NATIONAL AND KAPODISTRIAN UNIVERSITY OF ATHENS

SCHOOL OF SCIENCES
DEPARTMENT OF INFORMATICS AND TELECOMMUNICATIONS

BSc THESIS

Evaluation of a switched - QKD network performance compared to a relayed - QKD network

Persefoni Ch. Konteli

Supervisor: **George T. Kanellos,** Assistant Professor

ATHENS

MAY 2024

ΕΘΝΙΚΟ ΚΑΙ ΚΑΠΟΔΙΣΤΡΙΑΚΟ ΠΑΝΕΠΙΣΤΗΜΙΟ ΑΘΗΝΩΝ

ΣΧΟΛΗ ΘΕΤΙΚΩΝ ΕΠΙΣΤΗΜΩΝ
ΤΜΗΜΑ ΠΛΗΡΟΦΟΡΙΚΗΣ ΚΑΙ ΤΗΛΕΠΙΚΟΙΝΩΝΙΩΝ

ΠΤΥΧΙΑΚΗ ΕΡΓΑΣΙΑ

Αξιολόγηση της απόδοσης ενός switched - QKD δικτύου σε σύγκριση με ένα relayed - QKD δίκτυο

Περσεφόνη Χ. Κοντέλη

Επιβλέπων: **Γεώργιος Τ. Κανέλλος,** Επίκουρος Καθηγητής

ΑΘΗΝΑ

ΜΑΪΟΣ 2024

BSc THESIS

Evaluation of a switched - QKD network performance compared to a relayed - QKD network

Persefoni Ch. Konteli

S.N.: 1115201900328

SUPERVISOR: **George T. Kanellos,** Assistant Professor

ΠΤΥΧΙΑΚΗ ΕΡΓΑΣΙΑ

Αξιολόγηση της απόδοσης ενός switched - QKD δικτύου σε σύγκριση με ένα relayed - QKD δίκτυο

Περσεφόνη Χ. Κοντέλη

Α.Μ.: 1115201900328

ΕΠΙΒΛΕΠΩΝ: Γεώργιος Τ. Κανέλλος, Επίκουρος Καθηγητής

ABSTRACT

Quantum Key Distribution has recently dominated the field of optical communications cryptography. This thesis analyzes Quantum Key Distribution and delves into the possibilities offered by the implementation of a Switched-QKD network by comparing it with a Relayed-QKD network. The introduction surveys the principles of quantum mechanics and the techniques applied to the implementation and study of quantum key distribution. Then two experimental structures of a Switched-QKD network and a Point-to-Point QKD network are presented, in order to analyze the possibilities offered by the Switched-QKD architecture in high-speed networks. Furthermore, a fully-managed, field-deployed, three-node Hybrid Relayed-QKD ring network with L1-OTNsec encryption is presented, integrating the KMS and the application layer. Finally, it concludes with a comparison of the two Switched-QKD and Relayed-QKD architectures, based on the use cases of each of them and the challenges that characterize them.

SUBJECT AREA: Quantum Key Distribution

KEYWORDS: Quantum Key Distribution, Switched - Quantum Key Distribution, Relayed - Quantum Key Distribution, BB84 Protocol

ΠΕΡΙΛΗΨΗ

Η Κβαντική Διανομή Κλειδιού τα τελευταία έχει κυριαρχήσει στον τομέα της κρυπτογραφίας των οπτικών επικοινωνιών. Η παρούσα πτυχιακή εργασία αναλύει την Κβαντική Διανομή Κλειδιών και εμβαθύνει στις δυνατότητες που προσφέρει η υλοποίηση ενός δικτύου Switched-QKD συγκρίνοντας το με ένα δίκτυο Relayed-QKD. Η εισαγωγή μελετάει τις αρχές της κβαντικής μηχανικής και τις τεχνικές που εφαρμόζονται για την υλοποίηση και την μελέτη της κβαντικής διανομής κλειδιών. Έπειτα παρουσιάζονται δύο πειραματικές δομές ενός δικτύου Switched-QKD και ενός δικτύου Point-to-Point QKD, ώστε να γίνει η ανάλυση των δυνατοτήτων που προσφέρει η αρχιτεκτονική Switched-QKD στα σύγχρονα δίκτυα. Επιπλέον, παρουσιάζεται ένα πλήρως διαχειριζόμενο δίκτυο δακτυλίου τριών κόμβων Hybrid Relayed-QKD με κρυπτογράφηση L1-OTNsec που ενσωματώνει το KMS και το επίπεδο εφαρμογής. Τέλος, καταλήγει σε μια σύγκριση των δύο αρχιτεκτονικών Switched-QKD και Relayed-QKD, βάση των περιπτώσεων που μπορεί να αξιοποιηθεί το καθένα από αυτά αλλά και τις προκλήσεις που τα χαρακτηρίζουν.

ΘΕΜΑΤΙΚΗ ΠΕΡΙΟΧΗ: Διανομή Κβαντικών Κλειδιών

ΛΕΞΕΙΣ ΚΛΕΙΔΙΑ: Διανομή Κβαντικών Κλειδιών, Switched - Διανομή Κβαντικών Κλειδιών, Relayed - Διανομή Κβαντικών Κλειδιών, Πρωτόκολλο BB84

ACKNOWLEDGEMENTS

I would like to express special thanks to my supervisor, Ass. Prof. Dr. George T. Kanellos, for his valuable guidance not only in the completion of this work but also throughout my studies. I am thankful to Phd Candidate Nikolas Makris and Post Doc. Konstantinos Tsimvrakidis for their advice and expertise. I am also grateful to my family and friends for their strong support and encouragement.

CONTENTS

LIST OF FIGURES

PREFACE

This thesis was conducted through my undergraduate studies. I studied the theory of Quantum Key Distribution technologies and compared the performance of a switched-QKD network with the one of a relayed-QKD network. We, also, demonstrated a fully managed field deployed three-node QKD relayed network in a ring configuration.
In coordination with my supervisor and the researchers, we carried out the experiment by using commercial phase-encoding QKD technologies for the switched architecture and commercial QKD devices that implement Coherent One-Way (COW) protocol for the relayed architecture. We analyzed the results with OriginLab software to evaluated the performance of the two networks.
The two experiments presented in this thesis were part of my undergraduate collaboration with the Optical Communications and Photonics Technology Laboratory at the National and Kapodistrian University of Athens and were both showcased at conferences. The first experiment was published in the 2024 Optical Fiber Communications Conference and Exhibition (OFC) under the title ”Relayed-QKD and switched-QKD networks performance comparison considering physical layer QKD limitations” [22]. The second was presented at the 2024 European Conference on Optical Communication (ECOC) with the title ”Field Demonstration of a Fully Managed, L1 Encrypted 3-Node Network with Hybrid Relayed-QKD and Centralized Symmetric Classical Key Management” [21].

1. INTRODUCTION

The cryptography methods of modern communication networks are essential to protect the privacy of two parties who have never interacted before, then to guarantee confidentiality by securing their communications against eavesdropping, as well as to protect the data that they exchange.
The increase demand in new methods of network security has raised by multiple factors. The excessive need for network services and the rise of Internet of Things (IoT) are leading to the exponential growth of internet connectivity, creating a more complex system of interconnected devices that strengthens the possible security breaches and vulnerabilities of the network. Furthermore the continuous progress in quantum computing threatens the classical methods of encryption due to its rapid development [17, 30].
Quantum cryptography was introduced to eliminate those threats and ensure the quantum safe communication between two parties. It applies the principles of quantum mechanics in order to transfer or store data, based on the fundamental laws of nature and physics that allow the two parties to communicate safely [12]. Various quantum cryptography protocols have been developed the last decades that utilize methods of quantum cryptography, such as the Quantum Key Distribution (QKD). QKD has prevailed as a method because it generates truly random private keys to encrypt and transport messages which are considered theoretically secure under the attacks of the emerging advances of quantum computing [26].

2. QUANTUM KEY DISTRIBUTION

Quantum Key Distribution (QKD) is a security technology that implements the principles of quantum mechanics to securely share cryptographic keys between two parties, Alice and Bob, offering a level of security that is considered unbreakable even by quantum computers. Unlike conventional cryptographic methods, which rely on the computational difficulty of certain mathematical problems, QKD uses the fundamental properties of quantum mechanics to detect any attempt at eavesdropping. When an eavesdropper tries to intercept the communication, their actions are detected as errors in the transmitted quantum states, exposing the intruder to the two parties [12, 26]. The security provided by QKD is robust against eavesdropping attacks, because it relies on the fundamental attributes of quantum mechanics.

2.1 Quantum Mechanics Principles

2.1.1 Quantum State

A quantum state describes the fundamental knowledge of a quantum system. It is represented by the complex function $\Psi(x,t)$, which depends on the coordinate x and on time, and is denoted as $|\Psi_N\rangle$. It expresses the particular values of attributes, such as charge, spin and phase, or a combination of them, of a quantum mechanical system, like a particle or an atom. Moreover, the quantum states hold information to predict the results of measurements conducted on the system. In classical information theory, the fundamental unit of information processing is the bit, which can acquire one of two possible states 0 or 1. [23] In parallel, this basic unit of information in quantum computing is called quantum bit or qubit and it can also be in one of the two states. These states are represented as $|0\rangle$ and $|1\rangle$, describing the spin of a particle as 'up' and 'down', respectively. A quantum state can be expressed in terms of a sum of basis states, revealing the complexity and unique properties that differentiate it from classical states.

