systems. The results depicted in Figures 24, 25, which correspond to Alice1 and Bob1, demonstrate that the SKR exhibited an upward trend over time while maintaining a consistent QBER. This indicates that the counter propagation arrangement did not significantly impact the performance of the systems. The same results apply for the other pair of Toshiba transceivers Alice2 and Bob2 with the difference that the QBER of the second pair is lower and hence the SKR is

greater. The difference between them is a common observation we have made, even when both pairs are connected back to back without any modification or interference between them. This can be explained, if we assume that the machines have slightly different settings and characteristics by its manufacturer.

Below the condition of the communication is shown after several hours.

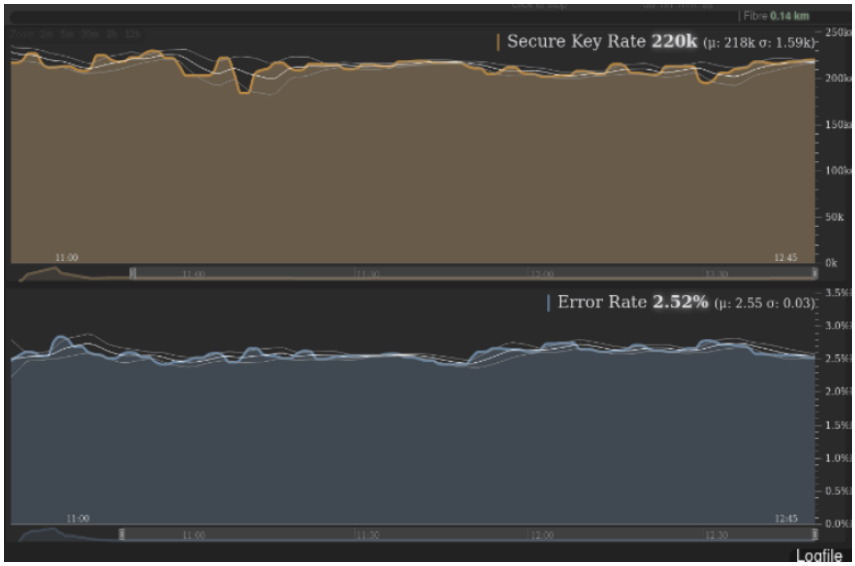

Figure 24: SKR and QBER for A1-B1 after 2 hours

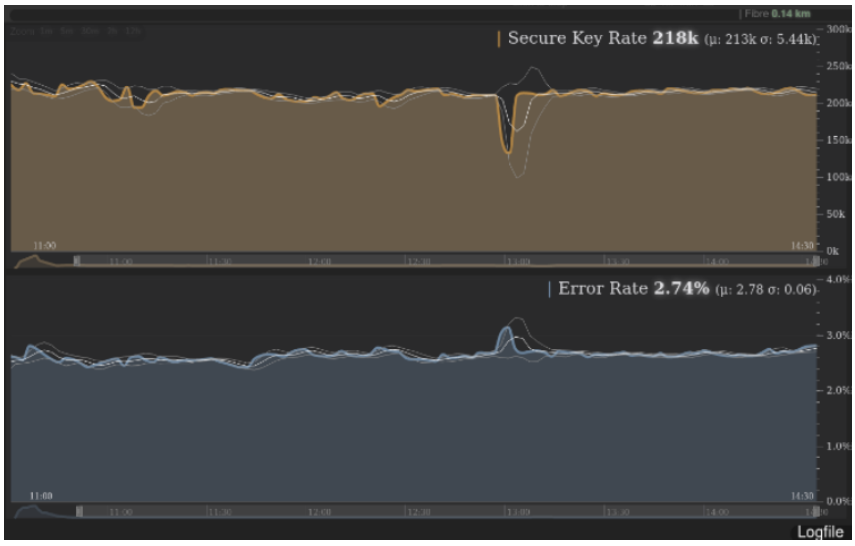

Figure 25: SKR and QBER for A1-B1 after 4 hours

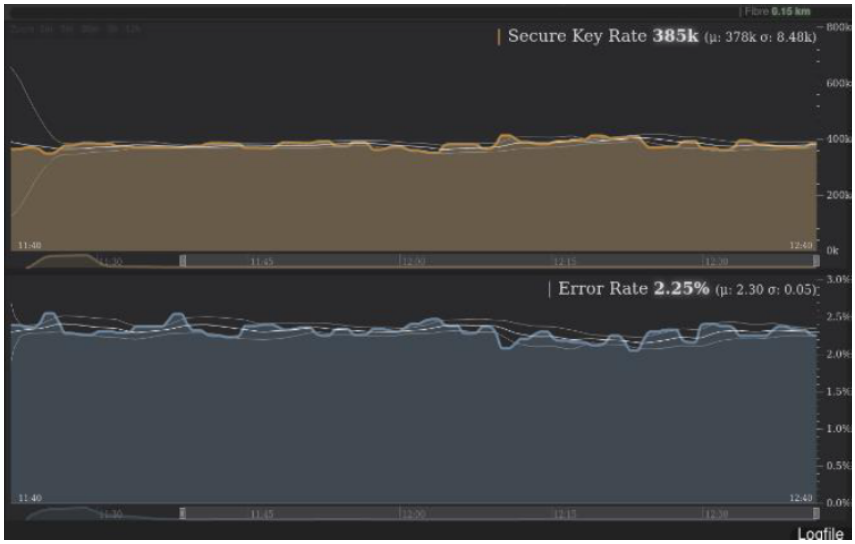

Figure 26: SKR and QBER for A2-B2 after 1 hour

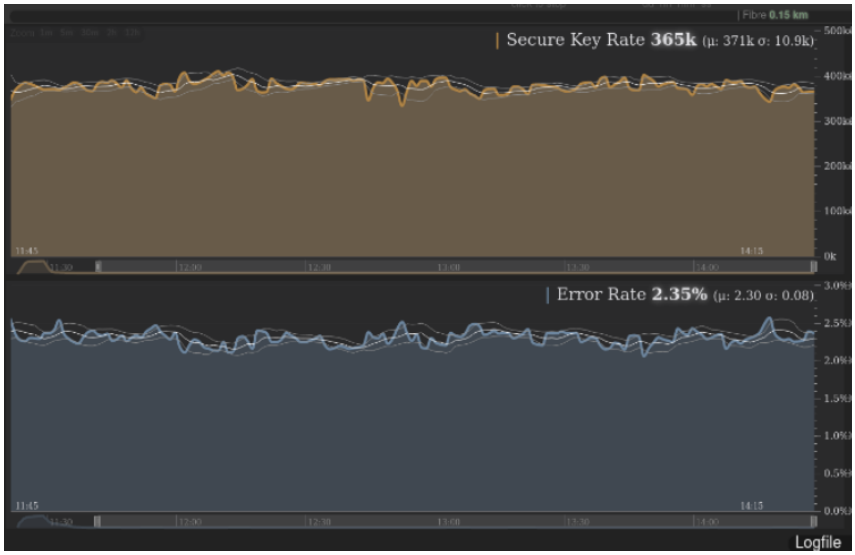

Figure 27: SKR and QBER for A2-B2 after 3 hours

We can also detect some fluctuations that occur over time which are a result originating from reflections and generally noise from the channels.

5.3 Investigation of Counter-Propagating Interactions with Classical channels Coexistence

In the second phase of our experiment, we aimed to investigate the impact of coexistence between quantum and classical channels on the performance of the QKD systems that are already put in counter-propagate positions. To achieve this, we introduced co-propagating classical optical channels gradually into the first coupler, alongside the existing classical and quantum channels of Alice1 and Bob1. This setup is illustrated below. The classical channels were multiplexed using a 1:4 coupler.

