SECURED SINGLE STAGE MULTIPHOTON APPROACH FOR QUANTUM CRYPTOGRAPHY PROTOCOL IN FREE SPACE OPTIC

NUR ZIADAH BINTI HARUN

FSKTM 2020 7

SECURED SINGLE STAGE MULTIPHOTON APPROACH FOR QUANTUM CRYPTOGRAPHY PROTOCOL IN FREE SPACE OPTIC

By

NUR ZIADAH BINTI HARUN

Thesis Submitted to the School of Graduate Studies, Universiti Putra Malaysia, in Fulfilment of the Requirements for the Doctor of Philosophy

November 2019

COPYRIGHT

DEDICATION

To my late father, Harun bin Osman:

May your soul rest in peace, and may Jannatul Firdaus be your final abode.

I still keep remembering your advice,

مَنْ جَدَّ وَجَدَ

“Whoever strives shall succeed”

Abstract of thesis presented to the Senate of Universiti Putra Malaysia in fulfilment of the requirement for the degree of Doctor of Philosophy

SECURED SINGLE STAGE MULTIPHOTON APPROACH FOR QUANTUM CRYPTOGRAPHY PROTOCOL IN FREE SPACE OPTIC

By

NUR ZIADAH BINTI HARUN

November 2019

Chairman : Professor Zuriati binti Ahmad Zukarnain, PhD
Faculty : Computer Science and Information Technology

In order to mitigate the problem of low transmission rate and limited communication distance in Quantum Communication (QCs), multiphoton over multi-stages approach has been proven to be a possible alternative to the conventional single-photon approach. Multiphoton has the ability to improve the range of distances and key generation rate over multi-stages photon transmission. However, the determination of optimal mean photon numbers and number of stages in multiphoton approach remains a key challenge to make the protocols well utilized during their operations. Following this concern, three problems and their corresponding proposed solutions in this thesis are presented below:

Firstly, the existing multiphoton approaches involve multiple photons to travel throughout a number of stage. Furthermore, extra time is required to update the polarization angle of optical device for encoding purposes. These conditions would result in an increase in the total transmission time of the photons to be transmitted over the quantum channel. Accordingly, a Hybrid M-Ary in Braided Single-Stage (HMBSS) approach by utilizing data compression concept is proposed to address these issues. In HMBSS, the sender is able to compress the secret message using Huffman encoding over the braided single-stage operation. This compression mechanism has reduced the number of bits required to represent a string of symbols, thereby reducing the time to encode the photons. The simulation experiments shows that HMBSS achieved promising result by 75.9% and 91.7% total average transmission time decrease as compared to the well-known Multiphoton-BSS, Multiphoton-M-ary and Multiphoton-TSIV.

Secondly, providing strong authentication is the main focus in this research which aims to make multiphoton QC secure against variety types of attacks. Current authentication procedure in multiphoton QC requires public agreement to pre-share the authentication key and secret angles before onset of the transmission, therefore increasing the communication cost. As a solution, a Secure Secret Authentication Key (SSAK) is proposed. In SSAK, the quantum handshake scheme is used to share initial secret polarization angle and authentication key which is utilized before quantum communication session. The results of simulation experiments reveal that SSAK significantly outperformed the Three-stage protocol in terms of average covered angle by Eve. The simulation experiments and security analysis of initial authentication and transmission of messages verified that an eavesdropper is unable to disclose any information about the transmitted message or the authentication key.

Lastly, most of the proposed QKD protocol employs a single-beam set up to transmit the photons over the free space optic which results in low bit rate and limited distance coverage due to high impact of geometrical loss. To deal with this, a transmission technique of Multiphoton Quantum Communication using multiple-beam concept (MQC-MB) is proposed. Comparison is conducted in terms of total loss and received power on different number of beam shows that 4-beam is acceptable to be adapted in MQC-MB. The statistical analysis shows that such approach has reduced the total attenuation by 6dB compared to single-beam setup.

Abstrak tesis yang dikemukakan kepada Senat Universiti Putra Malaysia sebagai memenuhi keperluan untuk ijazah Doktor Falsafah

PENDEKATAN BERBILANG FOTON PERINGKAT TUNGGAL SECARA SELAMAT UNTUK PROTOKOL KRIPTOGRAFI KUANTUM DI DALAM RUANG OPTIK KOSONG

Oleh

NUR ZIADAH BINTI HARUN

November 2019

Pengerusi : Profesor Zuriati binti Ahmad Zukarnain, PhD
Fakulti : Sains Komputer dan Teknologi Maklumat

Untuk mengurangkan masalah kadar penghantaran data yang rendah dan jarak komunikasi yang terhad dalam komunikasi kuantum, pendekatan berbilang foton telah terbukti menjadi alternatif kepada pendekatan photon tunggal yang konvensional. Berbilang foton mempunyai keupayaan untuk meningkatkan penjanaan kadar kunci dan jarak melalui penghantaran foton di pelbagai peringkat. Walaubagaimanapun, penentuan bilangan purata foton dan bilangan peringkat yang optimum kekal sebagai cabaran utama untuk menjadikan protokol dimanfaatkan dengan baik semasa mereka beroperasi. Dalam hal ini, tiga masalah dan penyelesaian telah dicadangkan dalam tesis ini seperti yang dibentangkan di bawah:

Pertama, pendekatan berbilang foton memerlukan foton yang berganda untuk bergerak di sepanjang beberapa peringkat. Selain itu, masa tambahan diperlukan untuk menukar sudut polarisasi peranti optik untuk tujuan pengekodan. Keadaan ini akan mengakibatkan peningkatan jumlah masa penghantaran foton yang perlu dihantar melalui rangkaian kuantum disebabkan masa tambahan tersebut. Oleh itu, pendekatan M-ary Hibrid di dalam Peringkat Jalinan Tunggal (HMBSS) menggunakan konsep pemampatan data dicadangkan untuk menangai isu-isu ini. Didalam HMBSS, penghantar dapat memampatkan mesej rahsia menggunakan pengekodan Huffman melalui operasi peringkat jalinan tunggal. Mekanisma pemampatan ini telah mengurangkan jumlah bit yang diperlukan untuk mewakili rentetan simbol, dengan itu mengurangkan masa untuk mengekod foton. Simulasi eksperimen menunjukkan bahawa HMBSS mencapai hasil yang menjanjikan kadar penurunan jumlah masa penghantaran sebanyak 75.9% dan 91.7% berbanding dengan Multiphoton-BSS, Multiphoton-M-ary dan Multiphoton-TSIV yang terkenal.

Kedua, menyediakan pengesahan yang kuat telah menjadi fokus utama didalam penyelidikan ini dengan menjadikan pelbagai foton QSDC selamat daripada pelbagai jenis serangan. Pengesahan sedia ada didalam berbilang foton QSDC memerlukan persetujuan awam untuk pra-kongsi kunci pengesahan dan sudut rahsia sebelum memulakan penghantaran, oleh itu meningkatkan kos komunikasi. Sebagai penyelesaian, Pengesahan Kunci Rahsia Keselamatan (SSAK) telah dicadangkan. Di dalam SSAK, konsep perjabatan tangan kuantum digunakan untuk berkongsi sudut awal polarisasi rahsia dan kunci pengesahan yang digunakan sebelum memulakan komunikasi kuantum. Hasil simulasi eksperimen dan menunjukkan bahawa SSAK mengatasi protokol Tiga-peringkat dari sudut purata bilangan sudut yang diketahui oleh Eve. Simulasi eksperimen dan analisis keselamatan diperingkat pengesahan awal dan penghantaran mesej mengesahkan bahawa *eavesdropper* tidak dapat mendedahkan sebarang maklumat tentang mesej yang dikirim atau kunci pengesahan.

