UNIVERSITY OF OKLAHOMA

GRADUATE COLLEGE

MULTI-PHOTON TOLERANT QUANTUM KEY DISTRIBUTION PROTOCOLS FOR SECURED GLOBAL COMMUNICATION

A DISSERTATION

SUBMITTED TO THE GRADUATE FACULTY

in partial fulfillment of the requirements for the

Degree of

DOCTOR OF PHILOSOPHY

By

BHAGYASHRI ARUN DARUNKAR

Norman, Oklahoma
2017

MULTI-PHOTON TOLERANT QUANTUM KEY DISTRIBUTION PROTOCOLS FOR SECURED GLOBAL COMMUNICATION

A DISSERTATION APPROVED FOR THE
SCHOOL OF ELECTRICAL AND COMPUTER ENGINEERING

BY

Dr. Kam Wai Clifford Chan, Chair

Dr. Pramode Verma

Dr. William Ray

Dr. Subhash Kak

Dr. Gregory MacDonald

© Copyright by BHAGYASHRI ARUN DARUNKAR 2017
All Rights Reserved.

To my loved ones

Acknowledgements

I would like to take this opportunity to sincerely thank all those who helped me to reach at this point of dissertation.

First of all, I would like to express my appreciation for my chair Dr. Chan who graciously accepted me as a student and lead my path. He encouraged me to complete my research. I am thankful to Dr. Verma who has guided me throughout this journey. Dr. Verma always believed in my abilities not only as a researcher but also as a leader in owning different events at school.

It gives me great pleasure to acknowledge the support of my committee members, Dr. Gregory MacDonald, Dr. Subhash Kak, and Dr. William O. Ray, for their valuable comments and suggestions.

I would like to extend special thanks to my husband, Nikhil Punekar who helped me in many hardships of writing and research. I am grateful to have wonderful supporting friends and delightful people like Renee Wagenblatt in my life.

My PhD path would have been impossible without the financial aid from Hilti Inc, Tulsa. My managers and CIO have helped me to gain corporate knowledge during my studies.

The research presented in this dissertation is supported in part by the National Science Foundation (NSF) under Grants 1117179.

The part of this research has been patented and published. Patent number is US2017/0208040 A1 published on Jul 20,2017.

I would like to dedicate this dissertation to my dear daughter Adira and my lovely family.

Table of Contents

List of Tables

List of Figures

Abstract

This dissertation investigates the potential of multi-photon tolerant protocols for satellite-aided global quantum key distribution (QKD). Recent investigations like braided single-stage protocol and the implementation of the three-stage protocol in fiber have indicated that multi-photon tolerant protocols have wide-ranging capabilities for increasing the distance and speed of *quantum-secure communication*. This dissertation proposes *satellite-based network multicasting* and its operation that can profitably use multi-photon tolerant protocols for quantum-secure global communication.

With a growingly interconnected world and an increasing need for security in communication, communication satellites at Lower Earth Orbits (LEO), Medium Earth Orbit (MEO) and Geostationary Earth Orbit (GEO) have a potential role in serving as a means to distribute secure keys for encryption among distant endpoints. This dissertation systematically evaluates such a role. The dissertation proposes a layered framework using satellites and fiber optic links that can form a composite system for carrying the information payload and distributing quantum-secure keys for encrypting information in transit.

Quantum communications links are currently point-to-point. Considering the concept of global QKD network, there is need for multicast quantum links. Multi casting can be achieved in quantum networks by (a) using multiple wavelengths, or (b) using use specific set of bases. In efforts to develop a composite quantum secure global communication system; this dissertation also introduces the concept of multi-photon tolerant *quantum threshold cryptography*. The motivation for development of threshold cryptography is that a secret can be encrypted with multiple users and requires multiple users to decrypt. The quantum threshold cryptography is proposed by using idea of multiple bases. This can be considered as step forward towards multiparty quantum communication. This dissertation also proposed layered architecture for key distribution.