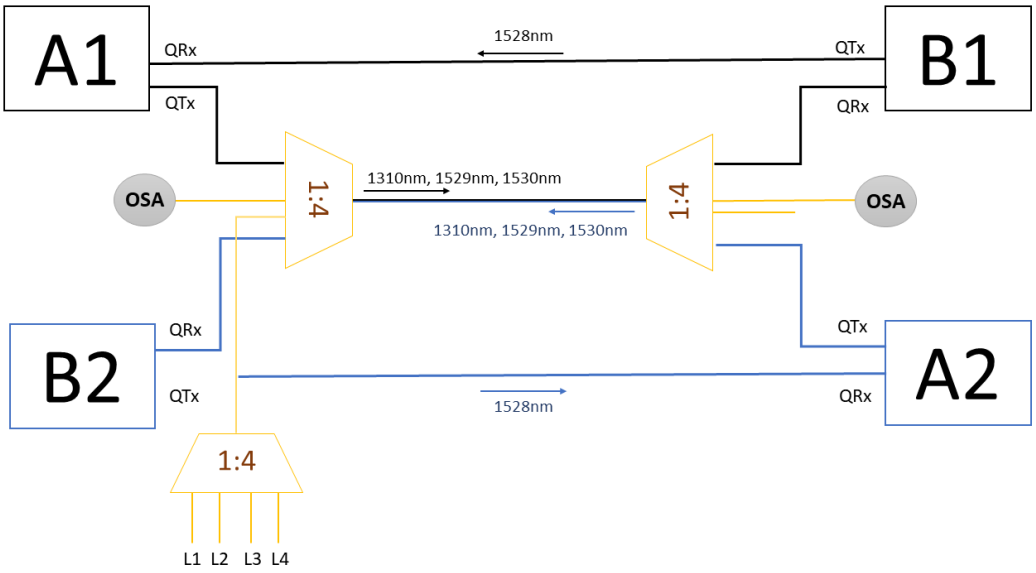

Figure 28: Experimental Testbed for two QKD setups with counter propagation and co-existence of CW lasers

The testing of coexistence was conducted in multiple stages, with each stage involving the addition of one or two classical channels. The specific details of each stage, including the number of channels added, are presented in the table below. By incrementally introducing the classical channels, we sought to observe and analyze the effects of coexistence on the QKD systems.

A1 – B1 Metrics with Coexistence of CW Lasers				
Wavelength (nm)	**First Stage**	**Second stage**	**Third Stage**	**Fourth Stage**
1547	OFF	OFF	OFF	ON
1549	OFF	ON	ON	ON
1550	OFF	OFF	ON	ON
1550.6	OFF	OFF	ON	ON
1552	OFF	ON	ON	ON
SKR (bps)	222k	120k	61k	0
QBER	2.72%	4.31%	6.38%	9.98%

Table 2: Lasers activation stages

Wavelength *(nm)*	**Multiplexed Signal Power** *(dBm)*
1547	*-8*
1549	*-10*
1550	*-10*
1550.6	*-12.6*
1552	*-12*

Table 3: Lasers power in dBm measured after passing an 1:4 coupler

As it can be observed in the table at the second stage two Lasers with wavelengths 1549 nm and 1552 nm are activated. After letting the graphic interface to refresh the statistics we see significant drop of the secure key rate and a significant increase of the QBER.

The same behavior is observed at stage 3 where two more lasers of wavelength 1549 nm and 1550.6 nm are activated. Although there is a major decrease of the secure rate along with an increase of the QBER, the QBER is 6,38% which is below the maximum permissible limit that lies above 7%

However, at the fifth stage where one more laser with wavelength 1547 in activated the QBER increases rapidly and reaches 9.96% , consequently SKR drops to zero and successful communication of the Toshiba machines is present no more.

Below the procedure including stages 2,3 and 4 with the co-propagating of lasers is presented thought the statistics of the graphical interface of B1.

Figure 29: Difference Between stage 2 and 3

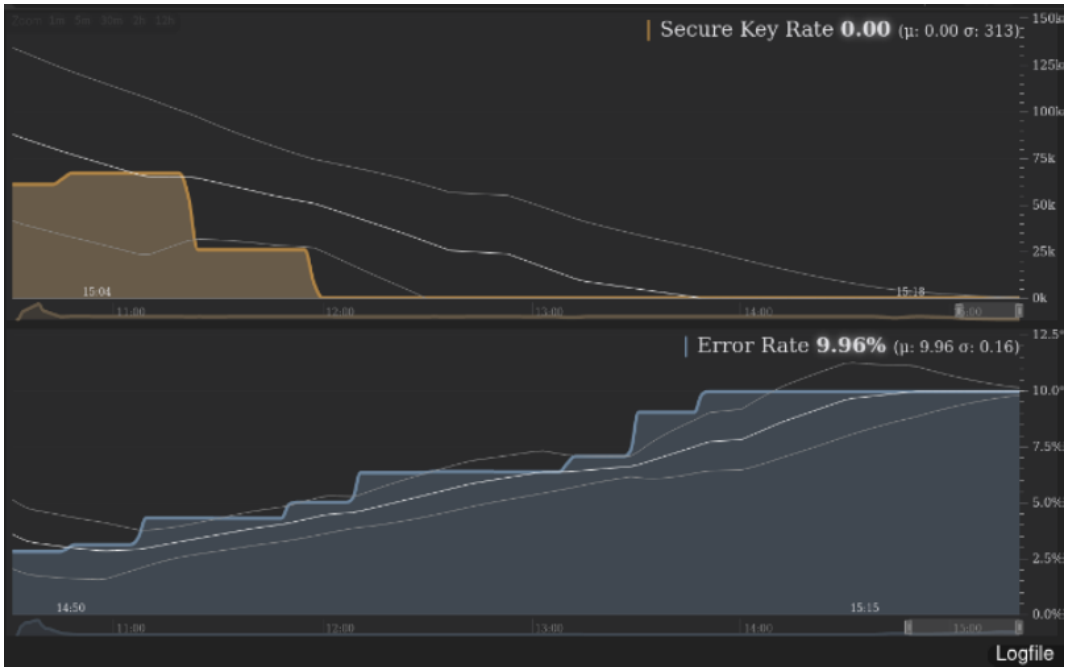

Figure 30: Stage 4

In order to fully understand how the additional classical channels affect the communication between the nodes, there should be an examination of the noise generated by the classical channels at the spectrum where the quantum channel lies. By utilizing an (OSA) on B1-A2 side we analyze the power levels and the results are shown below.

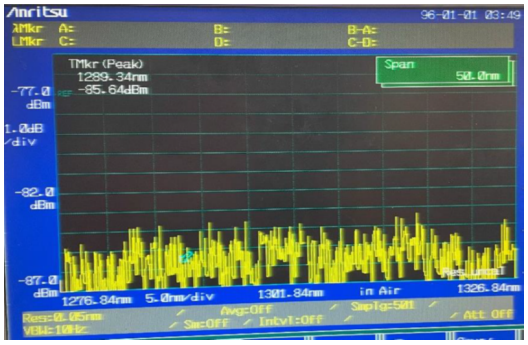

Figure 31: The optical spectrum between 1276 nm – 1326 nm, before the insertion of the classical channels

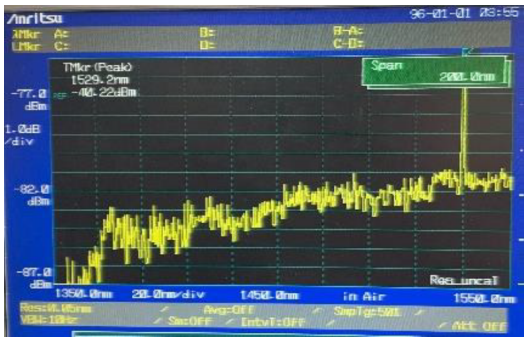

Figure 32: The optical spectrum between 1350 nm - 1550 nm, before the insertion of the classical channels

As we observe in 31 the power of the signals in the spectrum which lies on the region where the quantum channel operates is relatively low. The reason we are not able to detect the quantum channel is that is it much weaker than relative level of the noise. Typically one single photon around 1310 nm can have power lower that 100dbm. Toshiba's manual is not clear about that power. It states that the power of the quantum channel is less than 10nW which corresponds to -50dbm transmission power which clearly is not the case even if we take into account the losses that occur in the layout (10dbm attenuator attached on the Alice Tx and 12dbm losses from the two 1:4 couplers add up to a total of 72dbm loss). In

32, 33 we can observe the classical channels (1528 nm,1529 nm,1530 nm) that are used for the synchronisation of Alice and Bob.