Akhir sekali, kebanyakan protocol QKD yang telah dicadangkan menggunakan tetapan pancaran tunggal untuk menghantar photon melalui ruang bebas optik yang menghasilkan kadar bit yang rendah dan jarak yang terhad disebabkan kesan kehilangan geometri yang tinggi. Untuk menangani hal ini, teknik transmisi Komunikasi Kuantum Berbilang Photon menggunakan konsep Berbilang Pancaran (MQC-MB) telah dicadangkan. Perbandingan dijalankan dari segi jumlah kerugian dan penerimaan kuasa pada bilangan pancaran yang berlainan menunjukkan bahawa 4-pancaran diterima untuk disesuaikan dengan MQC-MB. Analisis statistik menunjukkan pendekatan sedemikian telah mengurangkan jumlah kelemahan sebanyak 6 dB berbanding tetapan sinaran tunggal.

ACKNOWLEDGEMENTS

Alhamdulillah, all praises is for Allah Subhanahu Wa Taala for his bounty of giving me health, strength, patience and guidance to be able to complete this thesis. May blessing and peace be upon Prophet Muhammad Sallahu Alaihi Wasallam, who was sent for mercy to the world.

I would like to express my sincere gratitude to my supervisor, Prof. Dr. Zuriati Ahmad Zukarnain for her support, encouragement, motivation and immense knowledge towards my study. Her guidance had helped me a lot in the process of brainstorming, writing, experimenting, analyzing and last but not least completing this research. I would like to extend my gratitude to the supervisory committee member, Associate Professor Dr. Zurina Mohd Hanapi and Dr. Idawaty Ahmad for their complimentary support and encouragements. This thesis would have not been written successfully without continuous supervision and guidance from them. I am very grateful to the Faculty of Computer Science and Information Technology and Universiti Putra Malaysia for providing me excellent and conducive research environment. I would like to thank Univesiti Tun Hussein Onn Malaysia and Ministry of Higher Education Malaysia for the scholarship and financial support.

My great and sincere appreciation to my lovely husband, En. Firdaus Ruslan for consistently inspiring, giving moral support and encouragement along my study. Special thank goes to my mother, Pn. Sariah Yon, my mother in law, Pn. Sharifah Arifin, my father in law, En. Ruslan Abd. Rasit and my sister in law, Fara Dianti for understanding and supporting me so much. Thank for sparing me your valuable time throughout this long process. Last but not least, I would like to express my appreciation to my lab mates and friends, for their unlimited support and encouragement.

This thesis was submitted to the Senate of the Universiti Putra Malaysia and has been accepted as fulfilment of the requirement for the degree of Doctor of Philosophy. The members of the Supervisory Committee were as follows:

Zuriati binti Ahmad Zukarnain, PhD
Professor
Faculty of Computer Science and Information Technology
Universiti Putra Malaysia
(Chairman)

Zurina binti Mohd Hanapi, PhD
Associate Professor
Faculty of Computer Science and Information Technology
Universiti Putra Malaysia
(Member)

Idawaty binti Ahmad, PhD
Senior Lecturer
Faculty of Computer Science and Information Technology
Universiti Putra Malaysia
(Member)

ZALILAH MOHD SHARIFF, PhD
Professor and Dean
School of Graduate Studies
Universiti Putra Malaysia

Date:

Declaration by graduate student

I hereby confirm that:

- this thesis is my original work;
- quotations, illustrations and citations have been duly referenced;
- this thesis has not been submitted previously or concurrently for any other degree at any institutions;
- intellectual property from the thesis and copyright of thesis are fully-owned by Universiti Putra Malaysia, as according to the Universiti Putra Malaysia (Research) Rules 2012;
- written permission must be obtained from supervisor and the office of Deputy Vice-Chancellor (Research and innovation) before thesis is published (in the form of written, printed or in electronic form) including books, journals, modules, proceedings, popular writings, seminar papers, manuscripts, posters, reports, lecture notes, learning modules or any other materials as stated in the Universiti Putra Malaysia (Research) Rules 2012;
- there is no plagiarism or data falsification/fabrication in the thesis, and scholarly integrity is upheld as according to the Universiti Putra Malaysia (Graduate Studies) Rules 2003 (Revision 2012-2013) and the Universiti Putra Malaysia (Research) Rules 2012. The thesis has undergone plagiarism detection software

Signature: _____ Date: _____

Name and Matric No: Nur Ziadah binti Harun, GS46865

Declaration by Members of Supervisory Committee

This is to confirm that:

- the research conducted and the writing of this thesis was under our supervision;
- supervision responsibilities as stated in the Universiti Putra Malaysia (Graduate Studies) Rules 2003 (Revision 2012-2013) were adhered to.

Signature: _____
Name of Chairman of Supervisory Committee: Professor Dr. Zuriati binti Ahmad Zukarnain

Signature: _____
Name of Member of Supervisory Committee: Associate Professor Dr. Zurina binti Mohd Hanapi

Signature: _____
Name of Member of Supervisory Committee: Dr. Idawaty binti Ahmad

TABLE OF CONTENTS

LIST OF TABLES

LIST OF FIGURES

LIST OF ABBREVIATIONS

AES	Advanced Encryption Standard
DES	Data Encryption Standard
EC	Error Correction
ECC	Elliptic Curve Cryptography
EPR	Einstein–Podolsky–Rosen
FO	Fiber Optic
FSO	Free Space Optic
GHZ	Green-Horne- Zeilinger
HMBSS	Hybrid M-Ary in Braided Single-stage
HWP	Half Wave Plate
IR	Intercept Resent
IRFS	Intercept-Resend Fake State
ITT	Information travel time
IV	Initialization Vector
MITM	Man In the Middle
MFQC	Modified Four Stage Quantum Communication
MPN	Mean photon number
MQC-MB	Multiple-beam Concept for Multiphoton in Free Space Optical Channel
Multiphoton-SS	Multiphoton Single-stage
Multiphoton-BSS	Multiphoton Braided Single-stage
Multiphoton-M-ary	Multiphoton Three-stage Protocol using M-ary signal
Multiphoton-TS	Multiphoton Three-stage
Multiphoton-TSIV	Multiphoton Three-stage Protocol Using Four Variables

NIST	National Institute of Standards and Technology
OBGA	Overlapping Gaussian beam array
PA	Privacy Amplification
PDTC	Probability distribution of the transmission coefficient
PNS	Photon Number Splitting
QBER	Quantum Bit Error Rate
QC	Quantum Communication
QKD	Quantum Key Distribution
QSDC	Quantum Secret Direct Communication
QSS	Quantum Secret Sharing
QT	Quantum teleportation
QTSP	Quantum Three Stage Protocol
RSA	Rivest-Shamir-Adleman
SKR	Secret Key Rate
SoP	State of polarization
SSAK	Secure Secret Authentication Key
TSA	Three-Stage Authentication
WCP	Weak coherent pulse
WLAN	Wireless Local Area Network

CHAPTER 1

INTRODUCTION

1.1 Research Motivation

The merging of quantum computation provides a tremendous solution for heat production and energy consumption compared to classical computation. For instance, while it took about more than one year to decrypt Rivest-Shamir-Adleman (RSA) algorithm using 4 cores at 2.8 GHz desktop, one of the popular quantum algorithms known as Shor algorithm has the ability to decrypt it in just one second (Nielsen & Chuang, 2011). Furthermore, Lov Grover invented Grover algorithm in 1996 specifically to operate for search and optimization has the ability to solve the data searching problem using only 32 comparisons in the 1024 dataset whereas Advanced Encryption Standard (AES) and Data Encryption Standard (DES) algorithm requires 1023 comparisons (Chen et al., 2015). As reported by National Institute of Standards and Technology (NIST) (Chen et al., 2016), it is predicted that once the quantum computer is entirely employed, most of the classical cryptographic algorithms, for example, Elliptic Curve Cryptography (ECC) and RSA are going to be insecure. The emergence of quantum technology has attracted significant interest and has become an active research in the cryptography area. The deployment of quantum mechanic law in the new era of cryptography is known as Quantum Cryptography (QC) where two or more parties have secure and unconditional communication. Since it became recognized that quantum computer could break the classical cryptography algorithm, QC has been actively studied to overcome the stated limitation. QC is not limited to share secret key; it can also be implemented as secure direct communication, secure computation, and secret sharing.