Concisely, this dissertation proposes the techniques like multicasting in quantum scenario, quantum threshold cryptography to achieve the goal of secured global communication.

Chapter 1: Introduction

Cryptography is only as strong as the weakest link –Bruce Schneier

Effective communication serves to inform, to motivate, establish control, and emotively express an individual's identity. As much as open communication plays an integral part in society, there is no denying that secrets have had an equally profound impact on history and human behavior. *Cryptology* is the science of secret writing. There are two parts of cryptology: first is cryptography that deals with communication security and the other is cryptanalysis that deals with breaking the cryptographic schemes.

This chapter discusses the evolution of cryptography, mathematical advancements in cryptography and concepts of quantum cryptography.

1.1 World of Cryptography

Cryptography has played an important role in the history of any society that depend on information [1]. The ingrained urge of human nature to discover secrets has led to attacks on the secret methods developed by scholars and making them un-operational. The ongoing battle between code makers and code breakers has truly inspired a whole series of remarkable scientific breakthroughs.

After looking at the history of cryptography, we see that the use of cryptography dates back to 2000 B.C., with non-standard, secret *hieroglyphics* was used in ancient Egypt and the *scytale* of Sparta were used in ancient Greece [2]. These techniques were very simple and easy to break with few trial and error methods. Julius Caesar introduced a cipher by a simple letter substitution method called as *Caesar Cipher*. In this method as long as shift key is secure, the data is secured [3]. In 1926, G.S.

Vernam published the idea of *one time pad,* where the secure key is used only once for a message [4]. One time pad was the first provably secure cipher. The basic idea behind it is to have each symbol of the plaintext added modulo alphabet size to another symbol of a random secret key. Together they form a cipher text that will undergo the exact same operation at the receiving end with the exact same symbol from the random key; now the cipher text is decrypted back into plaintext. Shannon showed that the security of information is guaranteed if the key it is encrypted with is as long as the message and never reused [5]. Various encryption techniques like the German Enigma machine and the Japanese Purple machine, secret telegram methods, and Morse code were developed for encryption during the period of World War I and II [6]. After World Wars, cryptography became more widespread and people in everyday life essentially used it. Furthermore, cryptography became a tool not only for encryption, but also for other tasks such as digital signatures and various forms of authentication. In 1977, IBM designed one of the most popular symmetric encryption algorithms used today; it is the Data Encryption Standard (DES). In 2001, the National Institutes of Standards and Technology chose Advance Encryption Standard (AES) as a successor to DES.

The mathematical approaches play a very important role in cryptographic techniques. Shannon quotes *"The problem of good cipher design is essentially one of finding difficult problems, subject to certain other conditions. We may construct our cipher in such a way that breaking it is equivalent to (or requires at some point in the process) the solution of some problems known to be laborious"*. One-way trapdoor functions, modular arithmetic are some of the examples that have shaped development of many currently used cryptographic protocols. There are two broad classes of cryptographic techniques: symmetric key cryptography where only single key is used for complete transaction and asymmetric key cryptography where a set of keys is used for encryption and decryption. Diffie and Hellman developed the concept of Public key cryptography. The crucial contribution of Diffie and Hellman's system was one-way functions or trap-door functions, which are simple to calculate in one direction. However while solving for the key, unless one knows certain key details, solving the key is challenging [7]. Rivest Shmair and Adleman introduced one of the most widely used public key cryptography namely, RSA [8]. Apart from the widespread Diffie Hellman, RSA, and El Gamal cryptographic systems, there are many modern mathematics-centered methods for securing data transfer. They include elliptic curve cryptography, lattice-based cryptography, and the NTRU cryptosystem, hash function-based digital signatures. The ongoing game of cat and mouse between cryptographers and cryptanalysts continuously generated a need for developing advanced techniques that provide perfect security. That realization led to leap in the field of quantum cryptography.