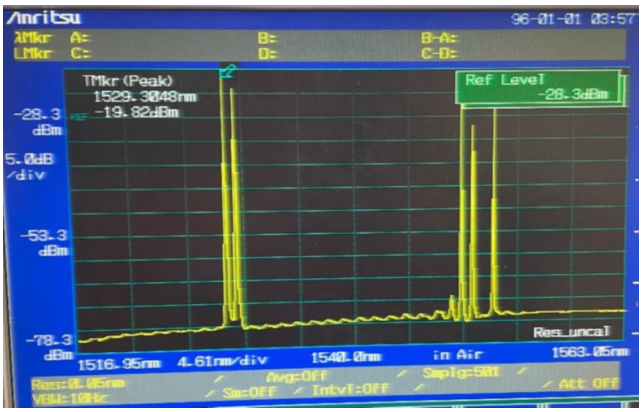

Figure 33: The optical spectrum between 1516 nm – 1563 nm with the three CW classical channels and the three service channels

On the following figures 34,35, 36, 37, we see the how the classical signals generated by the CW lasers affect the noise level of the spectrum. As expected noise levels increased and as shown before that results in higher QBER and lower SKR.

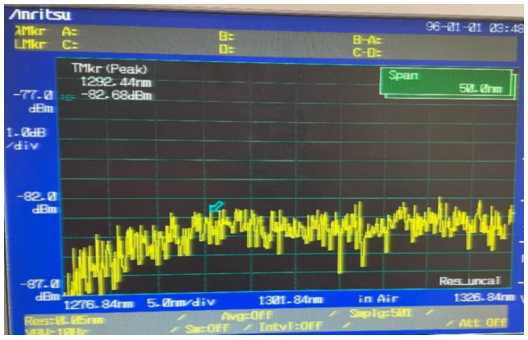

Figure 34: The optical spectrum between 1276 nm – 1326 nm, with three classical optical channels

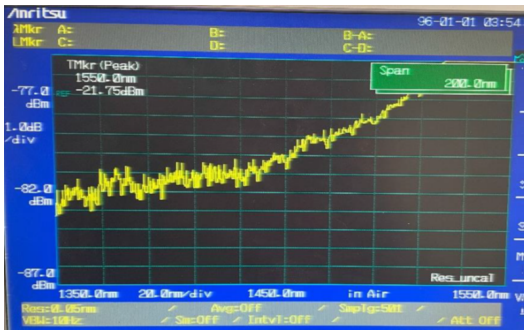

Figure 35: The optical spectrum between 1350 nm - 1550 nm, with three classical optical channels

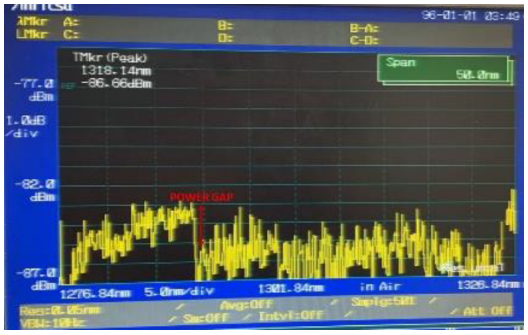

Figure 36: The power gap in the optical spectrum between 1276 nm – 1326 nm

Figure 37: The power gap in the optical spectrum between 1350 nm – 1550 nm

5.4 Investigation of Counter-Propagating Interactions with Classical channels Coexistence over longer distance

Following the successful experiment involving two counterpropagate quantum channels and 4 Cw lasers coexisting with them, we extended the setup by incorporating additional fiber. Specifically, the two counterpropagate quantum channels were transmitted over a shared fiber spanning a total distance of 19.914 km, divided into segments of 13.500 km and 6.414 km. The losses incurred in these segments were measured to be 2.65 dB and 1.12 dB, respectively. The experimental setup is depicted in 38.

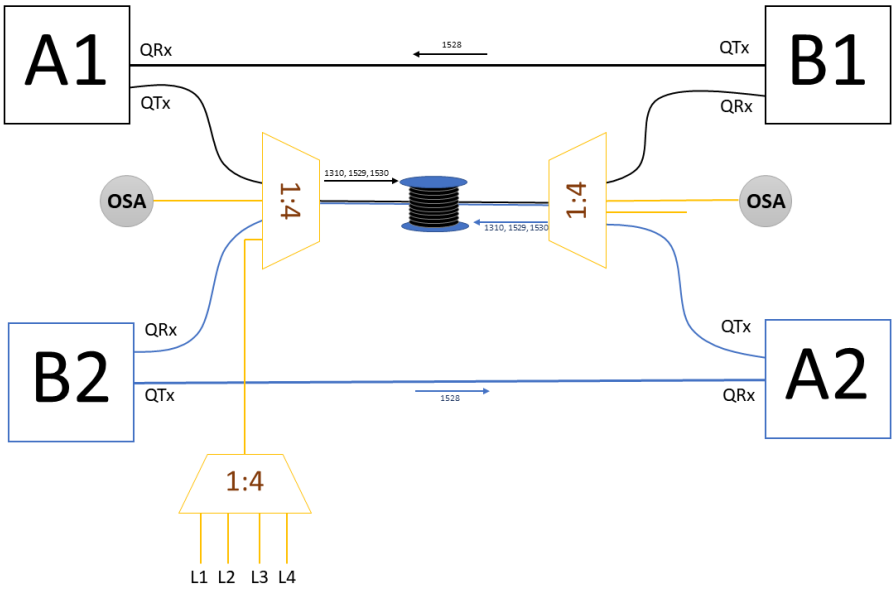

Figure 38: Experimental Testbed for two QKD setups with counter propagation and co-existence of CW lasers over longer distance

In this implementation, we aimed to gain a deeper understanding of the limitations of the setup by pushing the system to the limit. The total losses from the setup are:

1) 2 x FC/PC - > FC/APC (- 2dBm)

2) 2 x 1:4 splitter/coupler (- 12dBm)

3) 13.500 km optical fiber (- 2.65dBm)

4) 6.414 km optical fiber (- 1.12dBm)

Adding up to a total of 17.77 dBm. In fact the calculated losses were even more than expected (mainly due to connectors existing in the setup).Specifically the losses for the pair A1-B1 were 20dBm and for the A2-B2 pair were 25dBm.

Due to the significant losses within the setup the communication could not even be initialized and therefore no generation of key occurred.

After the unsuccessful try we removed the 6.414km of fiber in order to decrease the losses of the system and repeated the experiment. So, the total losses of the setup are:

1) 2 x FC/PC - > FC/APC (- 2dBm)

2) 2 x 1:4 splitter/coupler (- 12dBm)

3) 13.500 km optical fiber (- 2.65dBm)

Adding up to a total of 16.65 dBm.

In this try only one of the two QKD pairs (A2-B2) successfully managed to initialize while the other remained inactive.

