UNIVERSITAT POLITÈCNICA
DE CATALUNYA
BARCELONATECH

Techniques for efficient and secure optical networks

Masab Iqbal

Universitat Politècnica de Catalunya

Optical Communications Group

Computer Architecture

Techniques for Efficient and Secure Optical Networks

Masab Iqbal

Advisor:

Dr. Luis Velasco

Co-advisor:

Dr. Joao Pedro

A thesis presented in partial fulfilment of the requirements for the degree of

Philosophy Doctor

February 2023

Optical Communications Group (GCO)

Universitat Politècnica de Catalunya (UPC)

C/ Jordi Girona, 1-3

Campus Nord, D4-2013

08034 Barcelona, Spain

Acknowledgements

First and foremost, I am extremely grateful to my supervisor, Prof. Luis Velasco, for his valuable advice and continuous support that made this tough journey easy for me. His immense knowledge, experience, and strong character have not only greatly taught me in academic research but also in my daily life. I would also like to thank Dr. Marc Ruiz for always being there to solve my trivial problems and encouraging me at times when the frustration of failure loomed around me by expressing every failure as a step to learn and make the next one better. Marc, I eagerly mark the release of Indiana Jones and the lost qubit!

I would also like to thank my co-advisor Dr. Joao Pedro, who made my stay at Infinera pleasant. Whether it was reviewing my work in weekly meetings or playing foosball, his positive mood always encouraged me to do better. The way he leads his team on and off the field taught me a useful skill of how to keep your team motivated no matter what. Also, I thank Dr. Antonio Napoli for always appreciating me and making me feel like my work was always exceptional. Thanks to Dr. Nelson Costa, whose technical support is no less than a helping hand for a struggling PhD student.

I want to thank all my colleagues-Sima, Fatemeh, Morteza, Mariano, Diogo, Hailey, Shaoxuan, Pol, and Prasunika-for the cherished time we spent together in the GCO lab. They certainly made my stay in Barcelona pleasant. The ECOC trip and occasional gatherings helped me feel less homesick.

I would like to express my gratitude to my parents, lovely sisters (Wara and Ushna) and brother (Waneya). Without their tremendous understanding and encouragement in the past few years, it would have been impossible for me to complete my PhD. Thank you for being a part of my life!

I also wish to thank a special person with whom I got engaged and married during this journey. I love you, Zoha!

I would also like to thank the REAL-NET project that allowed me to live in culturally rich cities like Barcelona and Lisbon, which taught me much outside my PhD studies.

To my mom, Shaheen: I understand raising kids as a single mother in our culture and letting them go abroad to achieve their dreams in the times you need them the most is nothing but a supernatural act; no wonder you are a superwoman for me. Thanks for being my mom and making me who I am today. You are always appreciated. I love you!

Abstract

Optical communication systems are widely adopted and responsible for transporting data traffic from access to metro to core networks supporting society's information and communication functions. As the traffic growth is increasing more innovative and efficient optical networking solutions other than the existing ones are needed to provide the industry with long-term sustainable profits. Also, with the advent of quantum computers these networks are vulnerable to a variety of security threats. Thus, either additional means of making the networks secure are needed or quantum aided transportation of data signal is required. Considering the challenges of efficiency and security aspects of current optical networks, this PhD thesis aims to provide *techniques for efficient and secure optical networks*.

The current data traffic pattern in different segments of the optical networks can be a key factor to make the architecture more *efficient*. These traffic patterns are usually served by deploying point-to-point (P2P) connections which might not be the most cost-effective solution in certain segments like access and metro aggregation. This PhD thesis studies technologies supporting point-to-multipoint (P2MP) connections to serve dynamic and heterogenous data traffic flows. A well-known technology known as Digital Subcarrier Multiplexing to implement P2MP connection is used as a benchmark to evaluate the performance of a novel technology called Optical Constellation Slicing, to cater the same dynamic and heterogenous traffic requirements. For a dynamic profile these two technologies are compared against the traditional technology supporting P2P. The analysis in terms of cost, efficiency of data throughput and architecture simplicity is provided all along. The potential of P2MP connections is demonstrated.

To make the optical networks *secure*, the studies are carried out in two dimensions. Firstly, the vulnerability of the physical layer is targeted. To make the overall network more secure, methods for physical layer cryptography are studied. Secondly, quantum communication technology is investigated because it is inherently secured by the laws of quantum mechanics.

For physical layer security, we propose LPsec (lightpath security) where we target providing a complete solution of security from key exchange methods at physical

layer to investigate cryptographic techniques that can support encryption at line speed. LPsec tends to be secure according to current standard and introduces negligible delay in data transmission.

Although quantum communication is inherently secure, it faces different challenges. We explore two such challenges in presence of no-cloning theorem i) qubit retransmission and ii) P2MP quantum communication (QP2MP). As qubits are prone to a variety of sources of noise, qubit retransmission can enhance the successfully transmission of qubits from source to destination. Similarly, QP2MP can enable multiparty quantum communication which is far less explored in discrete variable quantum systems. For these two tasks, we consider creating imperfect clones through Universal Quantum Cloning Machine. We propose a novel protocol Quantum Automatic Repeat Request (QARQ) inspired by its classical equivalent. We have shown than that QARQ can significantly increase the successful recovery of qubits. QP2MP communication is examined for direct transmission (DT)-which is currently implementable considering hardware availability, teleportation (TP)-which is the future of quantum internet, and telecloning (TC)-which is the combination of cloning and TP. In presence of different types of decoherences it has been shown that TC provides the best quality of the qubit state but it the most complex protocol in terms of quantum cost.

After studying challenges in qubit transmission, we presented Q^2PSK, a quantum way to perform Quadrature Phase Shift Keying (QPSK). Current transmission systems rely on classical data and classical channels, which are not inherently secure. A widely adapted approach to make them secure is encrypting the data via Quantum Key Distribution which provides the secure key exchange for data encryption and transmits them through a classical channel. Q^2PSK provides a mean of communication that can make classical data transportation inherently secured without using encryption. We came to the conclusion that together with Forward Error Correction, Q^2PSK has the potential to work with devices that meet certain requirements of the quality of the qubit state.

Resumen

Los sistemas de comunicación ópticos están muy extendidos y son los responsables de transportar el tráfico de datos desde el acceso a las redes metropolitanas hasta las redes centrales que dan soporte a las funciones de información y comunicación de la sociedad. Dado que el crecimiento del tráfico es cada vez mayor, se necesitan soluciones de redes ópticas más innovadoras y eficientes que las actuales para proporcionar al sector beneficios sostenibles a largo plazo. Además, con la llegada de los ordenadores cuánticos, estas redes son vulnerables a diversas amenazas a la seguridad. Por lo tanto, o bien se necesitan medios adicionales para que las redes sean seguras, o bien se requiere un transporte de la señal de datos asistido por la cuántica. Teniendo en cuenta los retos que plantean los aspectos de eficiencia y seguridad de las redes ópticas actuales, esta tesis doctoral pretende proporcionar técnicas para conseguir redes ópticas eficientes y seguras.

El actual patrón de tráfico de datos en diferentes segmentos de las redes ópticas puede ser un factor clave para hacer la arquitectura más eficiente. Estos patrones de tráfico suelen atenderse mediante el despliegue de conexiones punto a punto (P2P), que pueden no ser la solución más rentable en determinados segmentos como el acceso y la agregación metro. Esta tesis doctoral estudia tecnologías que soportan conexiones punto a multipunto (P2MP) para dar servicio a flujos de tráfico de datos dinámicos y heterogéneos. Una tecnología bien conocida conocida como Digital Subcarrier Multiplexing para implementar la conexión P2MP se utiliza como referencia para evaluar el rendimiento de una tecnología novedosa denominada Optical Constellation Slicing, para atender los mismos requisitos de tráfico dinámico y heterogéneo. Para un perfil dinámico, estas dos tecnologías se comparan con la tecnología tradicional que soporta P2P. En todo momento se analiza el coste, la eficiencia del caudal de datos y la simplicidad de la arquitectura. Se demuestra el potencial de las conexiones P2MP.

Para que las redes ópticas sean seguras, se realizan estudios en dos dimensiones. En primer lugar, se aborda la vulnerabilidad de la capa física. Para que la red en su conjunto sea más segura, se estudian métodos de criptografía de la capa física. En

segundo lugar, se investiga la tecnología de comunicación cuántica porque está intrínsecamente asegurada por las leyes de la mecánica cuántica.

Para la seguridad de la capa física, proponemos LPsec (lightpath security), cuyo objetivo es proporcionar una solución completa de seguridad desde los métodos de intercambio de claves en la capa física hasta la investigación de técnicas criptográficas que puedan soportar el cifrado a velocidad de línea. LPsec tiende a ser seguro según la norma actual e introduce un retardo insignificante en la transmisión de datos.

Aunque la comunicación cuántica es intrínsecamente segura, se enfrenta a distintos retos. Exploramos dos de estos retos en presencia del teorema de no clonación i) la retransmisión de qubits y ii) la comunicación cuántica P2MP (QP2MP). Dado que los qubits son propensos a diversas fuentes de ruido, la retransmisión de qubits puede mejorar el éxito de la transmisión de qubits del origen al destino. Del mismo modo, QP2MP puede permitir la comunicación cuántica multipartita, que está mucho menos explorada en los sistemas cuánticos de variables discretas. Para estas dos tareas, consideramos la creación de clones imperfectos a través de la Máquina Universal de Clonación Cuántica. Proponemos un novedoso protocolo Quantum Automatic Repeat Request (QARQ) inspirado en su equivalente clásico. Hemos demostrado que QARQ puede aumentar significativamente la recuperación exitosa de qubits. Se examina la comunicación QP2MP para la transmisión directa (DT) -que actualmente es implementable teniendo en cuenta la disponibilidad de hardware-, el teletransporte (TP) -que es el futuro de internet cuántico- y la teleclonación (TC) -que es la combinación de clonación y TP-. En presencia de diferentes tipos de decoherencias, se ha demostrado que TC proporciona la mejor calidad del estado qubit, pero es el protocolo más complejo en términos de coste cuántico.

Tras estudiar los retos que plantea la transmisión de qubits, presentamos Q^2PSK, una forma cuántica de realizar la codificación por desplazamiento de fase en cuadratura (QPSK). Los sistemas de transmisión actuales se basan en datos y canales clásicos, que no son intrínsecamente seguros. Un enfoque ampliamente adaptado para hacerlos seguros es cifrar los datos mediante la distribución cuántica de claves, que proporciona el intercambio seguro de claves para el cifrado de datos y los transmite a través de un canal clásico. Q^2PSK proporciona un medio de comunicación que puede hacer que el transporte clásico de datos sea intrínsecamente seguro sin utilizar encriptación. Llegamos a la conclusión de que, junto con la corrección de errores hacia delante, Q^sPSK tiene potencial para funcionar con dispositivos que cumplan ciertos requisitos de calidad del estado de los qubits.

Poster

Techniques for Efficient and Secure Optical Networks

Masab Iqbal

Industry

New use cases of 5G and beyond make data traffic more dynamic and heterogenous at optical transport. Additionally, quantum computers provide security threats to classical optical communication.

There is a demand for making optical networks more efficient to provide the industry with long-term sustainable profits. Security threats need quantum communication to be robust, which faces several challenges. Hence, *techniques for efficient and secure optical networks* are needed.

Demand

Solution

Point-to-Multipoint optical technologies are potential contenders to provide cost-effective solutions. Qubit retransmission protocols can improve quantum performance, and Point-to-Multiple-Point Quantum Communication can enable multiparty communication.

The result encompasses the development of novel techniques like Optical Constellation Slicing (OCS), Light Path SECurity (LPsec), Quantum Automatic Repeat Request (QARQ), and Quantum Quadrature Phase Shift Keying (Q^2PSK). These techniques make optical network cost-effective, secure than ever, improve quantum performance, and make classical data inherently secure.

Results

Societal Value

OCS simplifies network architecture, LPsec provides additional security, QARQ helps quantum communication to be robust, and Q^2PSK make classical data inherently secure.

Table of Contents

Page

List of Figures

Page

List of Tables

Page

Chapter 1

Introduction

1.1 Motivation

Due to some of the key properties of optical technologies such as high bandwidth, low latency, and high reliability, the applications of optical technologies are massive [EON16]. Many telecommunications firms employ optical fiber to deliver telephone signals, Internet communication signals, and cable television signals. It is also employed in a variety of different areas including as medical, defense/government, data storage, and industrial/commercial. This is not only limited to the core network but also in the metro and even in the access network segments [Ve13] supporting society's information and communication functions. In addition, these applications cause massive growth in data traffic which becomes heterogenous and dynamic in nature. This demands more innovative and efficient solutions other than the existing ones to provide the industry cost effective solution. Furthermore, with the introduction of quantum computers, these networks are subject to a range of security concerns, necessitating the use of extra security measures or the use of quantum-aided data signal transportation. Because of these challenges present in optical networks' regarding efficiency and security, this PhD thesis focuses on developing solutions for *efficient and secure optical networks*.

For the long-term profits, it is required to use the most efficient and cost-effective technologies in each segment of the optical network, from core to metro and access [He20]. The current data traffic pattern in the different segments can be a key factor to make the architecture more *efficient*. Network operators are dealing with dynamic and heterogenous traffic requirements with the advent of massive deployment of 5G and beyond services, high-quality video streaming, and rise in Internet-of-things (IoT). Also, the traffic flows differ between core and metro networks. In metro-aggregation networks, traffic follows a hub-and-spoke pattern where a few high-

capacity nodes called hub, receive/transmit data from/to large number of low-capacity nodes called spokes and also serves as an interface with a metro-core or regional network. Currently, these traffic patterns are served as point-to-point (P2P) connections which might not be the most efficient way of connecting large number of low rates spoke nodes to a hub node. The alternative solution is to use point-to-multipoint (P2MP) connections in which one node at the hub serves several nodes at the spokes. This can also help to transport P2P, P2MP, and a mix of P2P and P2MP traffic fulfilling the requirement of current varied data traffic. By P2P connections not only all these transceivers are likely costlier than using fewer higher rate transceivers, but this can also entail a sub-optimal usage of the router/switch capacity at the hub node(s) [Ba20]. To support highly dynamic traffic P2MP connections might be beneficial.

This PhD thesis explores the advantages of P2MP connections over P2P connections.

The studies are conducted in two dimensions to ensure the *security* of optical networks. First, the physical layer's vulnerability is targeted. Methods for physical layer cryptography are investigated in order to improve the overall security of the network. Second, quantum communication is being studied because it is inherently secure under quantum physics laws.

At the physical layer, optical networks are vulnerable to a variety of attacks such as eavesdropping, physical infrastructure attacks, interception, and jamming (refer to [Fo11] for a survey on the topic). Most of the previous works focused on the upper layers, leaving the optical layer for pure transport. However, the security of the optical layer should not be overlooked, as building a secure platform on top of an unsecure one is a risky practice. Designing a security solution involves combining multiple technologies for key distribution and data encryption and decryption, among others. For the former, although Quantum Key Distribution (QKD) provides secure key agreement and initial experimental deployments of QKD are being currently reported (see, e.g., [AgA20]), it is not expected to be available in the near future. With regard to encryption, there are several solutions, from stream ciphers (each incoming plaintext digit is encrypted sequentially) to block ciphers (where plaintext digits are grouped into blocks and then encrypted together). Salsa20 and ChaCha [Be08] are examples of stream ciphers and Advanced Encryption Standard (AES) [AES01] is the most extended block cipher. However, one of the main challenges for securing the optical layer is that encryption and decryption need to operate at line speeds and should not introduce any meaningful delay to the optical transmission; That is the reason why studies need to be done to provide high speed cryptography techniques which is the target of this PhD thesis.

Currently, cryptography of the classical communication is based on the mathematical complexity of the ciphers. As, quantum computers are becoming mature with sufficient computational resources, they could soon pose a threat to classical mathematical ciphers. Considering this, quantum technology based on the principle of quantum mechanics might be a solution to secure communication whose

information-theoretical security is guaranteed by the fundamental principles of quantum mechanics [Lo99] [Sh02]. But despite of the advantages that the quantum technology provides, certain tasks cannot be performed perfectly mainly because of the no-cloning theorem [Wo82]. The main challenges are qubit retransmission and P2MP quantum (QP2MP) communication. In consequence, this PhD thesis also explores solutions to these challenges and it also provides means to perform classical tasks by quantum means that would be inherently secure.

1.2 Goals of the thesis

In the light of the above discussion, the PhD thesis focuses on studying the classical ciphers that can be designed for easy implementation at the optical layer while supporting line speed. As various advanced applications are much more cost effective when implementing high-bitrate low-latency P2MP connectivity, techniques to implement P2MP connections in coherent communication will also be explored. Also, secure quantum communication will be part of the study as it provides inherent security for data transmission.

Specifically, the following goals are defined to achieve this main objective:

G.1 – Fast cryptographic schemes for secure optical connections

This goal targets at designing a cryptographic scheme that is fast enough to support high speed optical communication. In this regards, studies of fast pseudo random number generators (PRNG) and encryption techniques on optical layer along with key generation, key expansion and key exchange on physical layer are the main targets.

G.2 – Secure and efficient P2P and P2MP optical communication

This goal focuses on finding the secure and efficient P2P and P2MP configurations that are especially required to meet the dynamic and heterogenous traffic demand of these days. The studies of these configurations are done to provide service providers with cost effective solutions for long-term sustainable profits. G.1 will help implement the security part.

G.3 – Addressing challenges of secure quantum communication

This goal addresses three major issues: i) qubit retransmission; ii) point-to-multipoint quantum communication (QP2MP); and iii) performing classical communication quantumly. In presence of the no-cloning theorem, the target is to develop simple techniques to do qubit retransmission and QP2MP while maintaining reasonable quality of qubits' states. As quantum communication is inherently secured, a mean to perform classical quadrature phase shift keying (QPSK) using quantum modulation is also investigated.

A summary of the goals of the Ph.D. thesis is presented in Table 1-1.

Table 1-1: Thesis goals

Goals
G.1 **Fast cryptographic schemes for secure optical connections**
G.2 **Secure and efficient P2P and P2MP optical communication**
G.3 **Addressing challenges of secure quantum communication**

1.3 Methodology

In this PhD thesis, first classical cryptography is studied followed by classical P2MP communication. Then challenges of quantum communications are addresses that utilize the knowledge of classical cryptography and P2MP.

This Ph.D. thesis assumes the architecture in Figure 1-1 that shows the complete optical link used to achieve G.1 and G.2 with coherent detection. The optical link includes the following:

i) An optical transmitter that generates the data to be transmitted on optical fiber channel. A Forward error correction (FEC) encoding is applied before sending the data to receive error-free signals. A modulator that modulates the signals. In this PhD thesis higher order modulation formats such as 16,32,64-QAM are considered.

ii) Fiber channel simulates the signal propagation in fiber. Split-step Fourier method (SSFM) is used to solve non-linear Schrodinger equation for this purpose using MATLAB.

iii) An optical receiver that performs the coherent detection of the signals, apply digital signal processing to compensate chromatic dispersion (CD) and apply FEC decoding to receive the demodulated signals.

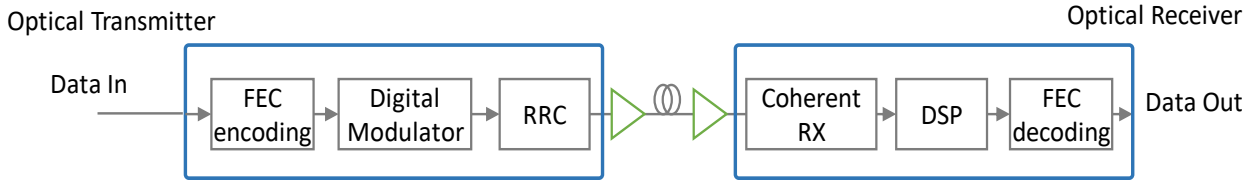


Figure 1-1: Overview of the proposed architecture. FEC (Forward Error Correction), RRC (Root-raised Cosine), and DSP (Digital Signal Processing).

To carry out the studies needed to meet the goals of this PhD thesis, the methodology in Figure 1-2 has been followed.

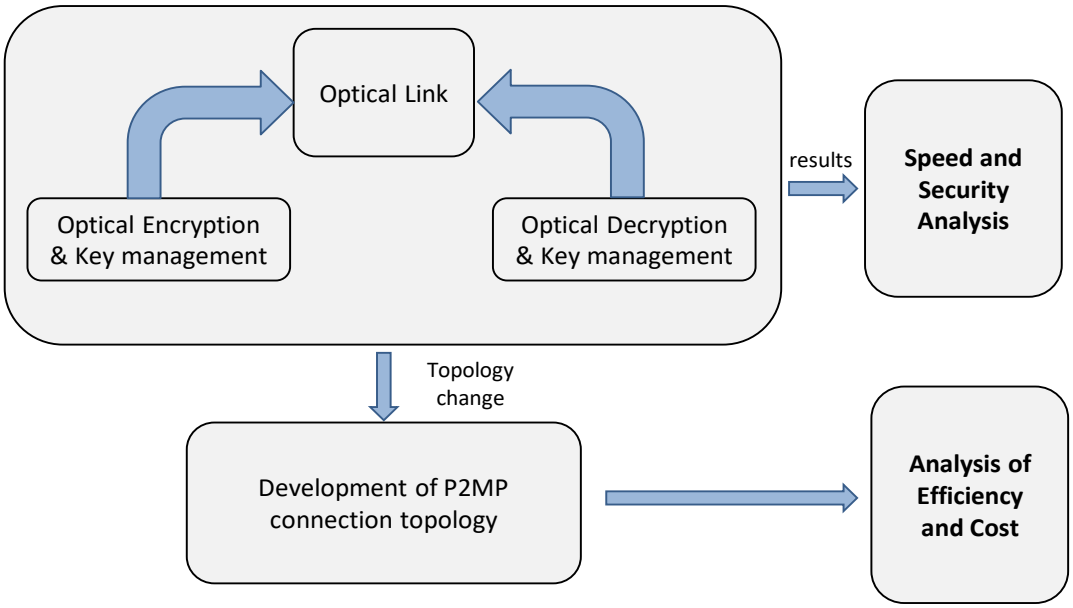


Figure 1-2: Methodology to be followed for G1 and G2

As the starting point of this PhD thesis, we developed a simulation environment on MATLAB to simulate a coherent optical communication link to demonstrate the optical encryption at the physical layer. Later, suitable optical encryption and decryption techniques are explored along with key management that can be implemented at line speed without introducing significant delays. These techniques can be applied on already developed optical links. In the end, performance of the optical cryptography is evaluated in terms of speed, delay, and overall security of the system.

Next, the possibilities of making the currently deployed optical connections more efficient, are studied. In this regard, the techniques for P2MP connection that can support P2P traffic and P2P+P2MP traffic at the same time are investigated. This can use the same secure optical link developed above. To understand the feasibility of the proposed scheme, analysis of cost and efficiency is done for different scenarios.

To achieve G.3, as it is a very new research field, a simulation environment for testing the quantum communication is developed. Two popular means of quantum networks: *i*) *direct transmission* networks that use a quantum channel for *qubit* transmission; and *ii*) *entanglement distribution* networks that use entanglement for transporting qubits are studied.

For qubit retransmission and QP2MP we create a non-perfect clone of qubit using a universal quantum cloning machine (UQCM) [Bu98]. The clone is then sent to the quantum channel (Figure 1-3). To analyze the performance of quantum system by using NetSquid [Co21]. It is a purpose-built simulator for modeling quantum networks. This simulator provides accurate modeling of quantum physical devices. Our goal is to investigate the effects of quantum memory, channel decoherence, quantum gate decoherence and imperfect entanglement. The qubit platform of nitrogen-vacancy (NV) center in diamond is the part of study.

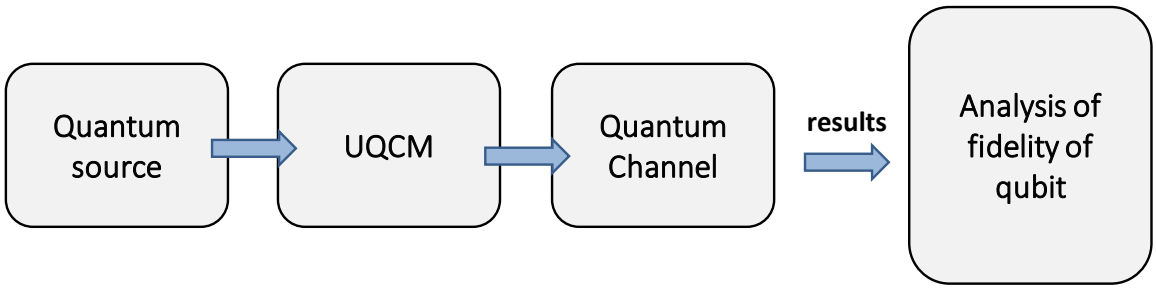


Figure 1-3: Methodology to be followed for G3

However, for quantum equivalent of QPSK, P2P quantum communication (QP2P) link is used. It is tested on IBMQ devices available on cloud and the analysis is performed to evaluate how far the current quantum hardware is to provide error-free quantum communication.

1.4 Thesis outline

The remainder of this Ph.D. thesis is organized as follows.

Chapter 2 provides the needed background on optical communication, cryptographic methods, P2MP communication and quantum communication.

Chapter 3 briefly reviews the state-of-the-art related to the objectives of this Ph.D. thesis such as fast and secure cryptographic schemes, secure and efficient P2P and P2MP communication and secure quantum communication.

Chapter 4 focuses on goal G.1 and covers physical layer cryptography. This chapter is based on the journal publication [JOCN22].

Chapter 5 relates to goal G.2 and investigates optical P2MP technologies. This chapter is based on the conference paper [OFC22]. A journal publication has been submitted [SENSORS23]

Chapter 6 concentrates on goal G.3 and is devoted to find the means of doing qubit retransmission and QP2MP communication. It is based on [ONDM22]. An extended version of this work has been submitted in Journal [JOCN23].

Chapter 7 focuses on goal G.3 and aims the to provide inherently secure quantum equivalent of classical QPSK communication. This chapter is based on submitted conference paper [CLEO23].

Finally, Chapter 8 concludes this Ph.D. thesis.

1.5 Contributions and References from the Literature

For the sake of clarity and readability, references contributing to this Ph.D. thesis are labelled using the following criteria: [<conference/journal> <Year(yy)[autonum]>], e.g., [ECOC20] or [JSAC21]; in case of more than one contribution with the same label, a sequence number is added.

The rest of the references to papers or books, both auto references not included in this Ph.D. thesis and other references from literature are labelled with the initials of the first author's surname together with its publication year, e.g., [Ve17].

Chapter 2

Background

In this chapter, we introduce the needed background of the core topics to be covered in this PhD thesis. We are proposing techniques for efficient and secure optical networks. For security, we provide solution to perform physical layer cryptography and explore quantum methods to make communication inherently secure. For that we provide the needed background for optical communication, cryptography and quantum communication. Optical communication deals with optical coherent communication. Cryptography section introduces some basic cryptographic concepts, such as ciphers, key extension, and key exchange. Quantum communication provides the basics of quantum information, qubit platforms and challenges that quantum communication face. For efficient optical networks we explore point-to-multipoint (P2MP) connections and discuss two technologies that support P2MP connection-optical constellation slicing (OCS) and digital subcarrier multiplexing (DSCM).

2.1 Optical communications

This section provides a short background related to advances in optical communication system. It also describes the coherent optical communication systems technologies on which the goals G1 and G2 are based. This section also describes the necessary knowledge to model optical communication system for simulation purposes used in this PhD thesis.

Since the advent of the laser and the discovery of its ability to transport data at a high rate over an optical fiber, optical communications systems and networks have advanced in all areas [Ag16]. To begin, the creation of pure silica optical fibers allows light to be transmitted via optical systems based on C-band at low attenuation

regimes of roughly 0.2 dB/km. Furthermore, the introduction of dispersion compensating fibers (DCF) in the mid-1980s to compensate for the chromatic dispersion (CD) effect in optical fiber propagation resulted in a major improvement in optical communications systems [Gr05]. The early commercially available optical communications systems intensity modulation and direct detection (IM/DD) [Ag16]. However, the necessity to increase the capacity and reach of optical communications systems leads to the development of numerous advanced technologies. The optical coherent detection technology, polarization division multiplexing (PDM), digital signal processing (DSP) blocks, and developments in optical amplification, primarily based on erbium-doped fiber amplifiers (EDFA) [EDFA02], are among the most notable. Among these innovations, coherent communication is the prominent one and part of the PhD thesis. This is a technology that combines modulation of the amplitude and phase of light, as well as transmission across two polarizations, to transfer significantly more information across a fiber optic cable. It uses DSP at both the transmitter and receiver to provide superior optical performance.

There are three basic building blocks of a coherent optical system: i) Transmitter; ii) Fiber channel; and iii) Receiver. At the transmitter, to transmit data signal optically, an optical carrier signal (laser light) is required to traverse the electrical data optically. The laser light is modulated by a modulator before transmission over the fiber channel. During propagation, the signal is amplified periodically after each span to compensate fiber losses. The fiber channel affects the signal with different linear impairments (LI) and non-linear impairments (NLI). In the first category lies attenuation, chromatic dispersion (CD) and polarization mode dispersion (PMD). While, the Kerr effects and inelastic scattering effects are due to the fiber non-linearity. The receiver converts the optical signal into electrical one by means of coherent detection. At the receiver the signal is processed digitally to recover data by mitigating linear and non-linear impairments. FEC is also used at the transmitter to potentially correct the received bit sequence.

The nonlinear Schrodinger equation (NLSE) can be used to model nonlinear optical fiber propagation in single mode fibers (SMF) for one polarization by [Ma97]

$$\frac{dE_x}{dz} = -\frac{\alpha}{2}E_x + \frac{j\beta_2}{2}\frac{d^2}{dt^2}Ex - j\gamma\frac{8}{9}(|Ex|^2 + |Ey|^2)Ex \qquad (2\text{-}1)$$

where Ex and Ey are the complex envelope of the propagated signal at x and y polarization, respectively, at time t and distance z. The α, β_2 and γ are the fiber attenuation, dispersion, and nonlinear parameters, respectively. Considering the averaged random evolution of the polarization effects over long optical fiber distances, as well as ideal transceivers (TRx), the Eq. (2-1) can be generalized for both polarizations [ZhQ19]. Additionality, because Eq. (2-1) does not have analytical solution, the SSFM was proposed to numerically solve it at the cost of high computational requirements due to large number of fast Fourier transform (FFT) and inverse FFT (IFFT) at each step considered. To face the trade-off between accuracy and computational requirements, other models have been proposed mainly

focus on the estimation of the accumulated NLI noise power, such as the Gaussian noise (GN) model [Po12], [Po14], at the cost of assuming some uncertainties and thus, leading to higher optical network design margins. However, recently, some studies show the good accuracy of GN model in multi-vendor optical networks [Fe20], [Cu22]. In this PhD thesis, SSFM is used to solve the NLSI

Eq. (2-1), models optical fiber propagation of an optical signal considering three effects: the fiber losses, CD, and Kerr nonlinearities effects. Firstly, to compensate the fiber losses while increasing the communication reach, optical amplifiers (OA) are used. Particularity, in C-band, EDFA are employed to amplify the optical signal at the cost of introducing amplified spontaneous emission (ASE) noise to it [EDFA02]. The ASE noise accumulation can be modeled by additive white gaussian noise (AWGN), and it is considered LI noise. Regarding the CD, it is basically caused by the dependence of phase velocity of a wave on its frequency. Since, the modulated light in not monochromatic in nature, different frequency components observe different phase shifts. Consequently, cause the broadening of short pulse and resulting in significant inter-symbol interference (ISI). Nowadays, the CD is mainly compensated by digital back propagation (DBP)-based DSP methods at the coherent Rx side, without implementation of in-line DCF, these kinds of systems are referred as dispersion uncompensated optical systems [Po12]. Finally, the Kerr nonlinearities effects are the main source of NLI noise in nowadays optical communications, the two main contributors are the self-phase modulation (SPM) and the cross-phase modulation (XPM)[NFO13]. Consequently, the NLI noise is highly associated with the number of wavelengths in a WDM signal, as well as, the optical power, transmission distance, signal configuration, etc., of each transmitted channel. All those parameters will lead to several signal-nonlinear interaction that will lead to several impacts of the NLI noise in an optical system. Recently, machine learning (ML)-based methods have been proposed to NLI noise mitigation due to their natural capability of understand nonlinear interactions between inputs and outputs.

2.2 Cryptography

This section first introduces some basic cryptographic concepts, such as ciphers, key extension, and key exchange that are used in achieving G1.

In cryptography, a cipher is an algorithm that transforms a plaintext message *(m)* into a ciphertext *(c)* (encryption), and vice versa (decryption). There are several types of ciphers, e.g., a substitution cipher encrypts units (e.g., each letter in a text) of plaintext by replacing them with the ciphertext with the help of a key. The receiver performs the inverse process to recover the original plaintext. Although the number of substitution alphabets might be large, substitution ciphers can be broken by frequency analysis.

To show that a cryptosystem is secure, mathematical modeling and proofs are used to verify that it satisfies a set of security properties. In particular, the One-Time Pad

(OTP) cipher shows perfect security, as proved by Shannon in [ShC49]. OTP encrypts m using a key (k) with the same length of m (denoted as n), by just implementing a bitwise XOR operation. Two important properties of XOR are: i) if k is uniformly distributed on $\{0,1\}^n$ then, the ciphered message $m \oplus k$ is also uniformly distributed; and ii) the inverse operation (decryption) consists on applying the XOR function with the same (symmetric) key k, i.e., $m \oplus k \oplus k = m$. Although OTP shows perfect security, it does not fit well for stream ciphers, where the length of the messages tends to infinity. Semantic security provides a weaker notion of security that allows to build secure ciphers that use reasonably short keys. That entails splitting the data stream into chunks of data of predefined size. However, k cannot be reused from one data chuck to another, as that would reduce the security level. Nonetheless, k can be extended using a cryptographically secure PRNG to generate a sequence of stream keys (k_s).