1.2 Quantum Cryptography

In 1970, Stephen Wiesner wrote a paper "Conjugate Coding," in which he explained how quantum physics can be used in principle to produce bank notes that would be impossible to forge [9]. Although the idea of quantum money proposed by Wiesner was impractical, the idea lead to series of experiments in the fiels of quantum cryptography. In quantum cryptography, security depends on two fundamental physical laws called as Heisenberg's uncertainty principle and no-cloning theorem [10].

Quantum information can be represented in the form of *a qubit* (short for quantum bit). *A quantum bit, or qubit, is a quantum system in which the classical Boolean states 0 and 1 are replaced by a pair of mutually orthogonal quantum states labeled by*$\{|0\rangle, |1\rangle\}$ [11]. Physically, a qubit corresponds typically to the two levels of some microscopic system such as a polarized photon, a trapped ion, a nuclear spin, etc. However, unlike the other classical quantities, qubit need not be in either the 0 or 1 state but can occupy both states at the same time. This characteristic is based on **superposition principle** of qubit [12].

Although currently information sent via quantum bits is unconditionally secure, there are practical limitations associated with transferring a qubit on a physical medium like an optical fiber, wireless, etc. The technologies necessary for transmission are still in the embryonic phase for quantum information processing. However to make use of the best available method, the following process can be followed: Rather than sending all the information on qubits, one can just send the essential "keys" for encrypting data. Several companies are focusing quantum key distribution (QKD) that protects data through this aspect of exchanging secret keys [13]. Charles H. Bennett of IBM and Gilles Brassard of the University of Montreal hence proposed the first protocol for quantum cryptography in 1984 the name BB84. A key distribution using QKD would be almost impossible to steal because QKD systems continually and randomly generate new private keys that the sender and the recipient share.

Foundation of QKD rests on Heisenberg's uncertainty principle. A standard laser can be modified to emit single photons, each with a particular orientation. Eavesdroppers in cryptography parlance can record the orientations with photon detectors, but doing so changes the orientation of some photons, thus alerting the sender and receiver of a compromised transmission and increasing bit error rate (BER) in the transmission. If the BER is sufficiently small, it can be assumed that information transferred is secure; and one can derive the right information with arbitrarily high precision. A high BER will likely indicate an intrusion, so the sender and receiver could discard those keys or bits and reinitiate the process of deriving the key. Two companies, MagiQ Technologies (New York, NY) and ID Quantique (Geneva, Switzerland) have released commercial QKD systems and are successful in accomplishing the first step toward quantum communication [14, 15].

"*The quantum communication is a combination of the quantum cryptography and modern communication techniques such as the optical communication, mobile communication, and Internet network techniques"* [16].

According to a paper entitled "Recent Development In Quantum Communication" by Song Si Yu and Wang Chuan [17], quantum communication offers more power than QKD. Quantum secret sharing (QSS) distributes secret keys to two or more shared users [18], which can be viewed as quantum key distribution between multi-users. Quantum teleportation is a basic ingredient in quantum information architectures [19]. The principle of quantum teleportation is to transfer an unknown state to the legal user at a distant distance. Quantum secure direct communication (QSDC) offers direct communication of secret messages between distant users, which eliminate the need for another classical communication as in the case with QKD

1.3 Aim and scope of the dissertation

The specific aim of this dissertation is to propose a composite system for quantum key distribution to secure global communication using multi-photon tolerant quantum cryptography protocols. There are three parts associated with proposed composite system: first is the network of satellites, second is the ground to air communication and third is the ground-to-ground communication. In this dissertation, we primarily focus on satellite network part and ground to air communication. For configuring the composite system, a logical layered architecture is proposed. This dissertation also proposes a quantum protocol suite to bring into attention the need of standardization in the field of quantum communication.