5.5 Conclusion

In this experiment, we successfully demonstrated the communication of two counter-propagating QKD pairs in our laboratory environment. The Toshiba machines generated a highly satisfying SKR and QBER for key generation. Additionally, we investigated the coexistence scenario where four CW lasers co-propagated in the same fiber to simulate classical channels. The wavelengths of the CW lasers ranged from 1547 nm to 1552 nm, and their multiplexed power ranged from -12 dBm to -8 dBm.

As expected, activating additional CW lasers resulted in decreased SKR and increased QBER. The communication between the machines ceased when a fifth CW laser was introduced. Furthermore, we examined the system's capability to maintain communication over longer distances by adding kilometers of optical fiber. When nearly 20 km of fiber was added, the machines were unable to initialize communication. Conversely, with approximately 13 km of fiber, only one pair managed to initialize and generate a key, albeit with a low SKR and high QBER due to the anticipated high losses.

6 QKD over GPON replica at OTE Academy

After conducting the experiments at the lab are second part of the experiment is our try to integrate the QKD system over an existing, carrier grade optical access network for Fiber to the Home (FTTH) using an exact replica of the components and setups employed in real life by the telecom operator COSMOTE. The experiments have been conducted in Cosmote Academy premises over an emulated GPON configuration and demonstrated that QKD transmission is feasible over a GPON setup.

6.1 Description of Cosmote PON system

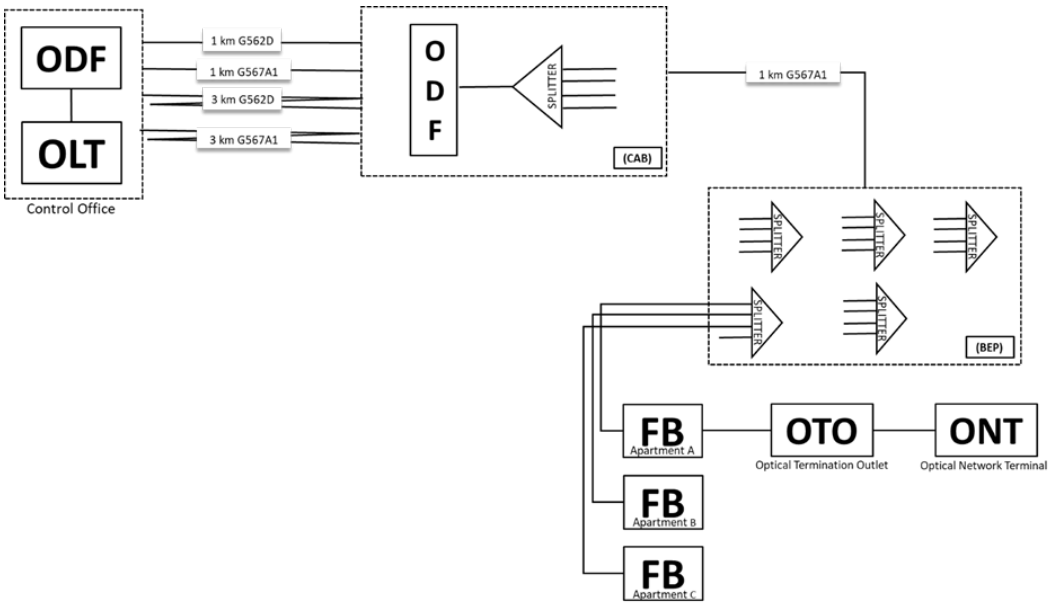

Figure 39: PON in OTE Academy The setup was implemented by COSMOTE to emulate a "real world" GPON network. In this sense, the setup employs a 3km fiber to emulate the average links expected between the Central Office and the first splitting cabin. The fiber used in the experiment is G657A1 but in real deployments G652 may also be used. The second stage comprises another 1km link that links to the FTTH premises and the floor boards. Again a G652 fiber specification is used.

Splitters can be positioned at two different locations within an access network. The initial placement is at the CABINET (CAB), typically found on the street, which offers great flexibility in FTTH networks. In addition to serving as splitting points, these cabinets can also be utilized for splicing and patching optical cable fibers. The second placement is at the Building Entry Point (BEP) Splitters that Cosmote use in their PON:

- For "CAB": 1:4, 1:8, 1:16, 1:32
- For "BEP": 1:2, 1:8

In Cosmote's real PON, the connection to end-users is usually 1:32, but recently for the coverage of large connections with FTTH, the ratio became 1:64, so splitters are combined as follows:

- 1:4 or 1:8 (CAB) & 1:8 (BEP)
- 1:16 or 1:32 (CAB) & 1:2 (BEP)

to achieve the numbers 32 & 64.

By following ITU guidelines, the initial high power transmission of upstream and downstream signals from the ONT and OLT enhances the signal quality, improves link performance, and minimizes the impact of losses and impairments during signal propagation. According to ITU-T G.984.2 (Recommendation ITU-T G.984.2) the transmit and receive classes of ONTs & ONUs are as follow:

Items	Single fibre
OLT	
Mean launched power MIN	+1.5 dBm
Mean launched power MAX	+5 dBm
Minimum sensitivity	−28 dBm
Minimum overload	−8 dBm
Downstream optical penalty	0.5 dB
ONU	
Mean launched power MIN	+0.5 dBm
Mean launched power MAX	+5 dBm
Minimum sensitivity	−27 dBm
Minimum overload	−8 dBm
Upstream optical penalty	0.5 dB

Figure 40: Class B+ Optical power levels for the 2.4 Gbit/s downstream, 1.2 Gbit/s upstream

Items	Single fibre
OLT	
Mean launched power MIN	+3 dBm
Mean launched power MAX	+7 dBm
Downstream optical penalty	1 dB
Minimum sensitivity	−32 dBm
Minimum overload	−12 dBm
ONU	
Mean launched power MIN	+0.5 dBm
Mean launched power MAX	+5 dBm
Upstream optical penalty	0.5 dB
Minimum sensitivity	−30 dBm
Minimum overload	−8 dBm

Figure 41: Class C+ Optical power levels for the 2.488 Gbit/s downstream, 1.244 Gbit/s upstream

6.2 Reflections measurements before experiment

GPON technology relies on the wavelengths 1310nm and 1490nm for user upload and download, respectively.Toshiba QKD systems (QKD4.2-MU/MB), which we use for Quantum Key Distribution (QKD), use the 1310nm wavelength for the quantum channel as well. We normally expect to be restricted by Raman noise even if two channels differ by 60 nm. Since the quantum channel falls exactly on the upstream connection of Cosmote the effect of Raman scattering should be severe enough to prevent the QKD endpoints two communicate. For these reasons we measure the reflections coming from the ONT and the minimum power the ONTs can work with.

In order to make the measurements needed we are going to use an Optical Time Domain Reflectometer (OTDR). An OTDR is a specialized instrument used in fiber optic network testing and troubleshooting. An OTDR is designed to analyze the performance and characteristics of optical fibers by sending short pulses of light into the fiber and measuring the reflections and scattering that occur along its length. For this experiment we are going to enable the setup with the minimum loss. To make that happen we use 1:4 (CAB) & 1:2 (BEP) splitters.