2.1.2 Superposition

Superposition is another mathematical concept in quantum mechanics, extending the quantum state concept, describes that a qubit can exist in more than two states. We assume that a quantum state can be a linear superposition of the states $|0\rangle$ and $|1\rangle$, where the superposition state is

$$|\Psi\rangle = \alpha\,|0\rangle + \beta\,|1\rangle$$

where α and β are complex numbers [23].
In the case of BB84 protocol - which we are going to discuss thoroughly, the states can represent the polarization and can be expressed as:

$$|0\rangle = |H\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle) \tag{2.1}$$

$$|1\rangle = |V\rangle = \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle) \tag{2.2}$$

where $|0\rangle$ and $|1\rangle$ describe the qubit states and $|H\rangle$ and $|V\rangle$ are the horizontal and vertical polarizations. Quantum cryptography uses these features of superposition to endcode information different quantum states [23].

2.1.3 Basis

The detection of photons between the two parties in QKD is crucial for the proper functioning of the QKD protocols. Many of them use polarization-based schemes to encode information. More specifically, the bits of the secret key, that is created between Alice and Bob, are interpreted by individual photons in different polarization states [23]. The polarization of each photon can be expressed as right or left circular polarization, or a superposition of the two, and it refers to the orientation of the electric field associated with it.
The detection involves the measurement of the photons' polarization states, which leads to knowledge of the key. However, the measurement of the photon disturbs the quantum state, according to the collapse of the wavefunction, a fundamental principle of quantum theory. So even an eavesdropper cannot gain knowledge about the key without disturbing the system in such a way that Alice and Bob can detect it [11].
Furthermore, the different polarizations (linear and rectangular) used for encoding the photons result from Polarizing beam splitters (PBS) and waveplates. The incoming light is split by the PBS, while the waveplates change the the polarization states by introducing controlled phase differences. In this way, many different polarization states are generated by adjusting the angles of waveplates in conjunction with PBS. Figure 2.1 shows some of the different polarization states, which are randomly generated each time for the QKD protocols.

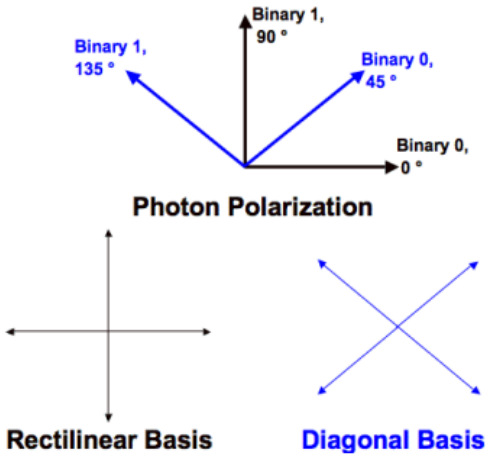


Figure 2.1: Basis and bit encoding [13]

2.1.4 The No-Cloning Theorem

The no-cloning theorem is one of the fundamental principles of quantum mechanics, proving that quantum mechanics do not allow to duplicate or copy an unknown quantum state. Considering two arbitrary quantum states, $|\Psi\rangle$ and $|\Phi\rangle$, the theorem can be mathematically expressed as:

$$|\Psi\rangle \otimes |\Phi\rangle \neq |\Psi\rangle \otimes |\Psi\rangle \tag{2.3}$$

This equation demonstrates that is impossible to make a perfect copy of an unknown quantum state, hence cloning it meets fundamental limitations. That theorem plays an important role in the implementation of the QKD protocols, as it ensures that an eavesdropper on the quantum line cannot copy the quantum states used to create the secret key for himself and then send the copies to Bob [23].

2.1.5 The Heisenberg Uncertainty Principle

The uncertainty principle can be and is mathematically expressed as:

$$\triangle A \triangle B \geq \frac{1}{2} |\langle [A, B] \rangle| \tag{2.4}$$

where the standard deviations of the observables A and B is denoted by $\triangle A$ and $\triangle B$, and [A, B] indicates the commutator of operators A and B. The equation above is a generalization of the famous Heisenberg uncertainty principle and expresses the limit in the accuracy that two incompatible observables can be measured at the sane moment [23].

2.1.6 Entanglement

Entanglement demonstrates another principle of quantum mechanics and it describes the phenomenon where particles or systems can become entangled. Generally, two systems A and B are entangled when the values of certain properties of the system A are correlated with the values that those properties will take in system B [23]. Quantum mechanics demonstrates that entanglement, a feature of non-locality, implies that measuring the properties of one particle will instantly determine the corresponding values that the properties of the other particle must take, suggested that the particles are so far away from each other that no signal can connect them over the time period when measurements are made. Considering a quantum state $|\psi\rangle$, the entanglement is the tensor product of the Alice and Bob basis states and can be mathematically described as:

$$|\Psi\rangle = \sum c_{ij} |\Psi_i\rangle \otimes |\Psi_j\rangle \tag{2.5}$$

where c_{ij} are complex coefficients and $|\Psi_i\rangle$ and $|\Psi_j\rangle$ represent the basis states of Alice and Bob.

2.1.7 Quantum Measurement

The quantum measurement results are expressed of a dynamical variable A using Hermitian operators and projection operators. The operator A can be stated as the terms of it's eigenvalues and corresponding projection operators and mathematically described as:

$$M_A = \sum_{a_i} |a_i\rangle \langle a_i| \tag{2.6}$$

where $|a_i\rangle$ and $\langle a_i|$ represents the eigenstates of observable A [23].

2.2 General methodology for QKD

In Figure 2.2, as shown, there are two authorized modules, Alice and Bob, that want to establish a secret key. To accomplice this, they are connected through two channels for the communication between them, the quantum and the classical channel. The combination of information from both channels is essential to ensure that the communication is secure from any attempted eavesdropping (Eve). The quantum channel is responsible for the of the photons, called quantum bits (qubits), for the creation of the secret key and is open to any third party for eavesdropping, while it guarantees security against such attempts due to the laws of quantum mechanics. On the other hand, the classical channel is used for the exchange of general information about the process of qubit transmission and for making decisions about the shared secret key. Nowadays there two types of mediums, that are used for the quantum channel, optical fiber and free space [28].

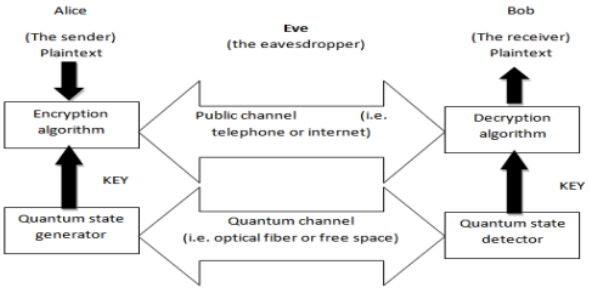


Figure 2.2: Basic Block Diagram of Quantum cryptographic communication system [29]

Furthermore, implementing the QKD protocols is a complex process, there are three distinct phases that are involved to establish the quantum-safe communication. As illustrated in Figure 2.3, these phases are the raw key exchange, the key sifting and the key distillation. It is necessary to discuss those procedures before presenting the QKD protocols, to gain a better understanding of the QKD basics.

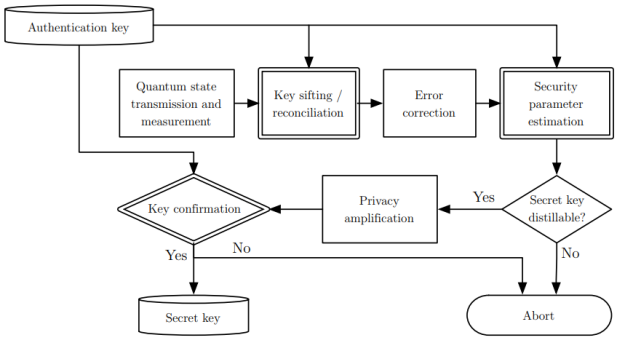


Figure 2.3: Flowchart presenting the stages of a quantum key distribution protocol, where stages with double lines indicate the need for classical authentication [31]

2.2.1 Raw Key Exchange

Quantum State Preparation

The fisrt step for the raw key exchange is for Alice to to prepare the photons in specific quantum states (qubits) by manipulation their quantum properties, such as polarization

or phase encoding. Depending on the protocol, Alice module can include various optical elements to achieve the encoding, such as wave plates or beam splitters. That process uses the photons to send information as qubits and called modulation [11].

Transmission

Alice sends the modulated qubits to Bob through the quantum channel, which can be optical fiber or free space. The quantum channel is sensitive to the various noise sources, such as attenuation and channel-induced errors, due to the transmission of the single-photons (qubits) [26, 13].

Measurement

Bob receives the single-photons and performs the measurement on each qubit, to decode the information about their quantum states. Firstly, Bob utilizes appropriate measurement operators to to determine the quantum state of the received photons and then uses measurement devices [26, 13], such as polarizers or interferometers, to decode the information about their state (polarization angle or phase). The Basis for the measurement of the qubits gets chosen randomly [26].