Quantum communication as of now is restricted for point-to-point communication. This dissertation proposes a multi-photon based threshold quantum cryptography where more than two parties are required to contribute to encrypt or decrypt a secret key. The idea of threshold cryptography is to protect information by distributing it among authenticated users. The scheme can be considered as a step towards multiparty to multiparty quantum cryptography. This dissertation also proposes a scheme based on wavelength division multiplexing for multi-photon tolerant protocol for multicasting over free space optics links. The proposed lab implementation setup is explained for the proof of concept of multicasting. The key management in case of multiparty is explained with the quantum thresholding protocol.

Thus, this dissertation explains aspects of a composite system for secured global communication.

1.4 Organization of the dissertation

This dissertation aims to establish multi-photon tolerant protocol based global quantum key distribution system. Chpater 1 begins with some background information about cryptography. Chapter 2 describes the research done in the fields of quantum cryptography. It starts with the description of BB84 protocol and its variants and practical challenges associated with implementing them. It further explains the multi-photon tolerant protocol like three-stage protocol. Chapter 3 explains braided single-stage protocol with its lab implementation details and error analysis related to implementation. It further describes the optical burst switched (OBS) network concepts and how braided single-stage protocol can be implemented on it. The aforementioned application in OBS takes care of the ground-to-ground communication part of the composite system. Chapter 4 aims at implementing the braided single-stage protocol for satellite to ground communication. It shows that the security can be applied to geostationary level of satellites. Chapter 5 explains the concept of multi-photon based threshold quantum cryptography scheme with possible application. Chapter 6 describes the global quantum key distribution system with layered architecture, multicasting, key management and overall information flow. Chapter 7 concludes this dissertation.

Chapter 2: Quantum Communications

Quantum communication is an art of transferring quantum state from one place to another. It is a filed of applied quantum physics closely related to quantum information processing and quantum teleportation. Its most interesting application is protecting information channel against eavesdropping by means of quantum cryptography. Before explaining the details of quantum key distribution protocols we understand an evaluation of the security schemes provided by the cryptographic techniques with following definitions [20].

i. *Provable security*: A cryptographic method is said to be provably secure (that is, proof is subject to assumption) if the struggle of cracking a code can be shown to be essentially as difficult as answering a well-known, very difficult problem.

ii. *Computational security*: A proposed security method is called as computationally secured if the amount of computational effort required to break the system security would require by a comfortable margin more computational resources than are available to the adversary.

iii. *Unconditional security:* The system approach to security is based on the supposition that even if the adversary possesses unlimited computational resources, the security of the system could not be broken by any means. This system is also called perfect security. To date, the one- time-pad technique is the only method considered to be included in this method.

Quantum cryptography has been proven unconditionally secured because it is invulnerable to attacks as it employs fundamental laws of physics like the uncertainty principle and the no-cloning theorem [21]. According to the principles of quantum mechanics, any type of attempt to measure photons will cause disturbances in their state. By detecting this disturbance, the presence of an adversary will be sensed on the channel. In other words, when information is encoded in non-orthogonal quantum states, one obtains a communication channel with a transmission that in principle cannot be copied or read by an eavesdropper.

This chapter addresses the most popular application of quantum cryptography, which is quantum key distribution. First we will understand BB84 protocol and its variants for QKD. The second section explains the challenges in the implementation of QKD protocols for quantum communication. Further the last section explains an approach for quantum secure communication using multiple photons.

2.1 Quantum Key Distribution

Quantum mechanics is the basis on which quantum key distribution protocols rely to transfer and share keys. In QKD, information is encoded into one degree of freedom of photons (e.g. polarization state), while the other degrees of freedom (phase, wavelength etc.) must contain no information[22]. The common entities used in the description of the protocols are: Alice, who is sender of keys; Bob, who is receiver; Eve is the intruder or eavesdropper. There are usually three phases for all QKD protocols namely raw key exchange, key sifting, and key distillation. The raw key exchange is the only quantum part of the overall process because it is the only stage at which quantum states are transmitted between Alice and Bob.