The reflections measured by the OTDR have the following power:

- At 1310nm -47.2 dBm
- At 1550nm -52.7 dBm

The results of the OTDR are shown below

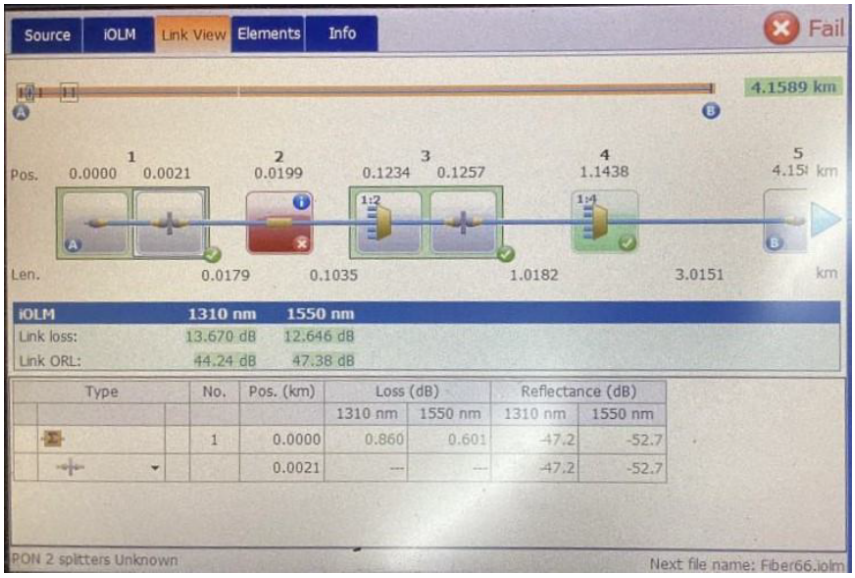

Figure 42: Representation of the connection in the direction ONT- >CO.

ONT measured Tx: 0dBm transmit power, so we conclude its class is B+. The losses of the link at 1310nm are 13.670dB. To study the signal transmitted by our ONT more closely, we connected a 1:2 splitter to the ONT. Without disrupting its communication with the CO (simply adding 3db loss), we were able to also measure the signal at 1310nm. The topology is shown below.

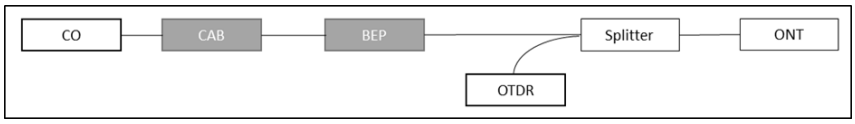

Figure 43: Topology of using OTDR to measure 1310nm Upload Channels of Cosmote ONTs.

By testing available ONTs (3 different ONTs), we found out that the signal wavelength varies between machines but stays close to 1310nm. This is a encouraging fact since the QKD quantum channel is at exactly 1310.00 nm. If the QKD pairs have a very narrow filter as we suppose then the communication between Alice and Bob in possible.

After measuring the 3ONTs we have the following results:

- ONT1: λ = 1316,199nm, P= -6,6dBm
- ONT2: λ = 1312,390nm, P= -7,64dBm
- ONT3: λ = 1315,997nm, P= -5,42dBm

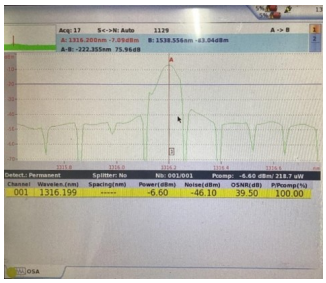

Figure 44: ONT1

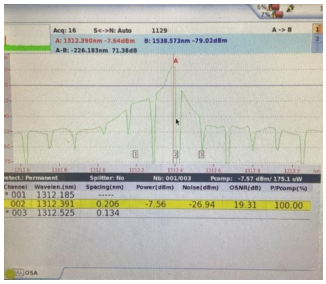

Figure 45: ONT2

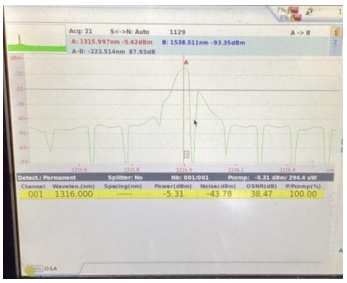

Figure 46: ONT3

6.3 Back reflections measurements before experiment

By reversing the orientation of our splitter and converting it into a coupler, with one side connected to both the ONT and the OTDR while the other side is connected to the network, we will be able to measure the back reflections.

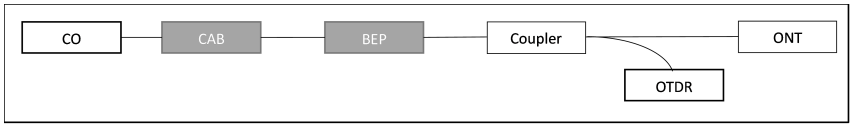

Figure 47: Topology of using OTDR to measure 1310nm Upload Channels reflections.

At the same time we will investigate the minimum transmitted power that ONTs can work with. To do this we will change the setup in various stages while measuring the reflections. This way we will test how resilient the connection is to noise and figure out the sensitivity of the machines by adding attenuators in ONT's connection.

Using an ONT with a power of 0dBm transmitting to the network, we receive as its reflections:

- λ = 1316,096nm, P= -55,75dBm

Test 1:
Losses:

- Link Loss: 13,6 dBm
- 1:2 Splitter: 3 dBm
- Attenuator : 13 dBm
- Total Loss: 29,6 dBm

Reflections:

- λ = 1316,244 nm, P = -67.65 dBm

Using the above losses the ONT is working.
Test 2: Losses:

- Link Loss: 13,6 dBm

- 1:2 Splitter: 3 dBm
- Attenuator 1 : 13 dBm
- Attenuator 2 : 5 dBm
- Total Loss: 34.6 dBm

Reflections:

- λ = 1316,188 nm, P = -74.37 dBm

Using the above losses the ONT is working.

Test 3:

For the third test we change the connection again and bring it closer to the real world by using 1:4 (CAB) & 1:8 (BEP) splitters. As a result, the total link loss increases to 20dB. Losses:

- Link Loss: 20 dBm
- 1:2 Splitter: 3 dBm
- Attenuator 1 : 13 dBm
- Attenuator 2 : 5 dBm
- Total Loss: 41 dBm

Reflections:

- λ = 1316,263 nm, P = -75.75 dBm

Using the above losses the ONT is working.

Test 4:

For the fourth test we removed the two attenuators with total loss of 18 dBm.
Losses:

- Link Loss: 20 dBm
- 1:2 Splitter: 3 dBm
- Total Loss: 23 dBm

Reflections:

- λ = 1316,263 nm, P = -50,75 dBm

Using the above losses the ONT is working. With these results we conclude that the ONT can hold communication even with 41 dBm attenuation. This fact is encouraging because in this case we measured back reflections of the order of -75 dBm , making the conclusion that these reflections may not be an immediate limiting factor.