Basis Announcement

After Alice sends all the photons for the Raw Key, Alice and Bob publicly communicate through the classical channel and exchange their chosen measurement bases for the transmitted photons. That assists later with error estimation and correction [26, 12].

2.2.2 Key Sifting

The Key Sifting process, or information reconciliation, involves reconciling deviations in the raw key generated by Alice and Bob. The raw key, as mentioned before, may contain errors and some measurements may be discarded due to mismatches in the Basis that Alice and Bob choose or other factors like high loss and noise. This process leads both parties to generate sifted agreed-upon key, provided they have both gained knowledge of the measured [26, 12].

2.2.3 Key Distillation

In the practical implementation of the QKD process there are many errors in the transmitted photons, when reviewing experimental results, due to imperfections of the optical components and the transmission medium [3]. Thus error correction and privacy amplification are required, which are important for the classical post-processing of the remaining qubits of the raw key.

Error Correction

The actual error rate of the transmission can be calculated using mathematical formulas, with the most common being the Quantum Bit Error Rate (QBER). The error rate is derived from differences in the measurement outcomes of the transmitted photons. During the sifting procedure, Alice and Bob compare the bases each of them used to generate the final raw key. If the QBER exceeds a predetermined maximum value, it is concluded that there is an eavesdropper in the quantum channel, and the raw key is discarded, restarting the entire process. Errors can also be induced by channel loss during transmission, as a consequence of noise, interference, and imperfections in the optical components. Typically, error correction codes are implemented to reduce such transmission-induced errors. Some of the most common ones are Cascade and LDPC codes, used in most QKD protocols [26, 12].

Privacy Amplification

Privacy amplification is a critical process that enhances the security of a shared secret key between Alice and Bob. This process works by reducing the length of the raw key, which may contain information that could have been leaked to an eavesdropper (Eve), into a more secure form. By applying cryptographic hash functions [4, 37], or other information-theoretic techniques, Alice and Bob create a distilled key with significantly less risk of exposure. The degree of compression, or ”gain,” is often determined by the QBER, a higher QBER indicates more information might have been leaked, requiring more aggressive compression to counteract this. Privacy amplification techniques, particularly those using two-universal hash functions, are designed to be unconditionally secure, meaning they remain secure against any computational power an adversary might have. This ensures that the final shared secret is robust against any potential interception [26, 12].

Authentication

The authentication of the every QKD module is utilized with secret pre-shared keys between them. The pre-shared keys are used for authentication of the very first quantum exchange. The initial authentication can be extended for every future quantum communication between the two pairs, increasing the security levels [32].

2.2.4 Key Generation

After completing all necessary procedures, Alice and Bob create a final secure key suitable for cryptographic applications. The length of this key depends on the error rates, the privacy amplification method applied, and the required security level [26, 12].

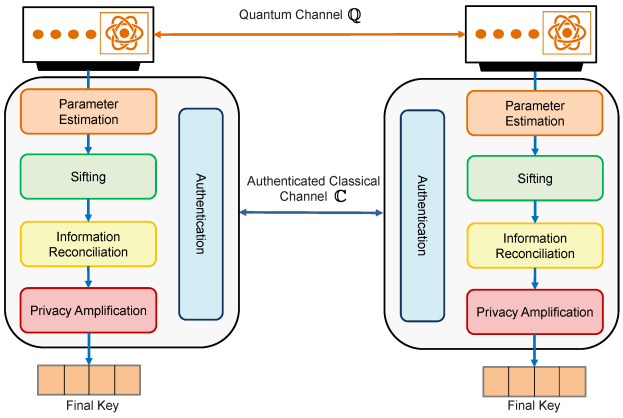


Figure 2.4: The postprocessing workflow of the QKD process [20]

2.3 QKD Protocols

Over the years, many QKD protocols have been introduced, each implementing different modulation techniques to accommodate various applications and transmission media. One of the most popular is the BB84 QKD protocol, which has many variations to suit diverse situations. In this thesis, only this protocol will be discussed, as it is one of the most widely implemented and is the protocol that will later be used for the experiment, specifically the BB84 Decoy State.

2.3.1 BB84 Protocol

In 1984, researchers Bennett and Brassard proposed the BB84 protocol, which revolutionized the field of quantum cryptography. The BB84 protocol utilizes principles of quantum mechanics, particularly Heisenberg's uncertainty principle, to securely share a secret key between two parties. As a prepare-and-measure-based quantum key distribution (QKD) protocol, it is shown below.

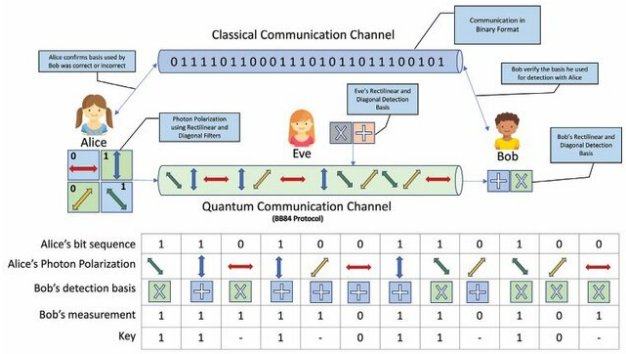


Figure 2.5: BB84 protocol implementation [16]

The core of the BB84 protocol is the use of photon polarization states to convey the information of the secret key over a quantum communication channel.As shown in the Figure 2.6 bellow, it utilizes single photons, each polarized in one of four possible states, chosen from two conjugate bases: the rectilinear basis, which includes vertical and horizontal polarizations, and the diagonal basis, which includes diagonal and anti-diagonal polarizations [26, 12, 13, 16].

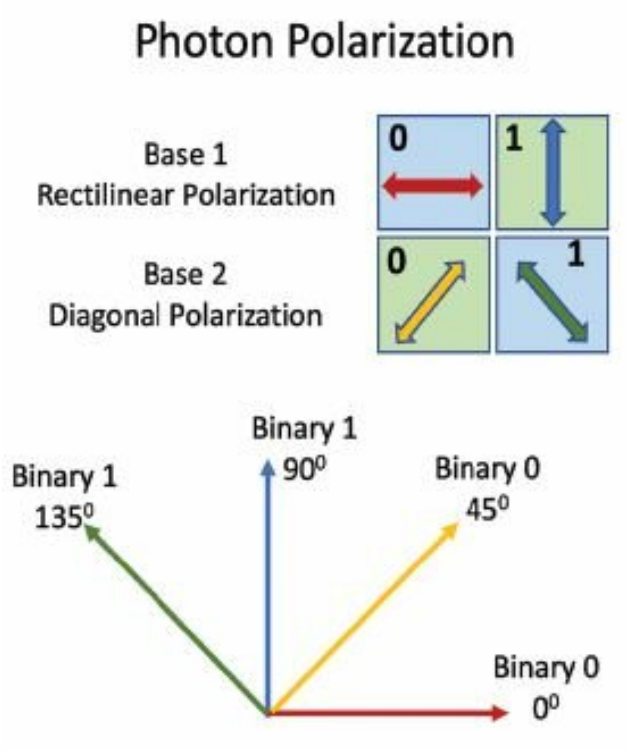


Figure 2.6: Photon polarization in BB84 protocol [16]

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 are represented mathematically using the basis states of the rectilinear basis ($|0\rangle, |1\rangle$) and the diagonal basis ($|+\rangle, |-\rangle$).

2. **Basis Selection:** Alice randomly selects a basis (either rectilinear or diagonal) for each photon she prepares, with her basis choice represented by the random variable A. Similarly, Bob's basis choice for each photon he receives is represented by the random variable B.

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

4. **Measurement:** Upon receiving the photons, Bob randomly chooses a measurement basis (rectilinear or diagonal) for each photon using his own random variable B, then measures each photon to determine its polarization state.

5. **Public Announcement:** After transmission, Alice and Bob publicly exchange their basis choices (A for Alice and B for Bob) for a subset of the transmitted photons, revealing only the basis used and not the measurement results.

6. **Error Estimation:** By comparing their basis choices, Alice and Bob identify a subset of photons to estimate the error rate, which reflects the differences in their measurement results for that subset.

7. **Key Generation:** They discard these photons after calculating the error rate and derive a secure key from the remaining photons, using the measurements taken in matching bases.

8. **Privacy Amplification:** To strengthen security further, Alice and Bob apply privacy amplification techniques, such as error-correcting codes and hashing algorithms, to produce a final, shorter but highly secure 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 security of the key distribution process is ensured by the randomness in basis selection and the intrinsic uncertainty of quantum measurements [26, 12, 19].
The BB84 protocol is a foundational element in quantum cryptography, demonstrating how quantum principles can be applied to achieve secure communication. In its original form, the BB84 protocol relies on single-photon encoding to transmit information securely. However, generating and reliably manipulating single photons presents practical challenges due to factors like the probabilistic nature of photon emission and optical components imperfections. In practice, it is difficult to produce exactly one photon per pulse, as photon generation often follows a statistical distribution, typically approximated by a Gaussian. Consequently, the number of photons per pulse can vary, with a non-zero chance of producing multiple photons. To address this, weak laser pulses—rather than single-photon sources—are commonly used. In these pulses, the photon count follows a Poisson distribution with an adjustable mean, or intensity, of the source. In quantum key distribution (QKD), the average photon number per pulse is generally kept below 0.5 to minimize the probability of emitting multiple photons, which is crucial for preserving the security and integrity of the QKD process.
The occasional presence of multiple photons in these weak pulses introduces a potential vulnerability known as the photon-number-splitting (PNS) attack. In a PNS attack, an eavesdropper could intercept a multi-photon pulse, split the photons, and measure one or more of them without altering the state of the remaining photons. This tactic allows the eavesdropper to gain information about the key with minimal error, thereby compromising the security of the communication channel [19].
To mitigate this vulnerability, any key material derived from multi-photon pulses must be assumed compromised, as it is possible an eavesdropper may have gained partial information about the key. Consequently, researchers have been motivated to develop new protocols to address the challenges and limitations inherent in the BB84 protocol.