Unlike classical cryptography that uses classical bit of 0 or 1, QC applies the properties of quantum mechanic called as quantum bit, or qubit in its operation. Qubit is the quantum state which consists of the smallest particle unit of quantum information that is mathematically represented by the Dirac notation. The quantum mechanic can be showed based on the state of bra (|) and ket (⟩) notation. The mapping from classical bit to qubit can be described as:

$$0 \rightarrow |0\rangle \qquad 1 \rightarrow |1\rangle \tag{1.1}$$

Quantum superposition allows a qubit to simultaneously exist in more than one state. The superposition states can be represented as:

$$|\Psi> \equiv \alpha|0\rangle + \beta|1\rangle = \begin{bmatrix}\alpha \\ \beta\end{bmatrix} \tag{1.2}$$

Where Ψ is the superposition states, α and β are the complex numbers, and $|0\rangle$ and $|1\rangle$ are qubits states. This means that a qubit can have a value of one or zero or any superposition states of both one and zero together. The $\begin{bmatrix}\alpha\\ \beta\end{bmatrix}$ is a two-dimensional vector, where $|0\rangle$ is equivalent to $\begin{bmatrix}1\\ 0\end{bmatrix}$ and $|1\rangle$ is equivalent to $\begin{bmatrix}0\\ 1\end{bmatrix}$. The probability of α and β coefficients can be satisfied by:

$$|\alpha|^2 + |\beta|^2 = 1 \tag{1.3}$$

where $|\alpha|^2$ is the probability of obtaining $|\Psi\rangle$ in $|0\rangle$ and $|\beta|^2$ is the probability of obtaining $|\Psi\rangle$ in $|1\rangle$.

In contrast to classical cryptography, the security of QC does not rely on computing power (Anghel, 2013). The QC is strengthened by the unconditional security in quantum mechanic law as proven by the no-cloning theorem and Heisenberg Uncertainty theory. No-cloning theorem states that the unknown quantum states cannot be copied without affecting the original states while Heisenberg Uncertainty theory states that the intruder cannot distinguish the properties of the quantum states without disturbing it. It should be noted that the generation of the qubit is assured by the quantum mechanics law. Therefore, when an eavesdropper intercepts the communication, the parties in the quantum channel will notice about the interception due to the changes in the properties of qubit (El Rifai, 2016).

The main objective of the QC protocol is to share secret information securely over the quantum channel. Typically, the quantum particles that are responsible to carry secret information need to be transmitted in the quantum channel. Senders and receivers are involved in a field of interest and they have the ability to performed several tasks such as sending and receiving the quantum particles, and other quantum operations according to specified protocols. Depending on the law of quantum physics, sender and receiver can disclose the existence of a third party, so-called as an eavesdropper that is trying to overhear and steal the message. The detection of the eavesdropper by the sender and receiver occurs when the error rate arises in quantum communication.

Practical security is a challenging issue in the realization of the QC protocol (Deng & Long, 2004). Eventhough the QC protocols are unconditionally secure in theory, the security might not be assured in practice due to the imperfection of devices. Transmitting the secret information without loss when it is encoded into the photon in any QC applications requires perfect devices in implementations (Hu et al., 2016). In most cases of QC, the imperfection of the single photon laser source used in practice is susceptible to mutiphoton signal attack. Apart from that, the parties might lose some photons due to the channel loss and deficiency of the detection device. Owing to this fact, the imperfect practical of implementations might open the loopholes in the QC, letting an eavesdropper to attack the system.

Basically, QC employs three types of states: Single photon, entangled, and multiphoton states. Single photon utilizes a laser to transmit a photon per laser pulse, entangled state utilizes the correlation between particles separated over distance, whereas multiphoton utilizes multiple photons per laser pulse. In long-distance network, single photon is however characterized by low transmission rate, limited distance coverage, and susceptible to the siphoning attacks. Besides, the entangled state is difficult to be implemented in the current network architecture due to the limitation of quantum device capabilities. To overcome these drawbacks, multiphoton (Darunkar & Verma, 2014; El Rifai, Punekar et al., 2013; Kak, 2016; El Rifai et al., 2015; Wai et al., 2015) were proposed. The information exchange in multiphoton approach is not limited to a single photon in a time slot. To improve the transmission's success rate, multiphoton allows multiple numbers of photons to be transmitted simultaneously to indicate one bit of information. Moreover, due to more than one photon are generated per pulse, the distance covered also increases.

1.2 Research Problems

Despite the successes achieved by multiphoton, determining the optimal mean photon numbers and the number of stages to ensure that the protocols are well-functioned during their operations still remain as critical issues. The previous multiphoton related works such as Multiphoton-TS (Kak, 2006), Multiphoton-M-ary (El Rifai et al., 2013), Multiphoton-TSIV (El Rifai et al., 2015) and Multiphoton-BSS (Darunkar & Verma, 2014), have proposed various techniques to mitigate the multiphoton issues and achieved their objectives. However, there are several limitations associated with multiphoton are left unresolved:

- Transmitting multiple photons along a number of stages using the existing multiphoton approaches, which are Multiphoton-TS (Kak, 2006), Multiphoton-M-ary (El Rifai et al., 2013), Multiphoton-TSIV (El Rifai et al., 2015) in QSDC is still a critical issue to be addressed. The transmission time in the multiphoton over multi-stage approach tends to increase due to the increase in the redundancy of sources. The multiphoton is made up of multiplicity number of photons generated by the sender over multi-stage transmission. Several multiphoton variants have been introduced in the literature. The strategy of transmitting the secret messages proposed by Multiphoton's variants aims to increase distance coverage and transmission rates. However, the transfer time to transmit the encoded information is still considered as a serious matter due to most of the multiphoton approaches involve the transmission of multiple photons over a number of stages. Furthermore, additional time is required to update the optical device's polarization angle for the purpose of encoding. This condition leads to source redundancy's growth, which then results in the increment of the transmission time.

- Most of the existing multiphoton approaches require the set of secret angles to be pre-shared before the onset of the transmission which is assumed to be done in public channels. Furthermore, the parties in quantum communication are assumed to be authenticated to each other using the three-stage protocol. This could lead the channel to be potentially vulnerable to several types of attack such MITM attack.
- Due to the quantum communication over fiber optic has reached optimal performance caused by fixed loss related to fiber and the restriction of the device, it (fiber optic) can be replaced by free space channel that offers several advantages including flexibility of installation, broader geographical coverage, and cost-effectiveness in terms of infrastructure deployment. Unfortunately, the development of free space quantum communication faces several major challenges(Yin et al., 2018). Most of the multiphoton approaches employ single-beam concept over the FSO that suffers high geometrical loss which has the limitation in terms of low secret key rate generation and distance covered.

This thesis addresses the above stated problems associated with multiphoton tolerant protocol. The Multiphoton-TS (Kak, 2006), Multiphoton-M-ary (El Rifai et al., 2013), Multiphoton-TSIV (El Rifai et al., 2015) and Multiphoton-BSS (Darunkar & Verma, 2014) approaches have been chosen as the comparison benchmark due to their variety type of enhancement to achieve successful performances.

1.3 Research Questions

The research questions to be answered are formulated as follows:

- How to reduce the usage of multiphoton so that the transmission time can be reduced significantly?
- How to share the authentication key and secret angles between parties securely in the quantum channel?
- How to increase the Secret Key Rate (SKR) and distance without consuming high implementation cost of the free space quantum infrastructure?