6.4 QKD deployment in GPON

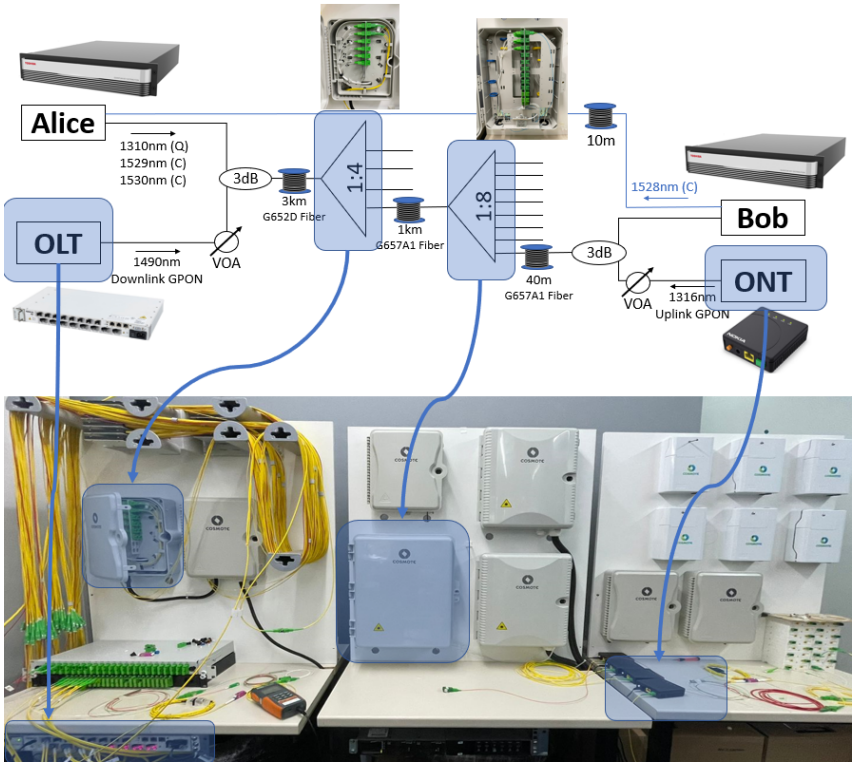

Figure 48: The GPON replica with all the components included

As shown in 48, the Toshiba QKD4.2A-MB (Alice) and QKD4.2B-MB (Bob) were deployed to establish communication over the GPON simulation. This experiment includes various stages and tests to determine whether it is possible for QKD to establish and maintain communication while the OLT is functioning normally and communicating with multiple ONTs that replicate the services provided to clients. The network topology is explained below. Transmitter's (Alice) quantum channel along with the two service channels are sent into the GPON network coupled with the OLT's downstream channel. Then these signals propagate through a 3km G652D fiber. This distance simulates the real distance between the CO (Central office) and the CAB (Cabinet). The signals are then split with a 1:4 splitter and continue propagation through a 1km G652D fiber which represents the physical distance between the CAB and the BEP (Building Entry Point). At the BEP the signals are split again with a 1:4 splitter and after propagating for another 40 meters they are again split with a 1:2 splitter (which is in fact a coupler if shown from the opposite direction) in order for the coupled signals to reach the ONT and quantum receiver. Another essential component is the Variable Optical Attenuator (VOA) with one located after the ONT and before the 1:2 coupler and another after the OLT. Their purpose is to attenuate the classical upstream and downstream channel respectively, reducing the backreflections generated at the couplers. However VOAs make challenging the communication between the OLT and the ONT , for this reason the experiment involves the procedure of fine tuning the attenuation of the VOAs. Finally, as regards topology the Tranmitter's (Alice) Rx is connected back to back with a 10 meters fiber cable to the Receiver's (Bob) Tx. In this cable the third

service channel with direction from Bob to Alice propagates// The primary objective of the experiment is to establish and sustain communication between Alice and Bob, as well as between the OLT and the ONT, while ensuring that the operational requirements of the QKD pair do not interfere with the classical communication over the GPON. The subsequent and more crucial goal is to maximize the utilization of the functioning ONTs connected at the available splitter ports, demonstrating that communication between Alice and Bob remains viable while simultaneously providing services to a typical number of clients under normal circumstances.

For every stage there will be a brief description of the topology and the SKR and QBER of the QKD nodes will be shown.

1) **First Stage**

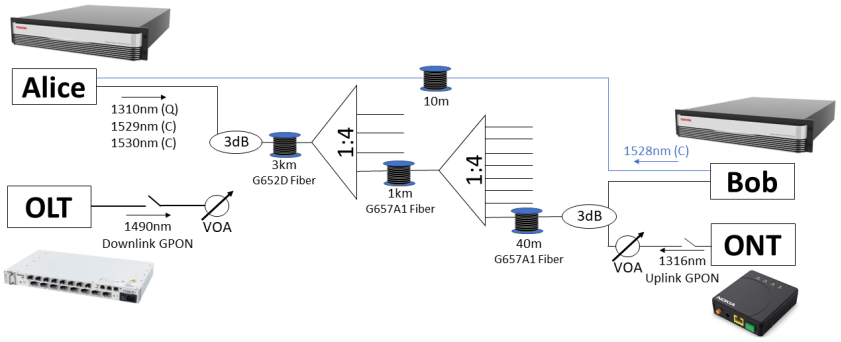

Figure 49: Initial topology with no OLT or ONTs enabled

In the initial stage, the OLT is not enabled, resulting in the absence of functioning ONTs. Therefore, we conducted a communication test between Alice and Bob by placing them 4km apart and allowing the signal to pass through two 1:4 splitters.

After ensuring the system work we continue to stages 2 and 3 where we enable the ONTs. Is it important to note that these ONTs are connected on the 1:4 BEP splitter where also BOB is connected.

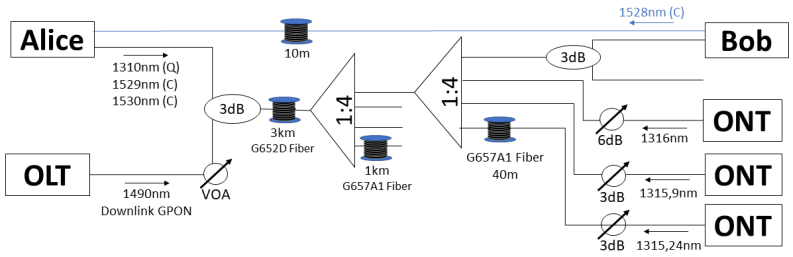

Figure 50: Topology after enabling the OLT and ONTs

2) **Second Stage** In the second stage the OLT is enabled and two ONTs are put into operation but none of them coupled with the QKD receiver (Bob). After the ONT with wavelength 1316 nm there is a 6db VOA and after the one with wavelength 1315,9 nm a 3db VOA in order to decrease the noise generated by reflections in the splitter.

3) **Third Stage** In the third stage one more ONT with wavelength 1315,2 nm along with a 3db is put in the network connected on the BEP splitter as well, so in total there are 3 ONTs operating.

4) **Fourth Stage**

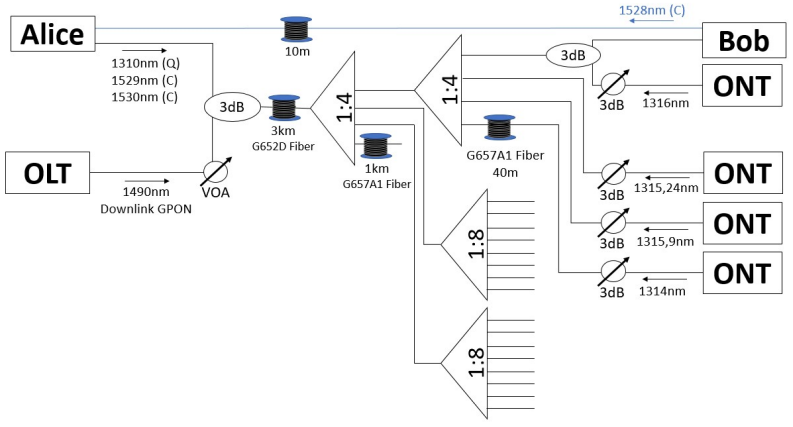

Figure 51: Final topology with 4 ONTs enabled

In the fourth stage, the ONT operating at a wavelength of 1316 nm is placed at the same node as BOB, as it operates at a wavelength farther from the quantum channel's 1310.00 nm. Additionally, another ONT operating at 1314 nm is enabled, equipped with 3 dB VOA. Thus, there are a total of four operational ONTs, each accompanied by a 3 dB VOA. One of the ONTs (1316 nm) is coupled to Bob.

The results of stages 1-4 are shown below in 52

Metrics with Coexistence in COSMOTE GPON replica				
ONT Wavelength (nm)	**First Stage**	**Second stage**	**Third Stage**	**Fourth Stage**
1316	OFF	ON	ON	ON
1315,9	OFF	ON	ON	ON
1315,2	OFF	OFF	ON	ON
1314	OFF	OFF	OFF	ON
SKR (bps)	21k	11k	9k	6k
QBER	3.29%	5,18%	5.66%	6.15%

Figure 52: GPON experiment results

All above ONTs where connected to the BEP splitter as shown in 51 The additional splitters shown are for future experiment purposes. As said before the long term goal is to put as many ONTs is possible in order to reach the number COSMOTE normally use which is 32 or 64. We believe that the additional ONT will not make the communication of Alice and Bob impossible since the will be connected to the splitter located at the CAB. This will result in satisfying attenuation of the backreflections and therefore ensuring the systems functionality.