2.3.2 BB84 Decoy State Protocol

The BB84 protocol with decoy states introduces key distinctions compared to the standard BB84, especially in key generation methods, modulation, and resilience against photon-number-splitting (PNS) attacks.
BB84: In the original protocol, the secure key is generated by comparing measurement outcomes from Alice and Bob for photons where their basis choices match, which they publicly announce. The key is extracted from these matching outcomes.
Decoy State BB84: In the decoy state variant, Alice sends additional intensity-modulated weak coherent states, called decoy states, or even vacuum pulses alongside the single-photon states. These decoy states strengthen protocol security, specifically against attacks like PNS.
Upon receiving Alice's pulses, Bob announces which pulses generated photon counts (were detected) and which did not. Only Alice knows the original order of these pulses. Alice can then compare the expected versus observed photon counts for both decoy and single-photon states. If the observed counts deviate from expected values beyond set

thresholds, it suggests a potential eavesdropping attempt, prompting termination of the protocol to prevent security breaches.
By monitoring photon counts, the protocol detects any discrepancies caused by interference or eavesdropping, allowing Alice and Bob to ensure the security of key distribution [36].
A practical implementation of BB84 with decoy states is described in , using two normal pulses for signal and key distillation with one decoy state, and mean photon values (μ1 and μ2) ranging from 0.2 to 0.5. Another experiment in utilized one normal pulse and two decoy states, with mean photon values of μ = 0.425, v (decoy state 1) = 0.044, and w (decoy state 2) = 0.001 [19].

2.4 Metrics

There are some metrics that are applied us to rate the performance and the efficiency, in order to characterize the systems which are used to implement every QKD protocol.

1. **Quantum Bit Error Rate (QBER):** The Quantum Bit Error Rate (QBER) assesses the error rate in qubit transmission between Alice (the sender) and Bob (the receiver). A lower QBER signifies more accurate transmission and better protection against potential eavesdropping.
2. **Key Generation Rate:** This refers to the rate at which Alice and Bob can establish a shared secret key, typically measured in bits per second (bps) or key bits per second (kbps). A higher rate indicates a more efficient protocol.
3. **Secure Key Rate (SKR):** This rate reflects how quickly Alice and Bob can produce a secure key after applying error correction and privacy amplification, considering the QBER, reconciliation efficiency, and any information leakage.

2.5 Loss

A significant limitation of Quantum Key Distribution (QKD) lies in the losses encountered as quantum signals propagate. When these signals travel over long distances through optical fibers or free space, various factors, such as absorption, scattering, and imperfections in the transmission medium, can degrade signal quality. Such losses reduce the signal-to-noise ratio, making it difficult to accurately detect and interpret quantum states at the receiver. High loss levels also restrict the communication range, as signal strength decreases over extended distances. To mitigate these losses, advanced techniques like efficient error correction codes, amplification methods, and optimized fiber optic links are essential. Addressing these losses is critical for enhancing the overall performance and feasibility of QKD in secure quantum communication.

3. RELAYED AND SWITCHED QKD

Nowadays most of the commercial QKD networks are implemented using many static point-to-point configurations, where each Alice communicates and creates keys with one predetermined Bob. However, the increasing need for security between multiple users, as the network expands, necessitates different QKD architectures, that are easily extensible for larger networks. Current p2p QKD networks require one dedicated QKD pair at each node to achieve a fully connected topology that is robust against single point failures. Although, expanding that configuration for larger networks is costly and complex with present technologies, as it will require a huge amount of QKD pairs, about N^2.

There are two different configurations that have been proposed to facilitate the need for larger QKD networks, relayed and switched QKD architectures. These architectures are based in the Software Defined Networking (SDN) approach, which introduces a centralized network controller to manage the configurations and the demands of the infrastructure using programmable resources [18]. For that purpose the Key Management System (KMS) layer has been established with standardized protocols[9].

3.1 Relayed - QKD

Relayed Quantum Key Distribution (Relayed - QKD) is a protocol for quantum cryptography that is based on the Prepare-and-measure Quantum key distribution (PM-QKD) protocols for quantum key distribution, commonly on the BB84 protocol [2]. It involves using a trusted quantum relay to facilitate secure communication between parties. Unlike point-to-point (p2p) QKD links, which are typically limited by distance due to the losses in optical fibers, a relay trusted node can serve as an intermediary to extend communication over longer distances that serves as a medium (trusted relay) for two non-neighboring nodes to create private shared keys although they do not have a direct QKD link. Many standards have released that regulate the operation of the relayed-QKD network.

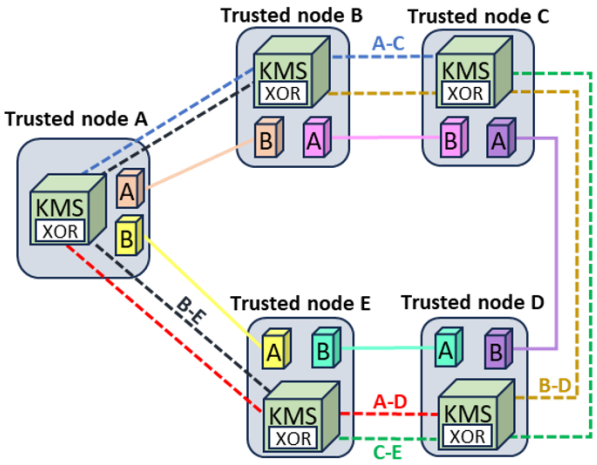


Figure 3.1: Relayed QKD architecture in a 5-node network example [22]

Most recent configurations are implementing the relayed-QKD in the KMS layer. The KMS server in each node assumes the relay function and creates different buffers for crossing relaying paths between the non-neighboring nodes [5, 27, 6].

Although this approach can be implemented with current technology, it introduces trade-offs, including a reduced key generation rate and the necessity of trusting the relay. In typical relayed-QKD networks with N nodes, each containing one Alice and one Bob QKD setup (resulting in N pairs overall), the nodes must allocate their resources both for direct communication with neighboring nodes and for operating as intermediaries to relay keys between non-adjacent nodes. This operation limits the resource usage, especially in networks with long links that require multiple intermediate nodes, reducing overall efficiency.

3.2 Switched - QKD

Switched or Dynamic Quantum Key Distribution (Switched - QKD) is a configuration that allows every QKD transmitter (Alice) to optically communicate with every QKD receiver (Bob) and vice versa. Low loss optical switches (OS) are used at each node to achieve direct optical connections between all the QKD nodes, avoiding the need for trusted nodes. This architecture can reduce the total number of QKD modules to almost N with the integration of Time Division Multiplexing (TDM), which will execute the communication between the modules in different time slots enabling dynamic QKD link establishments and key generations for multiple users.

The KMS server also plays an important role in this configuration. It controls the mechanism to buffer keys from the established QKD links and deploy them during the switching process [1, 33, 18, 34].

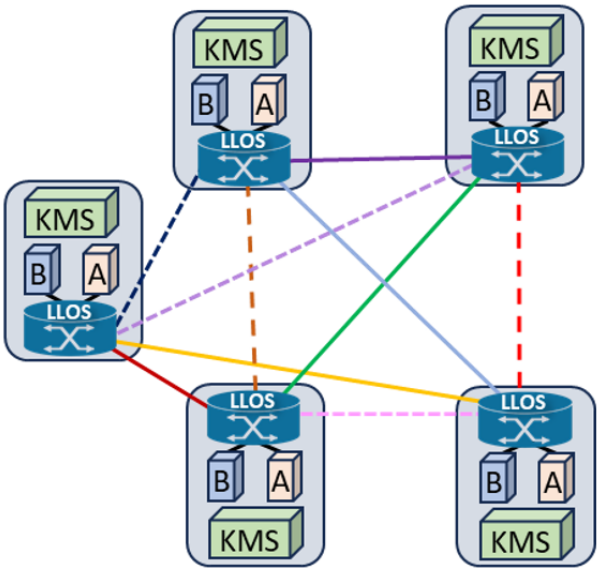


Figure 3.2: Switched QKD architecture in the same network by deploying N optical switches, one in every node [22]

Some advantages offered by the switched-QKD include the flexibility of switching to alternative recovery paths in case of a link failure or a disruption in the communication due to high losses or an eavesdropper. However, there are many challenges in implementing the concept of switched QKD in the current infrastructure [18]. Firstly, the current network cannot support the need for every Alice to be optically connected with every Bob within the network. The cost and the complexity of implementing that multi-point connectivity in the network are very high with the present technology. Secondly, it is crucial tp use

low loss optical switches (LLOS) due to the high sensitivity of the quantum channel to the attenuation in the link, as the SKR decreases when the QKD pairs operate close to their limit. Moreover, there are many other concerns about the implementation of switched - QKD, such as the switching and initialization time between the QKD links and the mis-matching of the transmitter's and receiver's optical modules, which are typically optimized for each QKD pair. Generally, there is a misalignment when connecting unoptimized QKD module, due to the non-optical alignment of the physical parameters of the QKD modules, like wavelength detuning or phase mis-matching.