Salsa and ChaCha are fast and secure stream ciphers that are appropriate for practical use and variants of them are being used in widely deployed protocols, such as Transport Layer Security (TLS) [Ni18]. The PRNGs use a 256-bit seed, a 64-bit nonce, and a 64-bit counter to form a 512-bit block to create up to 2^{64} 512-bit pseudo random blocks. The design of these stream ciphers is highly parallelizable to speed-up encryption [Be08].

Block ciphers can be used as well to build a stream cipher; one popular block cipher is AES. In AES, an input block of 128 bits is processed as a 4×4-byte matrix. The AES algorithm performs 10, 12 or 14 rounds depending on the size of the cipher key (128, 192 or 256 bits). The process begins with the expansion of the initial key to produce a series of keys used in each round. At every round, the encryption begins by adding the round key as a XOR cipher followed by a non-linear byte substitution through a predetermined substitution table. Then, row shifting followed by a mixing of columns and round key addition are performed. The procedure is repeated until completing the required number of rounds. Decryption is performed in the inverse manner.

The Diffie Hellman (DH) key exchange is a solution to exchange keys between two parties, Alice and Bob, that want to establish a secure communication channel. Both parties generate private (integer) keys k_p (i.e., k_a *and* k_b) and their related public keys k_P (i.e., k_A *and* k_B). The public keys are shared over the insecure channel, and each party computes the symmetric key k that is used for data encryption using their own private key k_p and their counterpart's public key k_P.

2.3 Optical constellation for optical constellation slicing

In this section, we concentrate on optical constellation (OC) and how it is generated. The optical constellation slicing (OCS) mainly depends upon OC which is one of the

novel parts of the PhD thesis and it can give an insight of how to perform slicing in OC.

OC is a way to represent an optical signal modulated by a digital modulation scheme, such as m- quadrature amplitude modulation (QAM) signals. Where m is the modulation format. Typically, at the optical Tx, the optical signal is generated by using an optical laser and an in-phase/quadrature (IQ) modulator [Xi17], [Se19]. The IQ modulator is responsible to modulate the waveform generated by the optical laser in accordance with the input data bits to be transmitted, following a constellation mapping. The main function of the mapping is to assign the proper amplitude levels corresponding with the I and Q components of the respective symbols. For that purpose, the input sequence of bits to be transmitted is grouped by a number of bits creating the symbols. The number of available symbols is given by the m and the number of bits transmitted by each symbol is given by the $\log_2 m$. For example, 16-QAM signals are characterized by 16 symbols each one carrying 4 bits. Normally, the mapped symbols are represented by complex numbers, where the real part corresponds to the I component and the imaginary part to the Q component of the optical signal. Thus, an optical signal is represented by a sequence of complex numbers, representing the respective symbols. Assuming an ideal Tx and the Gray mapping. Figure 2-1 represents the constellation of a 64-QAM signal.

These OCs play vital roles in performing OCS. Figure 2-2 explains the detail of how it can used to create slices in OCS. The first step in performing OCS is to choose the modulation format (m-QAM) that provides the highest achievable throughput and the maximum number of OCSs. As the lowest number of constellation points that may be allocated to a single OCS is two (each point representing a single data bit), the maximum number of simultaneous destinations is m/2.

The next step is to create the OCSs. The OCSs are created by dividing the symbol digitally in two parts <prefix, infobits>. Prefix indicates the destination that the data signal is sent to while the infobits represents the actual information. E.g., in Figure 2-2, the constellation is divided into four equal parts and sets of 4 bits are selected for each OCS whereas 2-bits are selected as a prefix to indicate the RX identity. Thus, each RX is served by an OCS formed from a unique <prefix, infobits> pair. Note that prefixes might be of different lengths. The prefixes are decided according to the constellation map. RX decodes the symbols according to the prefix.

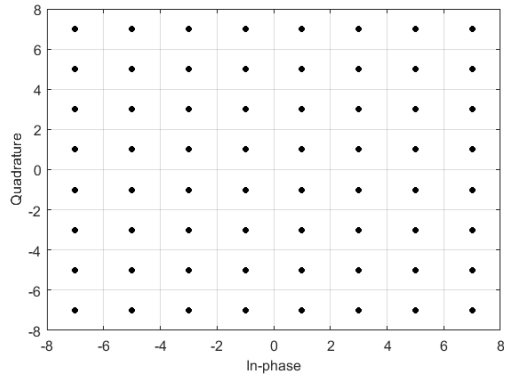


Figure 2-1 64-QAM Mapping

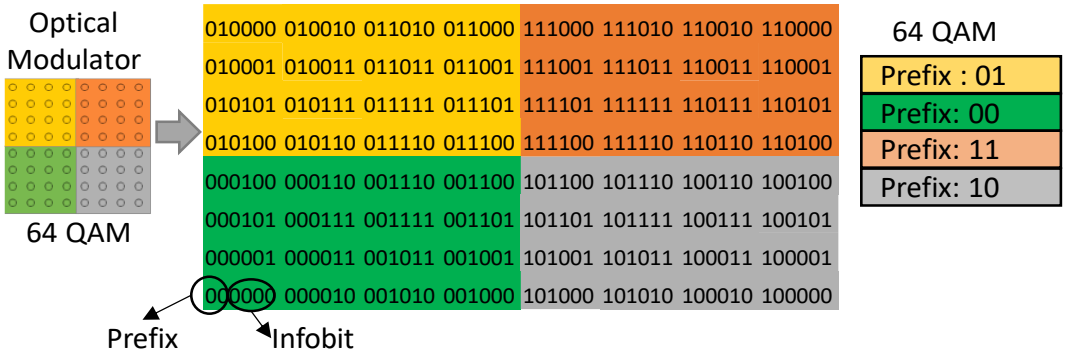


Figure 2-2 Optical constellation Slicing

2.4 Digital subcarrier multiplexing

DSCM systems have been proposed to increase the overall capacity and flexibility of the optical networks [Su20, We21, Ve21, [Infinera.1]. It is a key technology to provide more freedom in coherent optical networks design and management, offering the possibility to propagate an optical channel with multiple digital independent SC.

DSCM shows significant benefit in both point-to-point (P2P) transmission working at high symbol rates [Su20]) and in P2MP network topologies [We21]. The former, by employing an 8 DSCM signal powered by advanced parallelized DSP blocks and probabilistic constellation shaping (PCS) for 800G and beyond applications. The latter, taking advantage of the multiple independent subcarrier (SC), can offer a finer granularity in optical network resources assignment and management, from 25G up to 400G, which play an important role in future metro aggregation optical networks where the data traffic mainly follows a hub-and-spoke pattern [Ho22].

Following, we introduce Eqs. (2-2), (2-3) and (2-4) which govern the DSCM systems. The total DSCM signal is defined by [Ra17]

$$S_{DSCM}(t) = \sum_{i=1}^{N} S_i(t).\, e^{j2\pi f_i t} \tag{2-2}$$

where N is the total number of SC and f_i is the frequency shift applied for a given generated signal S_i to create a SC, it is defined by:

$$f_{i=1\ldots N} = \left[(i-1) - \frac{N-1}{2}\right].\Delta f_{SC} \tag{2-3}$$

where Δf_{SC} is the spectral width of one single SC, given by:

$$\Delta f_{SC} = \frac{R_s}{N}\,(1+\beta) \tag{2-4}$$

where R_s is the total symbol rate and β is the roll-off factor of the digital root-raised-cosine filter (RRC) used to optical signal shaping. Notice that, by Eq. (2-3), we considered a SC spectral assignment from low to high frequencies.

Figure 2-3 illustrates the basic step by step digital process at the optical Tx to create a DSCM signal. Firstly, generation of N pseudo-random binary sequences (PRBS) mapped by QAM formats and shaped by RRC filters is performed. Then, applying the frequency shift f_i computed by Eq. (2-3) and, finally, combining all the SC by means of an optical multiplexer, creating the DSCM signal, S_{DSCM}, to be propagated through the optical fiber.

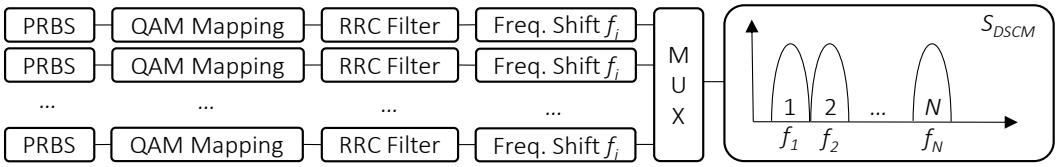


Figure 2-3. DSCM signal generation process at the optical coherent Tx.

DSCM signals are characterized to be more robust against the NLI noise because, normally, they are working inside the NLI "sweet spot" in term of symbol rates [Infinera.1, i.e., from 4GBd to 16GBd per SC. However, the impact of the NLI noise is lower, leading to mild to low nonlinear optical transmission regimes.

2.5 Quantum communication

This section gives the background on current quantum computing technologies and the challenges that it faces. Some key metrics to gauge the performance of quantum protocols are also described here. Quantum communication with focus on direct transmission (DT)-where qubit uses quantum channel to traverse, teleportation (TP)-which uses correlated qubits to avoid qubit to use quantum channel, and

telecloning (TC)-which is the combination of creating close copies of qubit and TP, are the main focus here.

Quantum communication involves moving away from classical forms of communication to instead take advantage of the laws of quantum physics. Classical computers send data as classical bits of either 0 or 1, whereas quantum computers communicate via the transmission of quantum states. The latter rely on qubits, where data is sent as superposition of 0 and 1. Similarly as classical logic gates, quantum computers use quantum gates to perform quantum operations that change the qubit's state to a desired one [BeC19].

Various platforms are available for quantum computing: superconducting qubits [Ri22], trapped ions [Pn22], and Nitrogen-Vacancy (NV) -centers in diamond [LiY22], to name a few. Each platform possesses its own pros and cons. Superconducting quantum computing implements quantum computing with superconducting electronic circuits. Superconducting qubits have fast decoherence times and gate operation, but they must also be kept in the extreme cold, which is costly and troublesome. Trapped ion computers –charged atomic particles are confined and suspended in free space– have longer decoherence times compared to superconducting quantum computers. While a trapped ion computer can run at room temperature, the ions must be cooled for optimal performance and they are slower than a superconducting qubit. Finally, the NV-center platform uses an electron spin inside a NV-center in a diamond lattice. It has a long coherence period and high gate decoherence but it can be operated at room temperatures. All three platforms tend to face qubit decoherence as the qubits are very fragile. This is the main limitation in quantum communication and needs to be carefully addressed. In this PhD thesis we use the NV-center platform for analysis and simulation because it makes possible to send quantum states far away to connect and entangle NV-centers over distance making quantum internet possible. Furthermore, diamond spin qubits [Hu20] enable quickly establishing robust entanglement links, which is one of the primary requirements of quantum networks.

When developing any quantum network protocol, a good metric to quantify the protocol's performance is fidelity, a purely quantum phenomenon. It has a value between 0 and 1 and quantifies the state's quality in terms of how "close" it is to the desired state. A fidelity of 1 means it is in the desired state and a value equal or below 0.5 means that the state is no longer usable. In contrast to classical networks, where data must be delivered error-free, quantum applications can operate with imperfect quantum states as long as fidelity is greater than an application-specific threshold. For basic QKD, the threshold fidelity is about 0.8 [Ko20]. In this PhD thesis, we use fidelity as a metric to evaluate the performance of the proposed protocols for the three quantum technologies studied.

Importantly, fidelity and decoherence are interdependent. Reduction in fidelity occurs as we lose qubit coherence, which makes decoherence one of the critical

challenges in quantum networks. The loss of quantum state fidelity in a quantum network occurs in several ways:

1. Qubits interacting with the environment, mainly when traversing a quantum transmission channel. This is particularly relevant in the DT case and it limits the length that a qubit can traverse. However, this can be avoided by using entanglement distribution networks [WaY22] that allow the qubit to be transported without traversing the channel.

2. Imperfect entanglement reduces fidelity in entanglement distribution networks. Therefore, we can receive benefits from entanglement distribution networks only when it outperforms the fidelity degradation through the channel.

3. Coherence degrades a quantum state's fidelity while the qubits are stored in a quantum memory and it puts highly stringent requirements on how long qubits can be held in memory. Although lab tests have shown memory lifetimes of up to one minute, experiments with network connected devices show memory times reduced to just a few milliseconds [Ko20].

4. Imperfect implementations of quantum gates reduce fidelity whenever any qubit is processed.

This PhD thesis considers all the above loss of quantum state fidelity to evaluate QARQ and QP2MP.

2.6 Conclusions

This section has introduced the basic concepts that are needed to understand the rest of the work of the PhD thesis. Two domains are targeted: i) classical optical communication and ii) quantum communication. For classical communication Section 2.1 discussed coherent optical communication. Section 2.2 discussed the physical layer security concepts. Section 2.3 and 2.4 covered two technologies OCS and DSCM that make the optical communication efficient by simplifying architecture and data transmission methods. Section 2.5 provided the basics of quantum communication.

Chapter 3

Review of the State-of-the-Art

While the previous chapter presented the main background for the concepts related to this PhD thesis, in this chapter, we present a review of the state-of-the-art of the different goals with a twofold objective: ensuring that these goals have not yet been covered in the literature, and serving as a starting point for this research work.

3.1 Fast cryptographic schemes for secure optical connections

Security at physical level needs to be implemented to make the whole network secure. In this regard, some works have already been proposed regarding encryption solutions for the optical layer. In the context of passive optical networks, the authors in [Ab15] proposed the optical spectral phase and delay encoding technique, where the optical signal is split into multiple spectral slices that are multiplexed after applying a delay and phase shift to produce the encrypted signal. However, this method has a constraint of generating narrow spectral slices, putting stringent requirements on optical bandpass filters [Ab18]. The authors in [Li16] reported a physical layer security method based on a piecewise chaotic permutation of symbols and subcarriers. The method relies on an initial key, thus requiring the implementation of a key exchange strategy. Recently, authors have shown the chaos-based encryption on physical layer for WDM networks [ZhA21] but decryption is also highly dependent on the synchronization of sent and received signal. Chaos-masking (CMS) encryption techniques for long distance communication is proposed in [Ji21]. However, this scheme does not provide sufficient security if high confidentiality is required. In access networks, Optical Code Division Multiple Access (OCDMA) provides intrinsic confidentiality through multiple access interface noise [ShT05],

[JiZ06]. Nonetheless, eavesdropping by coded waveform analysis was reported in [Si10] and data interception by differential detection was reported in [Da10]. Optical steganography has been proposed and demonstrated for wavelength-division multiplexing (WDM) systems [Wu08], [Kr07], [Wa11]. This technique hides the signal from the eavesdropper, e.g., through dispersion, to avoid interception. Another option is to carry the signal in Amplified Spontaneous Emission (ASE) noise, as proposed in [Wu13].

Some vendors implement AES at the Optical Transport Network (OTN) layer [ADVA21], where key exchange can be carried out using header bytes of the Optical Data Unit (ODU) frame. Note that such a solution brings the additional requirement of implementing OTN, in addition to the intrinsic complexity of AES. In this case, AES is used as a block cipher that encrypts blocks of 128 bits.

To the best of our knowledge, no fast enough cryptographic schemes along with key management have been proposed so far that are specifically tailored to be implemented on physical layer and be fast enough to operate at line speed. The focus of this PhD will be to find these fast-cryptographic schemes and analyze the speed, delay, and security level of the proposed scheme.

3.2 Secure and efficient P2P and P2MP optical communication

Optical communication has experienced several innovative phases over the past decade mainly driven by the breakthrough technologies that resulted in improved network architecture. The main goal of these innovations is to reduce the cost per transported bit (CpB) that allows the operators to deliver high data to end users without raising much of their Capital Expenditure (CAPEX) budgets. Several inventions of such kinds like Erbium doped fiber amplifiers (EDFA), Reconfigurable Optical Add and Drop Multiplexing (ROADM), Photonics integrated Circuits (PIC), and coherent optical transmission, to name but a few, are widely adopted in modern optical transmission systems.

Delivering high date rate reduces CpB but it is only significant if the operators utilize the capacity of transceivers efficiently. The rise of internet traffic and forecast of its growth with the advent of new use cases by 5G Radio Access Network (RAN)s and Internet of Things (IoT) [CISCO], [Sc15], [NOKIA] will require further need of reducing CpB. In metro and access aggregation network, instead of using point to multipoint architecture (P2MP), where the source node sends data to a set of destinations that may be scattered over a geographical area [We21], point to point architecture (P2P), where a source node sends data to a single destination node is deployed requiring same number and same capacity transceivers at both ends of network. The traffic pattern in these networks usually follows hub and spoke

architecture where the total traffic is high but the traffic at the leaf nodes is relatively low. Although these networks will hardly be able to utilize all the capacity for several upcoming years, leaving us in dire need of continue minimizing CpB in current network [Ba20]. What follows are the possible solutions to do this.

Various advanced applications are much more cost effective when implementing high-bitrate low-latency point-to-multipoint (P2MP) connectivity. Just like P2P, P2MP connections can be supported in Wavelength Switched Optical Networks (WSON) (see, e.g., [Ru15]); we denote these connections as lightpaths and light-trees [Ru14], respectively. Indeed, when the required bandwidth is in the range of a few tens of Gb/s, using dedicated high-capacity optical transceivers to establish independent direct optical connections would be highly inefficient. Alternatively, one single light-tree could be set to support both the P2P and P2MP traffic. In this case, the data signals would reach all destination nodes, which would then filter the relevant data and drop the remaining one. However, this solution entails security considerations (e.g., eavesdropping).

In this PhD thesis, our target is to use one single light-tree to transport a combination of P2P and P2MP traffic. This solution could be implemented using digital subcarrier multiplexing (DSCM) technology [We21], [Ra13] and dedicate one or more independent subcarriers to support P2P traffic between the source and each of the destinations, as well as P2MP traffic from the source to all or a subset of destinations. However, providing dynamicity once DSCM is installed is still a challenge. The study will focus on alternative solutions that can reduce the cost while being more dynamic and efficient.

3.3 Challenges of secure quantum communication

Despite the advantages of quantum mechanics, there is a fundamental barrier: the no-cloning theorem [Wo82], which makes perfect quantum bit (qubit)-the fundamental unit of quantum information-duplication impossible. This renders some quantum network tasks impossible, such as qubit retransmission and point-to-multipoint quantum communication (QP2MP).

Also, a widely adapted approach to make them secure is encrypting the data via Quantum Key Distribution [WeS18], which provides the secure key exchange for data encryption and transmits them through a classical channel. Given the inherent properties of quantum principles, an alternative to classical channels could be to send classical data quantumly.

3.3.1 Quantum bit retransmision and QP2MP

The current quantum computers belong to the Noisy Intermediate Scale Qubits (NISQ) era [Pr18], capable of working with a small set of noisy qubits. The noisy

operations limit the functionality of the quantum devices and lead to a great challenge in near-term quantum networks: the loss of the qubit. Several effects can contribute to the loss of qubits. A possible solution to recover a qubit loss might be to use error-correcting codes [ShP95.2], but these cannot recover information if errors are beyond the error-correcting capability. The authors in [Yu21] proposed a technique for reliable connection based on a secret sharing scheme. However, such a solution is suitable for packet quantum networks only when there are low transmission errors.

In classical packet networks, the Transmission Control Protocol (TCP) implements an error-control mechanism for reliable and error-checked transmission of messages. It is based on a variant of the Automatic Repeat Request (ARQ) protocol which utilizes the storage and retransmission of bits.

Quantum internet is still in its infancy but as the quantum network hardware protypes are appearing, new challenges for quantum networks are beginning. For the building of scalable quantum network, we need more than mere physical hardware. To have the future quantum internet, network protocols must be defined. The real challenge in near-term quantum networks brought by quantum mechanics is decoherence which specifies the decay of quantum information with respect to time which put stringent requirement on storage times of qubits and what distance it can traverse. So far, quantum communication for point-to-point case is the center of attention and protocols are being developed for this [Ko20]. However, in the future, quantum P2MP communication will be required for the application of multicasting and broadcasting. For P2MP quantum communication, some protocols have already been studied. In [ShP19] author present broadcasting protocol for Platform as a Service (PaaS)" type of cloud computing. In [ZhN20] quantum broadcasting using partially entangled photons is described. But these schemes, do not consider the decoherence that qubit experience at different stages of transmission. In the PhD thesis, our goal will be to incorporate decoherence losses due to transmission delay and storage time in analysis and observe the final fidelity of qubit.

3.3.2 Performing classical communication quantumly

To make the classical data inherently secure, avoiding the need for key distribution and encryption, *superdense coding* [Mc08], a well-known quantum communication protocol used in quantum computing, can be exploited. Superdense coding transmits two classical bits using one quantum bit (qubit) –the basic unit of quantum information. We adopt such technique for classical communication and form a quantum equivalent to quadrature phase shift keying modulation (Q^2PSK) to transmit high-speed classical digital data.

3.4 Conclusions

In this chapter, we have reviewed the state-of-the-art of relevant works related to the goals of this PhD thesis. Table 3-1 summarizes the study.

Table 3-1: State-of-the-art summary

Goals	References
Fast cryptographic schemes for secure optical connections	[Ab15], [Ab18], [Li16] [ZhA21], [Ji21], [ShT05] [JiZ06], [Si10], [Da10] [Wu08], [Kr07], [Wa11], [Wu13], [ADVA21]
Secure and efficient P2P and P2MP optical communication	[CISCO], [Sc15], [NOKIA] [We21] [Ba20] [Ru15] [Ru14] [Ra13]
Challenges of secure quantum communication	[Wo82] [WeS18] [ShP95.2] [Pr18] [Yu21][Ko20] [ShP19] [ZhN20] [Mc08],

We can conclude that, although some previous works related to security at physical layer have been proposed, more improvements are needed in terms of speed to make it easily implementable on optical layer. Also, to serve the dynamic and heterogenous requirements of traffic for metro-aggregation networks, and to reduce CpB, new architectures and techniques need to be presented. Despite of the fact that quantum communication is inherently secure, it faces some challenges in terms of qubit retransmission and P2MP communication protocols. Protocols need to be developed and their feasibility must be tested considering the decoherences that qubit can go through.

As a conclusion of the review of state-of-the-art related to the goals of this PhD thesis, relevant niches have been identified. The next chapters present the works that occupy these niches and meet the goals.

Chapter 4

LPsec: A Fast and Secure Cryptographic System for Optical Connections

In this chapter, we focus on developing and analyzing optical cryptography.

The high capacity and low latency of optical connections are ideal for supporting the current and future communication services, including 5G and beyond. Although some of those services are already secured at the packet layer using standard stream ciphers, like Advanced Encryption Standard (*AES*) and ChaCha, secure transmission at the optical layer is still not implemented. To secure the optical layer, cryptographic methods need to be fast enough to support high-speed optical transmission and cannot introduce significant delay. Moreover, methods for key exchange, key generation and key expansion require that can be implemented on standard coherent transponders. In this work, we propose LPsec (Light Path SECurity), a secure cryptographic solution for optical connections that involves fast data encryption using stream ciphers and key exchange using Diffie-Hellman (DH) protocol through the optical channel. To support encryption of high-speed data streams, a fast, general purpose Pseudo-Random Number Generator (PRNG) is used. Moreover, to make the scheme more secure against exhaustive search attacks, an additional substitution cipher is proposed. In contrast to the limited encryption speeds that standard stream ciphers can support, LPsec can support high-speed rates. Numerical simulation for 16-QAM, 32-QAM and 64-QAM show that LPsec provides sufficient security level while introducing negligible delay only.

4.1 Introduction

As previously stated, while describing the motivation of this work in Chapter 1, optical networks, are vulnerable to a number of attacks such as eavesdropping, physical infrastructure attacks, interception, and jamming. Earlier research concentrated on the higher layers, leaving the optical layer for pure transport. The security of the optical layer, on the other hand, should not be disregarded, as establishing a secure platform on top of an insecure one is a dangerous practice.

In this work, we propose LPsec, an approach that includes tailored solutions for both key exchange and encryption/decryption so they can be easily implemented at the optical layer. For the key exchange, we design a mechanism based on the Diffie-Hellman (DH) key exchange [Ne04], where the initial public keys of the two end parties, i.e., the Transmitter (Tx) and the Receiver (Rx), are exchanged via the Software Defined Networking (SDN) controller and are periodically updated through the optical channel to enhance the security level. For encryption, we rely on two ciphers: i) a traditional stream cipher that uses a symmetrical key and ii) permutations of symbols. Each cipher has its drawbacks, but when combined they provide the required security level to encrypt data at 100s of Gb/s. Besides, LPsec exhibits negligible transmission delay.

The rest of the chapter is organized as follows. Section 4.2 provides our proposal to secure optical connections (LPsec), where the proposed encryption scheme is described, and the key exchange is outlined. Section 4.3 presents the details of key exchange, including the initial one and the periodic key updates. Then, the symmetric key generation and its expansion are detailed. Security analysis based on the Pseudo-Random Number Generator (PRNG) is also discussed. Section 4.4 details the building blocks of LPsec, including optical encryption and key management. As the operations are governed by Finite State Machines (FSM), their construction at the Tx and Rx are also discussed. Illustrative results are presented in Section 4.5, including the introduced delay and security level against several attacks. Finally, Section 6 draws the main conclusions of this work.

4.2 Secure optical layer

4.2.1 Implementing LPsec in an optical coherent system

LPsec requires extending the standard coherent transponder with optical encryption and decryption blocks, as well as with some key management functionalities (see Figure 4-1). In addition, cryptographic blocks need to operate at line speeds and should not introduce any significant delay to data transmission. To achieve such an objective, optical encryption should be based on simple operations performed on the

input bit stream. The main design aspects of the cryptographic techniques proposed in this work are analyzed hereafter.

As previously introduced, the encryption is based on two nested ciphers that provide a high security level. The outer cipher is a substitution cipher that relies on a Lookup Table (LUT) used for the substitution of bits before sending it to the modulator. This creates a ciphered gray map constellation through LUT permutations of incoming bits as suggested in Figure 4-2a. Note that there are $M!$ permutations in an M-Quadrature Amplitude Modulation (QAM) system (e.g., there exist more than 2^{44} permutations in a 16-QAM system) and thus, we can use a random key (k_l) of the appropriate length (i.e., 44 bits in the example), to select the permutation of the LUT. The inner cipher is a stream cipher that encrypts data chunks of predefined size based on a cryptographically secure PRNG to generate a sequence of stream keys (k_s). The proposed encryption system is sketched in Figure 4-2b, where output ciphertext c_2 is produced by the combination of the inner stream cipher E_1 and the outer substitution cipher E_2.

Note, however, that the sequence of stream keys $k_s = [k_{sj}]$ generated by the PRNG from a given key k cannot be infinite as this would reduce the security level of E_1. In addition, the LUT should be periodically regenerated to minimize the vulnerability of E_2. As a consequence, we limit the lifetime of keys k and k_l, e.g., to 1 sec., which entails new keys being periodically generated at the Tx and exchanged with the Rx. Specifically, the DH key exchange method is used to generate the symmetric key k. The Tx and Rx generate a random private/public pair of keys ({<k_r, k_R>} and {<k_t, k_T>}) and exchange their public keys (k_T, k_R) with the other party. The initial key exchange can be facilitated by the SDN controller, which can collect the public keys and send them to the counterpart. However, symmetric keys should have a short lifetime and they need to be frequently updated, which makes the SDN not a suitable option.

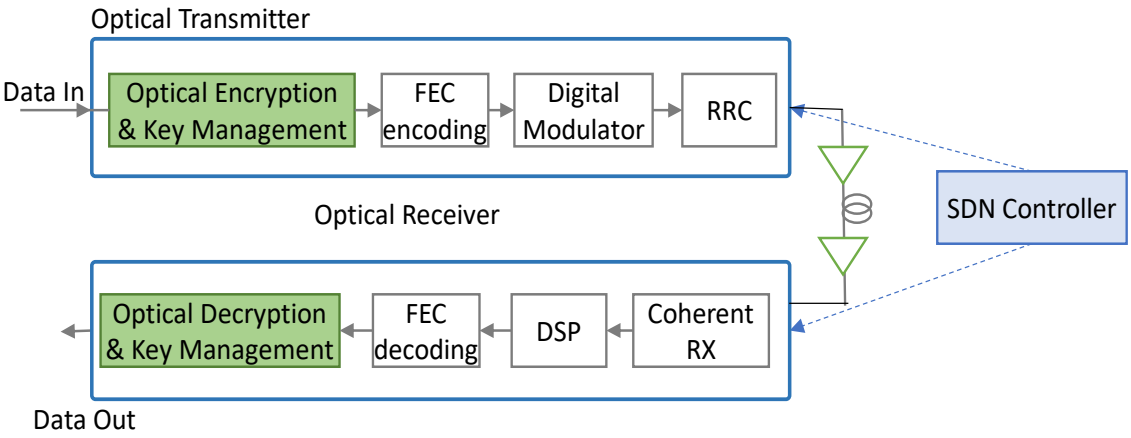


Figure 4-1 Optical communication system considered for the implementation of LPsec. FEC (Forward Error Correction) and RRC (Root Raised Cosine filter)

In our approach, we perform a partial key exchange, where only the Tx generates a new pair of keys <k_{ti}, k_{Ti}>, as well as a new key k_{li} for the next period i. Next, both the public key k_{Ti} and the new permutation LUT (k_{li}) are sent to the Rx through the optical channel. We propose to use a special frame (henceforth called Key exchange Frame, KxF) for the key exchange, (see Figure 4-2). A KxF is generated by the Tx and sent to the Rx periodically. The KxF includes a header of a fixed size that allows the Rx to detect its arrival. Because the Rx is not synchronized with the Tx for key exchange, any occurrence of the header pattern in the data stream must be prevented at the Tx side. Otherwise, the Rx would follow an erroneous key exchange procedure that will stop data transmission. The solution is to add escape bit sequences to break any KxF header pattern in the input data. To this end, two *Finite State Machines* (FSM) at the Tx and the Rx sides add and remove such escape bit sequences to/from the plain bit stream.

The next sections detail the design of LPsec, how keys are generated and exchanged, and how the FSMs are defined and particularized.

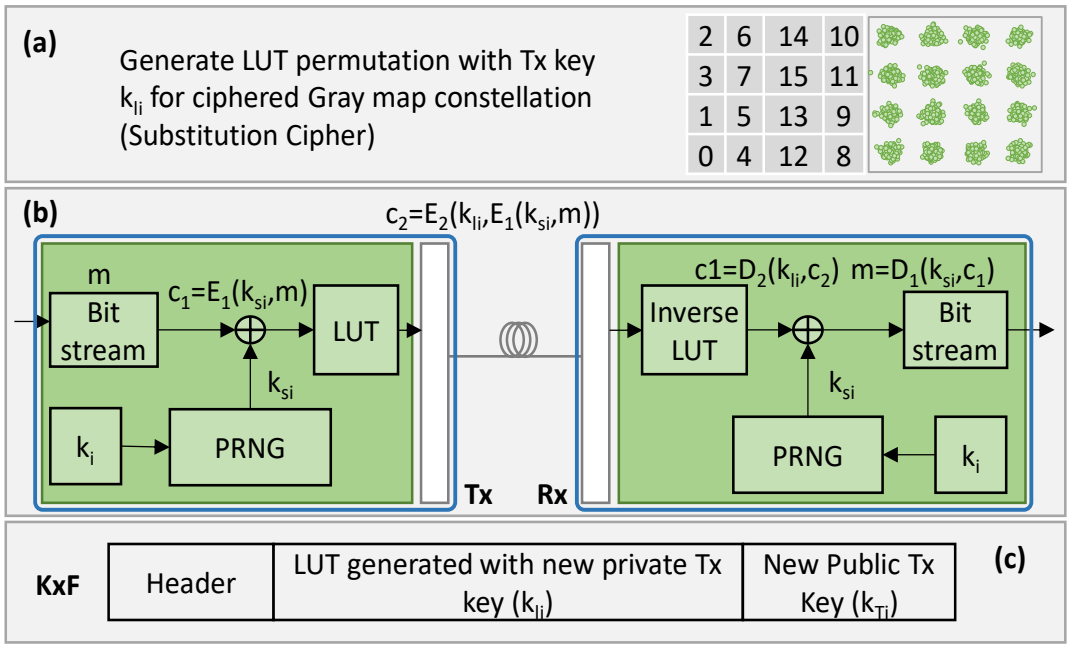


Figure 4-2 Overview of LPsec. Example of 16-QAM LUT for encoding (a), encryption / decryption (b), and frame structure for periodical LUT and key synchronization (c).

4.3 Keys and security level

This section first details the key exchange process, including the initial exchange and the periodical updates. The generation and expansion of symmetric keys is detailed next, after which the security level of the system is studied.

4.3.1 Key exchange

As introduced in Section 4.2, an initial key exchange is performed through the SDN controller and then, the Tx updates the Rx with the keys to be used through the optical channel. Figure 4-3 presents a sequence diagram detailing the computation performed by the Tx and Rx, as well as the messages exchanged through the control plane and the data and messages sent over the encrypted optical channel.

The initial key exchange is carried out at connection set-up through the SDN controller (messages 1-5 in Figure 4-3), which collects the public key of the Rx (1) and sends it to the Tx (2). The Tx generates a pair of private and public keys and a random key k_{l0}, which is used to generate the initial LUT permutation. In addition, the Tx generates the symmetric key k_0 with its private key and Rx's public key. Key k_0 is used at this time to generate the particular KxF header pattern that will be used for key exchange on the optical channel. Both FSM_{Tx} and FSM_{Rx} must be generated for that specific pattern. Before sharing the LUT, it is encrypted with symmetric key k_0 and sent together with the Tx public key to the SDN controller (3), which shares them with the Rx (4). Upon the reception, the Rx generates the symmetric key k_0 with its private key and Tx public key, generates the FSM, and decrypts the LUT. The Rx replies to the SDN controller when it is ready to start the secure communication and the SDN controller notifies the Tx (5), which generates a new set of private and public keys, the LUT, and the symmetric key for the next time interval. Then, the Tx replies to the controller that it is also ready, and the initialization phase concludes. At this time, the secure optical connection is established.