1.4 Research Objectives

The main objective of this thesis is to propose a secure multiphoton protocol by improving the transmission rate, provide secure authentication between legitimate parties, and enhance key generation rate as well as distance coverage. The specific objectives are explained as follows:

- To propose an enhanced multiphoton approach with data compression concept to increase the transmission rates by reducing the transmission time and preserving the secrecy of the message in Quantum Secure Direct Communication (QSDC) protocol.
- To propose a quantum handshake scheme for authetication to provide a secure way to share the initial secret polarization angles and authentication key between legitimate users.
- To propose a transmission technique for multiphoton Quantum Key Distribution (QKD) over Free Space Optic (FSO) based on multi-beam concept. The main aim of this design is to enhance key generation rate and distance coverage by minimizing the impact of geometrical loss that is faced by the standard single-beam concept during the transmission of photons.

1.5 Research Scope

This section outlines the scope of this study as demonstrated in the shaded area in Figure 1.1. This research mainly aims at improving transmission rates while single photon is not able of doing so. Furthermore, this research focuses on multiphoton based QC approaches that are designed to improve key generation rate and increase the range of distances in the communication channel. Apart from that, practical security regarding the authentication in quantum cryptography will also be covered in this research. This thesis focuses on improving the performance of multiphoton approaches which are single-stage, three-stage variants, and combination of single-stage and three-stage, so-called as braided single-stage. Thus, the implementation of the QC with entanglement photon approach lies beyond the scope of this research. Since there are several branches of quantum technology, this research study focusses on the QKD and QSDC over the free space optic due to both of them can be applied using multiphoton tolerant protocol and use similar quantum optical components (El Rifai, 2016; Wu & Chen, 2015).

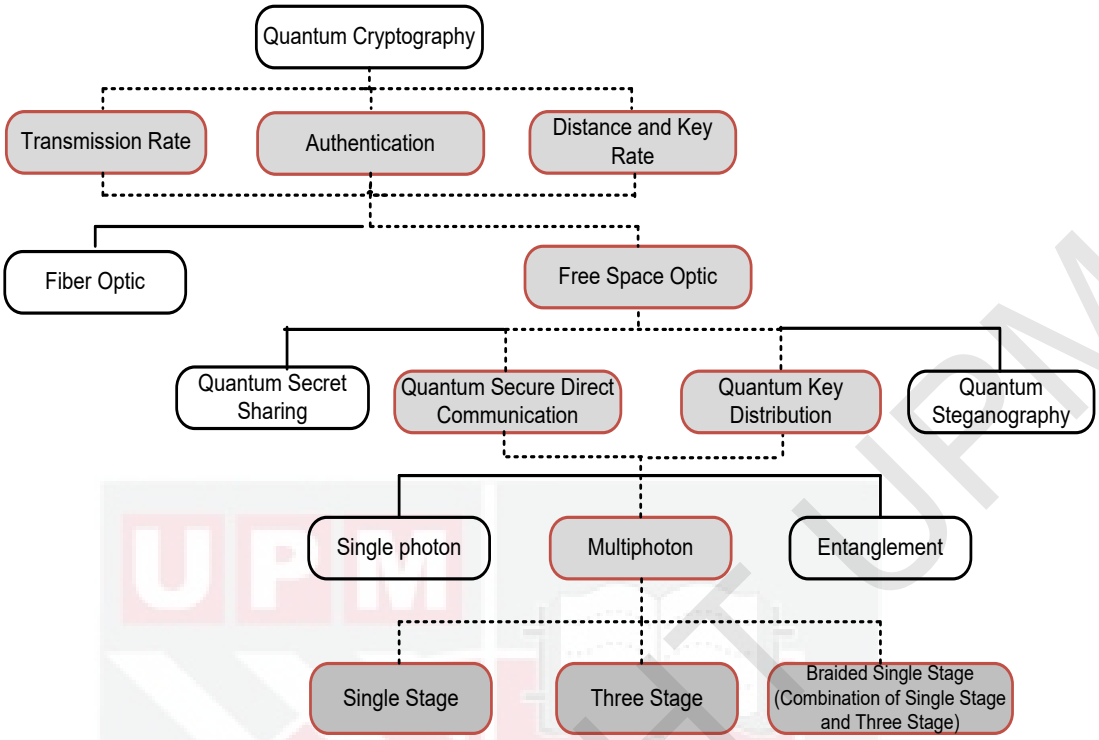

Figure 1.1 : Research scope

1.6 Organization of the Thesis

The rest of this thesis is organized in the following way:

Chapter 2 presents a literature review on quantum state transmission in QCs. It first discusses the issues in QC, followed by the introduction of quantum communication channel models for QC. Then, it shows the related works proposed in the literature for transmitting information based on single photon and multiphoton approaches. This chapter also presents a comparison of different multiphoton quantum protocol tolerants and its implementations' challenges. Finally, the chapter presents the QC's branches based on single and multiphoton tolerants.

Chapter 3 describes the research methodology used in this thesis. It starts with the identification of the notations and its definitions used throughout the thesis. Next, it presents the research framework, experimental setup and performance metrics conducted in this thesis. Finally, performance validation is presented to validate the experimental setting.

Chapter 4 presents a Hybrid M-Ary in Braided Single-stage (HMBSS) approach used to increase the transmission rates by reducing the transmission time in photon transmission. It demonstrates the design of the proposed HMBSS approach, and presents the evaluation and performance comparison with the existing multiphoton

approaches such as Multiphoton-TS, Multiphoton-M-ary, Multiphoton-TSIV and Multiphoton-BSS.

Chapter 5 presents the proposed quantum handshake scheme to share the initial secret polarization angle and the authentication key between legitimate parties. It presents the performance evaluation and security analysis of the proposed scheme with Multiphoton-M-ary and Multiphoton-BSS schemes.

Chapter 6 presents the design of the proposed multiple-beam for multiphoton in FSO (MQC-MB). It also describes the parameters used for the multiple-beam set up in order to transmit the quantum state. The performance evaluation and the results of the proposed design are presented and compared against standard single-beam design.

Chapter 7 concludes the thesis and recommends future research directions.

REFERENCES

Aaron Lopez-Leyva, J., Talamantes-Alvarez, A., A. Ponce-Camacho, M., Garcia-Cardenas, E., & Alvarez-Guzman, E. (2018). Free-Space-Optical Quantum Key Distribution Systems: Challenges and Trends. In *Quantum Cryptography* (pp. 1–14). IntechOpen. https://doi.org/10.5772/intechopen.81032

Aas, L. M. S. (2009). *Mueller Matrix Ellipsometric imaging*. Oslo, Norway.

Abushgra, A. A. (2017). A Shared Secret Key Initiated by EPR Authentication and Qubit Transmission Channels. *IEEE Access*, 17753–17763.

Al-Gailani, S. A., Mohammad, A. B., & Shaddad, R. Q. (2013). Enhancement of free space optical link in heavy rain attenuation using multiple beam concept. *Optik*, *124*(21), 4798–4801. https://doi.org/10.1016/j.ijleo.2013.01.098

Al-Gailani, Samir A., Mohammad, A. B., Shaddad, R. Q., Sheikh, U. U., & Elmagzoub, M. A. (2015). Hybrid WDM/multibeam free-space optics for multigigabit access network. *Photonic Network Communications*, *29*(2), 138–145. https://doi.org/10.1007/s11107-014-0482-y

Alizo, M. T. D. (2012). *Soft Processing Techniques for Quantum Key Distribution Applications*. Politecnico di Torino Porto.