5) **Stage 5**

To experimentally validate our hypothesis, we introduced an additional set of 5 ONTs, despite not having ONTs with transmission signals separated by at least 5 nm from the quantum signal. These newly added ONTs were configured with wavelengths varying from 1314 nm to 1315.2 nm.

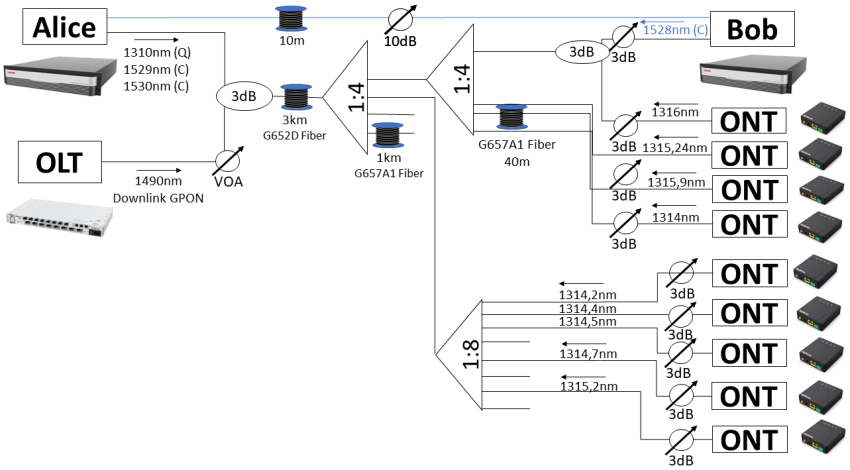

Figure 53: Topology after enabling a total of 9 ONTs

After taking the results from the QKD receiver BOB we observed that our hypothesis was indeed validated. In fact the additional ONTs at the CAB splitter not only did not have adverse impact on the measurements, but it actually resulted in improved outcomes. This fact could be explained due to the power budget available. In the

context of the power transmitted by ONTs and received by the OLT, the power budget is relevant in determining the maximum permissible power levels for both transmission and reception. The OLT sets the power budget for downstream transmission towards the ONTs, specifying the acceptable power range for the received signals. The ONTs, in turn, need to transmit their signals within this acceptable power range to ensure reliable communication.

If more ONTs are added to the network, the total power available for downstream transmission from the OLT remains constant. Therefore, the power allocated to each individual ONT decreases as the number of ONTs increases. This can result in a decrease in the power transmitted by each ONT, as they need to adhere to the power budget set by the OLT.

So the fact that ONTs' reflections at CAb splitter does not affect the quantum channel due to high attenuation in combination with the fact that the ONTs' powers are decreased with the presence of more ONTs -and more significantly the power of the ONT coupled with BOB - have as a result improved outcomes as shown below.

Metrics with Coexistence in COSMOTE GPON replica	
Fifth Stage	
SKR (bps)	15k
QBER	4.38%

Figure 54: GPON experiment results at fifth stage

We let the system work in this final topology (with 9 working ONTs) for almost three days in order to gather reliable data for the SKR and the QBER and the results are shown below.

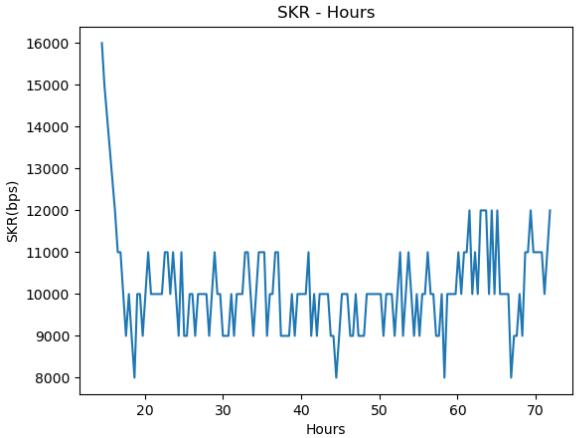

Figure 55: Secure Key Rate of stage 5 with 9 ONTs over 3 days

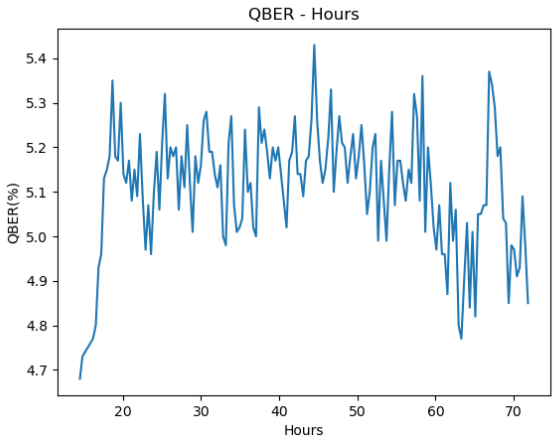

Figure 56: QBER of stage 5 with 9 ONTs over 3 days

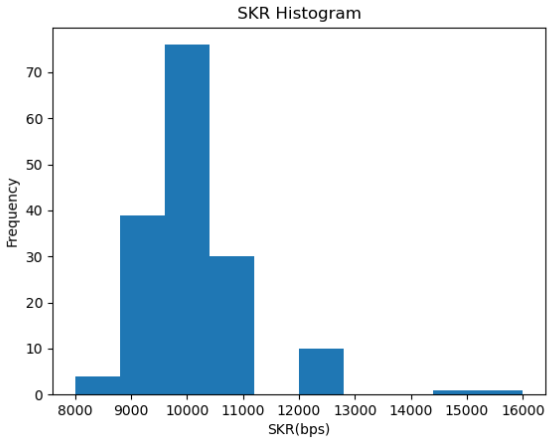

Figure 57: Secure Key Rate of stage 5 with 9 ONTs over 3 days

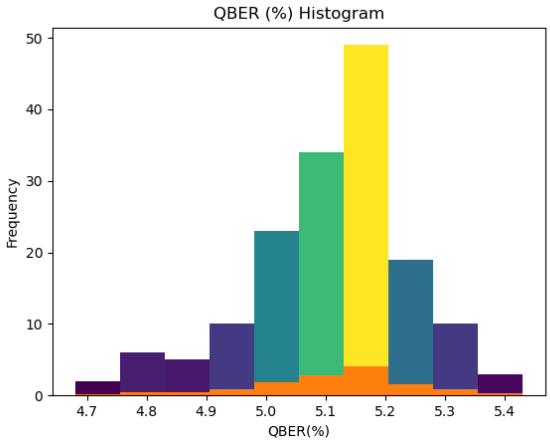

Figure 58: QBER of stage 5 with 9 ONTs over 3 days

We observe that both SKR and QBER have not large variations throughout the days.

We also observe from the histogram that both the SKR and QBER follow a Poisson distribution.

In addition to the previous observations, it is essential to consider the contextual information regarding the experiment. Specifically, throughout the experiment, three connected routers were utilized on the Optical Network Terminals (ONTs) to provide users with a normal internet connection, delivering speeds exceeding 300 Mbps.

6) **Stage 6**

In order to explore the limitations of QKD communication, we introduced three additional ONTs at the CAB splitter in the final stage of the experiment. These ONTs transmitted at wavelengths 1312.4 nm, 1312.5 nm, and 1312.8 nm. As anticipated, the close proximity of these wavelengths to the quantum channel at 1310 nm resulted in the disruption of communication between Alice and Bob. This outcome aligns with our expectations and further highlights the sensitivity of QKD systems to wavelength variations in the optical network.