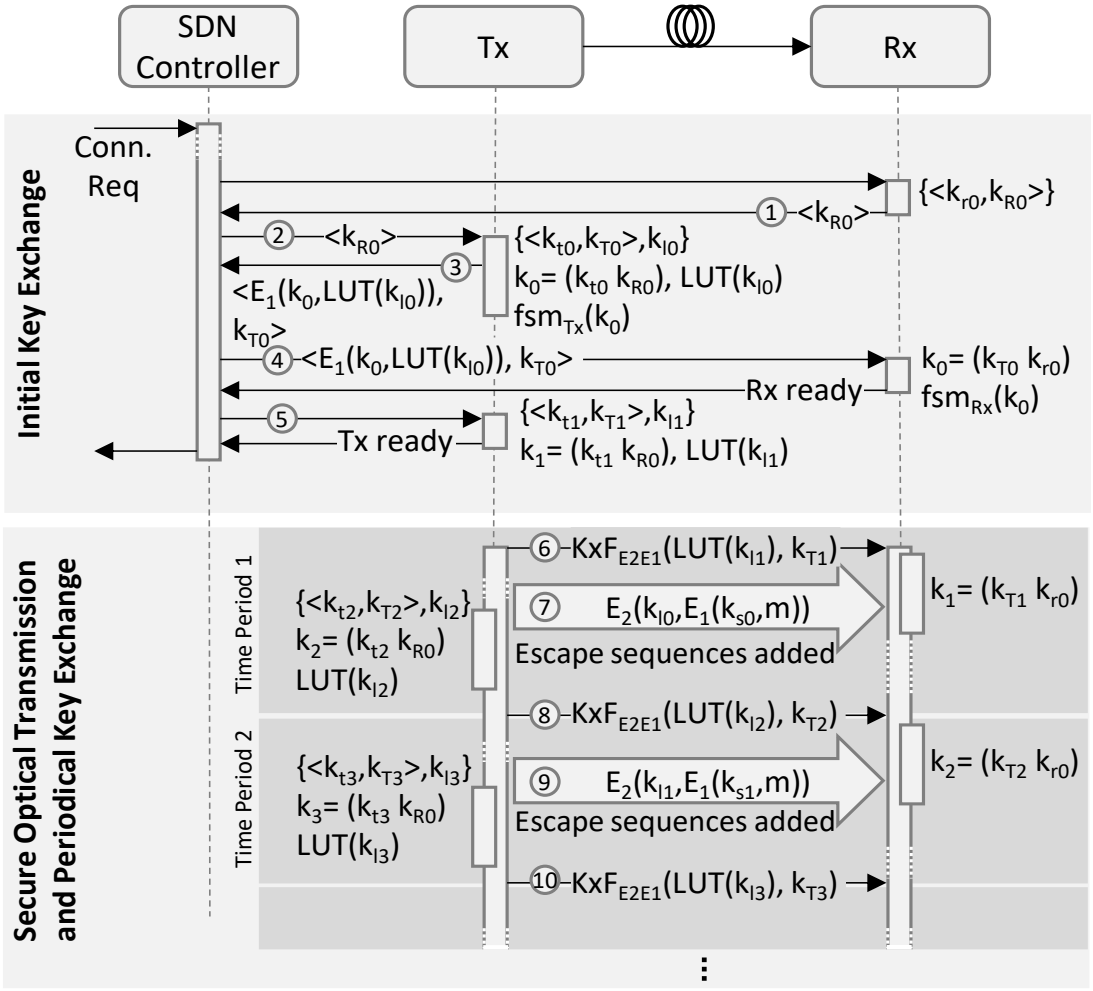


Figure 4-3 Connection set-up and secure optical transmission

Once the initialization phase ends, the secure optical transmission phase begins and continues until the connection is torn down. At the starting time, the Tx updates the LUT and public key (6). Note that such exchange is encrypted using the nested encryption used for data transmission; in this case, keys k_{s0} (extended from symmetric key k_0) and k_{l0} are used for ciphers E_1 and E_2, respectively (6).

For the sake of clarity, we denote with subindex i the keys that participate in key exchange at the starting of time period i. This entails that during every time period i-*1*, the Tx generates the set of public and private keys ($<k_{ti}$, $k_{Ti}>$), the symmetric key k_i, and the random key k_{li} (and the permutation of the LUT). Then, at the start of time interval i, the Tx updates the Rx, which computes symmetric key k_i. The exchanged keys will be in place during time period i+1. In particular, key exchange i and all data transmitted during time period i are encrypted using keys i-1.

4.3.2 Symmetric key generation and expansion

In the standard DH key exchange, two large prime numbers (p and g) are publicly selected. When Alice and Bob want to setup a secure communication channel, they generate private keys k_p, which are used to compute their public keys k_P, as:

$$k_P = g^{k_p} \, mod \, p \qquad (4\text{-}1)$$

After the public keys are exchanged, each party computes the symmetric key k for data encryption/decryption, as:

$$k = {k_B}^{k_a} \, mod \, p = {k_A}^{k_b} \, mod \, p \qquad (4\text{-}2)$$

Similarly, in LPsec, Tx and Rx exchange their public keys k_{T0} and k_{R0} through the SDN controller during the initial key exchange phase. Next, the Tx computes a new pair of keys every period and updates the Rx with the new public key k_{Ti}.

$$k_{R0} = g^{k_{r0}} \, mod \, p \qquad (4\text{-}3)$$

$$k_{Ti} = g^{k_{ti}} \, mod \, p \quad \forall i \qquad (4\text{-}4)$$

Note that the Rx does not compute new public and private keys afterwards, and the initial pair $<k_{r0}, k_{R0}>$ is used along the lifetime of the optical connection. Therefore, the symmetric key k that is used for the stream cipher is updated periodically (e.g., every 1 sec.) as:

$$k_i = {k_{R0}}^{k_{ti}} \, mod \, p = {k_{Ti}}^{k_{r0}} \, mod \, p \qquad (4\text{-}5)$$

Once the symmetric key is computed, it is expanded using a cryptographically secure PRNG to produce keys long enough for the stream cipher to encrypt / decrypt a chunk of data. Therefore, if the size of each chunk of data is U [b] and the transmission speed is B [b/s] then the number of chunks per second, J, can be computed as:

$$J = \frac{B}{U} \qquad (4\text{-}6)$$

Hence, each symmetric key k_i generated for the time interval i, is expanded into J k_{sij} keys that the stream cipher will use for chunks j in [0 .. J-1]; keys k_{sij} are U bits long. For example, assuming that the size of data chunks is U=64 bits, the transmission speed is B=100 Gb/s, a new key is generated every 1 second, the PRNG needs to expand the symmetric key k into J=$2^{30.5}$ keys k_{sij} per second (i.e., one key every 0.64 ns), each U bits long. Therefore, the PRNG must be fast enough to work at 100s of Gb/s line speeds, in order not to introduce meaningful delay to data transmission.

4.3.3 Security level and encryption speed

Let us assume that, under the DH protocol, an eavesdropper (i.e., Eve) knows the value of p, g, and the public keys of Alice and Bob. To compute the symmetric key, Eve still needs to know the private keys of either Alice or Bob, or to solve the discrete

logarithm problem [CoH18], which is considered computationally hard when p is large. However, the security level of a stream cipher depends on the randomness of the PRNG for key expansion [Bo20]. Recall that OTP shows perfect security since ciphertexts do not reveal any information of the related plaintext, so an adversary cannot distinguish between two ciphertexts m_i and m_j encrypted with key k selected at random. However, stream ciphers cannot attain perfect security because PRNGs are utilized, and the length of the generated keys are shorter than those of the messages.

A PRNG is secure if an adversary cannot distinguish between a truly random sequence and the pseudo random sequence generated by the PRNG with a significant advantage. This is related to the computational feasibility of adversaries to perform predictions with a reasonable amount of time and memory. In practice, although standard stream ciphers based on Salsa20 and ChaCha produce high-quality PRNGs, they are not fast enough to be applied to optical transmission. In contrast, we use a general-purpose PRNG because of its high speed. To mitigate the impact of using a general-purpose PRNG only, an optical constellation-based substitution cipher is added. This approach is still not perfectly secure, as the distribution of the encrypted data is not uniform. Therefore, if the characteristics of the plain text are known, an adversary can apply frequency analysis and break the cipher. However, since the substitution cipher is fed with data encrypted using the XOR operation, frequency analysis will not provide useful information. As a consequence, this symbiotic relationship between the stream cipher and the substitution cipher results in a fast and secure cryptographic system.

4.4 Design of LPsec

In this section, we design the blocks for optical encryption / decryption and key management in terms of interconnected modules, which are governed by FSMs. We define generalized templates for the FSMs governing Tx and Rx, which enables the definition of random KxF header patterns both in contents and length. The generation of specific FSMs is detailed.

4.4.1 Optical encryption / decryption and key management

Figure 4-4 presents a detailed design of the Optical Encryption and Key Management block at the Tx and that for Decryption and Key Management at the Rx. The Tx receives as input the data bit stream. Each individual plaintext digit is temporarily stored in a register while being checked by the FSM_{Tx} to prevent KxF header patterns. The encryption and decryption blocks perform operations over sets of bits, named *character* (char), where their size (b) coincides with the number of bits per symbol of the M-QAM modulation format used for the optical signal, e.g., $b = 4$

bits/symbol for 16-QAM (note that $M=2^b$). At every clock cycle during normal operation, the FSM_{Tx} reads one char from the input register (labeled *Da* in Figure 4-4) and executes an internal state transition, which generates a tuple <*Sh*, *Se*, *Xa*> as output, where: *i*) *Sh* performs a char-size shift operation on the input register; *ii*) *Se* selects the input that is chosen as output in the selector; and *iii*) *Xa* is active during key exchange. In the case that a KxF header pattern is detected in the input data stream, an escape char is inserted, so the input *esc* in the selector will be chosen. At regular intervals, a new key exchange is initiated, so the Key Exchange module activates the *Kx* input on the FSM_{Tx}, and the KxF is transmitted instead of input data. Every char in the output of the selector is encrypted by stream cipher E_1 using a char from key $k_{s(i-1)j}$; the key register shifts one char every cycle and when it is empty a new key $k_{s(i-1)j}$ is expanded and loaded. Once a char is encrypted (c_1), it is used as input for the LUT and the substituted char (c_2) is generated.

The Key Generator module is responsible for generating new keys. At every time interval, the module generates a new pair of Tx public and private keys and uses the public key from the Rx to generate a new symmetric key. It also generates a new random key and selects the LUT permutation. The generated keys and LUT are sent to: *i*) the Key Exchange module that packs the LUT and the Tx public key in a KxF and activate the Kx signal to stop data transmission and start the key update; *ii*) the PRNG module that uses the symmetric key for expanding stream keys for the next chunk of data; and *iii*) the LUT module that uses the new LUT to update its contents.

At the Rx, the inverse process is performed. Every c_2 char received enters in the LUT and the original char c_1 is generated, which is then decrypted using a char from key $k_{s(i-1)j}$. The FSM_{Rx} inspects the plain chars (input *m*) in the search of escape chars being inserted by the Tx and generates a tuple <*Se*, *Ld*, *Fl*, *LdF*, *FLd*, *Cl*> as output. The plain chars are chosen at the output of the selector (signal *Se*) and can be temporarily stored in an output register (signal load, *Ld*) until a decision is made to send them as output bit stream (signal flush, *Fl*) or ignore them (signal clear, *Cl*). For convenience, the signals Load and Flush (*LdF*) and Flush and load (*FLd*) are defined. When the KxF header pattern is detected, the stored chars are ignored and the payload of the KxF is sent to the Key Management module. On the contrary, if an escape character is detected, it is ignored by choosing the *esc* output in the selector, and the output register is flushed.

When a KxF header pattern is detected, the Key Management module receives it and announces the FSM_{Rx} its end (signal *Xa*). The Key Management module will then distribute the received LUT to the LUT module and generate the new symmetric key to be distributed to the PRNG module.

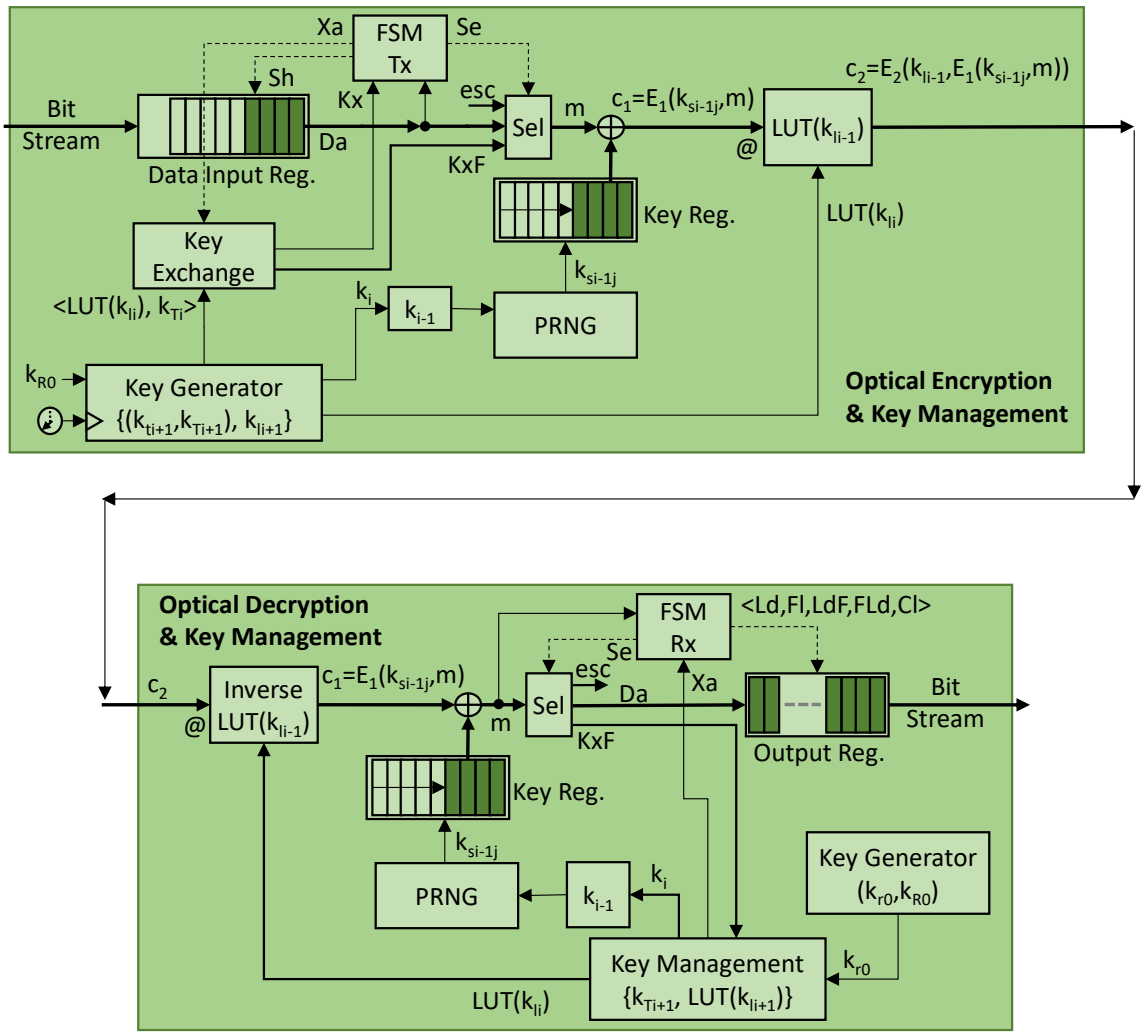


Figure 4-4: Design of LPsec: Optical Encryption/Decryption and Key Management at the Tx/Rx. FSM (Finite State Machine), LUT (Lookup Table), and PRNG (Pseudo Random Number Generator).

4.4.2 Generalized FSM templates

Specific FSMs need to be defined for the Tx and the Rx as a function of the generated KxF header pattern, which is generated at random during the initial key exchange phase. For the sake of the generalization of the FSMs, the header pattern is generated guaranteeing that any char does not appear more than once. In this way, the specific FSMs can be easily built from predefined parameterized templates by specifying the size of the header pattern and the specific chars.

Figure 4-5a illustrates a graph representing the parameterized template of FSM_{Tx}, where the n-char header pattern is specified by the char sequence $H = <h_0, h_1,.., h_k,.., h_{n-1}, h_n>$. In the graph, states S_{Tx} define the outputs (O_{Tx}) for *Sh*, *Se*, and *Xa* signals, while transitions among states are performed based on the char in the input *Da* and

Kx (I_{Tx}). Normal operation is represented by states S_i, whereas key periodical key exchange is represented by states S_i'. The graph consists of n+1 S_i and n S_i' states, where S_i represents the state where i chars in the header sequence and in the right order have been detected. A value '-' in one of the inputs means whatever other value, different than those specified for the rest of transitions leaving from that state. State S_0, the initial state, and state S_1 are the most frequently transitioned, and many of the rest of the states have a direct transition to them. The remaining normal operation states account for partial header patterns found in the input data. State S_n is the one responsible for adding an escape character, and it has priority even in the case of a key exchange request (note that whatever the input from S_{n-1} a transition to S_n is always made).

Note that FSM_{Tx} adds an extra char when *n-1* chars in the data stream coincide with those defined for the header. Hence, the probability of adding a new char can be defined as:

$$P_{char\_added} = \frac{1}{2^{b\cdot(n-1)}} \qquad (4\text{-}7)$$

Similarly, Figure 4-5b presents a graph representing the parameterized template of FSM_{Rx}. States S_{Rx} define the outputs for *Se*, *Ld*, *LdF*, *FLd*, and *Cl* signals (O_{Rx}) (outputs are specified in the inner table in Figure 4-5b), while transitions among states are performed based on the decrypted char *m* and the *Xa* inputs (I_{Rx}). S_o is the initial state and every transition to that state loads the received char and produces a flush on the output register. State S_{n-1} is responsible for distinguishing between an escape char inserted by the Tx and the complete KxF header pattern. In the first case, the transition is to S_n, which discards that char and flushes the register. In the second case, the transition is to S_n', which sends the payload of the KxF to the Key Management module and clears the output register. During the reception of the KxF payload, the Key Management module keeps the *Xa* signal active until all the chars have been received. In the meanwhile, transitions are to the state S_n'. When the complete KxF payload has been received, the FSM transitions to either state S_o or S_1, and incoming chars are stored again in the output register.

Both graphs can be particularized for any given length of the KxF header greater or equal to 3 by just adding as many S_k intermediate states as needed.

4.4.3 FSM particularization

We now illustrate the easiness to particularize the FSMs given the n-char KxF header pattern $H = <h_0, \ldots, h_{n-1}>$ and the bits per symbol of the modulation format (b). The specific FSMs for the Tx and the Rx are defined by: *i*) the state-transition matrix (STM) of dimensions $|S_{(\cdot)}| \times 2^{|I_{(\cdot)}|}$; and *ii*) the output matrix (OM) of dimensions $|S_{(\cdot)}| \times |O_{(\cdot)}|$. Specifically, $|S_{Tx}| = 2 \cdot |H| + 1$, $|S_{Rx}| = |H| + 2$, $|I_{Tx}| = |I_{Rx}| = b + 1$, $|O_{Tx}| = 3$, and $|O_{Rx}| = 7$.

Algorithm 1 presents the pseudocode to generate FSM_{Tx}. The algorithm first computes the number of different chars as a function b (for input Da) and the number of states, initializes vector S with the states, and the state-transition matrix STM (lines 1-3); note that the STM is initialized with all transitions to state S_0. Next, the transitions for states are computed as follows (lines 4-14): 1) transitions from state S_{n-1} are to S_n disregarding the value of Kx (lines 6-9); 2) whenever input Kx is active, transitions from state S_i are to S_i' (lines 10-12); 3) whenever input Kx is not active, transition is to S_1 if $Da = h_0$ or to state S_{i+1} when $Da = h_i$ (lines 13-14). The output matrix OM is filled (lines 15-19) and the generated FSM_{Tx} is eventually returned (line 20).

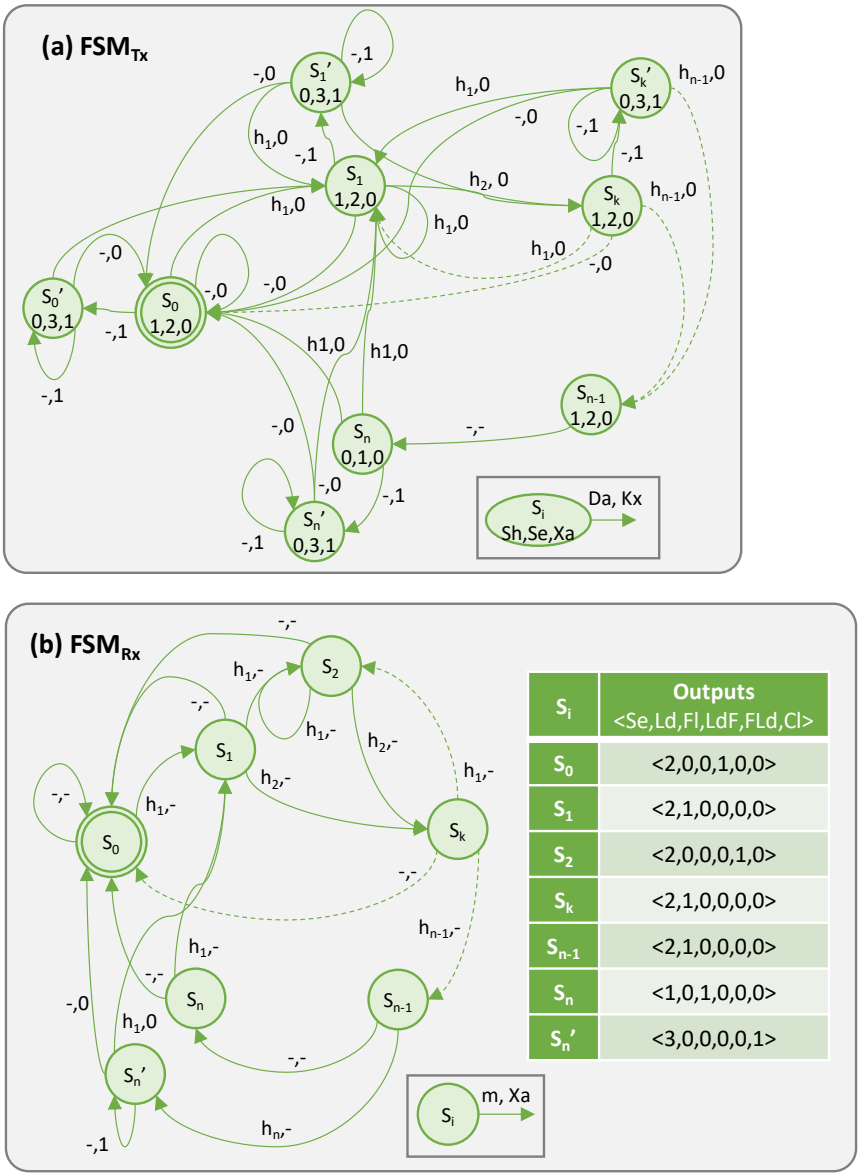


Figure 4-5: Graphs representing parameterized templates for FSM_{Tx} (a) and FSM_{Rx} (b).

Algorithm 1. FSM_{Tx} Generation

Input: *H*, *b*
Output: *STM*, *OM*

```
1:  Ch ← 2^b; n ← |H|; |S| ← 2n+1
2:  S ← [i for i: 0..|S|-1)]
3:  STM ← [|S|] [2Ch]
4:  for i: 0..n-1 do
5:    for c: 0..Ch-1 do
6:      if i = n-1 then
7:        STM[i][c] ← S[n]
8:        STM[i][Ch+c] ← S[n]
9:        continue
10:     if i = n OR i = 2n then STM[i][Ch+c] ← S[2n]
11:     else if i < n then STM[i][Ch+c] ← S[n+1+i]
12:     else STM[i][Ch+c] ← S[n+i%n]
13:     if c = H[0] then STM[i][c] ← S[1]
14:     else if c = H[i%n] then STM[i][c] ← S[i%n +1]
15: OM ← [|S|]
16: for i: 0..|S|-1 do
17:   if i < n-1 then OM[i] ← [1, 2, 0]
18:   else if i = n then OM[n] ← [0, 1, 0]
19:   else OM[i] ← [0, 3, 1]
20: return STM, OM
```

4.5 Illustrative results

We have implemented LPsec as a MATLAB-based simulation. In particular, we have integrated the encryption and decryption blocks in the Tx and Rx, as depicted in Figure 4-1, where a single polarization 64 GBd optical signal was considered. Three different modulation formats are assumed: 16-QAM, 32-QAM and 64-QAM. In this section, we present the obtained results to validate LPsec.

4.5.1 Optical system performance analysis

Let us first analyze the performance from the optical perspective. In the simulator, the signal was sampled and passed through a root-raised-cosine pulse shaper with roll off factor of 0.06. The signal was launched into a fiber channel with N spans, each being 80 km long. After every span, an optical amplifier with a noise figure of 4.5 dB compensates for fiber losses. Additive white Gaussian noise is added after each span to model ASE noise. For the simulation of the fiber channel, standard single mode fiber with the following parameters was considered: fiber loss α = 0.21 dB/km, dispersion D = 16.8 ps/(km-nm) and nonlinear coefficient γ = 1.14 $W^{-1}km^{-1}$. A

2^{16} pseudo-random sequence was used to generate the payload. The signal was propagated then using the symmetric split-step Fourier method, solving the non-linear Schrödinger equation [NFO13]. The signal was coherently received; it was down-sampled to 2 samples per symbol, and an ideal chromatic dispersion filter was used.

We first analyzed the performance of the system with and without encryption to verify that encryption does not degrade the performance of the system. Figure 4-6a shows the obtained results for 25 spans, where we observe that the BER remains the same with and without encryption for the selected modulation formats for different input powers.

Once the optical performance was verified, we implemented convolutional forward error correction (FEC) encoding and decoding; FEC code rate of 2/3 was used for data encoding, whereas the Viterbi decoding algorithm was used at the receiver [Ty06]. Figure 4-6b presents the BER as a function of the number of spans and the inner table summarizes the maximum number of spans where the FEC corrected any transmission error.

4.5.2 Delay introduced by the kxf and escape characters

Next, we evaluate the delay introduced by the proposed KxF that allow exchanging the new LUT and Tx public key (but requires to stop the normal data transmission), as well as the additional escape chars added to avoid collisions of the transmitted data with the KxF; we assume 256-bit keys. Recall that the operations related to the pure data encryption involve XOR operations (performed in blocks of b bits according to the used modulation format) and LUT access; we assume that those operations do not introduce significant delay.

Let us first analyze the probability of adding a new char as a function of the length of the header n for the considered modulation formats. Figure 4-7a shows the results from plotting eq. (4-7), where the probability is below 0.4% and 0.024% even for lengths as short as 3 chars for 16-QAM and 64-QAM, respectively. Such probability is related to the average delay, so a longer header would further reduce the delay; however, it would also increase the size of the FSMs to be implemented in the Tx and the Rx, so a reasonable trade-off needs to be found.

Figure 4-7b shows the average delay introduced as a function the header's length (n), assuming time periods of 1 s., i.e., key exchange is performed every 1 s. First, we observe that the introduced delay is negligible, just a few ps even for n=3 and 16-QAM. Interestingly, when the header length is small, the probability of adding escape chars is higher and the average delay mainly depends on the number of chars added. However, as the header length increases, the average delay decreases to a point when the delay is mainly influenced by the *KxF* itself. In view of these results, n=4 char length is selected as it can provide a good balance between delay and simplicity.

4.5.3 Frequency analysis attack

In this section, we analyze how a frequency analysis can be used by an attacker in case a LUT substitution only is implemented (similar approach as in [Li16]. This will highlight why symmetric encryption is an important part of the optical encryption block. Suppose that an attacker can send a significant amount of data over the

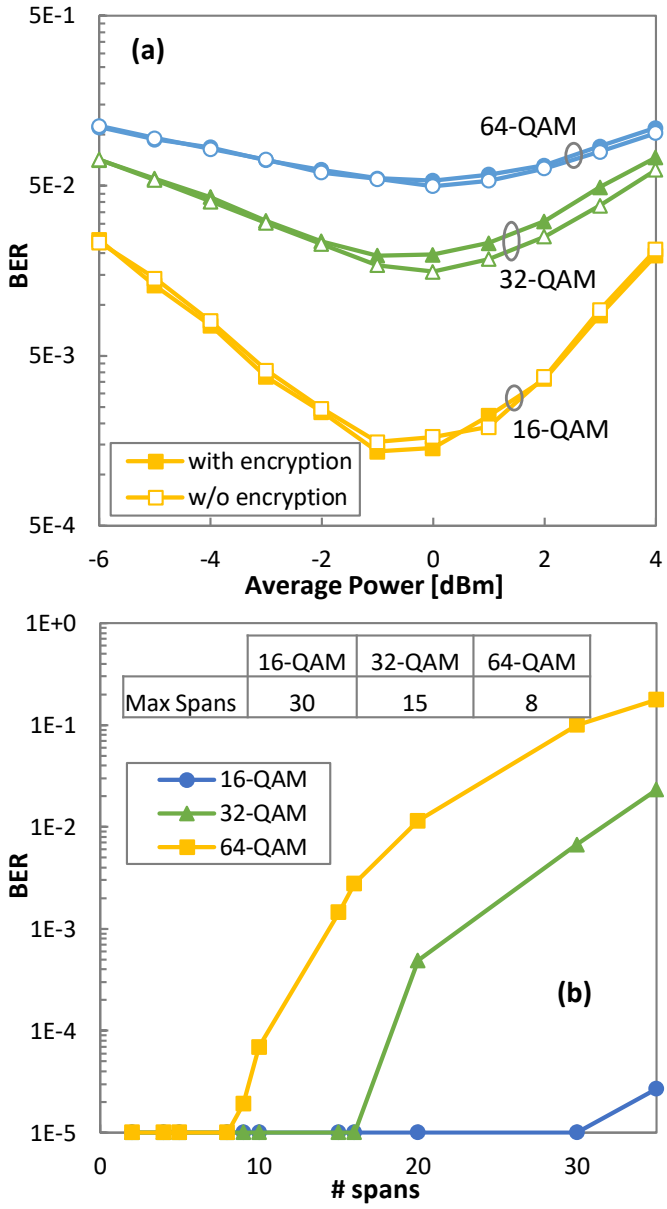


Figure 4-6: BER w/ and wo/ encryption (a) and BER vs number of spans with FEC (b)

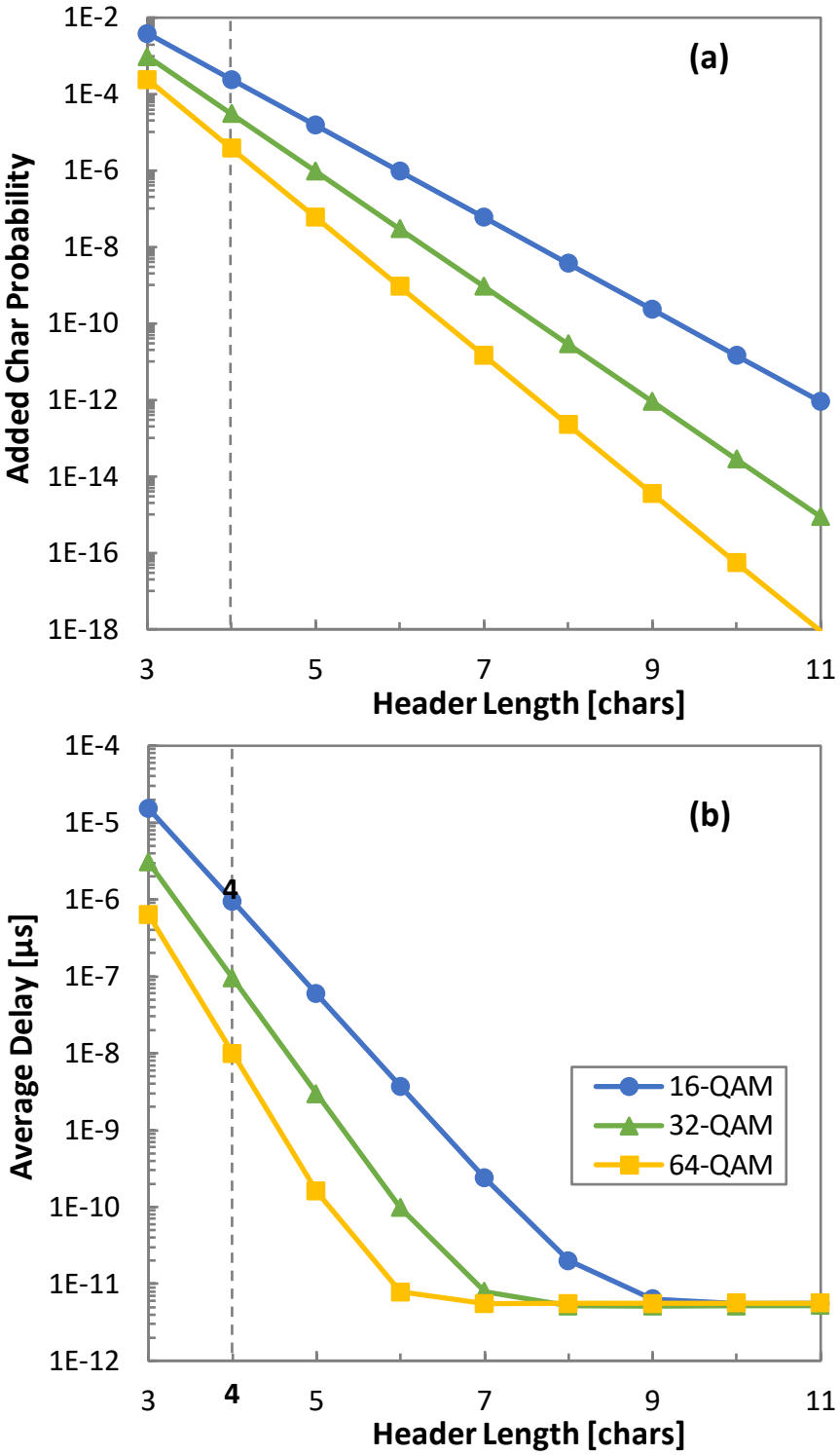


Figure 4-7: Added Char Probability (a) and average delay (b)

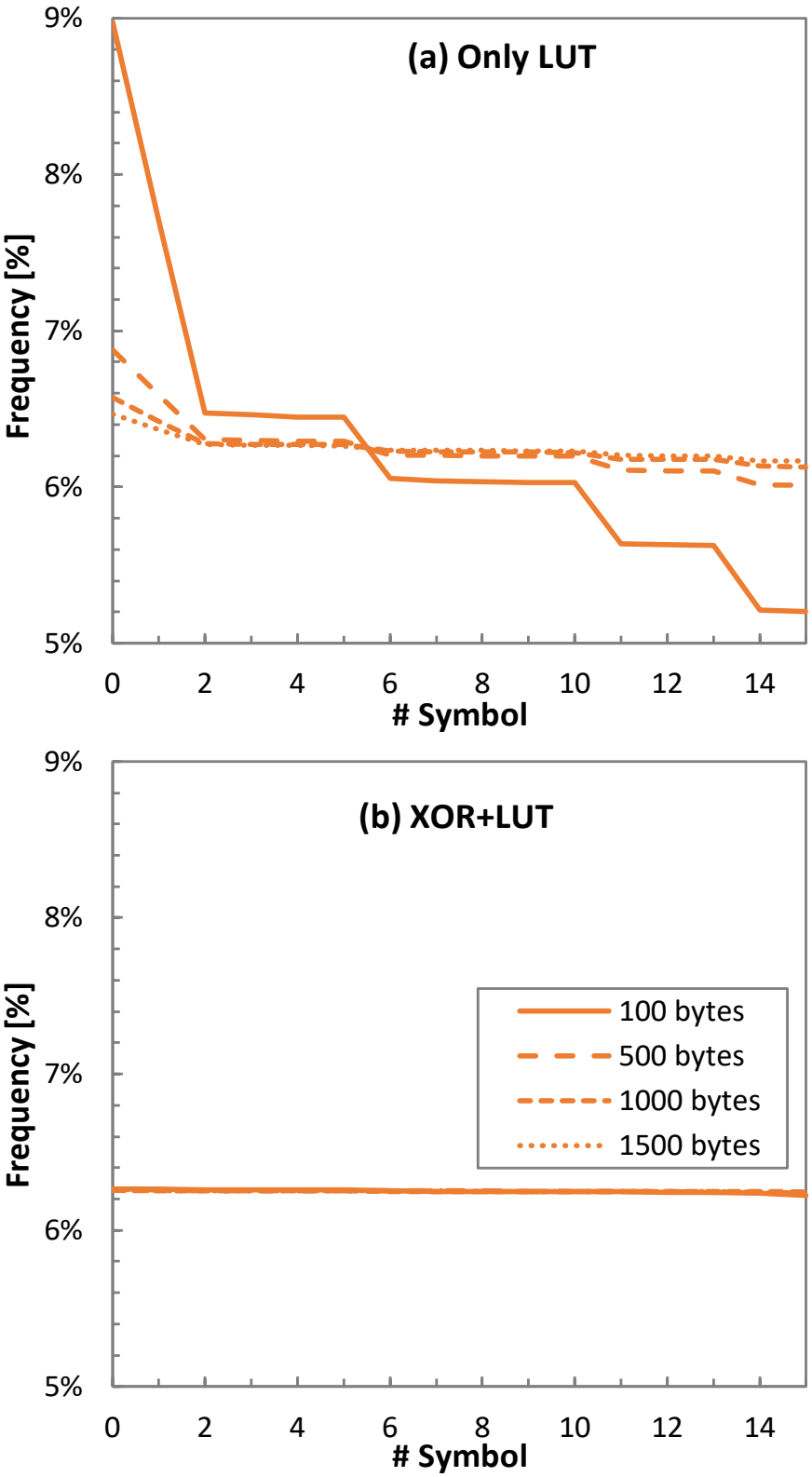


Figure 4-8: Frequency of symbols w/o (a) and w/ encryption (b)

optical system, e.g., in the form of IP packets, and she/he can also eavesdrop on the transmitted signal. Then, the attacker could send packets filled with selected payloads, e.g., all 0's and observe the data sent over the fiber. Because LUT just substitutes blocks of b bits of data, the attacker can then map the pattern in the payload of the injected packets with the symbols sent over the fiber. Figure 4-8 shows an example of frequency analysis, where the symbols are sorted by its frequency of appearance to facilitate its representation. For this test, we have generated Ethernet frames of fixed size starting in 100 bytes until 1500 bytes. In the frame, the only part that was not randomly generated was the MAC and IP addresses, which represent a small proportion of bits that are predictable. Even with long frames, differences in the frequency of the symbols can be observed in Figure 4-8a, which enables this attack regardless of how many different LUT permutations exist. Figure 4-8b shows that the attack by frequency analysis will not succeed when data is encrypted with the symmetric key, due to the properties of the XOR operation.