Alkholidi, A. G., & Altowij, K. S. (2014). Climate effects on performance of free space optical communication systems in Yemen. *Frontiers of Optoelectronics*, *7*(1), 91–101. https://doi.org/10.1007/s12200-014-0392-8

Alléaume, R., Branciard, C., Bouda, J., Debuisschert, T., Dianati, M., Gisin, N., … Zeilinger, A. (2014). Using quantum key distribution for cryptographic purposes: A survey. *Theoretical Computer Science*, *560*(P1), 62–81. https://doi.org/10.1016/j.tcs.2014.09.018

Amerimehr, A., & Hadain Dehkordi, M. (2018). Impersonation attack on a quantum secure direct communication and authentication protocol with improvement. *Applied Physics B: Lasers and Optics*, *124*(3), 0. https://doi.org/10.1007/s00340-018-6907-z

Anghel, C. (2013). Research, development and simulation of quantum cryptographic protocols. *Elektronika Ir Elektrotechnika*, *19*(4), 65–70. https://doi.org/10.5755/j01.eee.19.4.1700

Ayashi, B. M. H. (2017). Review Finite-block-length analysis in classical and quantum information theory. *Proceedings of the Japan Academy, Series B*, *93*(3), 99–124.

Bash, B. A., Chandrasekaran, N., Shapiro, J. H., & Guha, S. (2016). Quantum Key Distribution Using Multiple Gaussian Focused Beams. *ArXiv: 1604.08582*, 1–14. Retrieved from http://arxiv.org/abs/1604.08582

Bebrov, G. (2019). On the generalization and improvement of QSDC efficiency achieved through a quantum channel compression. *Quantum Information Processing*, *18*(4), 1–10. https://doi.org/10.1007/s11128-019-2227-4

Bebrov, G., & Dimova, R. (2019). Proposal of Optimality Evaluation for Quantum Secure Communication Protocols by Taking the Average of the Main Protocol Parameters : Efficiency , Security and Practicality. *International Journal of Physical and Mathematical Sciences*, *13*(2), 48–52.

Bennett, C. H., & Brassard, G. (2014). Quantum cryptography : Public key distribution and coin tossing. *Theoretical Computer Science*, *560*, 7–11. https://doi.org/10.1016/j.tcs.2014.05.025

Bhosale, S., Darunkar, B., Punekar, N., Macdonald, G., & Verma, P. (2016). Polarization based secure AES key transmission over optical fiber. In *IEEE ICC 2016 Communication and Information Systems Security Symposium Polarization*.

Cao, Z., Li, Y., Peng, J., Chai, G., & Zhao, G. (2018). Controlled Quantum Secure Direct Communication Protocol Based on Huffman Compression Coding. *International Journal of Theoretical Physics*, *57*(12), 3632–3642.

Caputo, A. C. (2014). Wireless Networked Video. In *Digital Video Surveillance and Security* (pp. 123–167). https://doi.org/10.1016/b978-1-85617-747-4.00005-6

Carrasco-casado, A., Fernández, V., & Denisenko, N. (2016). Free-space quantum key distribution. In *Optical Wireless Communications* (pp. 589–607). Springer (2016).

Chan, K. W. C., Rifai, M. El, Verma, P. K., Kak, S., & Chen, Y. (2015). Multi-Photon Quantum Key Distribution Based on Double-Lock Encryption. *International Journal on Cryptography and Information Security*, *5*, 1–13. https://doi.org/10.1364/CLEO_QELS.2015.FF1A.3

Chang, Y., Xu, C. X., Zhang, S. Bin, & Yan, L. L. (2013). Quantum secure direct communication and authentication protocol with single photons. *Chinese Science Bulletin*, *58*(36), 4571–4576. https://doi.org/10.1007/s11434-013-6091-9

Chang, Y., Zhang, S., Yan, L., & Li, J. (2014). Deterministic secure quantum communication and authentication protocol based on three-particle W state and quantum one-time pad. *Chinese Science Bulletin*, *59*(23), 2835–2840. https://doi.org/10.1007/s11434-014-0333-3

Chen, C. Y., Zeng, G. J., Lin, F. J., Chou, Y. H., & Chao, H. C. (2015). Quantum cryptography and its applications over the internet. *IEEE Network*, *29*(5), 64–69. https://doi.org/10.1109/MNET.2015.7293307

Chen, L., Jordan, S., Liu, Y.-K., Moody, D., Peralta, R., Perlner, R., & Smith-Tone, D. (2016). *Report on Post - Quantum Cryptography Report on Post - Quantum Cryptography*. https://doi.org/10.6028/NIST.IR.8105

Chen, Y. (2018). *U.S Patent 20180048466A1*. US.

Chen, Y., Kak, S., Verma, P. K., Macdonald, G., Rifai, M. El, & Punekar, N. (2013). Multi-photon tolerant secure quantum communication - From theory to practice. *IEEE International Conference on Communications*, 2111–2116. https://doi.org/10.1109/ICC.2013.6654838

Clifford Chan, K. W., El Rifai, M., Verma, P., Kak, S., & Chen, Y. (2015). Security Analysis of the Multi-Photon Three-Stage Quantum Key Distribution. *International Journal on Cryptography and Information Security*, *5*(3/4), 01–13. https://doi.org/10.5121/ijcis.2015.5401

Darunkar, B. A. (2017). *Multi-Photon Tolerant Quantum Key Distribution Protocols For Secured Global Communication*. University Of Oklahoma.

Darunkar, B., & Verma, P. (2014). The braided single-stage protocol for quantum secure communication. In *Proc. of SPIE,Quantum Information and Computation XII* (Vol. 9123, pp. 1–8). https://doi.org/10.1117/12.2050164

Deng, F.-G., & Long, G. L. (2004). Secure direct communication with a quantum one-time pad. *PHYSICAL REVIEW A*, *052319*(69), 1–4. https://doi.org/10.1103/PhysRevA.69.052319

Deng, F., Long, G. L., & Liu, X. (2003). Two-step quantum direct communication protocol using the Einstein-Podolsky-Rosen pair block. *Physical Review A*, *68*(4), 1–6. https://doi.org/10.1103/PhysRevA.68.042317

Dhawale, N. (2014). Implementation of Huffman algorithm and study for optimization. In *Proceedings - 2014 IEEE International Conference on Advances in Communication and Computing Technologies, ICACACT*. https://doi.org/10.1109/EIC.2015.7230711

Diamanti, E., Lo, H., Qi, B., & Yuan, Z. (2016). Practical challenges in quantum key distribution. *Nature Publishing Group*, (May), 1–12. https://doi.org/10.1038/npjqi.2016.25

El-latif, A. A. A. B. D., Abd-el-atty, B., Hossain, M. S., Samir, E., & Ghoneim, A. (2018). Secure Quantum Steganography Protocol for Fog Cloud Internet of Things. *IEEE Access*, *6*, 10332–10340. https://doi.org/10.1109/ACCESS.2018.2799879

El-Mashade, M., Aly, M., & Toeima, A. (2015). Performance Evaluation of FSO System with MIMO Technique in Different Operating Environments. *Physical Science International Journal*, *7*(1), 33–48. https://doi.org/10.9734/PSIJ/2015/17212

El Rifai, M. (2016). *Quantum Secure Communication Using Polarization Hopping Multi-Stage Protocols*. University Of Oklahoma.

El Rifai, M., Punekar, N., & Verma, P. K. (2013). Implementation of an m-ary three-stage quantum cryptography protocol. In *Proc. SPIE 8875, Quantum Communications and Quantum Imaging XI* (Vol. 8875, pp. 1–13). https://doi.org/10.1117/12.2024185

Elmabrok, O., & Razavi, M. (2018). Wireless quantum key distribution in indoor environments. *Journal of the Optical Society of America B: Optical Physics*, *35*(2), 197–207. https://doi.org/10.1364/JOSAB.35.000197

Erven, C., Heim, B., Meyer-Scott, E., Bourgoin, J. P., Laflamme, R., Weihs, G., & Jennewein, T. (2012). Studying free-space transmission statistics and improving free-space quantum key distribution in the turbulent atmosphere. *New Journal of Physics*, *14*. https://doi.org/10.1088/1367-2630/14/12/123018

Gawron, P., Kurzyk, D., & Id, Ł. P. (2018). QuantumInformation . jl — A Julia package for numerical computation in quantum information theory. *PLoS ONE 13(12):*, *13*(12), 1–45.