4. EXPERIMENT OVERVIEW OF SWITCHED - QKD

The experimental procedure that was followed for this experiment took place in the Optical Communications and Photonics Technology Laboratory National and Kapodistrian University of Athens and it was consisting the evaluation of two Switched-QKD pairs performance compared to the Relayed-QKD configuration.

4.1 Experimental Setup

The experiment included two QKD pairs, which are manufactured by Toshiba (Toshiba QKD4.2-MU/MB [35]), and implement the Efficient BB84 protocol with decoy states and phase encoding [19]. Every pair has two segments of operation, the first one consists of all the physical elements necessary to implement the BB84 protocol, like lasers, photodetectors, isolators etc. and the second one is the Control Server, a UNIX based system, for the user interface of the system.
The QKD pairs' operation channels for the forward propagation are 1310 nm for the quantum channel, 1530.33 nm for the synchronization channel and 1529.55 nm for the synchronization QKD classical channel and for the backward propagation is 1528.77 nm for the synchronization QKD classical channel. The channels in the forward propagation are in the telecom O-Band and copropagating with the QKD channel. The typical key rate for the QKD system is 300 kb/s at 10 dB loss in the line.

4.2 Switched-QKD networks performance

This experiment aims to evaluate the performance between two optimized QKD pairs, as manufactured by Toshiba, connected in a point-to-point configuration, or bar configuration, and two non-optimized QKD Toshiba pairs connected in a switched configuration. The setup includes two Toshiba QKD pairs, as mentioned before, and specifically each consisting of two pairs of one Alice and one Bob.
The first case of the experiment consists the two optimized pairs connected in a p2p configuration as shown in the Figure 4.1 below. For the first pair, the Alice 1 transmitter is connected to the Bob 1 receiver (A1B1) through a 6.4 km fiber link. Each link is fitted with 6 dB of attenuation to emulate the low loss optical switches (LLOS). The second pair of the optimized configuration involves a 10.6 km fiber link that connects Alice 2 transmitter to Bob 2 receiver (A2B2). As with the first QKD pair, each link is fitted with 5 dB of attenuation to emulate the low loss optical switches (LLOS). The configuration of the two pairs is shown in the Figure 4.1 bellow.

The second case of the experiment presents a switched configuration for each unmatched pair. The pairs were manually changed to the ”cross” configuration for this case. The first non-optimized pair includes Alice 1 and Bob 2, where the Alicer 1 transmitter is connected to the Bob 2 receiver (A1B2) through a 6.4 km fiber link. Likewise, the second non-optimized pair involves a 10.6 km fiber link that connects Alice 2 transmitter to Bob 1 receiver (A2B1). The attenuations simulating the optical switches' loss are matching the ones in the optimized configuration, as presented in the Figure 4.2 bellow.

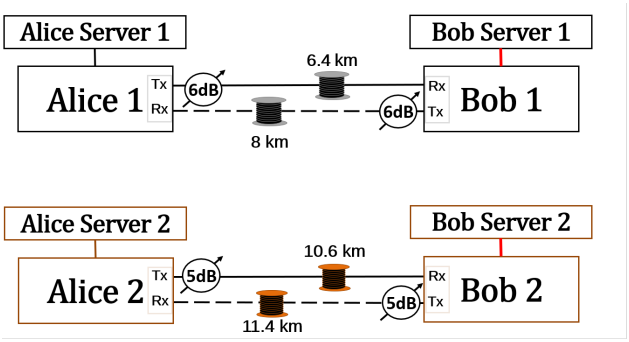


Figure 4.1: Optimized QKD pairs [22]

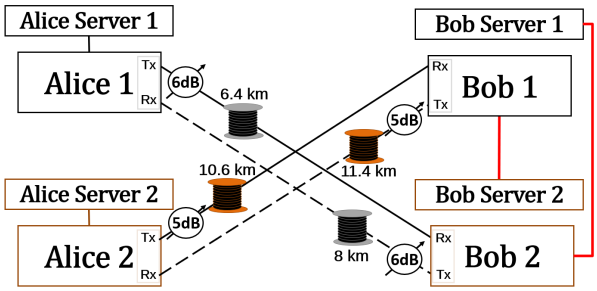


Figure 4.2: Non-optimized QKD pairs [22]

4.3 Experimental evaluation

4.3.1 Optimized QKD pairs compared to non-optimized QKD pairs

The distances and the attenuation between the pairs in the two cases were matching to achieve an accurate comparison. The change into the switched configuration included the swapping only of the the optical QKD parts and maintained the original servers' connectivity. The expected results were lower Secret Key Rate (SKR) for the switched pairs, due to the implemented phase encoding protocol, which requires precise alignment and perfect matching between the differential interferometers (DI) of Alice and Bob. In case of deviations in the alignment of the two DIs is going to lead in lower visibility of the quantum states, which will increase the QBER and eventually reduce the SKR. Regularly the servers of the QKD pair adjust the DIs during initialization and try to improve the connection based on the parameters of each optical QKD engine. However, we could not intervene with the software of the servers, so there were limitation to the switched connection of the servers.

4.3.2 Results

The system was up and running for approximately 18 hours and there was a reduction in SKR and a rise in the QBER for the non-optimized pair comparing to the optimized pair, as anticipated. Although the fiber of the quantum channel for the non-optimized pair A1-B2 is shorter than the one for the non-optimized pair A2-B1, there is a significant difference between the performance of the two pairs with the A2-B1 to mark an almost eight times higher SKR. We can assume that for the pair A2-B1 the alignment of the DIs was more precise and there was a better matching in contrast to the other pair. To evaluate the switched operation, we examine the connectivity illustrated in Figures 4.1 and

4.2. In each pair, QKD channels operate in the O-band, co-propagating with two service channels at 1529 nm and 1530 nm, while a third service channel at 1528 nm counter-propagates through a separate fiber. The results over an 18-hour operation period are detailed in Figures 4.4, 4.5, 4.6, 4.7, showing a total key generation of 221 Megabits for A1-B2 and 1.8 Gigabits for A2-B1. Table in Figure 4.3 provides a summary of average SKR and QBER values for each case„ which where calculated with equations based on [38], indicating a drop of approximately 14 dB for A2-B1 and over 20 dB for A1-B2. However, as mentioned before, the the QKD phase encoding protocol needs perfect matching between the differential interferometers (DI) integrated in Alice to temporally separate the weak coherent pulses and to properly recombine them in Bob. Imperfect matching will result in low visibility for the quantum states, causing an increase in QBER and a decrease in SKR, as shown in Figure **??**.

TABLE I
AVERAGE VALUES FOR SKR AND QBER FOR OPTIMIZED AND NON-OPTIMIZED PAIRS

Optimized Pairs	A1-B1	A2-B2
SKR (bps)	481 k	722 k
QBER (%)	3.13	2.93
Non - Optimized Pairs	A1-B2	A2-B1
SKR (bps)	3.3 k	27 k
QBER (%)	6.7	5.7

Figure 4.3: Average values for SKR and QBER [22]

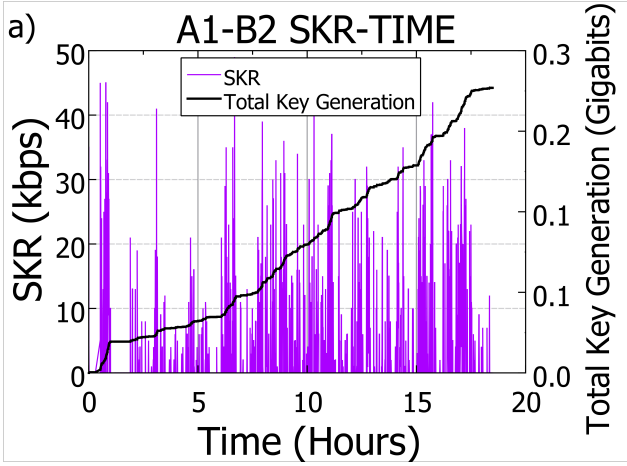


Figure 4.4: Secret Key Rate for non-optimized pair A1-B2 for 18-hours operation [22]

4.4 Switched vs relayed QKD performance

We conducted a numerical analysis and chose to compare the performance of switched to relayed QKD architecture over a ring topology, to extend our conclusions on the comparison between the two architectures. The ring topology is implemented with equal-length/attenuation links while the SKR is given by funstion $f(a)$, that was defined by the values of the previous experiment and inserted 5 dB attenuation to emulate the non-matching QKD pairs and losses in optical switches for the switched - QKD. We assume an all-to-all key consumption pattern among Security Application Entity (SAE) pairs. Our objective is