4.5.4 PRNGs analysis for stream cipher

When applying stream ciphers, the main consideration is the selection of PRNG, as discussed in Section 4.3.3. Standard stream ciphers (e.g., ChaCha or AES in counter mode) can be used to produce high-quality PRNG. The quality of a PRNG can be examined using some of the available empirical statistical tests; see, e.g., [TestU01], [NIST]. However, standard stream ciphers can hardly be used for the speeds that are targeted at the optical layer and, in consequence, other options should be analyzed. Specifically, the 64-bit all- purpose PRNGs in [Bl19] exhibits enough speed for the specific requirements of the optical layer. Such PRNGs pass many of the statistical tests and can partially fulfil the requirements to be used in cryptographic applications. From the set of PRNGs proposed in [Bl19], we selected Xoshiro256+ as stream cipher.

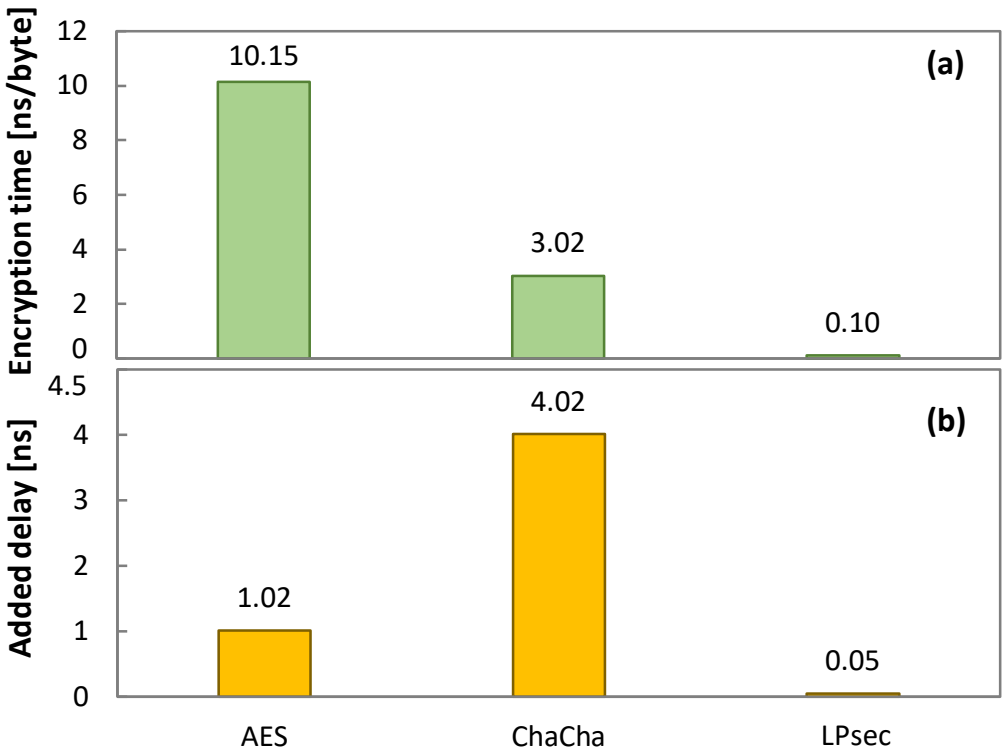


Figure 4-9: Encryption time (a) and added delay (b) for a 16-QAM @32Gbaud optical system.

Let us first compare the speed of AES, ChaCha, and LPsec for a 32Gbaud 16-QAM system. For AES and ChaCha, the OpenSSL library was used and blocks of 128 bits for AES and 512 bits for ChaCha are considered for encryption. In contrast, Xoshiro256+ was integrated in the design of the optical encryption block in LPsec (see Figure 4-4) and used as PRNG. Encryption times were computed on a stream of 1GB. The tests were performed on an Intel® Core™ i7-4790 CPU @ 3.60GHz using gcc version 9.3.0. O3 optimization was used in all the cases.

Figure 4-9a presents the obtained encryption times for AES, ChaCha and LPsec, where we observe that the latter reduces the encryption time of AES by 2 orders of magnitude, whereas ChaCha reduces the encryption time by a factor of about 30. Note that encryption time must be smaller than the time required to transmit a block. With the results from Figure 4-9a, AES can support up to 0.8 Gb/s, ChaCha up to 2.7 Gb/s, while LPsec can support up to 80 Gb/s, all using Intel® Core™ i7-4790 CPU. Of course, when those methods are implemented in specialized hardware, transmission times can scale several times, but these results show clearly the potential of LPsec.

Let us now analyze the average delay introduced by each encryption method. Recall that AES works on blocks of 128 bits, whereas ChaCha works on blocks of 512 bits and the encryption can only start when sufficient bits have arrived. Symmetrically, once a block has been encrypted, bits have to wait until they are actually transmitted

to the destination. In contrast, LPsec works in groups matching the bits per symbol of the modulation format, so bits in the input bit stream have to wait half of the inverse of the baud rate, on average. Figure 4-9b presents the average delay introduced for each of the encryption methods, where we can observe the very low delay of LPsec.

4.5.5 Security level against exhaustive search attack

Finally, let us explore the security level of LPsec in terms of exhaustive search or brute force attacks, where all possible keys are tested until the correct one is identified. For this attack, we assume the known-plain-text attack model, where a plain text along with the cipher text are known to the attacker; if the plain text has some repeated properties, like headers or identifiers in the communication, that is applicable on cipher text only attacks as well.

The key length used in the encryption method will determine the strength of encryption with the longer keys being more difficult to crack. For instance, with a 256-bit key, the brute-force attack has a complexity of 2^{256}. However, techniques like precomputation attacks are short-cuts to the exhaustive search attacks and can greatly reduce such complexity [CISCO.2]. Precomputation attacks exploit the birthday paradox (i.e., the probability that in a set of randomly chosen people, some pair of them will have the same birthday). The birthday attack is based on the fact that duplicate values or collisions appear much faster than expected. In general, if a system takes N different values, the first collision can occur after $\sqrt{N}$ random values [Bi96]. In practice, a precomputed table can be generated by the attacker in offline mode. E.g., for a 256-bit key system, the attacker can precompute a table with precomputed cipher texts by using only 2^{128} random key entries. Then, she/he eavesdrops on each message and checks whether the ciphertext appears in the table. If there is a collision, then the key is used in the encryption and arbitrary information can be added by the attacker till the key is valid. In this case, the workload for the attacker becomes 2^{128}, which is much smaller than the default expected 2^{256}.

We have evaluated the key sizes in terms of precomputation attacks for LPsec. On the one hand, Xoshiro256+ generates 256-bit keys. Besides, the substitution cipher adds more complexity to the brute-force attack, e.g., key spaces of 44, 117, and 295 bits are produced using 16, 32, and 64 -QAM, respectively, which results in total key sizes for LPsec of 300, 373, and 551. This means that the effective computation required by the birthday paradox is over 2^{150}, which can be considered safe enough for the foreseeable future [FeN10]. In conclusion, LPsec can be considered secure against exhaustive search attacks.

4.6 Concluding remarks

A complete solution to add encryption at the optical connection level has been presented in this chapter. The solution includes a mechanism for key distribution from the Tx to the Rx and two ciphers that, when combined, can provide the required security level and are able to work on 100s of Gb/s data flows. The key distribution is performed using a Key exchange Frame that is sent periodically from the Tx to the Rx. The Xoshiro256+ PRNG is used for symmetric key expansion, so as to provide keys that are used by the first XOR-based cipher. A second cipher based on LUT substitution improves the security level. The design of LPsec has been presented and is easily implementable on current coherent optical systems.

Simulation results carried out for 16, 32 and 64-QAM signals show that LPsec has negligible impact on the performance of the optical transmission system. Moreover, the required periodical key exchange does not add any significant delays. The security against two well-known attacks, frequency analysis and exhaustive search, has been analyzed and it was shown that LPsec provides a high level of security against them.

Chapter 5

Supporting Heterogenous Traffic on top of Point-to-Multipoint Light-Trees

New 5G and beyond services demand innovative solutions in optical transport to increase efficiency and flexibility and reduce capital (CAPEX) and operational (OPEX) expenditures to sup-port heterogeneous and dynamic traffic. In this context, optical point-to-multipoint (P2MP) connectivity is seen as an alternative to provide connectivity to multiple sites from a single source, thus potentially both reducing CAPEX and OPEX. Digital Subcarrier Multiplexing (DSCM) has been shown as feasible candidate for optical P2MP in view of its ability to generate multiple subcarriers (SC) in the frequency domain that can be used to serve several destinations. This paper proposes a different technology, named Optical Constellation Slicing (OCS), that enables a source to communicate with multiple destinations by focusing on the time domain. OCS is de-scribed in detail and compared to DSCM by simulation, where results show that both OCS and DSCM provide good performance in terms of bit error rate (BER) for access/metro applications. An exhaustive quantitative study is afterwards carried out to compare OCS and DSCM considering its support to dynamic packet layer P2P traffic only and mixed P2P and P2MP traffic; throughput, efficiency, and cost are used here as metrics. As a baseline for comparison, the traditional optical P2P solution is also considered in this study. Numerical results show that OCS and DSCM provide better efficiency and cost savings than traditional optical P2P connectivity. For P2P only traffic, OCS and DSCM are utmost 14.6% more efficient than the traditional lightpath solution, whereas for heterogeneous P2P+P2MP traffic, 25% efficiency improvement is achieved, being OCS 12% more efficient than DSCM. Interestingly, the results show that for P2P only traffic, DSCM provides more savings of up to 12%

than OCS, whereas for heterogeneous traffic, OCS can save up to 24.6% more than DSCM.

5.1 Introduction

The introduction of new services for different use cases, like augmented reality and virtual reality, internet of skills, industry 4.0 and robotics, etc. [HoZ21] will require extending the optical network towards the edges [Ve13] and integrate optical and radio networks [BaB23], will add more diversity to the requirements for the traffic that the optical transport needs to support. Such requirements, include not only data rates, but also varying directionality and traffic patterns, as well as connectivity types, e.g., between one source and one or multiple destinations. Therefore, innovative solutions in the optical transport need to be devised that provide the required agility in terms of dynamic traffic management and flexibility in terms of topology upgrade [Gi20].

In this regard, point-to-multipoint (P2MP) networking has been recently proposed at the optical layer to connect several mobile sites to a single metro datacenter [We21]. In P2MP connections one single source node *(hub)* is connected to a set of destinations (*spokes*) that may be scattered over a geographical area. Note, in contrast, that point-to-point (P2P) connectivity has been generally implemented in transport networks, which does not fit well to support *hub-and-spoke* arrangements like the above one. However, P2MP also presents some disadvantages, like that of the data privacy, since all the leaves receive all the data being sent.

Implementing P2MP at the optical layer requires not only establishing *light-trees* [Ru14, Ru15], but also innovative optical transmission technologies based on advanced Digital Signal Processing (DSP) [Sa13]. DSP is commonly used to implement higher modulation formats that increases the speed and reach of coherent optical systems [SeD22]. DSP can be also used to implement new optical communications technologies, like digital subcarrier multiplexing (DSCM) [We22,Qi22]. The primary advantage of DSCM is that it enables fixed bandwidth granularity, i.e., instead of generating a single carrier at the transmitter, several subcarriers (SC) are generated and multiplexed digitally before transmission. Additionally, SCs can be dynamically activated and deactivated to meet capacity requirements [Ve21]. DSCM was proposed for P2MP coherent communications in [We21, Ba20, DaR17, We23], where a subset of independent SCs can be dedicated to support P2P traffic between the source and each destination with the benefit of using one single optical transceiver in the source supporting all the P2P traffic flows.

A different optical communications technology for optical P2MP supporting P2P traffic is that of the optical constellation slicing (OCS) [OFC22]. OCS digitally slices the optical constellation of single carrier to transport a dynamically defined combination of P2P and P2MP traffic flows. The slicing is performed by dedicating a different subset of constellation points (CP) to different receivers. This work studies the feasibility of OCS for dual-polarization (DP), 64-GBd system. We compare the throughput and relative capital (CAPEX) and operational (OPEX) expenditures of OCS and DSCM technologies for different optical P2MP scenarios. Many previous

works have compared different solutions in terms of CAPEX and OPEX. For instance, the authors in [He20] compared next-generation central offices for metro networks, the authors in [Ve13.2] envision an optical transport extending from the core to the network edge, and the authors in [Pe12] studied the cost of solutions for multilayer packet over optical networks.

Additionally, this chapter addresses data privacy in P2MP connections. To prevent data breach, an independent lookup table (LUT) for each traffic flow is used to implement a substitution cipher [SaD05]. As in Chapter 3 for securing lightpaths, the LUT is used at the source to encode the transmitted data which also makes sure that only the destination(s) with the corresponding LUT can decode the data that have been assigned to it. Note that although substitution ciphers do not provide perfect secrecy, they provide enough degree of privacy for the type of applications that we target.

The rest of the chapter is as follows. Section 5.2 investigates P2P and P2MP connectivity considering the limits of the existing deployed P2P network and shows how P2MP at the optical layer might support both P2P and P2MP packet traffic and make the transport architecture more efficient. Two optical technologies, DSCM and OCS, are selected as candidates to implement P2MP connectivity using coherent optical communication systems. Section 5.3 discusses OCS in detail and highlights the construction, implementation and throughputs of OCS as compared to that of the DSCM. Section 5.4 compares the optical performance of OCS and DSCM by simulation and presents numerical results to provide a quantitative comparison between them under dynamic traffic scenarios. Finally, Section 5.5 draws the main conclusion of the chapter.

5.2 Optical layer supporting P2P and P2MP traffic

P2P and P2MP communications are represented in Figure 5-1a-b. Figure 5-1a presents a particular scenario of P2P connectivity, where all the sources are in the same location and the destinations are in multiple remote locations, i.e., a hub-and-spoke arrangement, which is typical in e.g., access networks. Figure 5-1b shows the same scenario for P2MP connectivity, where one single source communicates with destinations in multiple remote locations. Some differences are worth highlighting: *i*) from the pure connectivity viewpoint, in a P2P connection, the signal sent by a source is received only by its destination counterpart, while in a P2MP, connection the sourced signal is received by all the destinations; and *ii*) one single source is used and part of the communication resources can be shared in P2MP connectivity, whereas dedicated sources and connectivity resources are needed in P2P connectivity. Therefore, in the case of N destinations, $2\times N$ *terminals* with dedicated connectivity resources are involved in the case of P2P connectivity, whereas only $N+1$ *terminals* are involved in the case of P2MP connectivity.

P2MP can be easily implemented on the optical layer by creating light-trees connecting one hub node with multiple leaves [Ru14]. However, the majority of services involve P2P traffic and thus, the theoretical benefits of P2MP in terms of resource savings can be difficult to be collected in practice. For this very reason, we explore the application of P2MP communications at the optical layer while supporting P2P traffic, and possibly P2MP traffic, at the packet layer (Figure 5-1c). Here, the number and dimensioning of the optical transceivers are key performance indicators of the cost in terms of CAPEX and OPEX for the network operator, as compared to the traditional P2P connectivity with dedicated lightpaths and transceivers. In addition, the efficiency of the solution and the simplicity of the architecture should also be considered in the analysis.

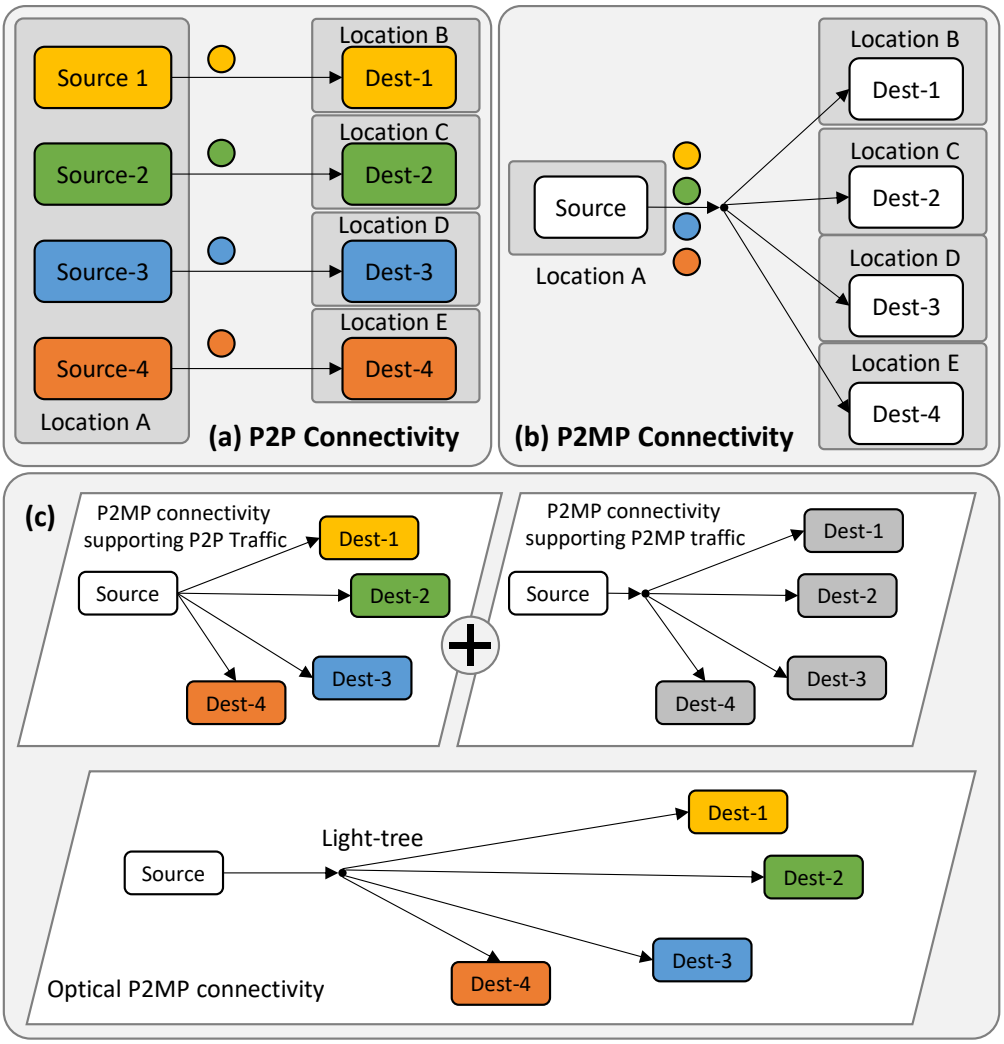


Figure 5-1: P2P (a) and P2MP (b) connectivity. Supporting P2P and P2MP traffic on top of optical P2MP (c).

Two optical technologies have been selected as they can be used for optical P2MP and support P2P traffic at the packet layer: DSCM and OCS. In the case of DSCM

(Figure 5-2a), the spectrum is separated into a number of Nyquist digital subcarriers (SC), e.g., 16, 4 GBd SCs, and multiplexed together at the hub node to create a 64 GBd signal. The hub node sends the SCs to all the leaves, where lower-capacity transceivers listen in to their assigned frequencies to receive their dedicated SCs. In the example, we represent 4 destinations all operating on 4 SCs. To simplify the hardware implementation of DSCM, the SCs assigned to each destination must be contiguous in the spectrum, which makes that P2MP traffic can be supported only for destinations with neighboring SCs.

In the case of OCS (Figure 5-2b), a single optical signal is generated at the hub node and sent to the leaves. The optical constellation is sliced and every slice is used to support P2P or P2MP traffic. In the example in Figure 5-2b, five optical constellation slices are defined (OCS 1..5), where four of them support P2P traffic between the source node and one of the destinations, whereas OCS5 supports P2MP traffic. It is worth noting that the effective bitrate of an OCS can be controlled by selecting the number of CPs that are assigned to it. In the example in Figure 5-2b, the optical signal is modulated using 64-QAM, so 64 CPs are available. From them, OCS1 is assigned 32 points, whereas OCS 3 and 4 are assigned just four. Only the CPs assigned to one OCS can be used for communication to the corresponding destination.

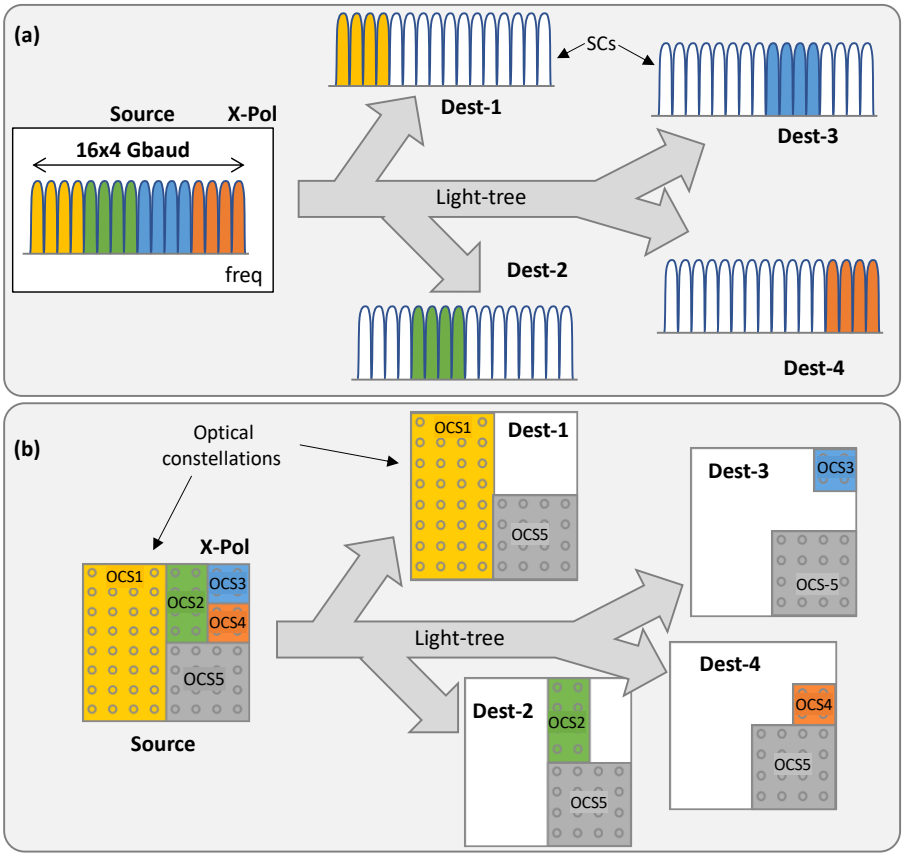


Figure 5-2: Application of DSCM (a) and OCS (b) for optical P2MP.

It seems clear that implementing optical P2MP using DSCM or OCS can bring benefits in terms of cost, efficiency, and simplicity of architecture. CAPEX reduction comes as a result of decreasing the number of required transceivers. Moreover, OCSs and SCs can be created, modified, and eliminated dynamically, which provides the needed flexibility of the connections as per traffic demands.

5.3 Optical constellation slicing

This section details the OCS solution that includes the design of the transmitter and receiver and the theoretical throughput.

Implementing OCS requires adding encoder and decoder blocks to the standard coherent transceivers, as shown in Figure 5-3. The encoder and decoder blocks are in charge of slicing the optical constellation to support P2P and P2MP traffic on top of the optical P2MP.

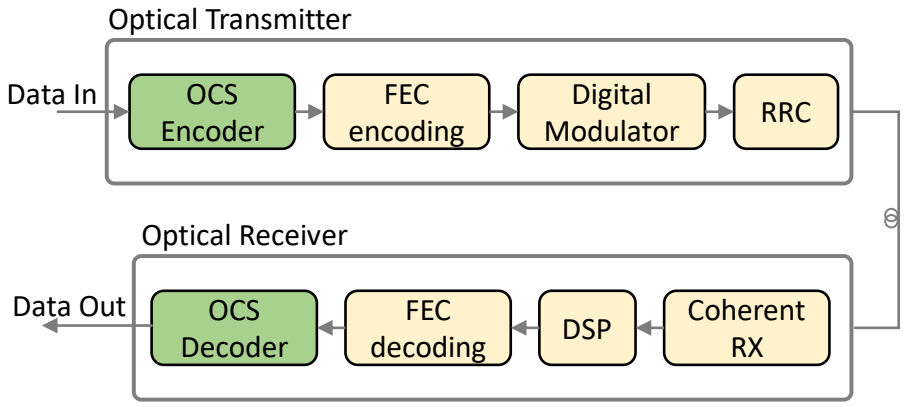


Figure 5-3: Optical communication system for OCS.

For illustrative purposes, Figure 5-4 shows two examples of alternative configurations that can be supported using OCS on the same light-tree. The example in Figure 5-4a, shows the traffic that can be supported with the configuration presented in Figure 5-2b, i.e., four P2P traffic flows between the source and every destination, as well as one P2MP traffic flow between the source and all the destinations. Only by configuring the encoder and decoder, the traffic shown in Figure 5-4b can be supported, which entails two P2MP traffic flows, each between the source and two different destinations. These examples are intended to demonstrate the flexibility of OCS to allow dynamic changes in the configuration of the optical system as a function of the traffic requirements, without changing the light-tree itself. To protect data that is not destined for a specific destination, the encoder block implements a substitution cipher for every OCS based on a specific LUT, which encrypts data before transmission, while the decoder implements the inverse operation for every OCSi individually.

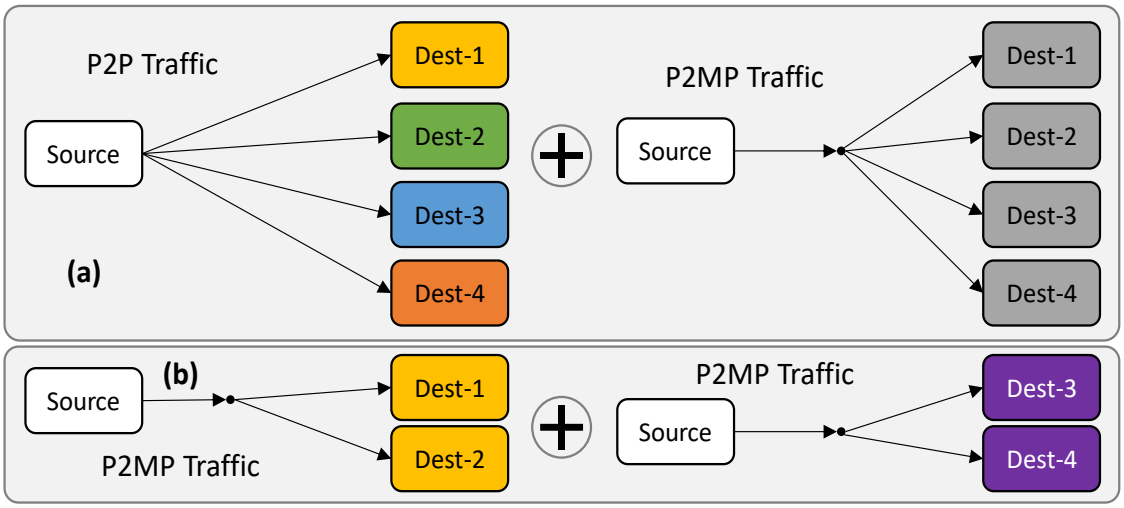


Figure 5-4: Example of traffic configurations supported by OCS.

Figure 5-5 details the OCS encoder for the configuration in Figure 5-2b. The first step is to choose the modulation format (m) of Quadrature Amplitude Modulation (QAM) that provides the highest throughput and the maximum number of OCSs. Because the lowest number of CPs that may be allocated to a single OCSi is two (each point representing a single data bit), the maximum number of simultaneous destinations is $m/2$. For the sake of clarity, we assume m=64 hereafter.

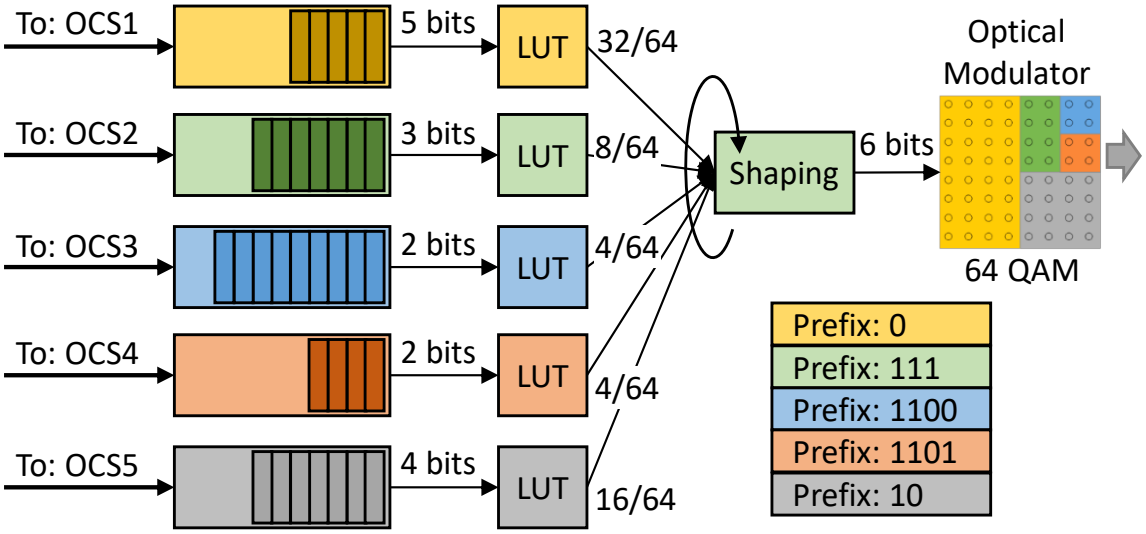


Figure 5-5: Example of slicing and individual data encryption.