Ghilen, A., Belmabrouk, H., & Bouallegue, R. (2014). Classification of quantum authentication protocols and calculation of their complexity. In *15th international conference on Sciences and Techniques of Automatic control & computer engineering* (pp. 169–173).

Gu, B., Huang, Y., Fang, X., & Chen, Y. (2013). Robust Quantum Secure Communication with Spatial Quantum States of Single Photons. *International Journal of Theoretical Physics*, *52*(12), 4461–4469. https://doi.org/10.1007/s10773-013-1765-2

Guedes, E. B., & Assis, F. M. de. (2011). An Approach To Evaluate Quantum Authentication Protocols. In *Congresso Brasileiro de Inteligência Computacional* (pp. 1–8). https://doi.org/10.21528/cbic2011-007

Han, Q., Yu, L., Zheng, W., Cheng, N., & Niu, X. (2014). A novel QKD network routing algorithm based on optical-path-switching. *Journal of Information Hiding and Multimedia Signal Processing*, *5*(1), 13–19.

Hecht, E. (2017). *Optics* (Fifth Edit). Essex, England: Pearson Education.

Hiroshi, Y. (2012). An Implementation of Steganography Using Construction of Huffman Tree. In *2012 International Symposium on Information Theory and its Applications* (pp. 634–637).

Hu, J. Y., Yu, B., Jing, M. Y., Xiao, L. T., Jia, S. T., Qin, G. Q., & Long, G. L. (2016). Experimental quantum secure direct communication with single photons. *Light: Science and Applications*, *5*(9), 1–5. https://doi.org/10.1038/lsa.2016.144

Husagić-Selman, A., Al-Khateeb, W., & Saharudin, S. (2012). Feasibility of QKD over FSO link. *2012 International Conference on Computer and Communication Engineering, ICCCE 2012*, (July), 362–368. https://doi.org/10.1109/ICCCE.2012.6271212

Hwang, W. Y. (2003). Quantum Key Distribution with High Loss: Toward Global Secure Communication. *Physical Review Letters*, *91*(5). https://doi.org/10.1103/PhysRevLett.91.057901

Iwakoshi, T. (2017). On problems in security of quantum key distribution raised by Yuen. *Quantum Information Science and Technology III*, *1044203*(October 2017), 3. https://doi.org/10.1117/12.2278625

Jain, A., Lakhtariab, K. I., & Srivastava, P. (2013). A Comparative Study of Lossless Compression Algorithm on Text Data. *Proc. of Int. Conf. on Advances in Computer Science, AETACS*, 536–543. https://doi.org/10.1109/DCC.2009.68

Jino, H., Jin, H., Jang, G., & Kwon, D. (2017). Quantum identity authentication with single photon. *Quantum Information Processing*, *16*(10), 1–20. https://doi.org/10.1007/s11128-017-1681-0

Kak, S. (2006). A three-stage Quantum Cryptography protocol. *Foundations of Physics Letters*, *19*(3), 293–296. https://doi.org/10.1007/s10702-006-0520-9

Kak, S. (2014). Authentication Using Piggy Bank Approach to Secure Double-Lock Cryptography. *ArXiv*, 1–8. Retrieved from https://arxiv.org/abs/1411.3645

Kak, S. (2016). State Ensembles and Quantum Entropy. *International Journal of Theoretical Physics*, *55*(6), 3017–3026. https://doi.org/10.1007/s10773-016-2934-x

Khaleel, A. I., & Tawfeeq, S. K. (2018). Key rate estimation of measurement-device-independent quantum key distribution protocol in satellite-earth and intersatellite links. *International Journal of Quantum Information*, *16*(03), 1850027. https://doi.org/10.1142/s0219749918500272

Khodr, M. (2017a). Evaluations of Maximum Distance Achieved Using the Three Stage Multiphoton Protocol at 1550 nm , 1310 nm , and 850 nm. In *CYBER 2017 : The Second International Conference on Cyber-Technologies and Cyber-Systems Evaluations* (pp. 32–34).

Khodr, M. (2017b). Evaluations of Quantum Bit Error Rate Using the Three Stage Multiphoton Protocol. In *2017 International Conference on Electrical and Computing Technologies and Applications (ICECTA) Evaluations* (pp. 2–5).

Kodabagi, M. M., Jerabandi, M. V., & Gadagin, N. (2016). Multilevel security and compression of text data using bit stuffing and huffman coding. *Proceedings of the 2015 International Conference on Applied and Theoretical Computing and Communication Technology, ICATccT 2015*, 800–804. https://doi.org/10.1109/ICATCCT.2015.7456992

Korchenko, O., Vasiliu, Y., & Gnatyuk, S. (2010). Modern quantum technologies of information security against cyber- terrorist attacks. *Aviation*, *14*(2), 58–69. https://doi.org/10.3846/aviation.2010.10

Korchenko, O., & Vorobiyenko, P. (2012). Quantum Secure Telecommunication Systems. *Telecommunications Networks - Current Status and Future Trends*, 1–5.

Korzh, B., Ci, C., Lim, W., Houlmann, R., Gisin, N., Li, M. J., … Zbinden, H. (2015). Provably secure and practical quantum key distribution over 307 km of optical fibre. *Nature Photonics*, *9*(February), 163–168. https://doi.org/10.1038/nphoton.2014.327

Li, J., Pan, Z., Sun, F., Chen, Y., Wang, Z., & Shi, Z. (2015). Quantum secure direct communication based on dense coding and detecting eavesdropping with four-particle genuine entangled state. *Entropy*, *17*(10), 6743–6752. https://doi.org/10.3390/e17106743

Li, L., Zhang, R., Zhao, Z., Xie, G., Liao, P., Pang, K., … Starodubov, D. (2017). High-Capacity Free-Space Optical Communications Between a Ground Transmitter and a Ground Receiver via a UAV Using Multiplexing of Multiple Orbital- Angular-Momentum Beams. *Scientific Reports*, *7*(1), 1–12. https://doi.org/10.1038/s41598-017-17580-y

Li, Q., Le, D., Wu, X., Niu, X., & Guo, H. (2015). Efficient bit sifting scheme of post-processing in quantum key distribution. *Quantum Information Processing*, *14*(10), 3785–3811. https://doi.org/10.1007/s11128-015-1035-8

Li, Y., Zhang, P., & Huang, R. (2019). Lightweight Quantum Encryption for Secure Transmission of Power Data in Smart Grid. *IEEE Access*, *7*, 1–9. https://doi.org/10.1109/ACCESS.2019.2893056

Lim, K., Ko, H., Kim, K., Suh, C., & Rhee, J. K. (2015). The Error Tolerance Bound for Secure Multi-Qubit QKD Against Incoherent Attack. *IEEE Journal of Selected Topics in Quantum Electronics*, *21*(3).