2.1.1 BB84

Theoretical physicists Charles Bennett (IBM) and Gilles Brassard (University of Montreal) proposed the first method of secure key transmission using quantum physics in

1984 [23]. Alice and Bob are connected by a quantum channel and classical public channel. The protocol uses four quantum states and two bases. In terms of polarization of light, the bases can be represented as either $|\rightarrow\rangle$ and $|\uparrow\rangle$ (or $|H\rangle$ and $|V\rangle$) for the horizontal/vertical (H/V or $+$) basis, and $|\nearrow\rangle$ and $|\nwarrow\rangle$ (or $|D\rangle$ and $|A\rangle$) for the diagonal/anti-diagonal (D/A or $\times$) basis. The procedure is as follow:

1. Alice chooses a random bit string and a random sequence of polarization bases for encoding the bits and sends the encoded qubits over the quantum channel to Bob.
2. As Bob receives the photons, he decides randomly, for each photon and independently of Alice, whether to measure using $+$ basis or $\times$ basis and interprets the result of the measurement as a binary 0 or 1.
3. A random answer is produced when one tries to measure horizontal polarization on diagonal photon and vice versa. Thus, Bob obtains useful data only from half of the photons on which Bob detects perfect polarization basis [24].
4. The key exchange stage is now completed. Now the key sifting stage will start. At this point, Alice and Bob discuss their bases. They will discard all the bits where different bases have been used. These steps come at high cost; almost 50% of the raw key bits are discarded in order to generate what we call a sifted key.
5. If the error level is higher than the security threshold previously agreed by both parties, Alice and Bob terminate the key agreement based on the assumption that "the quantum channel is eavesdropped," and the protocol is restarted [21].

Error correction and privacy amplification are then performed to distill the key and reduce the amount of information that Eve got by intercepting the channels. The following table shows the protocol steps with specific examples.

Legends used: D: × basis, R: + basis, = accepted positions

Quantum Transmission															
Alice's random bits	0	1	1	0	1	1	0	0	1	0	1	1	0	0	1
Random sending bases	D	R	D	R	R	R	R	R	D	D	R	D	D	D	R
Photons Alice sends	⤢	↕	⤡	↔	↕	↕	↔	↔	⤡	⤢	↕	⤡	⤢	⤢	↕
Random receiving base	R	D	D	R	R	D	D	R	D	R	D	D	D	D	R
Bits as received by Bob	1		1		1	0	0	0		1	1	1		0	1
Public Discussion															
Bob reports bases of received bits	R		D		R	D	D	R		R	D	D		D	R
Alice says which bases were correct			=		=			=				=		=	=
Presumably shared information			1		1			0				1		0	1
Bob reveals some key bits at random					1									0	
Alice confirms them					=							=			
Outcome															
Remaining shared secret bit			1					0				1			1

Table 1 Illustration of the BB84 protocol with specific example

At this moment, Alice and Bob possess identical strings, but those strings are not completely private. Eve may have gained some information about them either by beam splitting or through intercept/resend [25]. The procedures of reconciliation and privacy amplification are purely classical and were first introduced in 1992 by Bennett et al. *Privacy amplification is the art of distilling highly secret shared information, perhaps for use as a cryptographic key, from a larger body of shared information that is only partially secret* [26]. The aim behind PA is to diminish any information Eve has on the sifted key. According to Claude Shannon, the mutual information given by $I(A\colon B) = H(A) + H(B) - H(AB)$ is the fraction of perfectly correlated keys that can be extracted from the partially correlated sifted keys. The fraction of the key to be discarded is equal to min(I_{EB}, I_{EA}); I_E is Eve's information about the sifted key of Alice and Bob. I_{EB} *and* I_{EA} represents mutual information of Eve with Bob and Alice respectively. A PA procedure that works in a provable manner is based on two-universal hash functions. In summary, the extractable fraction of the key using one-way post processing is given by:

$$r = I(A\colon B) - \min(I_{EA}\ , I_{EB}).$$

Other forms of post-processing procedure exist, such as the two-way post- processing. In this type of post-processing both Alice and Bob can be senders and the bounds on the extractable fraction can be significantly improved [27-29].