The next step is to create the OCSs. Figure 5-5 illustrates the traffic shaping to be implemented at the TX side. Every OCSi is then associated with a buffer within the TX, where data streams are temporarily stored. From those buffers, sets of bits of size equal to the number of *bits with information* (*infobits*) in the OCSi are selected and encrypted using the LUT as a substitution cipher. E.g., in Figure 5-5, sets of 5 bits are selected for OCS1 whereas sets of 3 bits are selected for OCS2. Next, the

shaping block receives one of the encrypted sets from each OCS at a time and adds the prefix that identifies the OCS for which that data is intended; this results in a specific symbol in the optical constellation. Hence, each RX receives symbols formed from a unique <*prefix*, *infobits*> pair, where the prefixes are decided according to the constellation map. Note that prefixes might be of different lengths, so sets of 6 bits are obtained to feed the 64-QAM optical modulator. E.g., it adds prefix 0 to sets of bits from OCS1 and prefix 111 to sets of bits from OCS2 (see Figure 5-5). The shaping block follows a 64-step cycle, where at every step it receives a set of bits from an OCS*i*; the number of sets of bits selected from each OCS*i* is exactly the number of CPs assigned to that OCS*i*. E.g., the shaping block receives 32 out of 64 5-bit sets from OCS1, and 8 out of 64 3-bit sets from OCS2. Note that it is the source where most of the functionalities need to be implemented (including slicing and LUT coding), while destinations perform LUT decoding only. With this arrangement, the throughput of each OCS*i* can be computed as a function of the number of bits with information, the Symbol Rate (SR), the number of CPs assigned to the OCS*i* (#*CP*), and the modulation format used (m-QAM). Note that both gross or net throughput can be computed by considering gross or net SR in equation (5-1).

$$Throughput_{OCS_i} = \frac{infobits_i \times SR \times \#CP}{m} \tag{5-1}$$

In contrast, equation (5-2) can be used to compute the throughput of each SC in a DSCM system working on the same modulation format (*m*), where *N* is the number of SCs.

$$Throughput_{SC} = \frac{SR \times log_2 m}{N} \tag{5-2}$$

In both cases, the system's throughput is calculated as the summation of the individual throughputs. Let us assume SR = 64 GBd and 20% FEC overhead for a DP system. In the example in Figure 5-2b, the throughput of OCS1 and OCS2 is 250 Gb/s and 37.5 Gb/s, respectively. In contrast, for the DSCM system in Figure 5-2a, the throughput of each SC is 37.5 Gb/s and every RX gets a throughput of 150 Gb/s.

Additionally, for OCS we define *slice efficiency* (SE) of each slice OCS*i* as the ratio between the number of *infobits* with respect to the total number of bits per symbol (equation (5-3)), as well as *contributed efficiency* (CE) as a function SE and the number of CPs assigned to the OCS*i* (equation (5-4)).

$$SE_{OCS_i} = \frac{infobits_i}{log_2 m} \tag{5-3}$$

$$CE_{OCS_i} = SE_{OCS_i} \times \frac{\#CP}{m} \tag{5-4}$$

For illustrative purposes, Table 5-1 summarizes the maximum throughput, SE and CE of each OCS*i* in the system presented in Figure 5-2b. For this case, the transceiver provides 412.5 Gb/s total throughput and reaches 68.8% efficiency, computes as the summation of the individual throughput and CE of the OCS slices.

Table 5-1: Example of throughput, SE and CE of each OCS_i

OCS #	**#CP**	**Throughput [Gb/s]**	**SE [%]**	**CE [%]**
1	32	250	83.3	41.7
2	8	37.5	50.0	6.3
3	4	12.5	33.3	2.1
4	4	12.5	33.3	2.1
5	16	100	66.7	16.7
Total		**412.5**	**--**	**68.80**

5.4 Illustrative results

In this section, we first compare by simulation the optical performance of OCS and DSCM. Then, to assess the viability of OCS, quantitative analyses are performed for both OCS and DSCM considering dynamic traffic conditions, for two distinct scenarios in which the traffic handled by the light tree is *i*) P2P and *ii*) P2P +P2MP.

5.4.1 Performance evaluation of DSCM and OCS for optical P2MP

For the evaluation purposes, we implemented a MATLAB-based simulator. For OCS, a single carrier 64-QAM@64GBd DP OCS signal was generated, whereas for DSCM we implemented 64-QAM@64GBd DP with 16 SCs each operating at 4 GBd. The signal is then sampled and sent through a root-raised-cosine pulse shaper with a roll-off factor of 0.06. For DSCM, after applying frequency shift, the SCs were multiplexed. The signal was launched onto an 80-kilometer-long fiber line with N spans; an optical amplifier with a noise figure of 4.5 dB compensates for fiber losses after each span. To simulate ASE noise, additive white Gaussian noise is injected after each span. The fiber channel was simulated using standard single-mode fiber with the following parameters: fiber loss = 0.21 dB/km, dispersion D = 16.8 ps/(km-nm), and nonlinear coefficient = 1.14 W^{-1} km^{-1}. The payload was generated using 2^{13} pseudorandom symbols. The signal was then transmitted using the symmetric split-step Fourier method [NFO13], which solved the nonlinear Schrödinger equation for signal propagation in the fiber channel. The signal was received coherently, and an ideal chromatic dispersion filter was applied. For DSCM, the signal was first demultiplexed and passed through a matched filter before performing the down sampling.

On this simulation scenario, we first analyze the performance of both OCS and DSCM with 16 SCs. Firstly, Figure 5-6 depicts the spectra of the single carrier and

the DSCM signals, where we observe that both signals use the same bandwidth. To study the performance, we simulated a light-tree with two leaves with 8 and 10 spans, respectively. We vary the launch power in the range [-4, +2] dBm. Figure 5-7 presents the average Bit Error Rate (BER) of both polarizations as a function of the power for a light-tree with two leaves with 8 and 10 spans, respectively. We observe that DSCM provides better performance as compared to OCS at higher launch powers where non-linearities are significantly present. This is because each SC operates on a reduced baud rate of 4 GBd. An important point to note here is that although for 8 spans the performance of DSCM is better than OCS, for optimal power the BER remains lower than FEC threshold of 1e-2 in both the cases and post-FEC performance of both systems remain the same. Then, if the main goal is to reduce non-linearities, i.e., for long haul systems, DSCM is a superior solution.

Complementing Figure 5-7, Figure 5-8 details the optical performance of OCS for each individual polarization (Figure 5-8a) and the performance of each SC of the DSCM system (Figure 5-8b), considering for 8 spans. The BER of both polarizations are almost the same in OCS. However, the performance of each SC at -1dbm reveals that the SCs in the center are affected more than the SCs at the extremes, because of SC interaction mainly due to non-linearities. However, the BER remains under FEC threshold, thus guaranteeing the same post-FEC performance of each SC.

5.4.2 Quantitative Analysis

Let us first describe the scenario that we consider to analyze the performance of OCS and DSCM and compare it with a lightpath solution that uses traditional optical P2P co-herent transceivers. We consider two types of traffic for 2 and 4 destinations: i) P2P only; and ii) both P2P and P2MP. For the study, the performance metrics analyzed are the num-ber of required transceivers, the cost of deployment, and the efficiency.

For the traditional P2P lightpath solution, the optical transceivers considered are 25G, 50G, 100G, 200G and 400G [Al21], whereas for OCS and DSCM technologies we assume 600G 64-QAM@64GBd DP transceivers, as introduced in Section 5.4.1. Because in DSCM, receivers might have limitations in terms of the number of SCs they can process, two different availabilities are considered: *i*) *non-aggressive*, which corresponds to current status of P2MP transceivers (e.g., [We21]), where transmitters support 16 SCs for a total 600G capacity, whereas receivers support 8 or 4 SCs, for a total capacity of 300G and 150G, respectively; and *ii*) *aggressive*, where both sender and receivers have 600G installed which enables all possible configurations. The summary of the configurations to be used in the rest of the chapter are summarized in Table 5-2.

Regarding traffic, we consider dynamic traffic scenarios where the capacity requested by destinations vary over time. In this case, a destination needs to support

the maximum traffic of the traffic profile. Hence, destinations must require installing the optical transceiver that supports such data rate or it must possess the

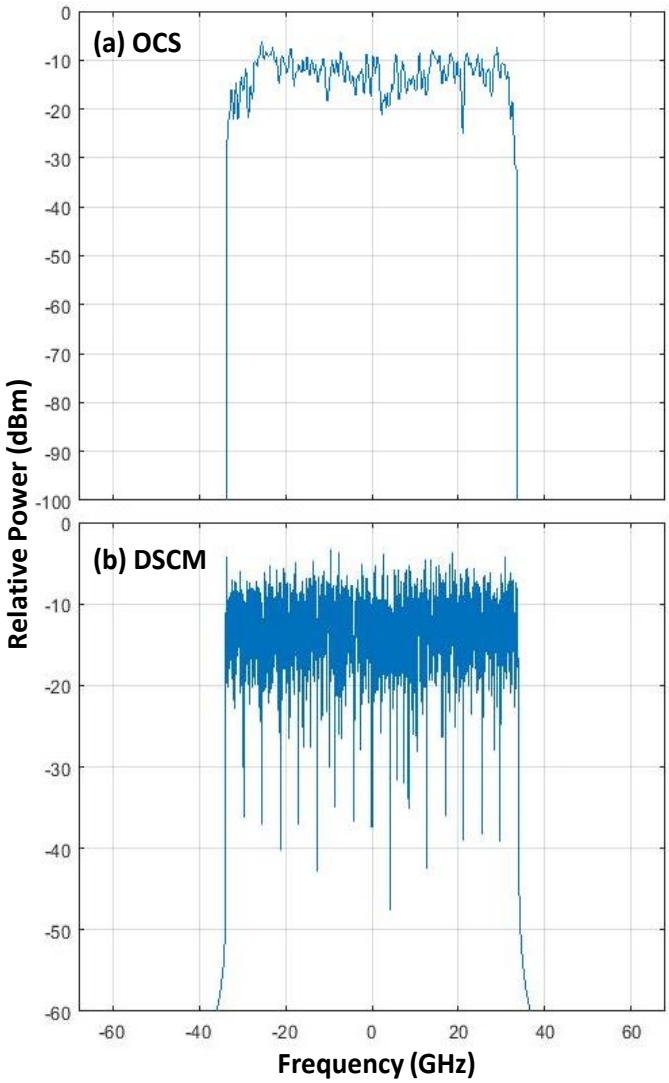


Figure 5-6: Spectrum of the single carrier signal used for OCS (a) and 16 SC DSCM (b)

capacity to dynamically manage the resource allocation according to the traffic profile.

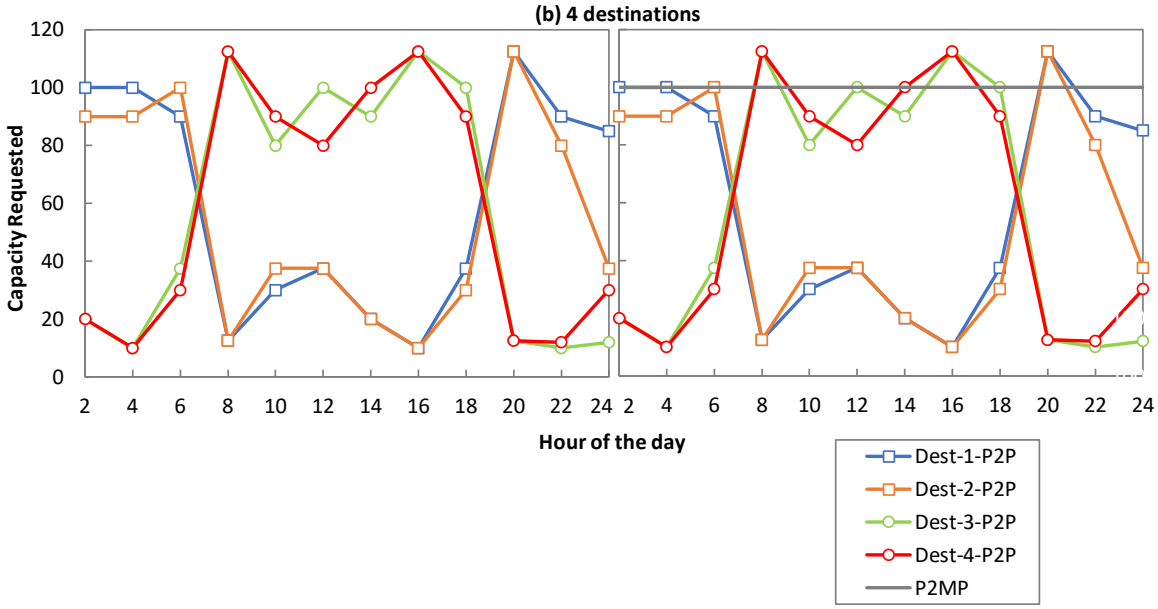


Figure 5-9a-b present the traffic profiles under consideration for 2 and 4 destinations, respectively for pure P2P traffic only and mixed P2P + P2MP traffic. We observe that P2P traffic varies over the day, with some destinations requiring more capacity during day light (8h-18h), whereas other require more traffic during the night (18h-8h). As for the P2MP traffic, we assumed constant 100 Gb/s capacity along the day. The total maximum capacity requirement in the pure P2P traffic scenario is 300 Gb/s, whereas in the mixed one it is 400 Gb/s.

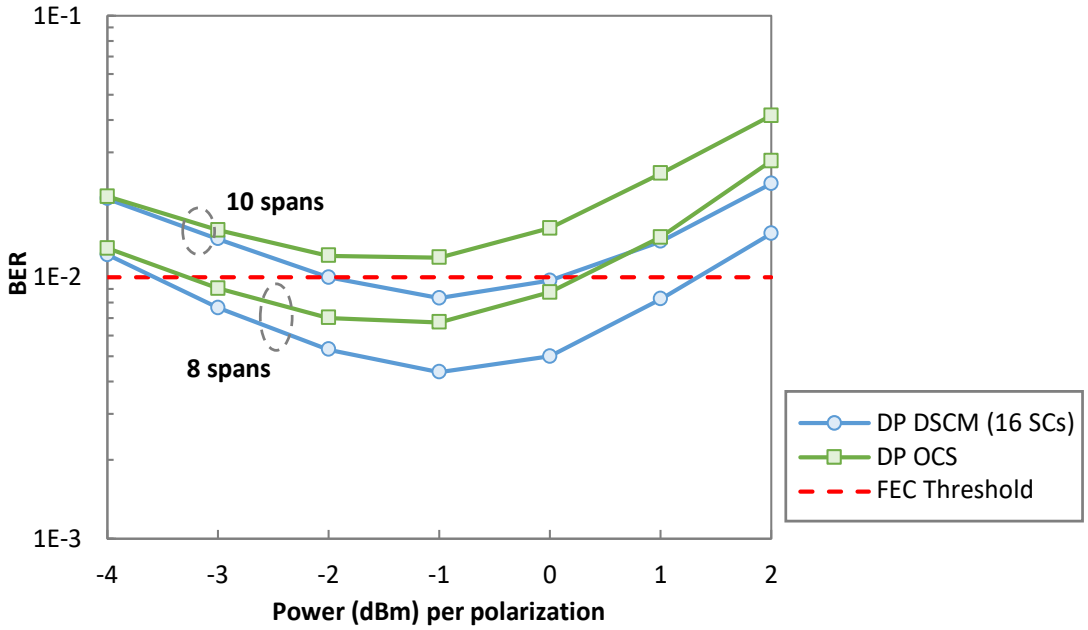


Figure 5-7: Optical System Performance for P2MP

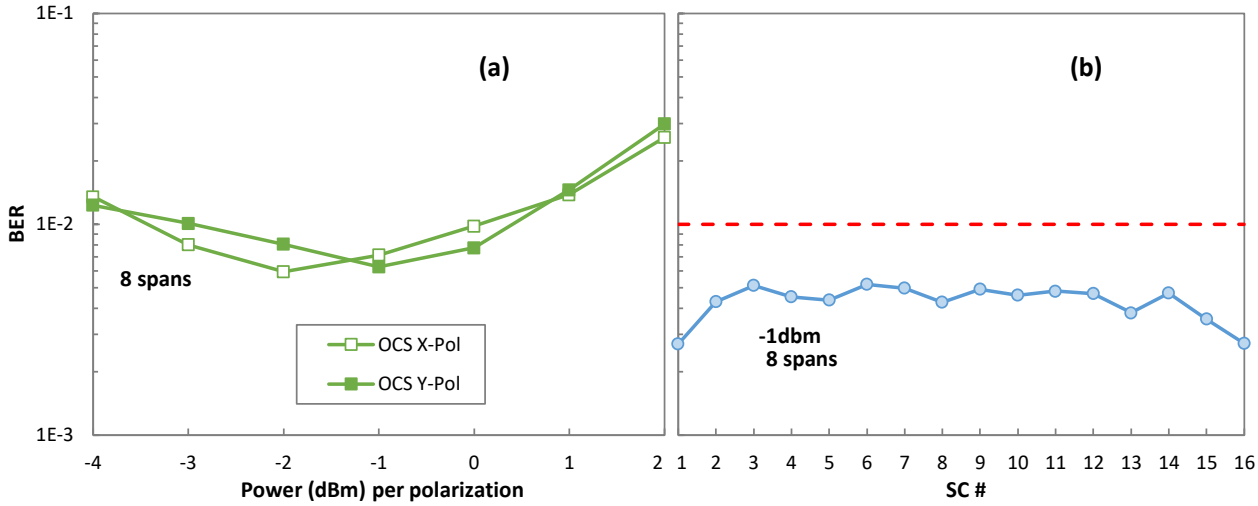


Figure 5-8. Details of Optical Performance of OCS (a) and DSCM (b)

Table 5-2: Available transceivers for P2P, OCS, and DSCM

P2P	OCS	DSCM	
25G	600G 64-QAM @64GBd DP	600G 64-QAM @64GBd DP	150G 4 SCs per polarization
50G			300G 8 SCs per polarization
100G			600G 16 SCs per polarization
200G			
400G			

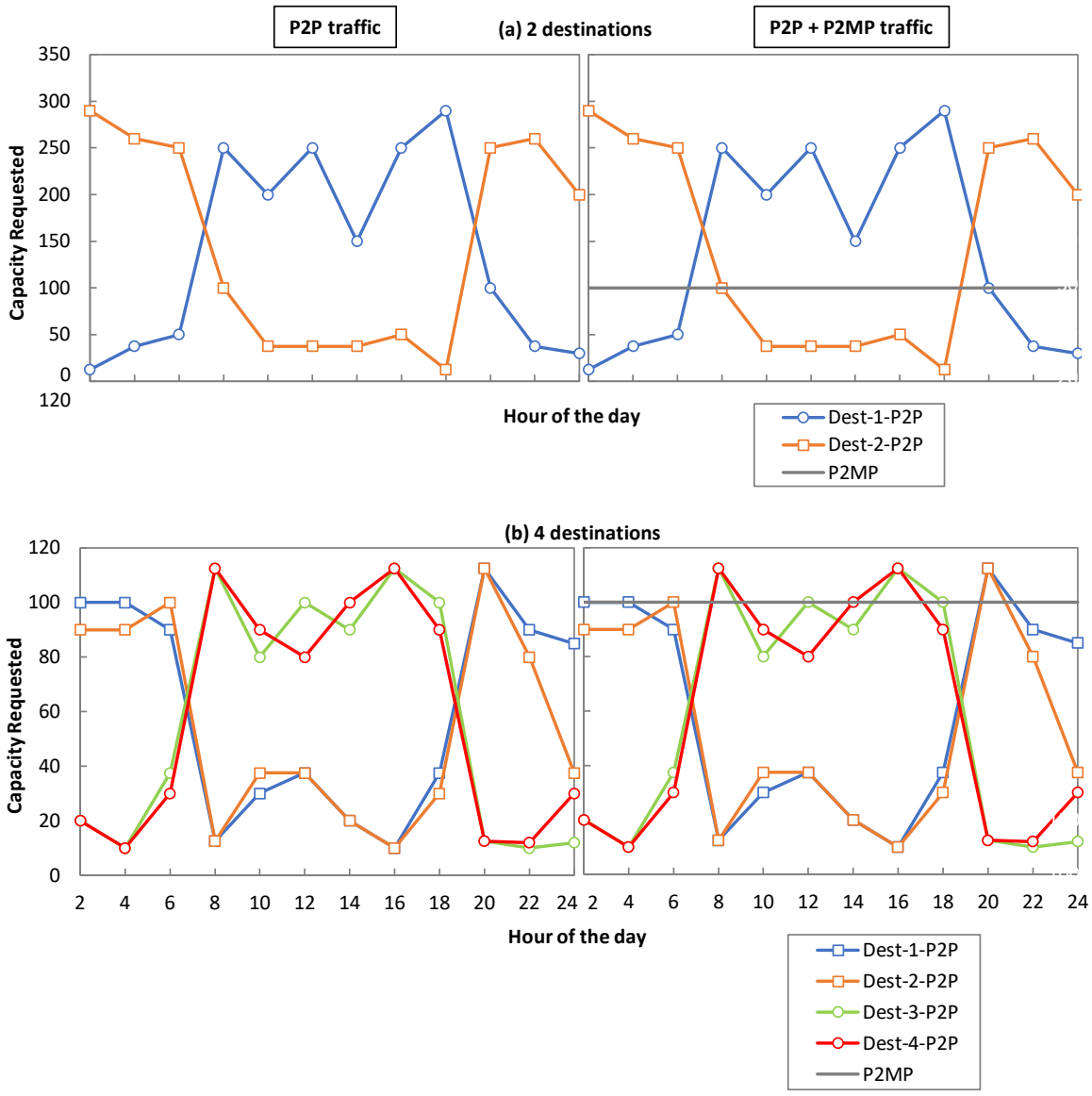


Figure 5-9: Traffic Profiles for P2P and P2P + P2MP traffic with 2 and 4 destinations

Considering the same traffic profile and transceivers' availability as described previously, Figure 5-10 represents savings in terms of number of transceivers required for OCS and DSCM as compared to the P2P lightpath solution. For the P2P traffic scenario, both OCS and DSCM provide equal savings in both aggressive and non-aggressive availabilities. For 2 destinations, reduction in transceivers is 25%, whereas for 4 destinations it is 38%. However, for the P2P+P2MP traffic scenario, we observe different trend. In the aggressive availability, OCS and DSCM provide the same savings, i.e., 57% and 62% for 2 and 4 destinations respectively. However, in non-aggressive availability, OCS outperforms DSCM, which provides 14% and 23% savings for 2 and 4 destinations respectively in comparison of 57% and 62% of OCS, i.e., 43% and 39%, more savings, respectively. The reason behind these results is the additional number of transceivers required in DSCM to serve P2MP traffic.

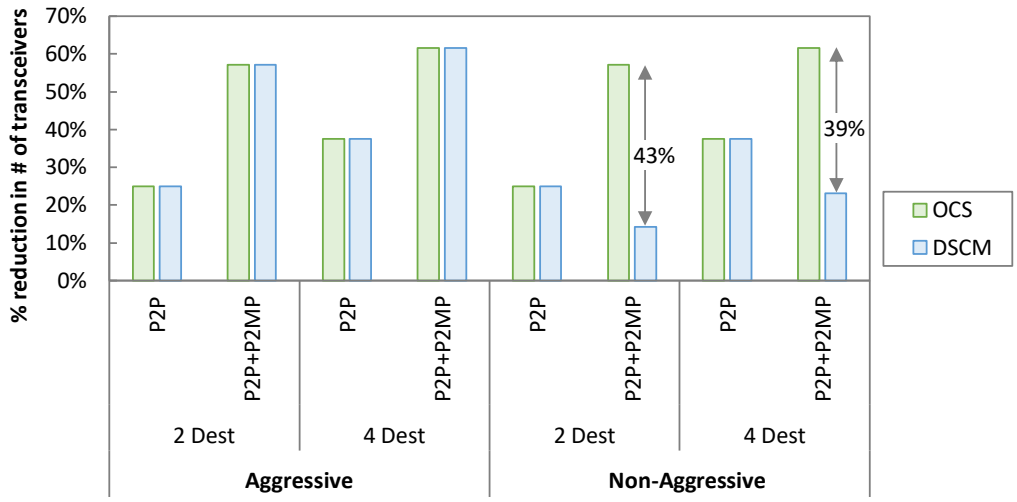


Figure 5-10:. Reduction in number of transceivers

Let us now to analyze the optimal cost of OCS and DSCM transceivers where they start to provide cost savings, as compared with the P2P lightpath solution. To this goal, we model the cost of P2P transceivers and apply the needed constraints to find the targeted cost of OCS and DSCM ones. For the P2P lightpath solution, we consider the optical transceivers availability as in Table 5-2. Based on the cost model in [Ho22], we model the cost (C) of these transceivers in monetary units (m.u.) as a function of bit rate (BR) with $C=\alpha \cdot BR^{\beta}$, where α is a normalization factor to set the cost of the 100G transceiver to 1 and β is a positive constant < 1 that we use to define different cost profiles.

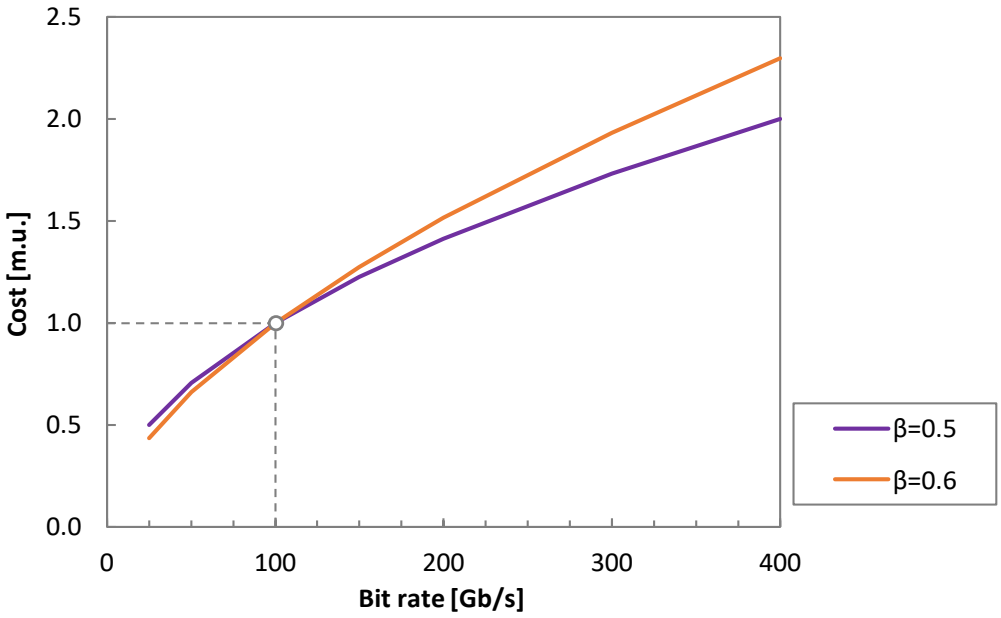


Figure 5-11:. Cost Profile for lightpath transceivers

Two cost profiles are considered for analysis, β=0.5 and β=0.6 (see Figure 5-11), which reproduces technology costs trend to exponentially decrease by generations [Ho22].

However, to enable optical P2MP connectivity, DSCM-600, DSCM-300, DSCM-150, and OCS-600 transceivers require additional DSP features, which translates into additional cost. Although the cost of such transceivers still needs to be determined, it is worth noting that we imposed these relations among costs follow the proportions in Figure 5-12, for β=0.5 and β=0.6

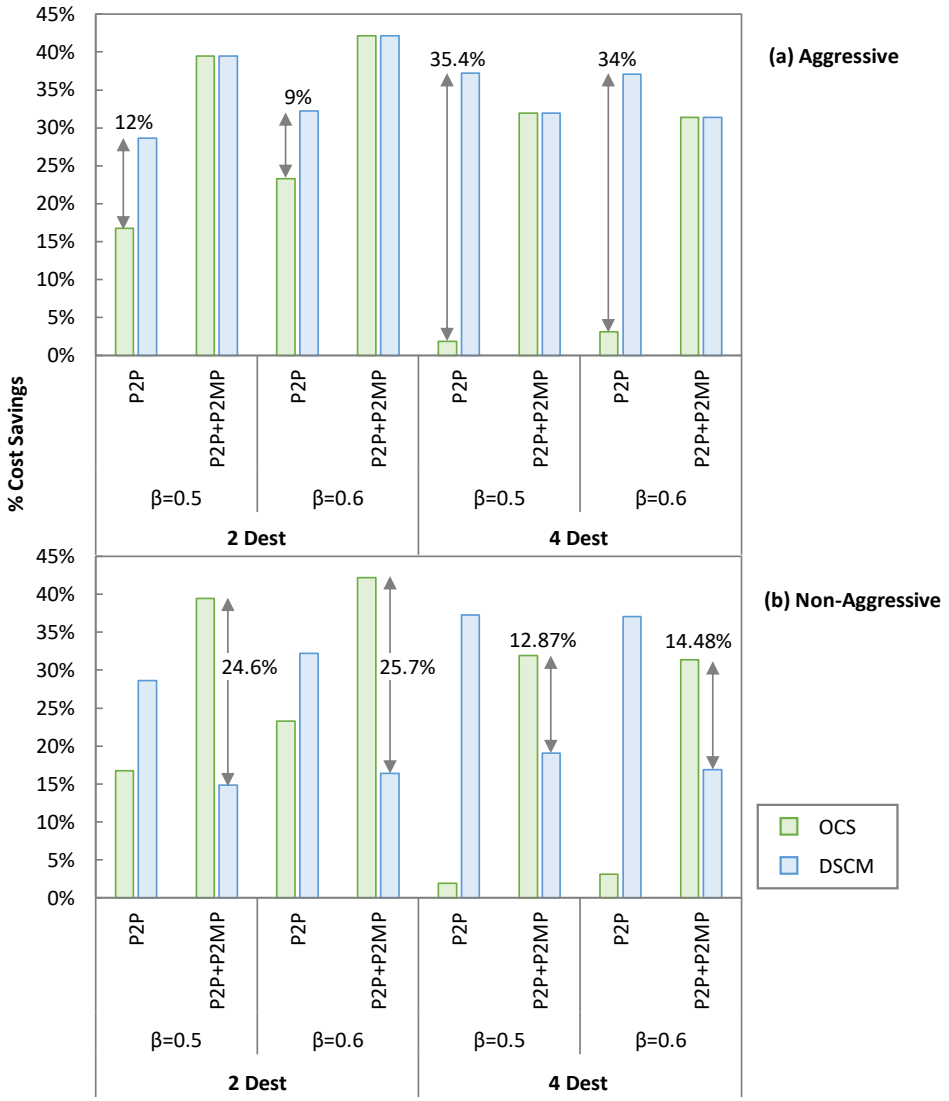


Figure 5-12: Cost Savings-Aggressive approach (a) and Non-Aggressive approach (b)

In the aggressive availability (Figure 5-12a), DSCM outperforms OCS for P2P traffic. For 2 destinations DSCM provides 12 % and 9% more cost savings than OCS for β=0.5 and β=0.6, respectively. The cost savings are more evident for 4 destinations,

where DSCM provides 35.36% and 34 % more cost savings than OCS. However, both OCS and DSCM provide the same savings in the case of mixed P2P+P2MP traffic. For β=0.5, we observe savings of 40% and 32% for 2 and 4 destinations, respectively, similarly as for β=0.6, where the savings are 42.2% and 31.39%, respectively. In the non-aggressive availability (Figure 5-12b), the same savings as for aggressive availability for P2P only traffic are observed, because the installed transceivers remain the same in both the cases. However, for mixed P2P+P2MP traffic, OCS outperforms DSCM mainly because additional transceivers for enabling P2MP traffic need to be installed. For 2 destinations, OCS provides 24.63% and 25.77% more cost savings than DSCM for β=0.5 and β=0.6, respectively. Cost savings are lower for 4 destinations, where OCS provides 12.87% and 14.48% more cost savings than DSCM.