Liu, B., Gao, Z., Xiao, D., Huang, W., Liu, X., & Xu, B. (2019). Quantum identity authentication in the orthogonal-state-encoding QKD system. *Quantum Information Processing*, *123*. https://doi.org/10.1007/s11128-019-2255-0

Liu, B., Gao, Z., Xiao, D., Huang, W., Zhang, Z., & Xu, B. (2019). Quantum Identity Authentication in the Counterfactual Quantum Key Distribution Protocol, 1–19. https://doi.org/10.3390/e21050518

Liu, Z. H., & Chen, H. W. (2018). Analysis and Improvement of Large Payload Bidirectional Quantum Secure Direct Communication Without Information Leakage. *International Journal of Theoretical Physics*, *57*(2), 311–321. https://doi.org/10.1007/s10773-017-3563-8

Liu, Z. H., Chen, H. W., & Liu, W. J. (2016). Information Leakage Problem in Efficient Bidirectional Quantum Secure Direct Communication with Single Photons in Both Polarization and Spatial-Mode Degrees of Freedom. *International Journal of Theoretical Physics*, *55*(11), 4681–4686. https://doi.org/10.1007/s10773-016-3089-5

Lizama-pérez, L. A., López, J. M., & López, E. D. C. (2017). Quantum Key Distribution in the Presence of the Intercept-Resend with Faked States Attack. *Entropy*, 1–15. https://doi.org/10.3390/e19010004

Lo, H.-K., Ma, X., & Chen, K. (2004). Decoy State Quantum Key Distribution. *PHYSICAL REVIEW LETTERS*, *230504*(September 2004), 15–18. https://doi.org/10.1103/PhysRevLett.94.230504

Lo, H., Curty, M., & Tamaki, K. (2014). Secure quantum key distribution. *Nature Photonics*, *8*(July), 595–604. https://doi.org/10.1038/nphoton.2014.149

Lopes, M., & Sarwade, N. (2016). Modeling and Performance Analysis of Free Space Quantum Key Distribution. In *Information Systems Design and Intelligent Applications* (Vol. 435, pp. 27–40). New Delhi: Springer. https://doi.org/10.1007/978-81-322-2757-1

Lopes, M., & Sarwade, N. (2018). Modeling optimized decoy state protocol for enhanced quantum key distribution. *Journal of Information Security and Applications*, *38*, 1339–1351. https://doi.org/10.1016/j.jisa.2017.11.003

Ma, X., Qi, B., Zhao, Y., & Lo, H.-K. (2005). Practical decoy state for quantum key distribution. *Physical Review A*, *72*(1), 012326. https://doi.org/10.1103/PhysRevA.72.012326

Mailloux, L. O., Hodson, D. D., Grimaila, M. R., Engle, R. D., McLaughlin, C. V., & Baumgartner, G. B. (2016). Using Modeling and Simulation to Study Photon Number Splitting Attacks. *IEEE Access*, *4*, 2188–2197. https://doi.org/10.1109/ACCESS.2016.2555759

Mailloux, LO, & Grimaila, M. (2015). Performance evaluations of quantum key distribution system architectures. *IEEE Security & Privacy*, *1*, 20–40.

Mailloux, Logan, Grimaila, M., Hodson, D., Engle, R., McLaughlin, C., & Baumgartner, G. (2017). Modeling, Simulation, and Performance Analysis of Decoy State Enabled Quantum Key Distribution Systems. *Applied Sciences*, *7*(3), 212. https://doi.org/10.3390/app7020212

Mayssaa El Rifai, Kam Wai Clifford Chan, & Verma, P. K. (2015). Multi-stage quantum secure communication using polarization hopping. *Security And Communication Networks*, *8*, 4333–4342. https://doi.org/10.1002/sec

Medeiros, H. P., Maciel, M. C., Demo Souza, R., & Pellenz, M. E. (2014). Lightweight data compression in wireless sensor networks using Huffman coding. *International Journal of Distributed Sensor Networks*, *2014*. https://doi.org/10.1155/2014/672921

Mehic, M., Maurhart, O., Rass, S., Komosny, D., & Rezac, F. (2017). Analysis of the Public Channel of Quantum Key Distribution Link. *IEEE JOURNAL OF QUANTUM ELECTRONICS*, *53*(5).

Miglani, R., & Malhotra, J. S. (2018). Statistical Analysis of FSO Links Employing Multiple Transmitter / Receiver Strategy over Double-Generalized and Gamma – Gamma Fading Channel Using Different Modulation Techniques. *Journal of Optical Communications*, *40*(3), 1–11.

Miljkovic, N. N., & Stojanovic, A. D. (2018). Multiparameter QKD authentication protocol design over optical quantum channel. *Optical and Quantum Electronics*, 1–11. https://doi.org/10.1007/s11082-018-1585-y

Nanvakenari, M., & Houshmand, M. (2017). An efficient controlled quantum secure direct communication and authentication by using four particle cluster states. *International Journal of Quantum Information*, *15*(01), 1750002. https://doi.org/10.1142/S0219749917500022

Nguyen, D. M., & Kim, S. (2019). Multi-Bits Transfer Based on the Quantum Three-Stage Protocol with Quantum Error Correction Codes. *International Journal of Theoretical Physics*, (April). https://doi.org/10.1007/s10773-019-04098-4

Nielsen, M. A., & Chuang, I. L. (2011). Quantum Computation and Quantum Information. In *Cambridge University Press* (p. 706). https://doi.org/10.2277/0521635039

Nomula, R., Rifa, M. El, & Verma, P. (2016). Multi-photon tolerant protocols for quantum secure communication in wireless standards. *Int. J. Security and Networks*, *11*.

Noor, N. H. M., Naji, A. W., & Al-Khateeb, W. (2012). Performance analysis of a free space optics link with multiple transmitters/receivers. *IIUM Engineering Journal*, *13*(1), 49–58.

Noor, N. H., Naji, A. W., & Al-khateeb, W. (2011). Theoretical Analysis of Multiple Transmitters / Receivers on the Performance of Free Space Optics (FSO) Link. In *Proceeding of the 2011 IEEE International Conference on Space Science and Communication (IconSpace) 12-13 July 2011, Penang, Malaysia* (pp. 12–13). https://doi.org/10.1109/IConSpace.2011.6015903

Patil, M. E., Hussain, M., & Sharma, S. (2019). Modeling and Simulation of Secure Data Transfer in High Level Language Using Quantum Communication Protocol. In *International Conference on Advanced Computing Networking and Informatics* (Vol. 870, pp. 271–278). Springer Singapore.

https://doi.org/10.1007/978-981-13-2673-8

Patil, M., & Sharma, S. (2017). Modeling And Simulation Of Secure Data Transfer In High Level Language Using Quantum Communication. *International Journal For Technological Research In Engineering*, *4*(10), 2256–2259.

Peatross, J., & M. Ware. (2015). Polarization of Light. In *Physics of Light and Optics* (2015 Editi, pp. 143–168). Provo, UT, USA: Brigham Young University. Retrieved from optics.byu.edu

Sangwan, N. (2013). Combining Huffman text compression with new Double Encryption Algorithm. In *2013 International Conference on Emerging Trends in Communication, Control, Signal Processing and Computing Applications (C2SPCA)*.

Sargent, R G. (2012). Verification and validation of simulation models. *Journal of Simulation*, *7*(1), 12–24. https://doi.org/10.1057/jos.2012.20

Sargent, Robert G. (2016). Verification and validation of simulation models. In *Proceedings of the 2011 Winter Simulation Conference* (pp. 183–198). https://doi.org/10.1109/WSC.2010.5679166

Scarani, V., Bechmann-Pasquinucci, H., Cerf, N. J., Dušek, M., Lütkenhaus, N., & Peev, M. (2009). The security of practical quantum key distribution. *Reviews of Modern Physics*, *81*(3), 1301–1350. https://doi.org/10.1103/RevModPhys.81.1301

Sharma, V., & Banerjee, S. (2019). Analysis of atmospheric effects on satellite-based quantum communication : a comparative study. *Quantum Information Processing*, *123*, 1–24. https://doi.org/10.1007/s11128-019-2182-0

Sharma, V., Thapliyal, K., Pathak, A., & Banerjee, S. (2016). A comparative study of protocols for secure quantum communication under noisy environment: single-qubit-based protocols versus entangled-state-based protocols. *Quantum Information Processing*, *15*(11), 4681–4710. https://doi.org/10.1007/s11128-016-1396-7

Shumani, M. M., Abdullah, M. F. L., & Suriza, A. Z. (2016). The Effect of Haze Attenuation on Free Space Optics Communication (FSO) at Two Wavelengths under Malaysia Weather. *Proceedings - 6th International Conference on Computer and Communication Engineering: Innovative Technologies to Serve Humanity, ICCCE 2016*, (1), 459–464. https://doi.org/10.1109/ICCCE.2016.102

Song, S., & Wang, C. (2012). Recent development in quantum communication. *Chinese Science Bulletin*, *57*(36), 4694–4700. https://doi.org/10.1007/s11434-012-5600-6

Stebila, D., Mosca, M., & Lütkenhaus, N. (2010). The case for quantum key distribution. In *Quantum Communication and Quantum Networking.*

QuantumComm 2009 (pp. 283–296). Retrieved from http://link.springer.com/chapter/10.1007/978-3-642-11731-2_35

Stojanovic, A. D., & Viana, R. (2016). Authenticated B92 QKD protocol employing synchronized optical chaotic systems. *Optical and Quantum Electronics*, *48*(5), 1–7. https://doi.org/10.1007/s11082-016-0559-1

Sun, X., Djordjevic, I. B., & Neifeld, M. A. (2016a). Multiple spatial modes based QKD over marine free-space optical channels in the presence of atmospheric turbulence. *Optics Express*, *24*(24), 27663–27673.