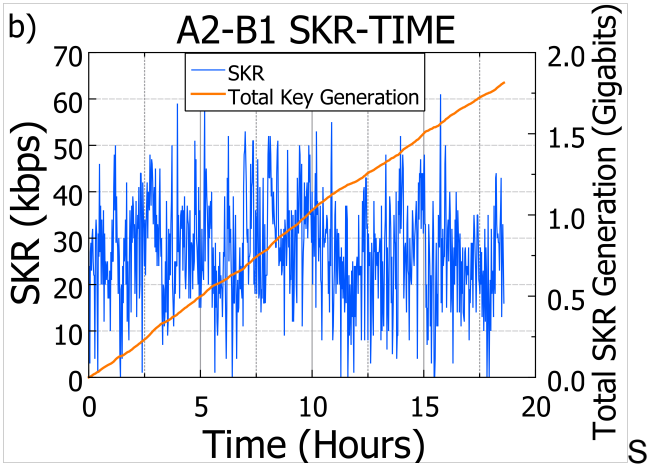


Figure 4.5: Secret Key Rate for non-optimized pair A2-B1 for 18-hours operation [22]

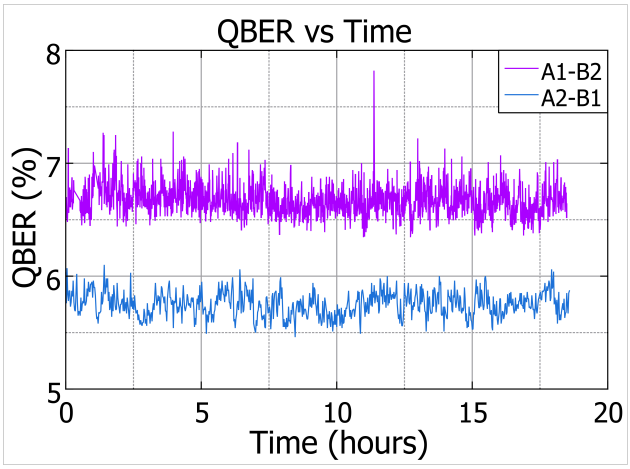


Figure 4.6: QBER for the two switched QKD pairs for 18-hours operation [22]

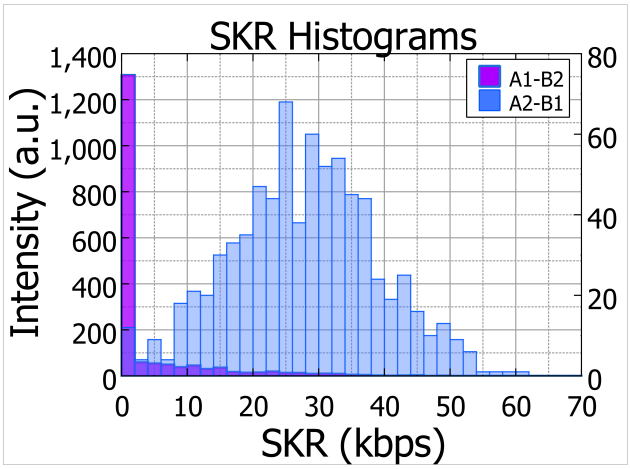
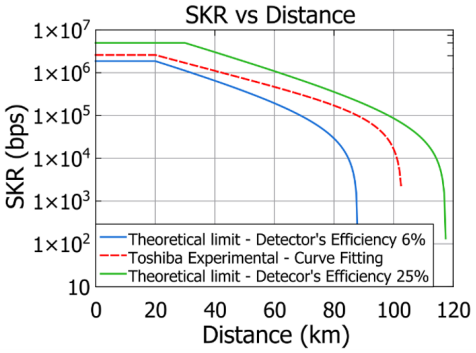


Figure 4.7: A Histogram of SKR with gaussian fit, illustrates that the A1-B2 was operating close to its operational limit and the A2-B1 was operating with more stability around 27.2 kbps [22]

to equalize the SKR across all SAE pairs fairly and to maximize it, thereby strengthening the overall network security.

In relayed QKD, each Alice node n_i connects to a matched Bob in the adjacent node n_{i+1}, creating a ring where nodes act as trusted relays to generate keys for non-adjacent node pairs. In a ring topology with equal link attenuation A_e, each QKD link supports $\frac{N^2-1}{8}$ node

a)



b)

Parameter	f	μ	q	α	e_0	Y_0	$e_{detector}$
Value	1.22	0.55	0.319	0.21	0.51	6.14×10^{-5}	5×10^{-3}

Figure 4.8: a) Experimental and simulated SKR over Distance for DV-QKD b) Parameters used for the theoretical estimation of the simulated SKR graph [22]

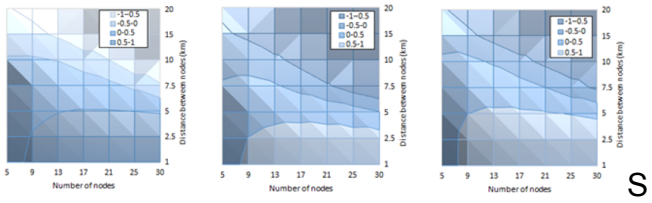


Figure 4.9: ($G_S - G_R$)/max(G_S, G_R) normalized SKR difference for a) experimental SKR, b) low SKR and, c) high SKR [22]

pairs (for odd N) that use that link in their key generation path. For fair SKR, each SAE pair achieves an SKR of

$$GR = \frac{8 \cdot f(A_e)}{N^2 - 1}.$$

In switched QKD, each node can connect directly to any other node through optical switches, enabling flexible paths. The lengths of all diagonal links are based on a circle with a diameter matching the ring. A scheduling algorithm configures the switches to form QKD links, and in rings with equal link lengths, scheduling is straightforward. To ensure fair SKR, each node n_i communicates with half the network nodes using Alice and half using Bob, for timeslots proportional to the inverse of the link SKR. Specifically, node n_i connects to n_j for a portion $T_{ij} = \frac{2}{f(A_{ij})}$ of a total $T_i = \sum_j T_{ij}$ time, where A_{ij} is the link attenuation of (n_i, n_j). This scheduling provides each SAE pair with an SKR of

$$GS = \frac{1}{T_i},$$

applied simultaneously across all nodes.

We compare the relayed and switched architectures based on maximum common SKR. Relayed QKD distributes the SKR of a QKD pair across $\frac{N^2-1}{8}$ pairs, while switched QKD divides it among $\frac{N}{2}$, though it spends more time on longer QKD links to counter the reduced SKR. For our study, we model rings with varying numbers of nodes (from 5 to 30), adjacent node distances from 1 to 20 km, and an attenuation coefficient of 0.21 dB/km. We examine three SKR functions $f(a)$ to emulate various QKD performance levels against distance-related losses. We then plot the normalized SKR difference $R = \frac{GS-GR}{\max(GS,GR)}$, where values range from -1 (relayed is better) to +1 (switched is better).

In Figure 4.9 (a), we see that for distances below 5 km, even with up to 30 nodes, switched

QKD outperforms relayed QKD. For 7.5 km links, switched QKD is better for up to 20 nodes, and for 10 km links, it holds up to 10 nodes. Short distances and multiple hops favor switched QKD, as it remains in the stable region of the key generation function and avoids high-attenuation links. For lower SKR performance, Figure 4.9 (b), the switched architecture shows slightly reduced efficiency. However, for high SKR performance (green $f(a)$ curve in Figure 4.8 (a), Figure 4.9 (c) reveals that switched QKD is better for configurations with 20 nodes and 10 km links.

4.5 Conclusion

In this experiment, we demonstrated the deviation in SKR generation and QBER between the two non-optimized QKD pairs due to the imperfections and the mismatching in the alignment of the physical parameters of the QKD modules. To examine this effect, we performed a numerical analysis comparing relayed and switched QKD architectures. Our study was based on specific assumptions—such as a ring network structure, equal distances and attenuation between adjacent nodes, and all-to-all communication demands—that simplify key distribution in both architectures. From this analysis, we found that the switched QKD network outperforms the relayed architecture at shorter distances with multiple hops, making it well-suited for urban network deployments. The switched network leverages QKD equipment with a stable SKR generation rate over short distances and maintains solid performance even without it. However, the significant differences in SKR generation rates and device incompatibility can reduce the efficiency of the switched architecture. Minimizing attenuation from non-optimized pairs is essential for practical application. In real-world use, a hybrid network combining both switched and relayed architectures could prove effective.

5. EXPERIMENT OVERVIEW OF HYBRID RELAYED - QKD

In this work we present a fully managed, operational three-node quantum cryptography network serving OTN circuits with (Layer 1 - OTNsec) encryption. Figure 5.1 illustrates the architecture of our network.

Each node utilizes a fully integrated vertical stack with a managed quantum layer, a Key Management System (KMS) layer, and an application layer, all working in coordination, based on European and International QKD standards [9, 7, 8, 15]. The quantum layer includes two IDQuantique Cerberis XGR QKD pairs [14] to establish two point-to-point QKD links. These links are then extended by the KMS layer (using a relay) to enable all-to-all communication, specifically supporting three bidirectional OTN circuits. This setup reduces the need for additional QKD resources by omitting a QKD pair for the third link.