Let us now study the efficiency of DSCM and OCS for optical P2MP, as this metric give us the insight of how efficiently a source can utilize total capacity to serve the requested dynamic traffic profile. For example, in

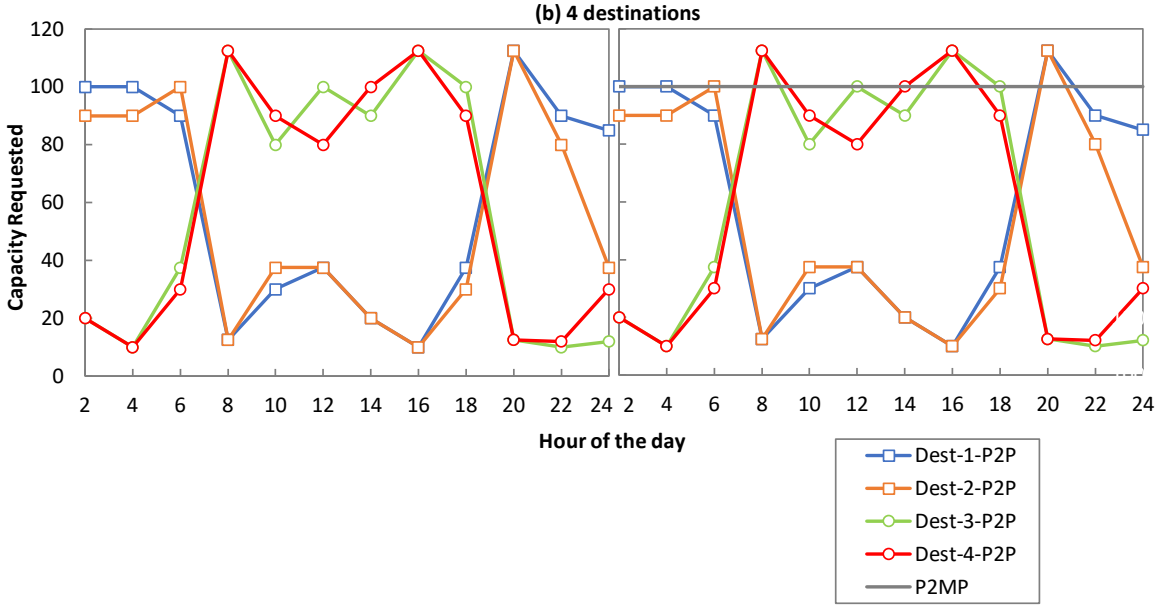


Figure 5-9a at 8h destination 1 requires 250 Gb/s and destination 2 requires 100 Gb/s. In this case efficiency of OCS and DSCM will be 58.33% (350/600), whereas for the P2P lightpath solution efficiency will be 43.75% (350/800). Figure 5-13 shows the efficiency for 2 destinations case for aggressive and non-aggressive availabilities for P2P (Figure 5-13a) and P2P+P2MP (Figure 5-13b) traffics. In the case of the aggressive availability, the efficiency of OCS and DSCM is the same throughout the traffic profiles whereas the efficiency of the P2P lightpath solution is always under that of OCS and DSCM. Under P2P only traffic, OCS and DSCM approaches are utmost 14.6% more efficient than the P2P lightpath solution that is observed at 8h. At that same hour of the day, the maximum efficiency improvement of 25% for P2P+P2MP traffic is observed. In the case of the non-aggressive availability, the same pattern as for the aggressive availability is observed for P2P only traffic.

However, for mixed P2P+P2MP traffic, OCS provides better efficiency than DSCM by being as maximum efficient as 12% at 8h.

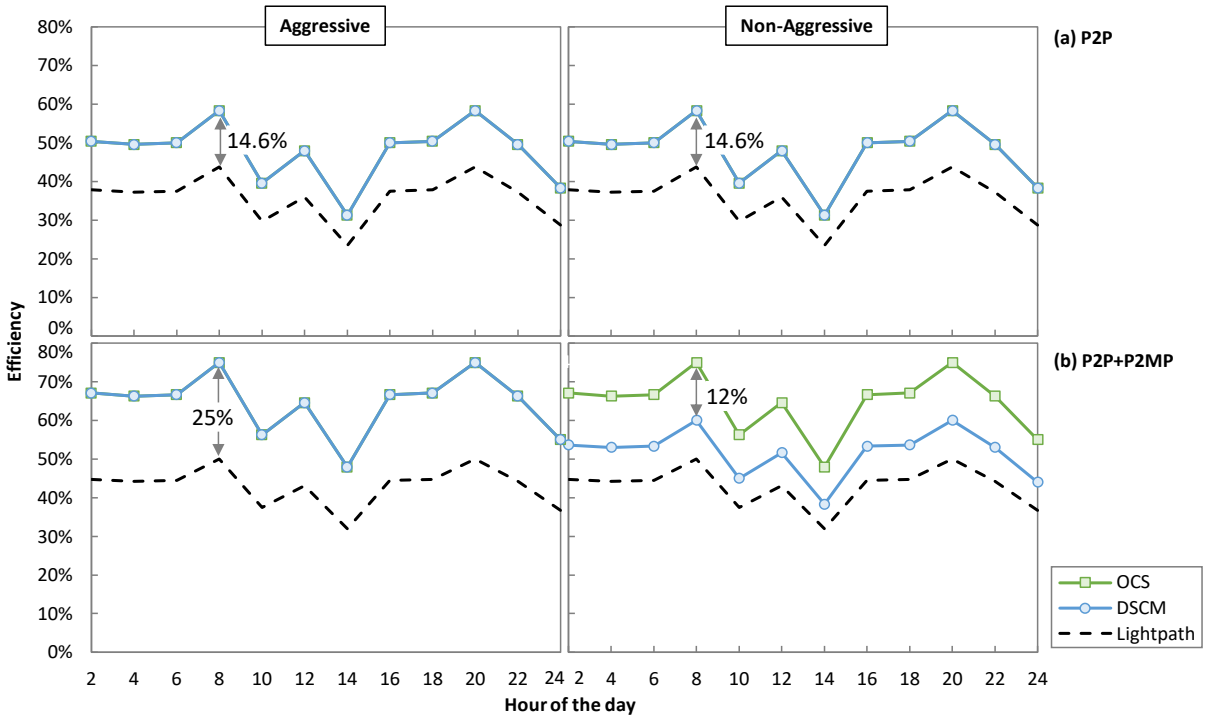


Figure 5-13: Efficiency of aggressive and non-aggressive availabilities for P2P (a) and P2P+P2MP (b) traffics.

In view of these results, let us examine implementing OCS on top of DSCM. For illustrating the OCS+DSCM solution, we consider a destination that is only operating on 1 SC of the DSCM system with 150 Gb/s capacity. Suppose that the capacity required by this node reduces over time and more nodes are needed to be installed. With the OCS on top of DSCM solution, the constellation can be sliced and more nodes can be added, allowing for topology reconfigurability. For example, instead of a single node, two nodes with a capacity of 62.5 Gb/s can be installed if 32 CPs are assigned to each node. Similarly, 4 nodes can be enabled by 16 CPs with capacity of 25 Gb/s each, as illustrated in Figure 5-14.

Furthermore, if the node's desired capacity is less than the overall capacity of the destination, capacity sits unused. We can make better use of destination capacity by adding more nodes by implementing OCS on top of DSCM. Consider the case as shown in Figure 5-15 where capacity requested by a destination working on a 150G SC decreases to 62.5 G. The efficiency of the destination in that case will be 42 % (62.5/150). On the other hand, OCS can provide the benefit of adding one more node by performing 32-CP slicing to increase the capacity utilization to 83.33%.

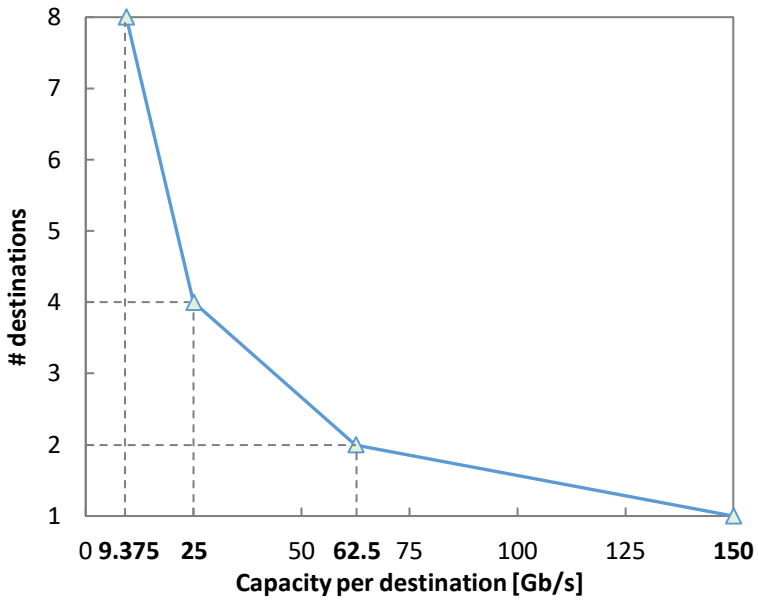


Figure 5-14: Reconfigurability options in OCS+DSCM

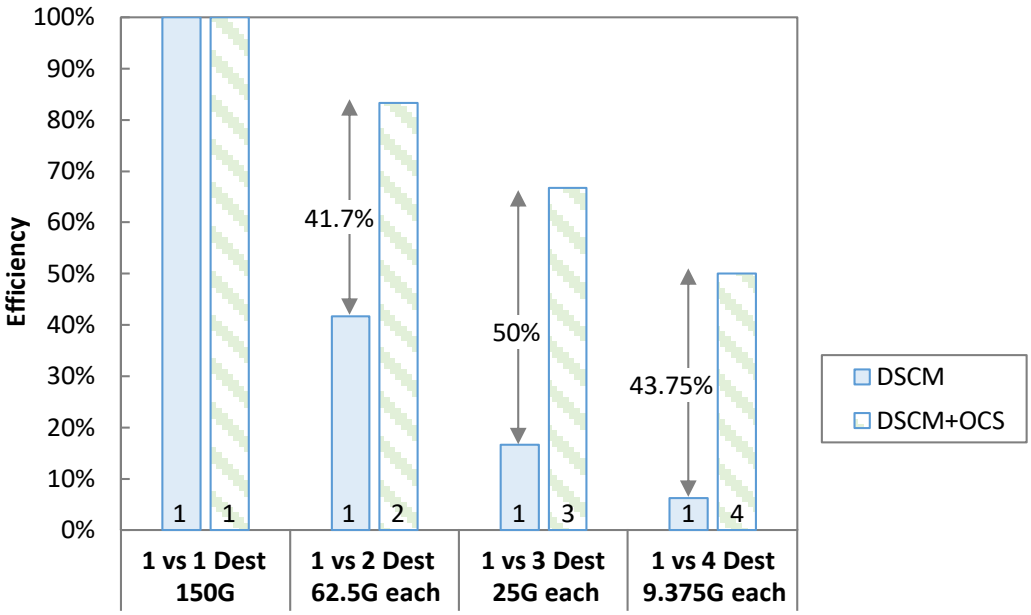


Figure 5-15: Efficiency improvement for OCS+DSCM

5.5 Conclusions

The optical P2MP is compared against traditional P2P when dealing with dynamic P2P and P2P+ P2MP traffic. Two optical P2MP technologies, OCS and DSCM, are studied and compared.

Simulation findings suggest that DSCM decreases non-linearities and outperforms OCS for long-haul applications. However, in access and metro applications, where non-linearities are assumed to be low, the optical performance of OCS and DSCM is similar.

For the sake of a quantitative comparison, aggressive and non-aggressive transceiver availabilities are defined. In the case of pure P2P traffic, both OSC and DSCM greatly re-duce the number of transceivers in the network by the same amount, between 25% and 38%, while simplifying network architecture. DSCM is more cost effective than OCS under both transceiver availabilities. However, when considering P2P+P2MP traffic under the non-aggressive approach, OCS is able to serve them simultaneously without the need for additional transceivers, whereas DSCM requires around 40% more transceivers. In this scenario, costs savings in OCS are noticeably larger than in DSCM. Finally, it is worth to note that OCS and DSCM can co-exist and that this combination can be exploited to real-ize further efficiency improvements.

The next chapters explore to quantum communications as a solution to bring perfect security to optical communications.

Chapter 6

Investigating Imperfect Cloning for Extending Quantum Communication Capabilities

Quantum computing allows the implementation of powerful algorithms with enormous computing capabilities and promises a secure quantum Internet. Despite the advantages brought by quantum communication, certain communication paradigms are impossible and cannot be perfectly implemented due to the no-cloning theorem. Qubit retransmission and point-to-multipoint quantum communication (QP2MP) are among them. In this chapter, we investigate whether a Universal Quantum Copying Machine (UQCM) generating imperfect copies of qubits can help. Specifically, we propose the Quantum Automatic Repeat Request (QARQ) protocol, which is based on its classical variant, as well as to perform QP2MP communication using imperfect clones. As current quantum devices are noisy and they decohere qubits, we analyze these two protocols under the presence of various sources of noise. Three major quantum technologies are studied for these protocols: direct transmission (DT), teleportation (TP), and telecloning (TC). The nitrogen-vacancy (NV)-center platform is used to create simulation models. Results show that TC outperforms TP and DT in terms of fidelity in both QARQ and QP2MP, although it is the most complex one in terms of quantum cost. A numerical study shows that the QARQ protocol significantly improves qubit recovery and that creating more clones does not always improve qubit recovery.

6.1 Introduction

Quantum computing is a promising solution for the next generation of advanced computing with enormous capabilities. The technology is developing rapidly, and soon quantum computers will exchange quantum messages among themselves, enabling distributed quantum computing. Such quantum computers, connected by quantum Internet, can be used for various applications ranging from quantum key distribution (QKD) [Ah22] to specialized quantum computing tasks [WeS18], while guaranteeing information-theoretic security governed by the laws of quantum mechanics, i.e., perfect security as compared to classical approaches [JOCN22]. However, there is a fundamental barrier: the no-cloning theorem [Wo82], which makes perfect duplication of a quantum bit (qubit) -the fundamental unit of quantum information-impossible. This renders some quantum communication paradigms impossible, such as qubit retransmission and point-to-multipoint quantum communication (QP2MP). For the introductory details and state-of-the-art on this topic refer Section 2.5 and Section 3.3

In this chapter, we extend our works in [ONDM22, OFC22] and propose taking advantage of the UQCM for reliable and P2MP quantum communications. Specifically, the contributions of this work are: i) the Quantum Automatic Repeat Request (QARQ) protocol, which combines classical and quantum channels to provide reliable transmission. Here, clones can be created and stored in quantum memories ready to be used in case of qubit loss; and ii) enabling Quantum P2MP (QP2MP) communications, where the transmitter generates multiple clones and sends them to the destinations. We have developed a simulation platform using NetSquid [Co21] to evaluate the feasibility of the QARQ protocol and QP2MP communications in the presence of various noise sources. These protocols are studied for three different quantum technologies: i) direct transmission (DT), which uses a quantum channel for qubit transmission; ii) teleportation (TP) [Ro20], which uses entanglement for transporting qubits; and iii) telecloning (TC) [PeE22] which uses teleportation and cloning natively in the protocol.

The rest of the chapter is organized as follows. Section 6.2 gives the needed background on quantum communications, shows how QARQ and QP2MP can be enabled, and presents the sources contributing to qubit decoherence (the gradual degradation of qubit coherence over time). Section 6.3 focuses on the implementation of QARQ and QP2MP. Section 6.4 evaluates the feasibility of QARQ and QP2MP for short and long-distance quantum communication and determines which method is best suited to achieve the best quality of qubit state. Complexity analysis is carried out for each case. Finally, Section 6.5 draws the main conclusions of this work.

6.2 Quantum bit retransmission and P2MP communications

This section introduces the basics on how a quantum communication channel is established using QARQ or QP2MP. Then, sources of decoherence present in QARQ and QP2MP for DT, TP and TC are eventually demonstrated.

6.2.1 Quantum communication enabling QARQ and QP2MP

Figure 6-1 describes the QARQ protocol, where we consider a quantum communication system consisting of two quantum nodes, namely Alice (*A*) and Bob (*B*). The quantum channels (solid lines) are used to transmit qubits from *A* to *B* by means of DT, TP or TC, while the classical channels (dashed lines) are used to exchange classical messages between them.

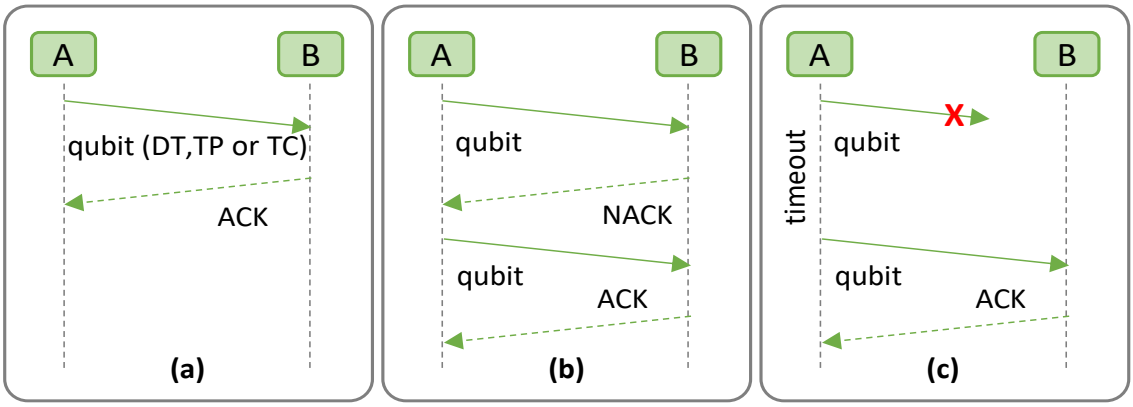


Figure 6-1 The QARQ Protocol

As in classical ARQ, QARQ uses acknowledgement (ACK) and timeout messages to achieve reliable quantum communication over an unreliable quantum system. *A* may send the quantum data with error detection codes, e.g., repetition codes to check whether the quantum data are received correctly. If no error is detected, *B* notifies *A* using a positive ACK (PACK) via the classical channel and the quantum memory is flushed (Figure 6-1a). Conversely, if an error is detected and it cannot be recovered, *B* discards the quantum data and sends back a negative ACK (NACK) (Figure 6-1b). When *A* receives the NACK, the cloned quantum data stored in the quantum memory are sent to *B*. Additional retransmissions can be done if more clones are generated but at the expense of degradation of qubit fidelity. Moreover, QARQ sets timeouts for retransmission, where A uses the stored qubits if no ACK is received after a specified time period (Figure 6-1c).

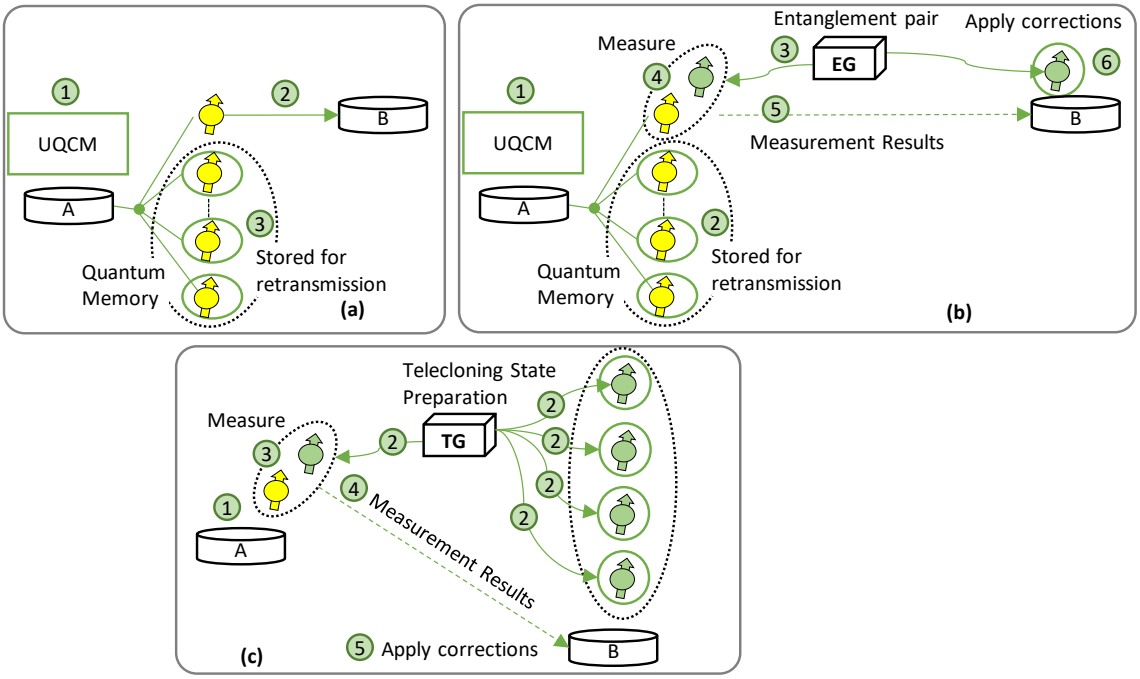


Figure 6-2 QARQ for (a) Direct transmission (b) Teleportation (c) Telecloning

Let us now describe the procedure to setup a quantum communication channel enabling QARQ. Figure 6-2 shows the basic principle of QARQ. The UQCM can create multiple clones for retransmission, where the number of clones to be generated highly depends on the quantum application. Additionally, the generation of multiple clones is done at the expense of degrading the qubit's state. Figure 6-2a represents QARQ when implemented on DT (QARQ-DT), where qubits go into the UQCM before transmission to generate imperfect clones; for each received qubit, one of the clones is sent to B using a quantum channel and the others are stored in quantum memories. Figure 6-2b shows the implementation of QARQ in TP (QARQ-TP). TP allows the qubit to be transported from one point to another without traversing the quantum channel by making use of quantum entanglement and classical measurement. In Figure 6-2b, qubits also go into the UQCM to generate clones, but instead of using the quantum channel pre-distributed entanglement pairs are provided to *A* and *B* by an Entanglement pair generator (EG). EG can be present at any intermediate point between *A* and *B*. Each transmission uses these entanglement pairs to perform teleportation of qubits. Figure 6-2c represents QARQ exploiting TC (QARQ-TC). TC requires the preparation of telecloning states by a telecloning state generator (TG) and a measurement to create and send all the clones together. It saves the classical channels and the number of measurements needed to send clones. In QARQ-TC, we prepare the TC states and distribute them between *A* and *B*. All clones are sent directly to *B* which uses the first clone if transmission is successful otherwise uses clones residing at its quantum memories.

Figure 6-3 shows the similar setup for QP2MP communications, where *A* holds a qubit and wishes to send it to several recipients (B, Charlie (C), etc.). The best *A* can do is to realize optimal copies of the quantum states, which are presumed to be workable if they are over some application-specific threshold, and send them to the desired destinations.

For the sake of explanation, only two destinations are considered in Figure 6-3. Figure 6-3a represents the QP2MP implementation for DT (QP2MP-DT). Here, quantum clones are sent to multiple destinations (to *B* and *C* in Figure 6-3a). In Figure 6-3b, which represents QP2MP implementation for TP (QP2MP-TP), all

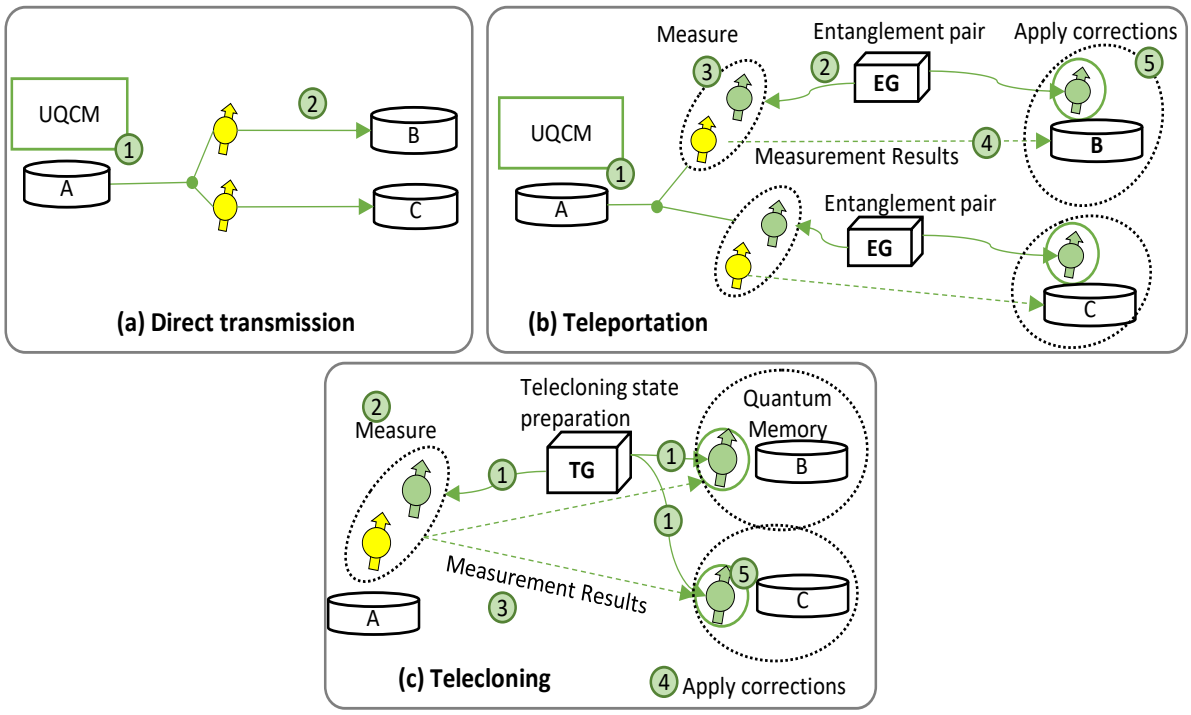


Figure 6-3 Example of QP2MP using direct transmission (a), teleportation (b) and telecloning (c)

clones are sent to multiple destinations by using the pre-distributed entanglement pairs. Figure 6-3c depicts the QP2MP using TC (QP2MP-TC), where all the clones are received by all the destinations at once and utilized for processing.

6.2.2 Sources of decoherence in QARQ and QP2MP

Once QARQ and QP2MP have been introduced, we can examine specific factors contributing to qubit decoherence in each of the three quantum technologies studied. This provides the insight of received qubit's fidelity, which is vital in both QARQ and QP2MP.

In QARQ-DT (Figure 6-2a), *A* generates optimal clones before transmission to *B* (labeled 1 in Figure 6-2a); this introduces decoherence due to the delay of gate operation. One of the clones is sent through the quantum channel in DT (2), which causes transmission channel decoherence. The remaining clones are stored in quantum memories where they decohere until utilized. In the case of QARQ-TP (Figure 6-2b) an EG is needed. *A* generates optimal clones (1); one is transported through teleportation and rest of the clones are stored in quantum memory (2). The EG (3) generates entangled pairs for *A*-*B*. We assume entanglement pairs for all the clones are generated at the beginning of session. The fidelity of the teleported qubit degrades if the entanglement generation is not perfect. Next, bell measurements between clones and entangled qubits are performed at *A* (4) and the results are sent to *B* via the classical channel (5). Due to this, the entangled qubit at *B* must wait in the quantum memory where decoherence also occurs before applying corrections (6). If retransmission is needed, it will occur by utilizing the decohered entanglement pairs and clones waiting in the quantum memories. In QARQ-TC (Figure 6-2c) *A* holds a qubit (1) and TG is needed to perform telecloning. TG prepares the TC state and distributes it among *A* and *B* (2). If the fidelity of the TC state is imperfect it impacts the fidelity of the transported qubit. Meanwhile, *A* performs measurement between source qubit and the TC one (3). Measurement results are sent to *B* via classical channel (4), where corrections are applied (5). Due to (3) and (4), the TC qubit at *B* must wait in a quantum memory where they experience decoherence (5).

In QP2MP-DT (Figure 6-3a), *A* generates optimal clones before transmission to destinations *B* and *C* (1); this introduces decoherence due to the delay of gate operation. Clones are sent through the quantum channel in DT (2), which brings transmission channel decoherence. In the case of QP2MP-TP (Figure 6-3b) EG is needed. We assume that the EG is at some intermediate location between *A, B*, and *C*. As in DT, A generates optimal clones for *B* and *C* (1). However, in this case the qubits are transported using quantum entanglement and classical measurement without traversing the quantum channel. The EG generates entangled pairs for *A*-*B* and *A*-*C* (2), which degrades the fidelity of the teleported qubit if the entanglement generation is not perfect. Next, bell measurements between clones and entangled qubits are performed at *A* (3) and the results are sent to *B* and *C* via the classical channel (4). Due to (3) and (4), the entangled qubits at *B* and *C* must wait in the quantum memory, where decoherence occurs before applying corrections (5). QP2MP-TC (Figure 6-3c) also needs a TG at some intermediate location. The TG prepares the TC state and distributes it among *A, B* and *C* (1 in Figure 6-3c). If the fidelity of the TC state is imperfect it impacts the fidelity of the transported qubit. Meanwhile, *A* performs measurements between source qubit and a TC qubit (2). Measurement results are sent to *B* and *C* via classical channel (3), where corrections are applied (4). Then, the TC qubit at *B* and *C* must wait in a quantum memory where they experience decoherence (5).

6.3 Implementation and quantum hardware design of QARQ and QP2MP

This section is devoted to the implementation of QARQ and QP2MP. First, it details the phases of QARP and QP2MP and then it presents the quantum circuit design for DT, TP, and TC used in QARQ and QP2MP.

6.3.1 Phases of QARQ and QP2MP

Let us now describe the specifics of QARQ and QP2MP. In the first case, QARQ-DT, QARQ-TP and QARQ-TC methods consists of three main phases: i) initialization; ii) transmission; and iii) QARQ. Initialization and transmission phases are jointly executed by both the sender and the receiver, while the QARQ protocol is introduced after the transmission begins with sender and receiver listening to each other for ACKs. The initialization and transmission phases are different in each of the quantum technologies, i.e., DT, TP, and TC (see Figure 6-2), while the QARQ phase is similar for DT and TP, but different for TC (see Figure 6-3).

In the initialization phase in DT and TP, clones using UQCM, are created. In DT, the initialization phase stops here, whereas in TP M entanglement pairs are also requested and distributed in parallel to nodes A and B to be used during the teleportation phase. In TC, however, a qubit is prepared and a TC state is requested. During the transmission phase in DT, clones are sent to B via the quantum channel. In TP and TC clones are sent by TP and TC protocols as described in Section 2.

Finally, in the QARQ phase, in the case of DT and TP, the receiver waits for successful recovery of transmitted clone and sends ACK if the reception was successful and NACK otherwise. The sender waits for the response from the receiver and if NACK is received or a time limit is exceeded, it retransmits stored clones via DT or TP. The cycle repeats until either PACK is received by the sender or there are no clones left. For TC, all clones are at the side of B, which sends PACK if one of the clones was successfully received and sends NACK if none of the clones was useful and transmission begins again.

Table 6-1 shows two types of probabilities of successful transmission of a qubit with QARQ as a function of the number of generated clones r: *i)* $p_{qr}(p)$, where p is the probability of successful transmission without QARQ; and *ii*) $p_{qfr}(p,f_r)$, where f_r is the fidelity of the transported qubit. Note that $p_{qr}(\cdot)$ increases with the number of clones. However, cloning in the UQCM reduces f_r, which reduces the probability of successful recovery given by $p_{qfr}(\cdot)$. As a consequence, the optimal number of clones needs to be investigated to maximize $p_{qfr}(\cdot)$.

As for QP2MP, only the initialization and transmission phases are present, which are the same as QARQ except that the clones sent to destinations are directly

processed and not stored in the quantum memory. Also, entanglements are directly utilized for transporting qubits instead of waiting to be utilized when retransmission is requested as in case of QARQ

Table 6-1: Probability of successful transmission

# clones	$p_{qr}(p)$	$p_{qfr}(p,f_r)$
2	$p_{q2} = p + (1-p) \times p$	$p_{qf2} = p_{q2} \times f_2$
3	$p_{q3} = p_{q2} + (1-p_{q2}) \times p$	$p_{qf3} = p_{q3} \times f_3$
4	$p_{q4} = p_{q3} + (1-p_{q3}) \times p$	$p_{qf4} = p_{q4} \times f_4$

6.3.2 Quantum circuits design for QARQ and QP2MP

This section analyses the quantum hardware on gate level to perform DT, TP and TC to realize QARQ and QP2MP. Table 6-2 summarizes the used notation.

Table 6-2 Notation

q0	Original qubit
q1	Blank paper
b	Qubit representing photocopier machine
qxi	x part of the *ith* entanglement pair
qyi	y part of the *ith* entanglement pair
qP	Port bit of TC state
Ani	Ancilla bits
qMi	Qubits used for cloning in TC state
$\|\Psi\rangle$	State of original qubit
$\|\Psi^*\rangle$	State of cloned qubit
$\|0\rangle$	Qubit at 0 state
$\|\varphi+\rangle$	State of the entanglement pair
$\|\theta\rangle$	State of the telecloning state
$\|.\rangle_{(.)}$	Single qubit state
$\|.\rangle_{(.)....(.)}$	Multiple qubits state

Figure 6-4a shows a case where the UQCM generates two clone states $|\Psi^*\rangle_{q0}$ and $|\Psi^*\rangle_{q1}$ of a qubit *q0*, which is prepared in random state $|\Psi\rangle$ ($|\Psi\rangle_{q0}$). These clones can be used either for DT (Figure 6-4a) or TP (Figure 6-4b) in QARQ or QP2MP. Figure 6-4c describes the TC hardware.

Let us describe how $|\Psi^*\rangle_{q0}$ and $|\Psi^*\rangle_{q1}$ are created by the UQCM, in Figure 6-4a. The cloning at the UQCM can be subdivided into a preparation phase and copying phase. Input *q1* represents a *blank paper* on which information is copied and *b* is a *photocopier machine* that aids in the creation of copies but does not include any information of the input qubit; both are initialized to state $|0\rangle$. Before interacting

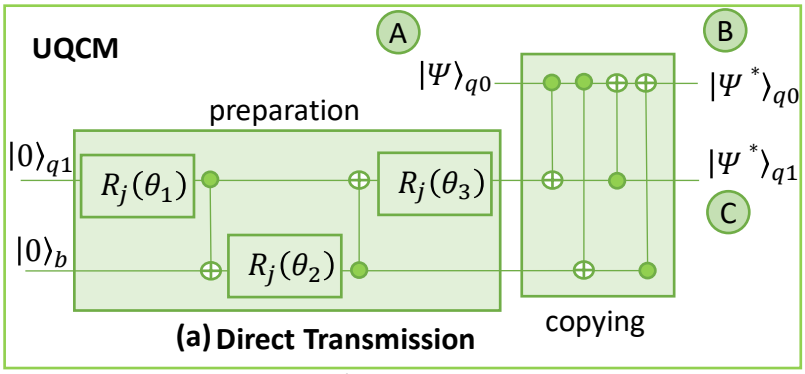
with the original qubit state $|\Psi\rangle_{q0}$, the quantum copier is set in a specified state generated by the preparation block during the preparation state. In the preparation block, three rotations ($R(\theta_j)$) are performed by three Y-rotation gates and two controlled-not (CNOT) gates to impose the desired state [Bu98]. After preparing the qubit states of the quantum copier, four CNOT gates can be utilized sequentially in the copying network to obtain a copy of the initial state. Figure 6-5 shows the Bloch sphere representation of the output of UQCM in ideal operating conditions. $|\Psi\rangle_{q0}$ is initialized randomly and the two clones ($|\Psi^*\rangle_{q0}$ and $|\Psi^*\rangle_{q1}$) are created with 83.33% fidelity. Figure 6-4a, DT is shown where for QARQ $|\Psi^*\rangle_{q0}$ is sent to B and $|\Psi^*\rangle_{q1}$ is stored in quantum memory. For QP2MP, $|\Psi^*\rangle_{q0}$ is sent to B and $|\Psi^*\rangle_{q1}$ is sent to C.