Sun, X., Djordjevic, I. B., & Neifeld, M. A. (2016b). Secret Key Rates and Optimization of BB84 and Decoy State Protocols over Time-Varying Free-Space Optical Channels. *IEEE Photonics Journal*, *8*(3). https://doi.org/10.1109/JPHOT.2016.2570000

Tang, F. (2013). Scintillation discriminator improves free-space quantum key distribution. *Chinese Optics Letters*, *11*(9), 9–12. https://doi.org/10.3788/COL201311.090101.In

Thomas, J. H. (2007). Variations on Kak's Three Stage Quantum Cryptography Protocol. *ArXiv Preprint*, (arXiv:0706.2888), 1–7. Retrieved from http://arxiv.org/abs/0706.2888

Trinh, P. V., Pham, T. V., Dang, N. T., Nguyen, H. V., Ng, S. X., & Pham, A. T. (2018). Design and Security Analysis of Quantum Key Distribution Protocol over Free-Space Optics Using Dual-Threshold Direct-Detection Receiver. *IEEE Access*, *6*, 4159–4175. https://doi.org/10.1109/ACCESS.2018.2800291

Trinh, P. V., Pham, T. V., Nguyen, H. V., Ng, S. X., & Pham, A. T. (2016). Performance of free-space QKD systems using SIM/BPSK and dual-threshold/direct-detection. *2016 IEEE Globecom Workshops, GC Wkshps 2016 - Proceedings*, 1–6. https://doi.org/10.1109/GLOCOMW.2016.7848999

Uthayakumar, J., Vengattaraman, T., & Dhavachelvan, P. (2018). A survey on data compression techniques: From the perspective of data quality, coding schemes, data type and applications. *Journal of King Saud University - Computer and Information Sciences*. https://doi.org/10.1016/j.jksuci.2018.05.006

Vasylyev, D., Vogel, W., & Semenov, A. A. (2018). Theory of atmospheric quantum channels based on the law of total probability. *Physical Review A*, *97*(6). https://doi.org/10.1103/PhysRevA.97.063852

Verma, P. K., Mayssaa El Rifai, & Kam Wai Clifford Chan. (2019). *Multi-photon Quantum Secure Communication*. Springer Singapore.

Vogl, T. (2016). *Mobile Free Space Quantum Key Distribution for short distance secure communication*. Ludwig-Maximillians-Universtität München.

Wahab, F. A., Leong, T. K., Zulkifli, H., Izuan, M., Ibrahim, B., Akmal, M., … Ibrahim, O. K. (2016). Multiple Transmitters & Receivers for Free Space Optical Communication Link Performance Analysis. *Journal of Telecommunication, Electronic and Computer Engineering*, *8*(5), 29–32. https://doi.org/2180-1843

Wahba, W. Z., & Maghari, A. Y. A. (2016). Lossless Image Compression Techniques Comparative Study. *International Research Journal of Engineering and Technology (IRJET)*, *3*(2), 1–9.

Wai, K., Chan, C., Rifai, M. El, Verma, P., Kak, S., & Chen, Y. (2015). Multi-Photon Quantum Key Distribution Based on Double-Lock Encryption. *Optical Society of America*, 3–4.

Wang, L. L., W. P. Ma, D. S. Shen ·, & M. L. Wang. (2015). Efficient Bidirectional Quantum Secure Direct Communication with Single Photons in Both Polarization and Spatial-Mode Degrees of Freedom. *International Journal of Theoretical Physics*, *54*(10), 3443–3453. https://doi.org/10.1007/s10773-016-3089-5

Wang, L., & Ma, W. (2016). Controlled quantum secure communication protocol with single photons in both polarization and spatial-mode degrees of freedom. *Modern Physics Letters B*, *30*(05), 1650051. https://doi.org/10.1142/s0217984916500512

Wang, Li Li, Ma, W. P., Wang, M. L., & Shen, D. S. (2016). Three-party Quantum Secure Direct Communication with Single Photons in both Polarization and Spatial-mode Degrees of Freedom. *International Journal of Theoretical Physics*, *55*(5), 2490–2499. https://doi.org/10.1007/s10773-015-2886-6

Wang, W., Xu, F., & Lo, H. K. (2018). Prefixed-threshold real-time selection method in free-space quantum key distribution. *Physical Review A*, *97*(3), 1–13. https://doi.org/10.1103/PhysRevA.97.032337

Wang, X., Zhao, N., Chen, N., Zhu, C., & Pei, C. (2018). Effects of atmospheric turbulence on the single-photon receiving efficiency and the performance of quantum channel with the modified approximate elliptic-beam model assumption. *Quantum Information Processing*, *17*(1), 14. https://doi.org/10.1007/s11128-017-1780-y

Wu, L. (2015). *Reconfigurable Optical Networks And Multi-Photon Quantum Cryptography*. University of Houston.

Wu, L., & Chen, Y. (2015). Three-Stage Quantum Cryptography Protocol under Collective-Rotation Noise. *Entropy*, *17*(5), 2919–2931. https://doi.org/10.3390/e17052919

Xiao, H., & Zhang, Z. (2017). Subcarrier multiplexing multiple-input multiple-output quantum key distribution scheme with orthogonal quantum states. *Quantum Information Processing*, *16*(1). https://doi.org/10.1007/s11128-016-

1474-x

Xu, K., Sun, L., Xu, K., Sun, L., Xie, Y., & Song, Q. (2016). Transmission of IM / DD Signals at 2 μ m Wavelength Using PAM and CAP Transmission of IM / DD Signals at 2 μ m Wavelength Using PAM and CAP. *IEEE Photonics Journal*, *8*(5). https://doi.org/10.1109/JPHOT.2016.2602080

Yan, L., Sun, Y., Chang, Y., Zhang, S., Wan, G., & Sheng, Z. (2018). Semi-quantum protocol for deterministic secure quantum communication using Bell states. *Quantum Information Processing*, *123*, 1–12. https://doi.org/10.1007/s11128-018-2086-4

Yang, Y. yan. (2014). A Quantum Secure Direct Communication Protocol Without Quantum Memories. *International Journal of Theoretical Physics*, *53*(7), 2216–2221. https://doi.org/10.1007/s10773-014-2021-0

Yin, L., Pan, D., & Long, G. (2018). Quantum Secure Direct Communication : A Survey of Basic Principle and Recent Development. *Jurnal Fizik Malaysia*, *39*(2), 2–7.

Zhang, W., Ding, D. S., Sheng, Y. B., Zhou, L., Shi, B. Sen, & Guo, G. C. (2017). Quantum Secure Direct Communication with Quantum Memory. *Physical Review Letters*, *118*(22), 1–6. https://doi.org/10.1103/PhysRevLett.118.220501

Zhao, X.-L., Li, J.-L., Niu, P.-H., Ma, H.-Y., & Ruan, D. (2017). Two-step quantum secure direct communication scheme with frequency coding. *Chinese Physics B*, *26*(3), 030302. https://doi.org/10.1088/1674-1056/26/3/030302