In the KMS layer, we deployed EvolutionQ BasejumpQDN key management software [10] alongside the Network Controller for the QKDN, which operates according to ETSI GS QKD 015 standards [7]. This setup retrieves quantum keys, stores them in dedicated buffers, and manages the synchronization and scheduling of key delivery to Secure Application Entities (SAEs). The network secures OTN circuits between all three node pairs while using only two QKD pairs, allowing intermediate relay nodes to consume keys and enabling priority or QoS settings for key consumption. This functionality, though valuable, adds requirements for additional scheduling, buffering, and key monitoring. The Nokia 1830 Security Management Server (SMS) [25] oversees and controls the EvolutionQ key management software, functioning as a security orchestrator in line with ETSI GS QKD 18 [8]. The SMS not only distributes keys across network nodes but also aligns key requirements with the classical OTN layer. Notably, it provides a seamless fallback to quantum-safe classical encryption (based on AES256) if a DoS attack or failure in the QKD layer disrupts key generation/distribution. This is achieved through centralized symmetric classical key generation and distribution. In the application layer, each node is equipped with a Nokia layer 1/OTN Photonic Service Interconnection - Modular (PSIM) encryptor [24] (300 Gbps), which encrypts data using quantum keys with rotation rates as frequent as one key per minute.

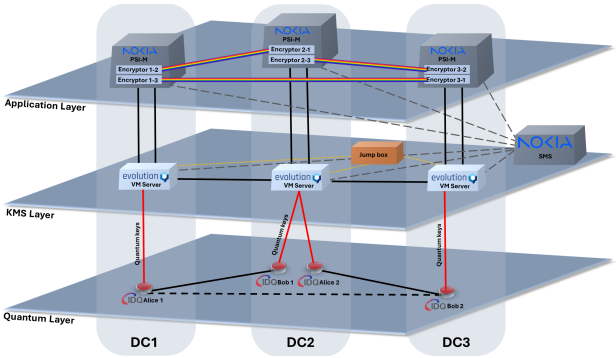


Figure 5.1: Illustration of the layered architecture [21]

5.1 Experimental Setup

The experimental testbed, illustrated in Figure 5.2, includes three trusted nodes: DC1 (GRNET DC node), DC2 (NKUA Optical Communications and Photonic Technologies

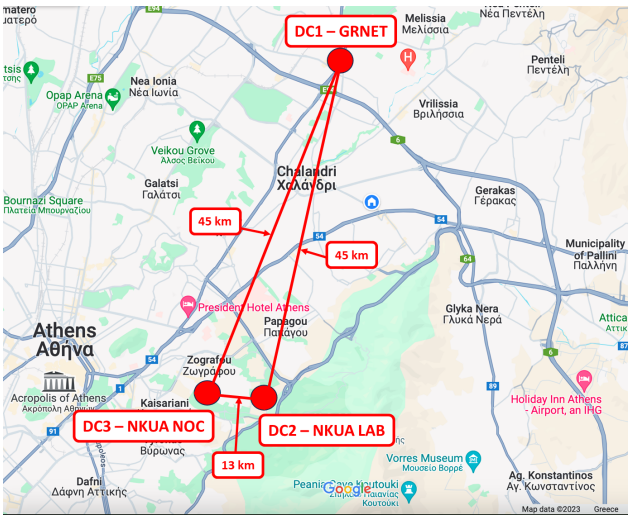


Figure 5.2:) DC1, DC2 and DC3 marked by their approximated physical location [21]

Lab), and DC3 (NKUA Networks Operation Centre-NOC). DC1 hosted QKD Alice 1 (A1), DC2 served as a relay node hosting QKD Bob 1 (B1) and Alice 2 (A2), while DC3 hosted QKD Bob 2 (B2). The fiber link between DC1 and DC2 spans approximately 45 km, whereas DC2 and DC3, located at separate sites on the NKUA campus, were linked by a 13 km fiber spool to simulate an extended distance. Figure 5.3 shows the physical optical connections for QKD pairs and PSI-M encryptors. DC2 and DC3 (NKUA nodes) connected to DC1 (GRNET) via two unidirectional dark fibers.

To prevent in-band noise that could impair QKD performance, the 1550 nm quantum channel occupied only one dark fiber, which was essential given that the A1-B1 link experienced 18 dB of loss—near the operational limit for the IDQuantique Cerberis XGR QKD pair. The PSIM OTN data channels (C36, C34) and the QKD service channel (C30) were multiplexed, with circulators enabling bidirectional operation over the second fiber. Additional losses totaled 2.8 dB. The OTN data channel between PSI-M 2 and PSI-M 3 (C38 channel) was created through an intra-campus link, also used for communication between Alice 2 and Bob 2. Each PSI-M line supported a 300 Gbps data rate using 67 GBaud, 16QAM, and SDFEC-G2 for flex OTU in OTSiG. For the management network, each node had a local private Ethernet connection between the QKD and KMS servers, allowing secure quantum key delivery from the quantum layer to the KMS layer. Additionally, a VLAN within the GRNET-NKUA domain was established for management, orchestration, and communication among components in the multi-layer architecture.

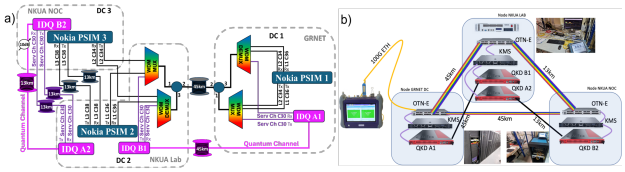


Figure 5.3: a) Optical connections of the three-node relayed quantum network b) Schematic demonstration of the layered setup [21]

5.2 Results

The system was evaluated across multiple key rotation intervals (1, 5, 15, 30, 60 minutes) over extended durations. Table in Figure 5.5 shows the percentages for each key rotation

interval, with a 98% success rate in key rotation using either QKD or classical key distribution even under the demanding condition of 1 key per minute. For the remaining 2%, encryption continued with the previous key, and a new rotation request was issued after 30 seconds. Therefore, data encryption remained uninterrupted, with reported failures indicating only minor issues at specific key rotation points. Additionally, a 100 Gb/s Exfo Network Analyzer continuously monitored network performance, recording average jitter and latency values of less than 0.015 ms and 2.06 ms, respectively. Network resilience was tested through two simulated attacks: (i) a KMS attack disrupting communication between the application and KMS layers and (ii) a QKD attack, effectively nullifying the Secure Key Rate (SKR). The KMS attack was simulated by shutting down the KMS server on all nodes, while the QKD attack was simulated by disconnecting the quantum channel fiber. During both tests, the key rotation interval was set to 1 minute, the QNL buffer (EvolutionQ KMS input buffer holding keys from the quantum layer) capacity was 1,000 keys, and the key expiration time was 4 hours.

As shown in Figure 5.4 (a), a simulated KMS attack illustrates the network's hybrid functionality. When each KMS server is attacked, the KMS layer is unable to supply quantum keys to the encryptors. In response, the SMS generates and provides classical, quantum-safe keys to the PSIMs. Once the key management servers are restored, the QNL (KMS input) buffers start refilling, and, shortly afterward, begin supplying keys to the KMS (output) buffers for quantum key rotation. Figure 5.4 (b) demonstrates a QKD attack on the DC12 link. During this attack, the network relies on buffered keys, resulting in a steady decrease in key count with a slight overhead. Depending on the attack duration, the system may either deplete the key supply or avoid exhaustion. In our experiment, the attack duration was short enough to ensure uninterrupted quantum key transmission. After the QKD link was restored, the QNL buffers began refilling, gradually restoring the KMS buffering process.

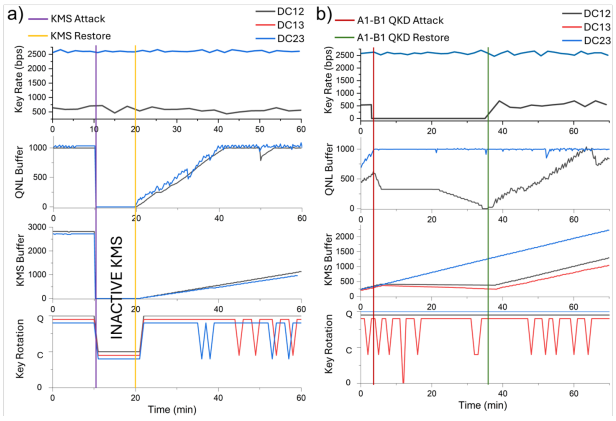


Figure 5.4: Diagrams for the SKR, QNL buffers, KMS buffers and SMS key rotation for all links at the emulated KMS (a) and QKD (b) attacks. The key rotation is characterized as 'Q' for quantum key rotation, 'C' for the SMS' classical key rotation and, '0' for no key rotation [21]

5.3 Conclusions

We report on the successful demonstration of a fully managed field deployed three-node QKD relayed network in a ring configuration, where each node comprises a fully integrated vertical stack. We demonstrated the network's stable operation providing Layer 1 (OTN-sec) data encryption with quantum keys. In case of an attack or unavailability of quantum

Rotation Interval (min)	Classical Key Rotation (%)	Quantum Key Rotation (%)	SNMP error (%)
1	8.8	89.2	2.0
5	10	90	0.0
15	14.8	83.6	1.6
30	33	66.4	0.6
60	7.8	90.7	1.5

Figure 5.5: Network's key rotation percentages for different key rotation intervals [21]

keys, we demonstrated the network's capability to seamlessly transition to classical encryption with symmetric quantum-safe keys provided by the central security manager / SMS, exhibiting, thus, a reliable hybrid network operation and ensuring the continuous supply of keys. Notably, the keys were consumed in all three nodes, including the intermediate relayed node, and we demonstrated that the operations, including relaying, recover against various attacks.