Figure 6-4b shows the quantum circuit for TP. The first step is to create the maximally entangled states ($|\varphi^+\rangle_{qxiqyi}$), all between A and B for QARQ or among multiple parties for QP2MP. In Figure 6-4b two entanglement pairs are generated in the state $|\varphi^+\rangle_{qx0qy0}$ and $|\varphi^+\rangle_{qx1qy1}$. To generate the entanglement pairs qubits *qx0 (A), qy0 (B), qx1(A),* and *qy1(B)* are prepared in state $|0\rangle$. The Hadamard gate (*H*) followed by a CNOT gate is used to generate the entangled state. Then, *A* performs a bell measurement on $|\Psi^*\rangle_{q0}$ and $|\Psi\rangle_{qx0}$ which is done by applying a CNOT gate followed by an *H* gate. Measurement results are sent to *B* as a classical message which applies correction in terms of Pauli Gates (the quantum gates) I, X, Z, and ZX [BeC19], if the measurement results were 00, 01, 10, and 11, respectively. After corrections, the state of *qy0* becomes equal to $|\Psi^*\rangle_{q0}$. For QARQ, $|\Psi^*\rangle_{q1}$ is stored in the quantum memory and teleported later to *B*, if needed, using $|\varphi^+\rangle_{qx1qy1}$, whereas for QP2MP $|\Psi^*\rangle_{q1}$ is teleported to C immediately using $|\varphi^+\rangle_{qx1qy1}$.

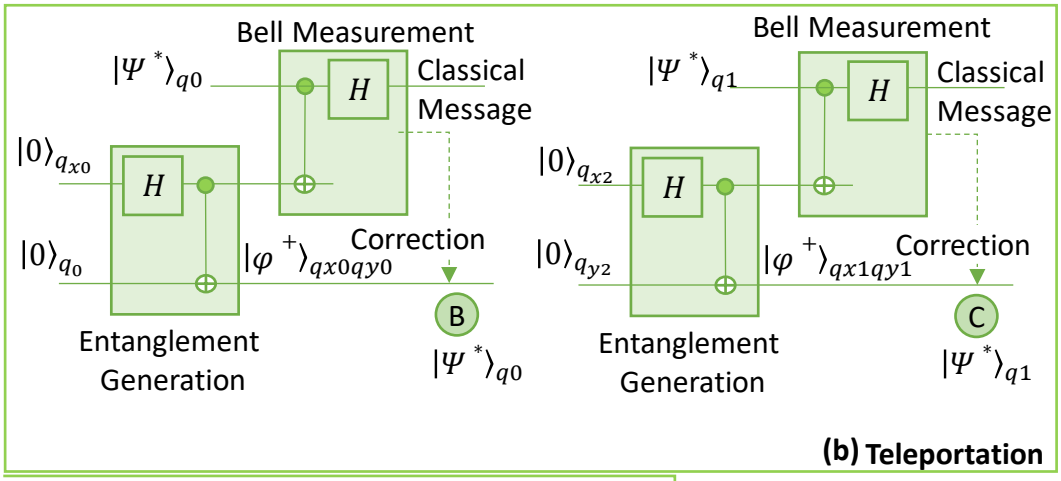
Figure 6-4c represents the quantum circuit for telecloning. The circuit requires preparing the TC state which is achieved with 1 port qubit (*qP*), potentially M−1 *ancilla* qubits (*qAni*) and *M* qubits to be used for clones (*qMi*) in the state $|\theta\rangle_{TCM} = |\theta\rangle_{qPqAniqMi}$ [PeE22]. *qP* is at sender side (*A*), *qMi* at the receiver side (*B* and/or *C*), and *qAni* can be anywhere. Figure 6-4c shows the circuit for two clones. To prepare $|\theta\rangle_{TC}$ first *qP, qAn1, qM1,* and *qM2* set to $|0\rangle$ and then corresponding gate operations are applied to obtain $|\theta\rangle_{TC}$ as

$$|\theta\rangle_{TC_2} = \left[\frac{1}{\sqrt{3}}, 0,0,0,0, \frac{1}{\sqrt{12}}, \frac{1}{\sqrt{12}}, 0,0, \frac{1}{\sqrt{12}}, \frac{1}{\sqrt{12}}, 0,0,0,0, \frac{1}{\sqrt{3}}\right] \quad (6\text{-}1)$$

In Figure 6-4c, *A* performs a bell measurement on its qubit *q0* with *qP* of $|\theta\rangle_{TC2}$ same as TP and sends the measurement results to *B* in case of QARQ, and to B and *C* in case of QP2MP, where corrections are applied similarly to TP to convert the state of *qM1* and *qM2* into $|\Psi^*\rangle_{q0}$ and $|\Psi^*\rangle_{q1.}$



In QARQ and QP2MP $|\Psi^*\rangle_{q0}$ goes to B.
In QARQ $|\Psi^*\rangle_{q1}$ goes into quantum memory and in QP2MP it goes to C.



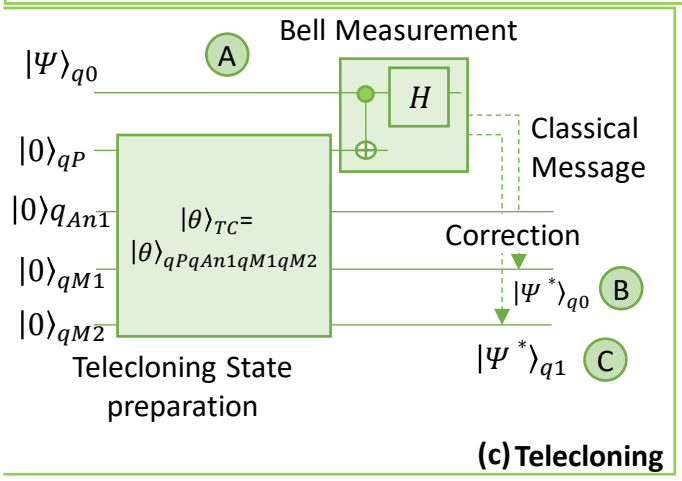


Figure 6-4 Quantum circuit for QARQ and QP2MP. Direct transmission (a), teleportation (b) and telecloning (c)

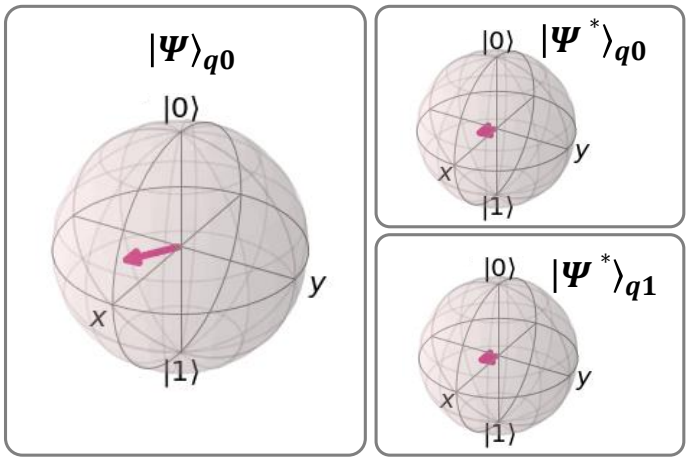


Figure 6-5 Bloch sphere representation of UQCM output

6.4 Illustrative results

In this section, we focus on the evaluation of the performance of QARQ and QP2MP. To that end, we used NetSquid [Co21], a simulator designed specifically for modeling quantum networks that allows precise modeling of quantum physical devices. The gates used in the simulations are based on the parameters given in Table 6-3 [LiC22], which indicate NV-center implementation and are modeled as depolarizing noise. For a fair comparison, we assume that the depolarization probability (*dp*) of all gates is equal to 0.01. The depolarization probability per km of the fiber is examined also for channel decoherence. The T1T2 noise model is used for quantum memory, with T1=10h and T2=1s, where T1 and T2 are the decay and decoherence time constants for the NV-center platform [LiC22]. For the sake of simplicity, the entanglement is generated for each clone at the start of the protocol. Then, each clone has an entanglement pair ready before transmission. The maximum theoretical fidelity of UQCM is 0.833, 0.77, and 0.75 for 2, 3, and 4 clones, respectively.

Table 6-3: Time duration of gates

Operation	Duration
Single-qubit gate	5ns
CNOT gate	20μs
Measurement	3.7μs
Rotation gate	20μs

6.4.1 QARQ

Let us first focus on the performance of quantum technologies for QARQ. Figure 6-6 compares the performance of QARQ-DT and QARQ-TP for 2 clones in terms of fidelity of the received qubit. This can be used later to analyze the significance of implementing QARQ in quantum communication. In Figure 6-6a for QARQ-DT, we observe the fidelity of the transmitted and retransmitted qubit. The fidelity of qubit in DT highly depends on the length of the quantum channel and degrades faster as *dp* increases (from 0.001to 0.005 in Figure 6-6a). This leaves the QARQ-DT protocol as an unsuitable candidate for long-distance transmission as QARQ performance depends on f_r (see Table 6-1). The degrading effect of the distance is not observed in Figure 6-6b, when teleportation is used, since f_r mainly depends on entanglement fidelity (fe_{TP}) of entanglement pairs and not on the distance. fe_{TP} represents the end-to-end fidelity of the pair once reached to desired ends. However, fe_{TP} depends on the distance traversed by entanglement pairs during distribution. To cater this effect, we consider imperfect fe_{TP} (0.988 and 0.962 in case of Figure 6-6b). Remember that entanglement distillation can be performed to achieve the desired entanglement [Ge22], which is out of the scope of this PhD thesis. This suggests that QARQ-TP might be a better solution for longer distances. Comparing both solutions, we observe in Figure 6-6c that DT provides better fidelity in short distances (up to 9km), whereas QARQ-TP is superior for longer distances.

QARQ-DT and QARQ-TP depend upon creating clones by UQCM before sending the qubits to destinations and UQCM degrades the fidelity of qubit. In the case of QARQ-TC, a special entangled state TC is used to perform cloning and teleportation, so fidelity mainly depends on the fidelity of the entangled state (fe_{TC}). Figure 6-6d compares the performance of QARQ-TP and QARQ-TC and it demonstrates that if we consider fe_{TC} equal to fe_{TP} (0.988 and 0.962), QARQ-TC can provide better fidelity than QARQ-TC (only transmission case is plotted here). Specifically, we found that the improvement in fidelity of the received qubit is 2.73% and 3.24% for fe_{TC}=0.988 and fe_{TC}=0.962, respectively.

Let us now to perform a quantitative analysis of QARQ by comparing the probability of successful transmission with QARQ (p_{qfr}) and without QARQ (p) (Figure 6-7). The impact of fidelity degradation in the protocol due to various sources of decoherences is considered. Figure 6-7a describes the cases where the QARQ protocol could provide better qubit recovery, assuming 2 clones. Three fidelity values are studied: 0.75, 0.8, and 0.833. When p=0.7, p_{qf2} rises to 0.76 for fidelity 0.833. However, when p increases to 0.9, p_{qf2} is only 0.825 as it can never exceed the maximum theoretical value of 0.833. This means that the protocol can only offer better p_{qfr} when p is lower than the fidelity of UQCM. Figure 6-7b shows the improvement of QARQ in probability of successful transmission for 2 clones. In the case of p=0.6, improvements of 16.67%, 12%, and 5% are observed for fidelity of 0.833, 0.8 and 0.75, respectively. However, for p=0.7, QARQ fails to provide improvement for fidelity of 0.75. Finally, Figure 6-7c

analyzes QARQ performance for 2, 3 and 4 clones (results consider maximum theoretical fidelity) and provides insight about the cases where increasing the number of clones can help. With 4 clones and $p \leq 0.6$ we observe better p_{qf4} than with only 3 (p_{qf3}). The same effect can be observed with 3 clones, which provides better p_{qf3} than with only 2 (p_{qf2}). However, for p=0.7 and 3 or 4 clones, QARQ provides improvement in qubit recovery, but 2-clones seems a better solution in this case due to the large impact of fidelity on QARQ performance. As a conclusion, QARQ-TC provides better fidelity than QARQ-TP whereas the later provides better fidelity than QARQ-DT. All these quantum technologies can significantly improve the probability of successful transmission of qubits. In addition, increasing the number of clones does not always increase the probability of successful transmission of qubits.

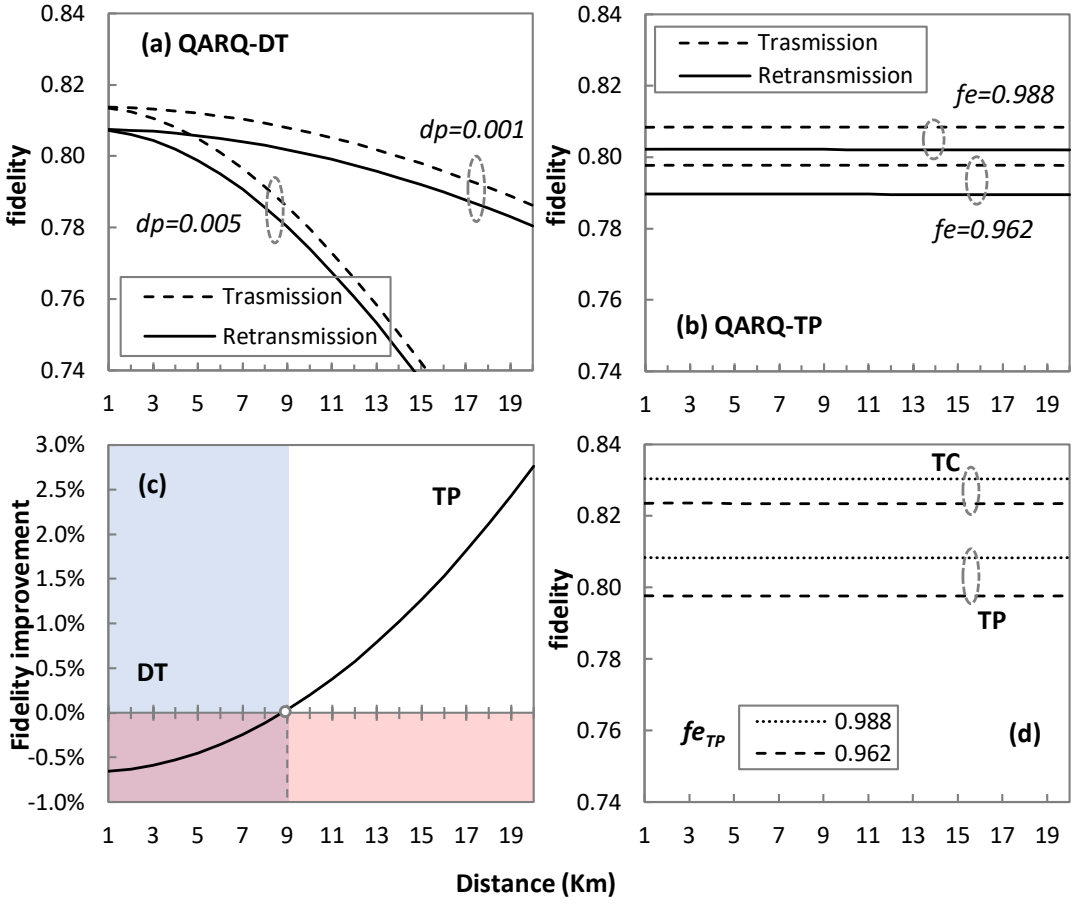


Figure 6-6 QARQ quantum technologies performance comparison. QARQ-DT(a), QARQ-TP (b), DT and TP comparison (c), and TC and TP comparison (d)

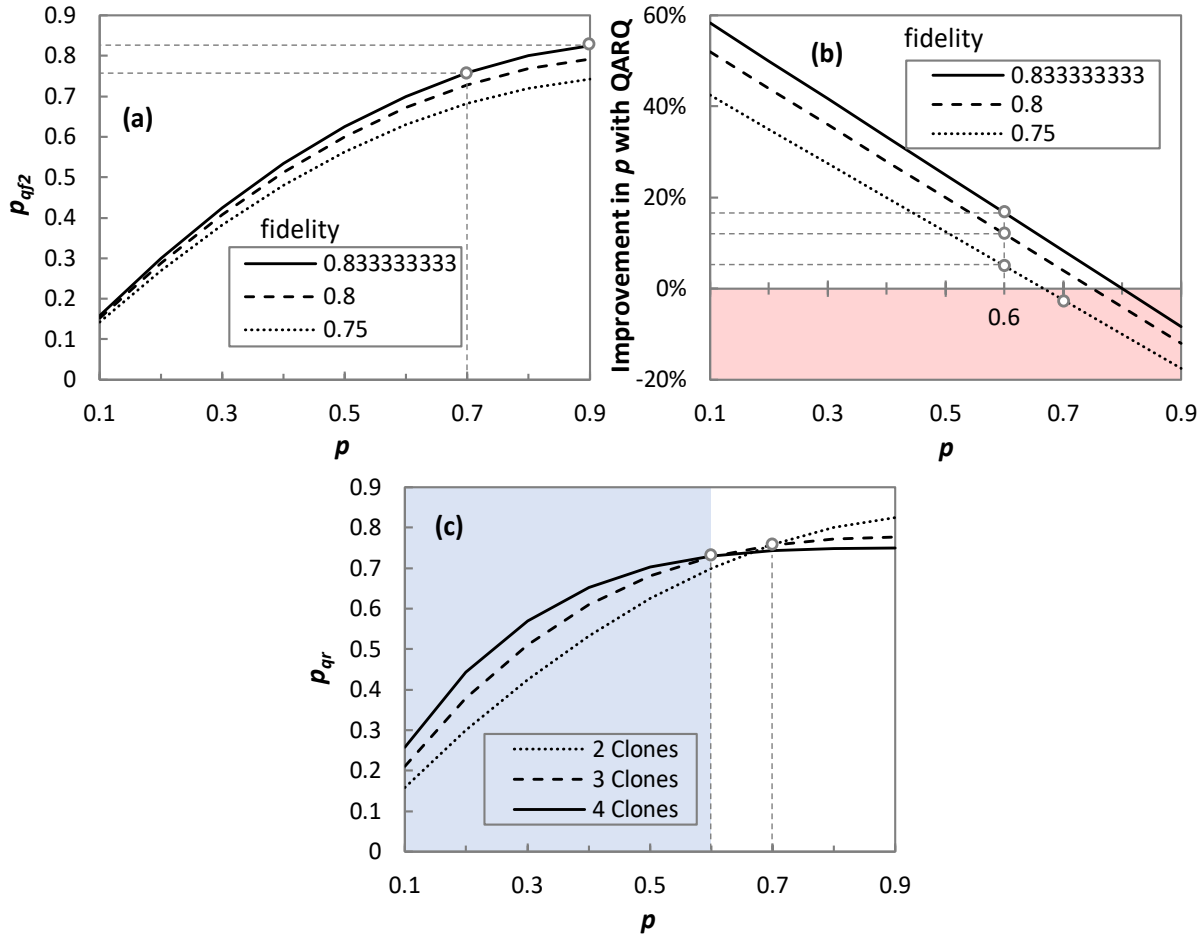


Figure 6-7 Probability of successful transmission with and without QARQ. Probability of successful transmission with two clones (a), Improvement in probability of successful transmission with two clones, and Probability of successful transmission with 2, 3, and 4 clones (d)

6.4.2 QP2MP

Let us first study the fidelity of the three quantum technologies applied to QP2MP (Figure 6-8). We assume fidelity threshold equal to 0.8, as in QKD [Ko20].

In the case of DT (Figure 6-8a), the fidelity of the received qubit highly depends on the channel depolarization and degrades drastically as the distance increases. For this reason, results are shown for different values of *dp*, which reveal that DT may not be the best solution for longer distances. For *dp*=0.001, fidelity below 0.8 starts to be observed after 10 km. Similarly, for *dp*=0.003, 0.005, and 0.007 fidelity remains above the threshold until 6, 4, and 3 km, respectively. As for TP (Figure 6-8b) and TC (Figure 6-8c), the fidelity of the qubit is highly dependent on the fidelity of the entanglement pair (f_{eTP}) and the fidelity of the telecloning state (f_{eTC}), respectively.

We observe that when f_{eTP} in Figure 6-8b and f_{eTC} in Figure 6-8c decrease, the fidelity of the teleported and telecloned qubit also decreases. For TP, the fidelity threshold is met only for f_{eTP}=0.988. However, for TC, all the f_{eTC} values provide fidelity above the desired threshold.

TP and TC protocols tend to have no significant effect on fidelity in terms of the transmission distance, but they provide major degradation of fidelity if entanglement is not perfect. For example, from f_{eTP}=0.988 to 0.979 (Figure 6-8b) and at 1 km, the fidelity of the teleported qubit drops from 0.802 to 0.798. Similarly, for the telecloned qubit from f_{eTC}=0.988 to 0.979 (Figure 6-8c) at 1 km, the fidelity drops from 0.830 to 0.828. This could suggest that if the entanglement is not perfect, then the DT may provide better results for short distances than TP or TC. To illustrate this better, Figure 6-8d represents the improvement in fidelity by using TP and TC over DT. For f_{eTP}=f_{eTC}=0.988 and dp=0.001, DT outperforms TP for a distance of up to 9 km. However, TC performs better than DT and TP for the same case scenario and improvement increases with transmission distance. In particular, the improvement in fidelity of TC is around 3.5% with respect to TP, which increases to 3.77% for f_{eTP}=f_{eTC}=0.979.

The results highlight that TC performs better than TP, whereas TP outperforms DT for longer distances. However, the implementation of TC and TP entails higher complexity. In order to estimate complexity, we compute quantum cost and quantum bits. Quantum cost is computed as the number of 1×1 and 2×2 quantum gates required in the circuit, i.e., we assume that the quantum cost of all 1×1 and 2×2 quantum circuit is the same [MaM14]. For finding the quantum cost of TC, the TC state is prepared using state vector notations and then decomposing it into quantum circuits by using Qiskit [QISKIT]. Quantum bits represent the total number of bits required to create each protocol. Table 6-4 summarizes the complexity of each protocol, clearly indicating that TC is the most complex protocol in terms of quantum cost, whereas TP is the most complex in terms of qubits (which is not significant for small-scale quantum systems). Therefore, it can be concluded that the optimal protocol depends on the desired fidelity requirement, distance between the nodes, and complexity of each protocol.

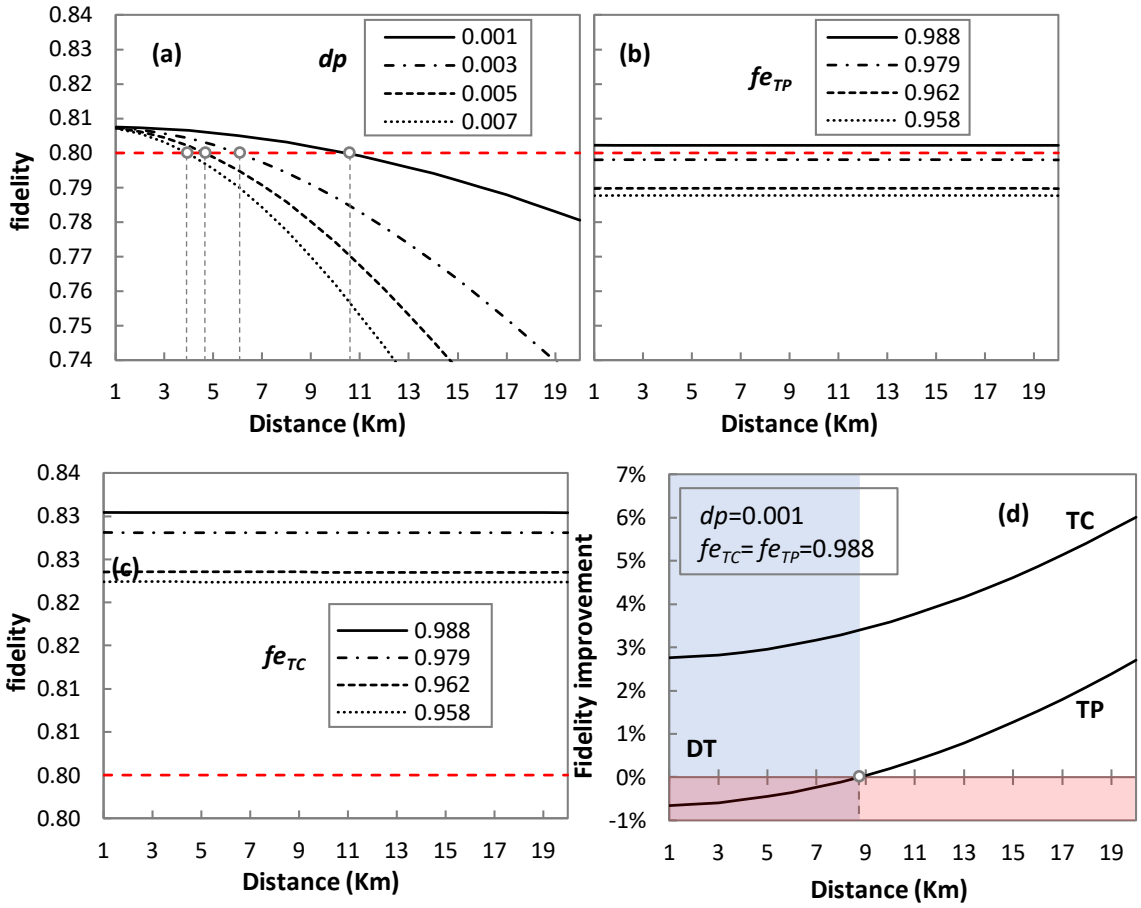


Figure 6-8 QP2MP Quantum technologies performance comparison

Table 6-4: Complexity of DT, TP, and TC

Transmission mode	Quantum cost	Qubits
DT	9	3
TP	21	7
TC	36	5

6.5 Conclusion

In quantum communication, perfect qubit retransmission and P2MP communication are not possible due to the no-cloning theorem. To mitigate such fact, a UQCM has been proposed in this chapter to create imperfect qubit copies, while sacrificing fidelity. The QARQ protocol has been proposed for qubit retransmission and the QP2MP has been proposed for P2MP communication. To implement both QARP and

QP2MP, three quantum technologies have been investigated, as they use different means for transporting qubits: DT, TP, and TC.

The performance of the QARQ and QP2MP was studied through simulation. It was shown that the performance of QARQ highly depends on the fidelity of the received qubit and QARQ-TC provides the highest fidelity of the three QARQ protocols. The probability of successful qubit transmission was investigated and it was shown that increasing the number of clones does not always increase such probability. Regarding QP2MP, results showed that TP and TC provide better fidelity with TC outperforming TP for longer distances. However, the fidelity of entangled pair and telecloning states is critical in these two quantum technologies, which is a major research challenge. Finally, analysis of the complexity of DT, TP, and TC revealed that TC is the most complex protocol in terms of quantum cost.

.

Chapter 7

Q^2PSK – A Quantum Equivalent to Classical QPSK Optical Communication

This chapter concludes this PhD Thesis by focusing on the implementation of a quantum equivalent to classical QPSK communication on IBMQ. IBMQ-implementation shows that forward error correction (FEC) fails to provide error-free transmission on near-term devices. Simulation shows that when qubit fidelity reaches 0.981, such hardware can provide error-free transmission.

7.1 Introduction

Quantum computing and communication bring powerful advantages over classical communication, being the most important advantage secure communication brought by quantum mechanics. Current transmission relies on classical data and classical channels, which are not inherently secure. A widely adapted approach to make them secure is encrypting the data via Quantum Key Distribution [Di16], which provides the secure key exchange for data encryption and transmits them through a classical channel. Given the inherent properties of quantum principles, an alternative to classical channels could be to send classical data quantumly, which would make the classical data inherently secure, avoiding the need for key distribution and encryption. To do so, *superdense coding* [Mc08], a well-known quantum communication protocol used in quantum computing, can be exploited. Superdense coding transmits two classical bits using one quantum bit (qubit) –the basic unit of

quantum information. We adopt such technique for classical communication and form a quantum equivalent to quadrature phase shift keying modulation (Q²PSK).

The current landscape of quantum computing is defined as the Noisy Intermediate-Scale Quantum era [Pr18], where functioning quantum devices are available on cloud for end users. Such devices are only capable of working with a small set of noisy qubits, because when a qubit interacts with the environment it decoheres and introduces errors. This limit: *i*) the functionality of these devices until *fault-tolerant* quantum devices become available; and *ii*) the implementation of Q²PSK as using noisy devices would result in high bit error rate (BER). In this work, we present the design and implementation of Q²PSK and evaluate its performance utilizing near-term quantum devices. We also apply (FEC) technique in classical data and show how much improvement is required in the near-term quantum devices to have error-free transmission using Q²PSK.

7.2 Design and implementation of Q²PSK

Figure 7-1 shows the high-level design of Q²PSK, where Alice (A) wants to send classical information to Bob (B) using quantum channel. To perform Q²PSK five blocks are required *i*) Entanglement pair generator (EG), which can be placed at any intermediate point between Alice and Bob; *ii*) Quantum memory; *iii*) Quantum Modulator (QM); *iv*) quantum communication channel; and *v*) Quantum demodulator (QDM).

Firstly, ahead of time, the EG (labeled as 1 in Figure 7-1), creates an entanglement pair. The quantum state of the qubit in the pair is highly correlated (the pair shares a superposition where both are either false or true) no matter how far apart they are. Alice gets one half of the pair (2a) and Bob receives the other half (2b) and they store them in quantum memory.

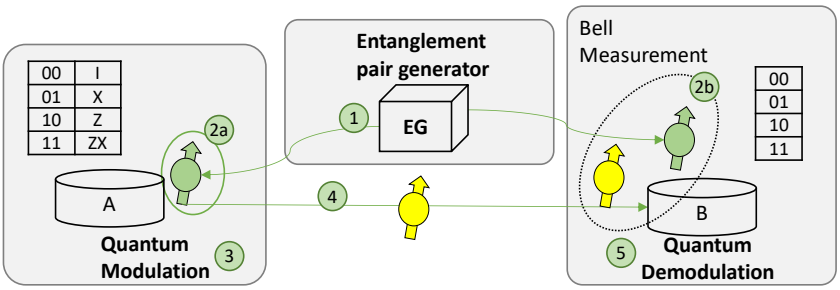


Figure 7-1: Design of Q²PSK

Alice performs the quantum modulation and encodes classical data into her half of the entangled pair (3). The modulation is done by applying quantum gates, which perform quantum operations that change the qubit's state to a desired one, similar to classical logic gates. As an equivalent to QPSK, Alice can encode four possible

messages 00, 01, 10 and 11: *i*) to send 00, Alice does nothing; *ii*) for 01 she applies Z-gate that rotates the qubit 180° around Z-axis; *iii*) for 10 she applies X-gate that rotates qubit 180° around X-axis; and iv) for 11 she applies both X and Z gates. Alice sends her qubit to Bob using the quantum channel (4). Now, Bob has both halves of the entangled pair, but Alice has operated on one of them. Bob performs quantum demodulation (5) using a conditional-not (CNOT) gate on his qubit conditioned on Alice's qubit. This will flip the value of his qubit in the parts of the superposition where hers is true. Then, Bob rotates Alice's qubit by 180° around the diagonal (X+Z) axis and finally, he measures the two qubits and retrieves the message.

The communication provided by Q²PSK is inherently secure. If an eavesdropper, Eve, intercepts Alice's qubit en- route to Bob, all she obtains is part of an entangled state and she is unable to obtain information from Alice's qubit because she lacks access to Bob's qubit. A third party cannot eavesdrop on information communicated using this protocol and any attempt to measure either qubit would collapse its state and may alert both Alice and Bob.

7.3 Test setup and results

Figure 7-2 shows the setup implemented to evaluate the performance of Q²PSK. A back-to-back system is considered with EG, QM, and QDM. These blocks are modelled using gate model implementation of quantum circuits provided by IBM [IBMQ]. An entanglement pair is generated by applying Hadamard gate (H) followed by a CNOT gate. 4000 symbols are generated and encoded with a convolutional FEC. Encoded data is fed into a QM at Alice's side, which modulates her half of the pair. The data pass through a QDM at Bob's side, which performs bell measurements, similar to the inverse of making a bell pair. After that, the FEC decoder recovers the signal. For FEC encoding and decoding; the FEC code rate of 2/3 is used, whereas the Viterbi decoding algorithm is applied at the receiver [Ty06]. FEC encoding and decoding are performed offline in MATLAB.

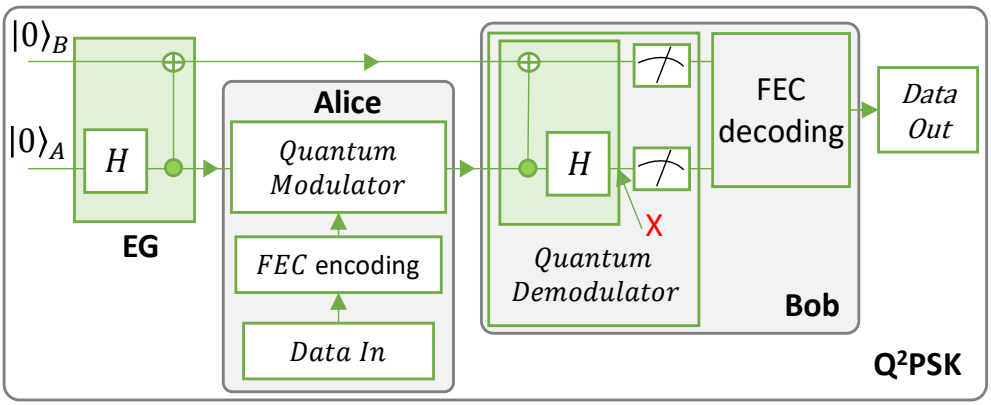


Figure 7-2: Test Setup

As IBM provides a cloud-based service to access real NISQ quantum computer, we use the ibmq-lima and ibmq-manila noisy models as backend to mimic real quantum hardware. Table 7-1 presents obtained BER calculated without FEC (pre-FEC) and with FEC (post-FEC). We observe that the devices improve the performance of the system with FEC, but are unable to provide error-free transmission, indicating that Q²PSK implementation with near-term quantum devices is not feasible. However, to study how much quantum hardware should improve to provide error free transmission using Q²PSK, a controlled simulation environment can be created.