7 Conclusion

The successful experiment of achieving communication between Alice and Bob (quantum machines) within a GPON network, along with the deployment of four working ONTs, including one coupled with Bob, holds significant implications for secure communications. By integrating Quantum Key Distribution (QKD) with classical channels, this experiment demonstrates the feasibility of establishing secure and encrypted communication channels over existing optical access networks. This achievement opens up avenues for enhanced security in various applications, such as secure data transmission, confidential communication between parties, and protection against eavesdropping. The coexistence of QKD with classical channels in a practical network setting provides a promising foundation for advancing secure communication technologies and fostering trust in modern information exchange systems.

References

[1] *Classical Theory of Rayleigh and Raman Scattering*, chapter 4, pages 49–84. John Wiley Sons, Ltd, 2002.

[2] Lewis A and Travagnin M. A secure quantum communications infrastructure for europe: Technical background for a policy vision. (KJ-NA-31133-EN-N (online)), 2022.

[3] Govind P. Agrawal. Preface. In Govind P. Agrawal, editor, *Applications of Nonlinear Fiber Optics (Second Edition)*, pages xiii–xiv. Academic Press, Burlington, second edition edition, 2008.

[4] Obada Alia, Rodrigo S. Tessinari, Sima Bahrani, Thomas D. Bradley, Hesham Sakr, Kerrianne Harrington, John Hayes, Yong Chen, Periklis Petropoulos, David Richardson, Francesco Poletti, George T. Kanellos, Reja Nejabati, and Dimitra Simeonidou. DV-QKD coexistence with 1.6 tbps classical channels over hollow core fibre. *Journal of Lightwave Technology*, 40(16), aug 2022.

[5] Ekin Arabul, Rodrigo Stange Tessinari, Obada Alia, Romerson Oliveira, George T. Kanellos, Reza Nejabati, and Dimitra Simeonidou. 100 gb/s dynamically programmable sdn-enabled hardware encryptor for optical networks. *Journal of Optical Communications and Networking*, 14(1), 2022.

[6] Osamu Aso, Masateru Tadakuma, and Shu Namiki. Four-wave mixing in optical fibers and its applications. *dEp*, 1(2), 1999.

[7] Alberto Carrasco-Casado, Veronica Marmol, and Natalia Denisenko. *Free-Space Quantum Key Distribution*, pages 589–607. 08 2016.

[8] J. F. Dynes, A. Wonfor, W. W.-S. Tam, A. W. Sharpe, R. Takahashi, M. Lucamarini, A. Plews, Z. L. Yuan, A. R. Dixon, J. Cho, Y. Tanizawa, J.-P. Elbers, H. Greißer, I. H. White, R. V. Penty, and A. J. Shields. Cambridge quantum network. *npj Quantum Information*, 5(1), Nov 2019.

[9] James Dynes, Winci Tam, Alan Plews, Bernd Fröhlich, Andrew Sharpe, Marco Lucamarini, Zhiliang Yuan, Christian Radig, Andrew Straw, Tim Edwards, and Andrew Shields. Ultra-high bandwidth quantum secured data transmission. *Scientific Reports*, 6, 10 2016.

[10] Veronica Fernandez, Robert J. Collins, Karen J. Gordon, Paul D. Townsend, and Gerald S. Buller. Passive optical network approach to gigahertz-clocked multiuser quantum key distribution. *IEEE Journal of Quantum Electronics*, 43(2):130–138, 2007.

[11] Bernd Fröhlich, James F. Dynes, Marco Lucamarini, Andrew W. Sharpe, Simon W.-B. Tam, Zhiliang Yuan, and Andrew J. Shields. Quantum secured gigabit optical access networks. *Scientific Reports*, 5(1):18121, Dec 2015.

[12] Laszlo Gyongyosi, Laszlo Bacsardi, and Sandor Imre. A survey on quantum key distribution. *Infocommunications journal*, 01 2019.

[13] Mart Haitjema. A survey of the prominent quantum key distribution protocols. 2007.

[14] W Heisenberg. The physical content of quantum kinematics and mechanics. In J A Wheeler and W H Zurek, editors, *Quantum Theory and Measurement*, volume 43, pages 172–198. Princeton University Press, Princeton, 1927.

[15] Refat Kibria and Michael W. Austin. All optical signal-processing techniques utilizing four wave mixing. *Photonics*, 2(1):200–213, 2015.

[16] M. Lucamarini, K. A. Patel, J. F. Dynes, B. Fröhlich, A. W. Sharpe, A. R. Dixon, Z. L. Yuan, R. V. Penty, and A. J. Shields. Efficient decoy-state quantum key distribution with quantified security. *Optics Express*, 21(21):24550, oct 2013.

[17] Jesus Martinez-Mateo, Alex Ciurana, and Vicente Martin. Quantum key distribution based on selective post-processing in passive optical networks. *IEEE Photonics Technology Letters*, 26(9):881–884, 2014.

[18] David McMahon. *Quantum Computing Explained.* 2007.

[19] Ali Ibnun Nurhadi and Nana Rachmana Syambas. Quantum key distribution (qkd) protocols: A survey. In *2018 4th International Conference on Wireless and Telematics (ICWT)*, pages 1–5, 2018.

[20] Sivarajan-K. N. Sasaki G. H. Ramaswami, R. *Optical Networks a practical perspective.* Elsevier/Morgan Kaufmann., 2010.

[21] Antonio Ruiz Alba Gaya, David Calvo Díaz-Aldagalán, Víctor García Muñoz, Alfonso Martínez García, Waldimar Alexander Amaya Ocampo, JUAN GUILLERMO ROZO CHICUE, José Mora Almerich, and José Capmany Francoy. Practical quantum key distribution based on the bb84 protocol. In *Waves*, volume 1, pages 4–14. Instituto de Telecomunicaciones y Aplicaciones Multimedia (iTEAM), 2011.

[22] Nina Skorin-Kapov, Marija Furdek, Szilard Zsigmond, and Lena Wosinska. Physical-layer security in evolving optical networks. *IEEE Communications Magazine*, 54(8):110–117, 2016.

[23] Wei Sun, Liu-Jun Wang, Xiang-Xiang Sun, Yingqiu Mao, Hua-Lei Yin, Bi-Xiao Wang, Teng-Yun Chen, and Jian-Wei Pan. Experimental integration of quantum key distribution and gigabit-capable passive optical network. *Journal of Applied Physics*, 123(4), 01 2018. 043105.

[24] Liu-Jun Wang, Kai-Heng Zou, Wei Sun, Yingqiu Mao, Yi-Xiao Zhu, Hua-Lei Yin, Qing Chen, Yong Zhao, Fan Zhang, Teng-Yun Chen, and Jian-Wei Pan. Long-distance copropagation of quantum key distribution and terabit classical optical data channels. *Phys. Rev. A*, 95:012301, Jan 2017.

[25] Rui Wang, Rodrigo S. Tessinari, Emilio Hugues-Salas, Anderson Bravalheri, Navdeep Uniyal, Abubakar S. Muqaddas, Rafael S. Guimaraes, Thierno Diallo, Shadi Moazzeni, Qibing Wang, George T. Kanellos, Reza Nejabati, and Dimitra Simeonidou. End-to-end

quantum secured inter-domain 5g service orchestration over dynamically switched flex-grid optical networks enabled by a q-roadm. *Journal of Lightwave Technology*, 38(1), 2020.

[26] Xiang-Bin Wang. Beating the photon-number-splitting attack in practical quantum cryptography. *Phys. Rev. Lett.*, 94:230503, Jun 2005.

[27] Yodai Watanabe. Privacy amplification for quantum key distribution. *Journal of Physics A: Mathematical and Theoretical*, 40(3):F99, dec 2006.