6. CONCLUSIONS AND FUTURE WORK

In this thesis, switched and relayed QKD architectures were analyzed, highlighting their advantages and the challenges they still face. The first experiment demonstrated the potential of switched-QKD through SKR and QBER analysis, showing that switched QKD outperforms the relayed architecture at shorter distances, making it well-suited for urban deployments despite SKR deviations. This comparison suggests that a hybrid scheme combining both architectures may offer optimal real-world applications based on specific network needs.

The second experiment explored a hybrid-QKD architecture by successfully implementing a fully managed, field-deployed three-node QKD relayed network in a ring configuration. The network demonstrated stable operation and Layer 1 (OTN-sec) data encryption with quantum keys, showing quantum encryption's feasibility at every network layer. A notable innovation was the network's ability to switch to classical encryption if quantum keys were unavailable, ensuring continuous encryption for Layer 1 data. The hybrid relayed scheme illustrates the feasibility of a fully operational quantum-safe network capable of resilience against various attacks or hardware failures.

This thesis demonstrated the feasibility of using hybrid switched and relayed QKD architectures within current network infrastructures. While promising, significant challenges remain for developing long-distance, fully integrated QKD networks. QKD devices are still highly sensitive to high attenuation, and single-photon technologies need further maturity to support these applications effectively.

ABBREVIATIONS - ACRONYMS

QKD	Quantum Key Distribution
SKR	Secret Key Rate
QBER	Quantum Bit Error Rate
COW	Coherent One-Way
P2P	Point To Point
PBS	Polarizing Beam Splitter
SDN	Software Define Networking
KMS	Key Management System
DI	Differential Interferometers
OS	Optical Switches
TDM	Time Division Multiplexing
LLOS	Low Loss Optical Switches

BIBLIOGRAPHY

[1] Obada Alia, Rodrigo Stange Tessinari, Emilio Hugues-Salas, George T. Kanellos, Reza Nejabati, and Dimitra Simeonidou. Dynamic dv-qkd networking in trusted-node-free software-defined optical networks. *Journal of Lightwave Technology*, 40(17):5816–5824, 2022.

[2] H. Bechmann-Pasquinucci and A. Pasquinucci. Quantum key distribution with trusted quantum relay, 2005.

[3] Charles H. Bennett, François Bessette, Gilles Brassard, Louis Salvail, and John Smolin. Experimental quantum cryptography. *Journal of Cryptology*, 5(1):3–28, 1992.

[4] J. L. Carter and M. N. Wegman. Universal hash functions. *Journal of Computer and System Sciences*, 18:143–154, 1979.

[5] T. Y. Chen, X. Jiang, S. B. Tang, et al. Implementation of a 46-node quantum metropolitan area network. *npj Quantum Information*, 7:134, 2021.

[6] J. F. Dynes, A. Wonfor, W. W. S. Tam, et al. Cambridge quantum network. *npj Quantum Information*, 5:101, 2019.

[7] ETSI. ETSI GS QKD 015 - Quantum Key Distribution (QKD); Control Interface for Software Defined Network. Technical report, European Telecommunications Standards Institute (ETSI), 2022. Accessed: 2024.

[8] ETSI. ETSI GS QKD 018 - Quantum Key Distribution (QKD); Orchestration Interface for Software Defined Networks. Technical report, European Telecommunications Standards Institute (ETSI), 2022. Accessed: 2024.

[9] ETSI GS QKD 014. Quantum Key Distribution; Protocol and Data Format of REST-based Key Delivery API. Technical report, European Telecommunications Standards Institute, 2019.

[10] EvolutionQ. BasejumpQDN: Quantum-Safe Key Management System, 2024. Accessed: 2024.

[11] 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.

[12] Laszlo Gyongyosi, Laszlo Bacsardi, and Sandor Imre. A survey on quantum key distribution. *Infocommunications journal*, pages 14–21, 01 2019.

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

[14] ID Quantique. Cerberis xgr qkd system. `https://www.idquantique.com/quantum-safe-security/products/cerberis-xgr-qkd-system/`. Accessed: 2024.

[15] International Telecommunication Union. Recommendation ITU-T Y.3803: Quantum Key Distribution – Key Management. Technical report, International Telecommunication Union (ITU), 2020. Accessed: 2024.

[16] Tajdar Jawaid. Quantum computing and the future internet, 03 2022.

[17] A. Lewis and M. Travagnin. *A Secure Quantum Communications Infrastructure for Europe: Technical Background for a Policy Vision*. Number JRC129425 in EUR 31133 EN. Publications Office of the European Union, Luxembourg, 2022.

[18] D.R. Lopez, V. Martin, V. Lopez, F. de la Iglesia, A. Pastor, H. Brunner, A. Aguado, S. Bettelli, F. Fung, D. Hillerkuss, et al. Demonstration of software defined network services utilizing quantum key distribution fully integrated with standard telecommunication network. *Quantum Rep.*, 2:453–458, 2020.

[19] 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. *Opt. Express*, 21(21):24550–24565, Oct 2013.

[20] Y. Luo, X. Cheng, H.-K. Mao, and Q. Li. An overview of postprocessing in quantum key distribution. *Mathematics*, 12:2243, 2024.

[21] N. Makris et al. Field demonstration of a fully managed, L1 encrypted 3-node network with hybrid relayed-QKD and centralized symmetric classical key management. 3 2024.

[22] N. Makris, A. Papageorgopoulos, P. Konteli, I. Tsoni, K. Tsimvrakidis, I. Papastamatiou, K. Christodoulopoulos, G. T. Kanellos, and D. Syvridis. Relayed-qkd and switched-qkd networks performance comparison considering physical layer qkd limitations. In *2024 Optical Fiber Communications Conference and Exhibition (OFC)*, pages 1–3, 2024.

[23] David McMahon. *Quantum Computing Explained*. Wiley-IEEE Computer Society Press, Hoboken, NJ, 2008.

[24] Nokia. 1830 photonic service interconnect – modular (psi-m), 2024. Accessed: 2024.

[25] Nokia. Nokia 1830 Security Management Server (SMS), 2024. Accessed: 2024.

[26] 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.

[27] M. Sasaki, M. Fujiwara, H. Ishizuka, W. Klaus, K. Wakui, M. Takeoka, S. Miki, T. Yamashita, Z. Wang, A. Tanaka, K. Yoshino, Y. Nambu, S. Takahashi, A. Tajima, A. Tomita, T. Domeki, T. Hasegawa, Y. Sakai, H. Kobayashi, T. Asai, K. Shimizu, T. Tokura, T. Tsurumaru, M. Matsui, T. Honjo, K. Tamaki, H. Takesue, Y. Tokura, J. F. Dynes, A. R. Dixon, A. W. Sharpe, Z. L. Yuan, A. J. Shields, S. Uchikoga, M. Legré, S. Robyr, P. Trinkler, L. Monat, J.-B. Page, G. Ribordy, A. Poppe, A. Allacher, O. Maurhart, T. Länger, M. Peev, and A. Zeilinger. Field test of quantum key distribution in the tokyo qkd network. *Opt. Express*, 19(11):10387–10409, May 2011.

[28] Valerio Scarani, Helle Bechmann-Pasquinucci, Nicolas J. Cerf, Miloslav Dušek, Norbert Lütkenhaus, and Momtchil Peev. The security of practical quantum key distribution. *Rev. Mod. Phys.*, 81:1301–1350, Sep 2009.

[29] Hitesh Singh, D.L. Gupta, and A.K Singh. Quantum key distribution protocols: A review. *IOSR Journal of Computer Engineering*, 16:01–09, 01 2014.

[30] 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.

[31] Douglas Stebila, Michele Mosca, and Norbert Lütkenhaus. The case for quantum key distribution. In Alexander Sergienko, Saverio Pascazio, and Paolo Villoresi, editors, *Quantum Communication and Quantum Networking*, pages 283–296, Berlin, Heidelberg, 2010. Springer Berlin Heidelberg.

[32] Douglas Stebila, Michele Mosca, and Norbert Lütkenhaus. *The Case for Quantum Key Distribution*, page 283–296. Springer Berlin Heidelberg, 2010.

[33] R. S. Tessinari, E. Arabul, O. Alia, A. S. Muqaddas, G. T. Kanellos, R. Nejabati, and D. Simeonidou. Demonstration of a dynamic qkd network control using a qkd-aware sdn application over a programmable hardware encryptor. In *2021 Optical Fiber Communications Conference and Exhibition (OFC)*, pages 1–3, 2021.

[34] R. S. Tessinari, R. I. Woodward, and A. J. Shields. Software-defined quantum network using a qkd-secured sdn controller and encrypted messages, 2023.

[35] Toshiba Corporation. Quantum key distribution (qkd) products, 2024.

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

[37] Mark N. Wegman and J.Lawrence Carter. New hash functions and their use in authentication and set equality. *Journal of Computer and System Sciences*, 22(3):265–279, 1981.

[38] Yi Zhao, Bing Qi, Xiongfeng Ma, Hoi-Kwong Lo, and Li Qian. Simulation and implementation of decoy state quantum key distribution over 60km telecom fiber. pages 2094 – 2098, 08 2006.