We implemented such environment on NetSquid [Co21], where the amount of noise injected into the quantum communication system is controlled. For simulation, depolarizing, phase damping, and amplitude damping noise are considered, which are the most common models to introduce qubit decoherence [GeK21]. A useful metric to quantify the performance of a quantum system is *fidelity*, which describes the quality of the quantum state. A fidelity value of 1 means that it is in the desired state, while a value below 0.5 means that the state is no longer usable. Varying the noise will have direct impact on fidelity of qubit state. We evaluated the performance of Q²PSK using the fidelity of Alice's qubit received by Bob ($f_{B<A}$) just before applying measurement (labeled as *X* in Figure 7-2). For simulation, the ideal quantum circuit is considered and overall decoherence is applied at point *X* to reduce $f_{B<A}$.

Figure 7-3 shows the results of pre-FEC BER and post-FEC BER as a function of $f_{B<A}$. If $f_{B<A}$ is low, then BER is high. Specifically, if $f_{B<A} < 0.981$, FEC fails to provide error-free transmission, but for $f_{B<A} \geq 0.981$ error-free transmission, i.e., below BER threshold of 1.05e-2, is observed. Thus, current quantum devices should be improved to a point of providing $f_{B<A}$ of at least 0.981 to have error-free transmission.

Table 7-1: Q²PSK performance on IBMQ devices

Quantum Device	Pre-FEC BER	Post-FEC BER
ibmq_lima	2.51e-02	1.78e-03
ibmq_manila	3.38e-02	1.73e-02

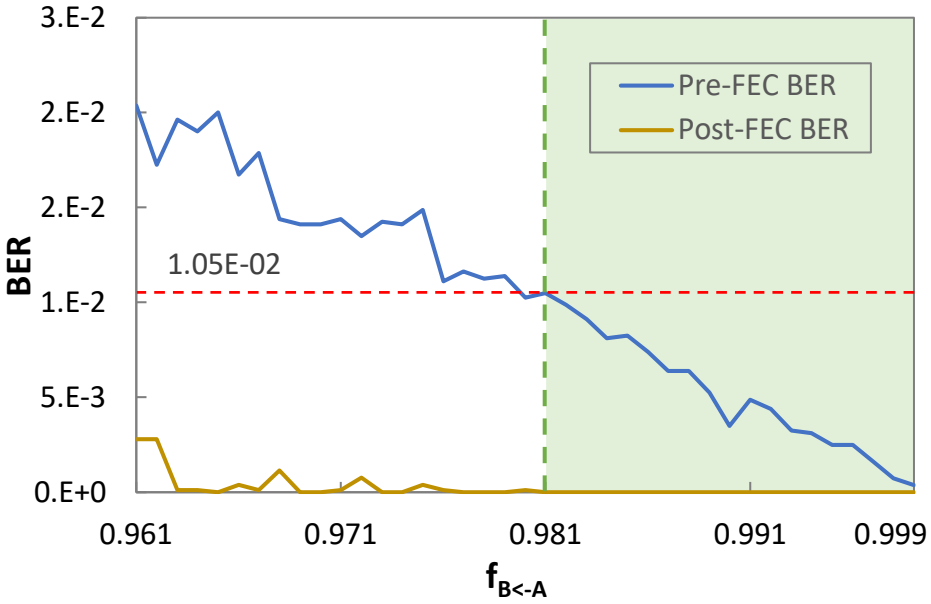


Figure 7-3: Performance of Q²PSK

7.4 Conclusions

As a conclusion, an inherently secure Q²PSK communication, a quantum equivalent of performing classical QPSK, has been proposed in this chapter. Together with FEC, Q²PSK has the potential to work with devices that can provide fidelity over 0.981.

Chapter 8

Closing Discussion

8.1 Main Contributions

This Ph. D. thesis has focused on providing techniques for making the optical networks efficient in terms of technologies supporting P2MP architectural design. It also focused on making network secure by providing techniques for physical layer cryptography and by exploring quantum means. The main contributions are summarized as following:

- First, in Chapter 4, a comprehensive approach for implementing encryption at the optical link layer has been demonstrated. The system comprises a mechanism for key distribution from the Tx to the Rx, as well as two ciphers that, when combined, may provide the requisite security level and can work on data flows of up to 100 Gb/s. The Xoshiro256+ PRNG is used for symmetric key expansion to generate keys for the first XOR-based encryption. A second cipher based on LUT substitution boosts security. The LPsec design has been presented, and it is simple to implement on current coherent optical systems. Simulation findings for 16, 32, and 64-QAM signals reveal that LPsec has no effect on optical transmission system performance. Furthermore, the required periodic key exchange adds no major delays.
- Chapter 5, focused on dealing with P2P traffic and P2P+ P2MP traffic, and the advantages of P2MP optical links over P2P connections were highlighted. For dynamic capacity requirements, two P2MP technologies, OCS and DSCM, were explored and compared to typical P2P optical transceivers. Chapter 5 provided guidelines to help operators to explore new methods of cost savings. The simulation results further indicated that DSCM reduces nonlinearities and outperforms OCS. However, in access and metro applications where non-

linearities are not as important, the BER of both scenarios remains under the threshold.

- Chapter 6 was devoted to cater the problem of qubit retransmission and point-to-multipoint quantum communication (QP2MP) in presence of no-cloning theorem. For qubit retransmission, quantum automatic repeat request protocol (QARQ) was proposed. Its implementation on direct transmission (DT), teleportation (TP) and telecloning (TC) was elaborated. Cases were described to show the users where QARQ can be beneficial. QP2MP was also explored for DT, TP, and TC. Both protocols are analyzed qualitatively in presence of different types of decoherences.
- In Chapter 7 we took advantage of the experience from Chapter 6 and practically demonstrated Q^2PSK which is a way to perform QPSK quantumly. This makes the classical communication inherently secure. We also pointed out the fact in this chapter that current quantum devices are not capable to provide error-free Q^2PSK transmission but has the potential to do so if certain thresholds are met.

8.2 List of Publications

8.2.1 Publications in Journals

[JOCN22] **M. Iqbal**, L. Velasco, N. Costa, A. Napoli, J. Pedro and M. Ruiz, "LPsec: a fast and secure cryptographic system for optical connections," in Journal of Optical Communications and Networking, vol. 14, no. 4, pp. 278-288, April 2022, doi: 10.1364/JOCN.444398.

[SENSORS23] **M. Iqbal**, L. Velasco, N. Costa, A. Napoli, J. Pedro, M. Ruiz and J. Comellas, "Supporting Heterogenous Traffic on top of Point-to-Multipoint Light-Trees", 2023. Submitted in Sensors

[JOCN23] **M. Iqbal**, L. Velasco, N. Costa, A. Napoli, J. Pedro and M. Ruiz, "Investigating Imperfect Cloning for Extending Quantum Communication Capabilities," 2023. Submitted in JOCN

8.2.2 Publications in Conferences

[OFC22] **M. Iqbal**, M. Ruiz, N. Costa, A. Napoli, J. Pedro and L. Velasco, "Dynamic and Efficient Point-to-Point and Point-to-Multipoint Communications by Slicing the Optical Constellation," 2022 Optical Fiber Communications Conference and Exhibition (OFC), 2022, pp. 1-3

[ONDM22] **M. Iqbal**, L. Velasco, M. Ruiz, A. Napoli, J. Pedro, and N. Costa, "Quantum bit retransmission using universal quantum copying machine," in International Conference on Optical Network Design and Modelling (ONDM), 2022

[CLEO23] **M. Iqbal**, M. Ruiz, N. Costa, A. Napoli, J. Pedro and L. Velasco, "Q²PSK – A Quantum Equivalent to Classical QPSK Optical Communication," Conference on Lasers and Electro-Optics, 2023. Submitted in CLEO

8.3 List of Research Projects

8.3.1 European Funded Projects

This PhD thesis is in the scope of the REAL-time monitoring and mitigation of nonlinear effects on optical NETworks - REAL-NET. The REAL-NET project has received funding from the European Union's Horizon 2020 research and innovation program under the Marie Skłodowska-Curie grant agreement No 813144.

8.3.2 Pre-doctoral Scholarship

- Pre-doctoral scholarship related to REAL-NET Marie Skłodowska-Curie grant.

8.4 Collaborations

In the scope of the REAL-NET project, an 18 months industrial secondment in Infinera Unipessoal Lda., Carnaxide, Portugal was carried out between Infinera and UPC where P2MP communication was explored.

List of Acronyms

ACK	Acknowledgement
AES	Advanced Encryption Standard
ARQ	Automatic Repeat Request
ASE	Amplified Spontaneous Emission
AWGN	Additive White Gaussian Noise
BER	Bit Error Rate
CAPEX	Capital Expenditure
CD	Chromatic Dispersion
CDMA	Optical Code Division Multiple Access
CE	Contributed Efficiency
CMS	Chaos-Masking
CNOT	Controlled-Not
CpB	Cost per transported bit
DBP	Digital Back Propagation
DCF	Dispersion Compensating Fibers
DH	Diffie Hellman
DP	Dual-Polarization
DSCM	Digital Subcarrier Multiplexing
DSP	Digital Signal Processing

DT	Direct Transmission
EDFA	Erbium-Doped Fiber Amplifiers
EG	Entanglement Pair Generator
FEC	Forward Error Correction
FFT	Fast Fourier Transform
FSM	Finite State Machines
GN	Gaussian Noise
IFFT	Inverse Fast Fourier Transform
IM/DD	Intensity Modulation and Direct Detection
IoT	Internet of Things
IQ	In-Phase/Quadrature
KxF	Key Exchange Frame
LI	Linear Impairments
LPsec	LightPath Security
LUT	Lookup Table
ML	Machine Learning
NACK	Negative Acknowledgement
NISQ	Noisy Intermediate Scale Qubits
NLI	Non-Linear Impairments
NLSE	Nonlinear Schrodinger Equation
NV	Nitrogen-Vacancy
OA	Optical Amplifiers
OC	Optical Constellation
OCS	Optical Constellation Slicing
ODU	Optical Data Unit
OEO	Optical-Electrical-Optical
OM	Output Matrix

OPEX	Operational Expenditure
OTN	Optical Transport Network
OTP	One-Time Pad
P2MP	Point to multipoint
P2P	Point to Point
PACK	Positive Acknowledgement
PCS	Probabilistic Constellation Shaping
PDM	Polarization Division Multiplexing
PIC	Photonics Integrated Circuits
PRBS	Pseudo-Random Binary Sequences
PRNG	Pseudo Random Number Generator
Q^2PSK	Quantum Quadrature Phase Shift Keying
QAM	Quadrature Amplitude Modulation
QAM	Quadrature Amplitude Modulation
QARQ	Quantum Automatic Repeat Request
QDM	Quantum Demodulator
QKD	Quantum Key Distribution
QM	Quantum Modulator
QP2MP	Point-To-Multipoint Quantum Communication
QP2P	Point-to-Point Quantum Communication
QPSK	Quadrature Phase Shift Keying
RAN	Radio Access Network
ROADM	Reconfigurable Optical Add and Drop Multiplexing
RRC	Root-Raised-Cosine Filter
SC	Subcarrier
SDN	Software Defined Networking
SE	Slice Efficiency

SMF	Single Mode Fibers
SPM	Self-Phase Modulation
SSFM	Split-Step Fourier Method
STM	State Transition Matrix
TC	Telecloning
TCP	Transmission Control Protocol
TG	Telecloning State Generator
TP	Teleportation
UQCM	Universal Quantum Cloning Machine
WDM	Wavelength Division Multiplexing
WSON	Wavelength Switched Optical Networks
WSS	Wavelength Selective Switches
XPM	Cross-Phase Modulation

References

[Ab15] M. Abbade, M. Cvijetic, C. Messani, C. Alves, and S. Tenenbaum, "All-optical cryptography of M-QAM formats by using two-dimensional spectrally sliced keys," Applied Optics, vol. 54. pp. 4359-4365, 2015.

[Ab18] M. Abbade, L. Lessa, M. Santos, A. Prado and I. Aldaya, "A New DSP-Based Physical Layer Encryption Technique Applied to Passive Optical Networks," in Proc. ICTON, 2018

[ADVA21] ADVA Layer 1 security. https://www.adva.com/en/innovation/ network-security/layer-1-security. [Accessed: Sept. 2021].

[AES01] "Specification for the Advanced Encryption Standard (AES)," FIPS-197, National Institute of Standards and Technology (NIST), 2001.

[Ag16] E. Agrell et al., "Roadmap of optical communications," Journal of Optics, vol. 18, 2016

[AgA20] A. Aguado, D. Lopez, A. Pastor, V. Lopez, J. Brito, M. Peev, A. Poppe, V. Martin, "Quantum cryptography networks in support of path verification in service function chains," IEEE/OSA J. of Optical Communications and Networking, vol. 12, pp. B9-B19, 2020

[Ah22] M. Ahmadian, M. Ruiz, J. Comellas, and L. Velasco, "Cost-Effective ML-Powered Polarization-Encoded Quantum Key Distribution," IEEE/OPTICA Journal of Lightwave Technology (JLT), 2022.

[Al21] I. Alimi, R. Patel, N. Silva, C. Sun, H. Ji, W. Shieh, A. Pinto, N. Muga, "A Review of Self-Coherent Optical Transceivers: Fun-damental Issues," Recent Advances, and Research Directions. Applied Sciences, vol. 11, pp. 7554, 2021.

[Ba20] J. Bäck, P. Wright, J. Ambrose, A. Chase, M. Jary, F. Masoud, N. Sugden, G. Wardrop, A. Napoli, J. Pedro, M. A. Iqbal, A. Lord, D. Welch, "Capex savings enabled by point-to-multipoint coherent pluggable optics using digital subcarrier multiplexing in metro aggregation networks," in ECOC, (IEEE, 2020)

[BaB23] B. Bao, H. Yang, Q. Yao, L. Guan, J. Zhang and M. Cheriet, "Resource Allocation with Edge-Cloud Collaborative Traffic Prediction in Integrated Radio and Optical Networks," in IEEE Access, vol. 11, pp. 7067-7077, 2023

[Be08] D. Bernstein, "ChaCha, a variant of Salsa20," in Workshop Record of SASC, 2008

[BeC19] C. Bernhardt, Quantum computing for everyone, The MIT Press, 2019.

[Bi96] E. Biham, "How to Forge DES-encrypted messages in 228 steps," Technion, Technical Report CS0884, 1996.

[Bl19] D. Blackman and S. Vigna, "Scrambled Linear Pseudorandom Number Generators," [Online] arXiv:1805.01407, 2019.

[Bo20] D. Boneh and V. Shoup, A Graduate Course in Applied Cryptography, http://toc.cryptobook.us [Accessed: Sept. 2021], 2020.

[Bu98] R. Buzek.et al., "Universal optimal cloning of qubits and quantum registers.", QCQC, 1998

[CISCO.2] D. Mcgrew, "Counter Mode Security: Analysis and Recommendations," vol. 2, Cisco Systems, 2002.

[CISCO] "Cisco Annual Internet Report (2018-2023) White Paper," [Online]. Available: https://www.cisco.com/c/en/us/solutions/collateral/executiveperspectives/annual-internet-report/white-paper-c11-741490.html

[Co21] T. Coopmans et al., "NetSquid, a network simulator for quantum information using discrete events," Communication Physics, 2021.

[CoH18] H. Corrigan-Gibbs and D. Kogan "The Discrete-Logarithm Problem with Preprocessing," in Proc. EUROCRYPT 2018.

[Cu22] V. Curri, "GNPy model of the physical layer for open and disaggregated optical networking [Invited]," IEEE/OSA Journal of Optical Communication and Networking, vol. 14, pp. C92-C104, 2022

[Da10] B. Dai, Z. Gao, X. Wang, N. Kataoka and N. Wada, "Demonstration of differential detection on attacking code-shift-keying OCDMA system," Electronics Letters, vol. 46, pp. 1680-1682, 2010.

[DaR17] R. Dar and P. Winzer, "Digital Subcarrier Multiplexing in Optically Routed Networks," in Proc. Optical Fiber Communications Conference and Exhibition (OFC), 2017

[Di16] E. Diamanti et al. "Practical challenges in quantum key distribution." npj Quantum Inf 2. 2016

[EDFA02] E. Desurvire, Erbium-Doped Fiber Amplifiers: Principles and Applications, Wiley, 2002

[EON16] Victor López and Luis Velasco, *Elastic Optical Networks: Architectures, Technologies, and Control*, in Optical Networks book series, ISBN 978-3-319-30173-0, Springer, 2016.

[Fe20] A. Ferrari et al., "GNPy: an open source application for physical layer aware open optical networks," IEEE/OSA Journal of Optical Communication and Networking, vol. 12, pp. C31-C40, 2020

[FeN10] N. Ferguson, B. Schneier, T. Kohno, Cryptography Engineering: Design Principles and Practical Applications, Wiley Publishing, 2010.

[Fo11] M. Fok, Z. Wang, Y. Deng, and P. Prucnal, "Optical Layer Security in Fiber-Optic Networks," IEEE Transactions on Information Forensics and Security, vol. 6, pp. 725-736, 2011

[Ge22] J. Germain, R. Dantu, M. Thompson and M. Dockendorf, "Quantum Networks: Reset-and-Reuse can be a Game-changer for Entanglement via

Distillation," 2022 IEEE International Conference on Quantum Computing and Engineering (QCE), 2022

[GeK21] K. Georgopoulos et al., "Modeling and simulating the noisy behavior of near-term quantum computers", Phys. Rev. A, 2021.

[Gi20] M. Giordani, M. Polese, M. Mezzavilla, S. Rangan and M. Zorzi, "Toward 6G Networks: Use Cases and Technologies," IEEE Communications Magazine, vol. 58, no. 3, pp. 55-61, 2020.

[Gr05] L. Gruner-Nielsen et al., "Dispersion-compensating fibers," IEEE/OSA Journal Lightwave Technology, vol. 23, pp. 3566-3579, 2005.

[He20] J. Hernandez, M. Quagliotti, L. Serra, L. Luque, R. Lopez, A. Rafel, O. Gonzalez, V. Lopez, A. Eira, R. Casellas, A. Lord, J. Pedro, D. Larrabeiti, "Comprehensive model for technoeconomic studies of next-generation central offices for metro networks," J. Opt. Commun. Netw. 12, 414–427, 2020

[Ho22] M. Hosseini, J. Pedro, A. Napoli, N. Costa, J. Prilepsky and S. Turitsyn, "Optimization of survivable filterless optical networks exploiting digital subcarrier multiplexing," IEEE/OSA Journal Optical Communications and Networking, vol. 14, pp. 586-594, 2022

[HoZ21] Z. Hou, C. She, Y. Li, D. Niyato, M. Dohler and B. Vucetic, "Intelligent Communications for Tactile Internet in 6G: Require-ments, Technologies, and Challenges," IEEE Communications Magazine, vol. 59, pp. 82-88, 2021.

[Hu20] P. Humphreys, N. Kalb, J. Morits, R. Schouten, R. Vermeulen, D. Twitchen, M. Markham and R. Hanson, "Deterministic delivery of remote entanglement on a quantum network," Nature, vol. 558, pp. 268–273, 2018.

[Ib05] S. Iblisdir et al., "Multipartite asymmetric quantum cloning." Phys. Rev. A, vol. 72, pp. 042328, 2005

[IBMQ] IBM quantum [Online] Available: https://quantum-computing.ibm.com. (Accessed: November, 2022).

[Infinera.1] Infinera, "The-Ultimate-Guide-to-Nyquist-Subcarriers-0208-WP-RevA-0719.pdf (infinera.com)"

[Infinera.2] Infinera, "Maximizing-the-Capacity-Reach-of-800G-Generation-Coherent-0271-WP-RevA-0920.pdf (infinera.com)"

[Ji21] L. Jiang, Y. Pan, A. Yi, J. Feng, W. Pan, L. Yi, W. Hu, A. Wang, Y. Wang, Y. Qin, and L. Yan, "Trading off security and practicability to explore high-speed and long-haul chaotic optical communication," Opt. Express, vol. 29, pp. 12750-12762, 2021.

[JiZ06] Z. Jiang, D. Leaird, and A. Weiner, "Experimental investigation of security issues in O-CDMA," IEEE J. Lightwave Technol., vol. 24. pp. 4228-4334, 2006.

[Ko20] W. Kozlowski, A. Dahlberg, S. Wehner, "Designing a quantum network protocol.", pp. 1-16,2020

[Kr07] K. Kravtsov, B. Wu, I. Glesk; P. Prucnal, E. Narimanov, "Stealth transmission over a WDM network with detection based on an all-optical thresholder," in Proc. IEEE/LEOS, 2007.

[Li16] B. Liu, L. Zhang, X. Xin and N. Liu, "Piecewise Chaotic Permutation Method for Physical Layer Security in OFDM-PON," IEEE Photonics Technology Letters, vol. 28, pp. 2359-2362, 2016

[LiC22] C. Liao et al., "Benchmarking of quantum protocols," Scientific Reports, 2022

[LiY22] Y. -C. Liu, Y. -C. Dzeng and C. -C. Ting, "Nitrogen Vacancy-Centered Diamond Qubit: The fabrication, design, and application in quantum computing," in IEEE Nanotechnology Magazine, vol. 16, no. 4, pp. 37-43, Aug. 2022

[Lo99] H. K. Lo and H. F. Chau, "Unconditional security of quantum key distribution over arbitrarily long distances," Science, vol. 283, no. 5410, p. 2050, 1999. [Online]. Available: http://science.sciencemag. org/content/283/5410/2050

[Ma97] D. Marcuse, C. Manyuk and P. Wai, "Application of the Manakov-PMD equation to studies of signal propagation in optical fibers with randomly varying birefringence," IEEE/OSA Journal of Lightwave Technology, vol. 15, pp. 1735-1746, 1997

[MaM14] M. Mamun et al., "Quantum Cost Optimization for Reversible Sequential Circuit.", IJACSA, 2014.

[Mc08] D. McMahon, "Applications of Entanglement: Teleportation and Superdense Coding." Quantum Computing. 2008.

[MIQCN21] Z. Qingcheng, Y. Wang, L. Lu, Y. Zhao, X. Yu, Y. Cao, J.Zhang, "Multipoint-Interconnected Quantum Communication Networks." DOI: 10.5772/intechopen.101447, 2021

[Ne04] D. Neuenschwander, "Diffie-Hellman Key Exchange," Probabilistic and Statistical Methods in Cryptology, 2004.

[NFO13] G. Agrawal, Nonlinear Fiber Optics, Academic Press, 5th edition, 2013

[Ni18] Y. Nir and A. Langley, "ChaCha20 and Poly1305 for IETF Protocols," IRTF RFC-8439, 2018.

[NIST] NIST Empirical Testing of Random Number Generators [Online]. https://www.nist.gov/publications/statistical-test-suite-random-and-pseudorandom-number-generators-cryptographic.

[NOKIA] "Network Traffic Insights in the Time of COVID-19," [Online]. Available: https://www.nokia.com/blog/network-traffic-insights-in-the-timeof-covid-19-june-4-update/

[Pe12] O. Pedrola, A. Castro, L. Velasco, M. Ruiz, J.P. Fernández-Palacios, D. Careglio, "CAPEX study for Multilayer IP/MPLS over Flexgrid Optical Network," IEEE/OSA Journal of Optical Communications and Networking, vol. 4, pp. 639-650, 2012.

[PeE22] E. Pelofske, A. Bartschi, B. Garcia, B. Kiefer and S. Eidenbenz, "Quantum Telecloning on NISQ Computers," in Proc. IEEE Int. Conference on Quantum Computing and Engineering, 2022.

[Pn22] W. -H. Png, T. Hsu, T. -W. Liu, G. -D. Lin and M. -S. Chang, "Quantum computing with trapped ions: An overview," in IEEE Nanotechnology Magazine, vol. 16, no. 4, pp. 30-36, Aug. 2022

[Po12] P. Poggiolini, G. Bosco, A. Carena, V. Curri, Y. Jiang, and F. Forghieri, "The GN-Model of Fiber Non-Linear Propagation and its Applications," IEEE/OSA Journal of Lightwave Technology, vol. 32, pp. 694-721, 2014

[Po14] P. Poggiolini, "The GN Model of Non-Linear Propagation in Uncompensated Coherent Optical Systems," IEEE/OSA Journal of Lightwave Technology, vol. 30, pp. 3857-3879, 2012

[Pr18] J. Preskill, "Quantum Computing in the NISQ era and beyond." Quantum, 2, 2018

[Qi22] M. Qiu, Q. Zhuge, M. Chagnon, Y. Gao, X. Xu, M. Morsy-Osman, and D. Plant, "Digital Subcarrier Multiplexing for Fiber NonLinearity Mitigation in Coherent Optical Communication Systems," Opt. Express, vol. 22, pp. 18770-18777, 2022.

[QISKIT] Qiskit.org [Online]: https://qiskit.org/. [Accessed: Jan 2023].

[Ra13] F. Rambach et al., "A multilayer cost model for metro/core networks," IEEE/OSA JOCN, 2013

[Ra16] T. Rahman, D. Rafique, B. Spinnler, A. Napoli, M. Bohn, A. Koonen, C. Okonkwo, and H. Waardt, "Digital Subcarrier Multiplexed Hybrid QAM for Data-rate Flexibility and ROADM Filtering Tolerance," IEEE/OSA Optical Fiber Communication Conference, 2016

[Ra17] T. Rahman, Flexible and high data-rate coherent optical transceivers. Diss. Ph. D. Thesis. Technische Universiteit Eindhoven, 2017

[Ri22] H. Riel, "Quantum Computing Technology and Roadmap," ESSDERC 2022 - IEEE 52nd European Solid-State Device Research Conference (ESSDERC), 2022, pp. 25-30

[Ro20] M. Rota, F. Basset, D. Tedeschi, and R. Trotta, "Entanglement Teleportation with Photons from Quantum Dots: Toward a Solid-State Based Quantum Network," in IEEE Journal of Selected Topics in Quantum Electronics, vol. 26, pp. 1-16, 2020.

[Ru14] M. Ruiz and L. Velasco, "Performance Evaluation of Light-tree Schemes in Flexgrid Optical Networks," IEEE Comm. Letters, 2014.

[Ru15] M. Ruiz and L. Velasco, "Serving Multicast Requests on Single Layer and Multilayer Flexgrid Networks," IEEE/OSA JOCN, 2015.

[Sa13] S. Savory, "Digital Signal Processing for Coherent Optical Communication Systems," in Proc. OptoElectronics and Communications Conference, 2013

[SaD05] Salomon, D., Coding for Data and Computer Communications, Springer, 2005.

[Sc15] M. Schiano, A. Percelsi, and M. Quagliotti, "Flexible node architectures for metro networks," J. Opt. Commun. Netw., vol. 7, no. 12, pp. B 131– B140, 2015.

[Se19] H. Sepehrian, J. Lin, L. A. Rusch and W. Shi, "Silicon Photonic IQ Modulators for 400 Gb/s and Beyond," IEEE/OSA Journal Lightwave Technology, vol. 37, pp. 3078-3086, 2019

[SeD22] D. Sequeira, M. Ruiz, N. Costa, A. Napoli, J. Pedro, and L. Velasco, "Accurate Low Complex Modulation Format and Symbol Rate Identification for Autonomous Lightpath Operation," MDPI Sensors, vol. 22, pp. 9251, 2022.

[Sh02] B P. W. Shor and J. Preskill, "Simple proof of security of the BB84 quantum key distribution protocol," Phys. Rev. Lett., vol. 85, no. 2, pp. 441–444, 2000

[ShC49] C. Shannon, "Communication theory of secrecy systems," Bell Labs Tech. J., vol. 28, pp. 656-715, 1949

[ShP19] P. Shi, N. Li, S. Wang, Z. Liu, M. Ren, H. Ma, "Quantum Multi-User Broadcast Protocol for the "Platform as a Service" Model" Sensors, vol 23, 2019

[ShP95.2] P. Shor, "Scheme for reducing decoherence in quantum memory," Physical Review A, 1995.

[ShT05] T. Shake, "Security performance of optical CDMA against eavesdropping," IEEE J. Lightwave Technol., vol. 23. pp. 655-670, 2005.

[Si10] Z. Si, F. Yin, M. Xin, H. Chen, M. Chen, and S. Xie, "Code extraction from encoded signal in time-spreading optical code division multiple access," OSA Optics Letters, vol. 35, pp. 229-231, 2010.

[Su20] H. Sun et al., "800G DSP ASIC Design Using Probabilistic Shaping and Digital Sub-Carrier Multiplexing," IEEE/OSA Journal of Lightwave Technology, vol. 38, pp. 4744-4756, 2020

[TestU01] TestU01, Empirical Testing of Random Number Generators [Online]. http://simul.iro.umontreal.ca/testu01/tu01.html.

[Ty06] A. Tychopoulos, O. Koufopavlou and I. Tomkos, "FEC in optical communications - A tutorial overview on the evolution of architectures and the future prospects of outband and inband FEC for optical communications," IEEE Circuits and Devices Magazine, vol. 22, pp. 79-86, 2006.

[Ve13.2] L. Velasco, P. Wright, A. Lord, and G. Junyent, "Saving CAPEX by Extending Flexgrid-based Core Optical Networks to-wards the Edges," (Invited Paper) IEEE/OSA Journal of Optical Communications and Networking, vol. 5, pp. A171-A183, 2013.

[Ve13] L. Velasco, P. Wright, A. Lord, and G. Junyent, "Saving CAPEX by Extending Flexgrid-based Core Optical Networks towards the Edges," IEEE/OSA Journal of Optical Communications and Networking (JOCN), vol. 5, pp. A171-A183, 2013.

[Ve21] L. Velasco, S. Barzegar, D. Sequeira, A. Ferrari, N. Costa, V. Curri, J. Pedro, A. Napoli, and M. Ruiz, "Autonomous and Energy Efficient Lightpath Operation Based on Digital Subcarrier Multiplexing," IEEE Journal on Selected Areas in Communications, vol. 39, pp. 2864-2877, 2021

[Wa11] Z. Wang and P. Prucnal, "Optical steganography over a public DPSK channel with asynchronous detection," IEEE Photonics Technology Letters, vol 23, pp. 48-50, 2011.

[WaY22] Y. Wang, X. Yu, Y. Zhao, A. Nag, and J. Zhang, "Pre-established entanglement distribution algorithm in quantum networks," Journal of Optical Communications and Networking, vol. 14, pp. 1020-1033, 2022

[We21] D. Welch, A. Napoli, J. Bäck, W. Sande, J. Pedro, F. Masoud, C. Fludger, T. Duthel, H. Sun, S. J. Hand, T.-Kuang, A. Chase, A. Mathur, T. A. Eriksson, M. Plantare, M. Olson, St. Voll, K. Wu, "Point-to-multipoint optical networks using coherent digital subcarriers," IEEE/OSA JLT, 2021

[We22] D. Welch, A. Napoli, J. Bäck, N. Swenson, W. Sande, J. Pedro, F. Masoud, A. Chase, C. Fludger, H. Sun, T. Chiang, A. Mathur, and K. Wu, "Digital Subcarriers: A Universal Technology for Next Generation Optical Networks," in Proc. Optical Fiber Communications Conference and Exhibition (OFC), 2022.

[We23] D. Welch. A. Napoli, J. Back, S. Buggaveeti, C. Castro. A. Chase, X. Chen *et al.*, "Digital Subcarrier Multiplexing: Enabling Software-Configurable Optical Networks," Journal of Lightwave Technology, vol. 41, pp. 1175-1191, 2023.

[WeS18] S. Wehner et al., “Quantum internet: A vision for the road ahead,” Science, 362, 2018.

[Wo82] W. Wootters et al., “A single quantum cannot be cloned,” Nature, 1982

[WoE13] E. Woodhead, “Quantum cloning bound and application to quantum key distribution.”, Phys. Rev. A, vol. 88, pp. 012331, 2013.

[Wu08] B. Wu, A. Agrawal, I. Glesk, E. Narimanov, S. Etemad and P. Prucnal, “Steganographic fiber-optic transmission using coherent spectral-phase-encoded optical CDMA,” in Proc. CLEO, 2008.

[Wu13] B. Wu, Z. Wang, Y. Tian, M. Fok, B. Shastri, D. Kanoff, P. Prucnal, “Optical steganography based on amplified spontaneous emission noise,” OSA Optics Letters, vol. 35, pp. 2065-2071 2013.

[Xi17] X. Xiao, M. Li, L. Wang, D. Chen, Q. Yang, and S. Yu, “High Speed Silicon Photonic Modulators,” IEEE/OSA Optical Fiber Communication Conference, 2017

[Yu21] N. Yu et al., “Protocols for packet quantum network intercommunication,” IEEE Transactions on Quantum Engineering, 2021.

[ZhA21] A. Zhao, N. Jiang, S. Liu, Y. Zhang, and K. Qiu, “Physical Layer Encryption for WDM Optical Communication Systems Using Private Chaotic Phase Scrambling,” J. Lightwave Technol., vol. 39, pp. 2288-2295, 2021

[ZhN20] N. Zhao, W. Li and Y. Yu, “Quantum Broadcast and Multicast Schemes Based on Partially Entangled Channel,” in IEEE Access, vol. 8, pp. 29658-29666, 2020

[ZhQ19] Q. Zhuge et al., “Application of Machine Learning in Fiber Nonlinearity Modeling and Monitoring for Elastic Optical Networks,” IEEE/OSA Journal of Lightwave Technology, vol. 37, pp. 3055-3063, 2019