2.1.2 Variants of BB84

After the successful experimental realization of the BB84 protocol [30], there were many variants that emerged. To name a few, decoy state protocol[31], SARG04 protocol[32]and B92 protocol [33].

E91 Protocol: This was proposed before implementation of BB84. The approach is different than BB84 because the Ekert scheme [34] uses entangled pairs of photons instead of single photons and Bell state measurement. The scheme relies on two properties of entanglement. First, the entangled states are perfectly correlated in the sense that if Alice and Bob both measure whether their particles have vertical or horizontal polarizations, they always get the same answer with 100% probability. Second, any attempt at eavesdropping by Eve destroys these correlations in a way that Alice and Bob can detect.

Decoy state protocol: In QKD protocols, it is difficult to generate single photon because perfect single-photon source does not exist. Instead, practical sources, such as weak coherent state laser source, are widely used for QKD. In Decoy state QKD, a few different photon intensities instead of one. The details are mentioned in chapter 4.

SARG04 protocol: It is provably better than BB84 against photon number splitting (PNS) attacks at zero error. If the pulse contains more than one photon, then Eve can split off the extra photons and transmit the remaining single photon to Bob. This is the basis of the PNS attack. It shows that by encoding a classical bit in sets of non-orthogonal qubit states, quantum cryptography can be made significantly more robust against PNS attacks. The protocol is identical to the BB84 protocol for all the manipulations at the quantum level and differs only in the classical sifting procedure.

2.2 Challenges to QKD

Despite the important theoretical and experimental achievements, a number of key challenges remain for QKD to be widely used for securing everyday interactions. Few of the major challenges for developing high performance and low cost QKD systems are discussed as follows.

2.2.1 Key rate and distance

Currently a strong disparity exists between current classical communication and QKD data rates. While classical systems are achieving the speeds of few Tbit/sec; quantum systems are able to reach only few Mbits/sec. This is because the key rate depends crucially on the performance of the detector used. Some of the photo detectors are avalanche photodiodes that operate above the breakdown voltage in Geiger mode. The maximum operating speed is in few ns [35]. Key rate increase is possible using wavelength or spatial mode multiplexing technologies that have been routinely used for increasing the bandwidth in data communications[36]. Extending the communication range of QKD systems is a major driving factor for technological developments in view of future network applications. The use of single photon detectors with low noise is the key in increasing distances of communication. In particular, the attainable distance range depends on the type and operation temperature of the detectors[37]. InGaAs avalanche photodiodes can tolerate losses of 30 and 52 dB when cooled to -30 and -120 °C. This loss is equivalent to 360 km of standard single mode fiber. Free space optics techniques work great for achieving more distances.

2.2.2 Cost and robustness

For QKD systems to be used in real world networks, the system needs to be robust and low cost along with highly efficient. Experiments like mentioned in [38, 39] show that QKD systems can co-exist within existing fiber architecture. The high cost is a result of the highly specialized single photon generators and detectors. Another important avenue to address the issue of cost and robustness is photonic integration. Chip-scale integration will bring high level of miniaturization, leading to compact and light- weight QKD modules that can be mass-manufactured at low cost.

2.2.3 Security aspects

Though quantum cryptography provides unconditional security *theoretically,* there are certain security challenges for practical implementations. These challenges arise due to imperfections of the devices used in QKD systems. For example, QKD always rely on detectors to measure the relevant quantum property of single photons. The paper [40] demonstrate experimentally that the detectors in two commercially available QKD systems can be fully remote-controlled using specially tailored bright illumination. Reference [41] studied the risk of **Trojan horse attacks** due to back reflections from commonly used optical components in QKD. The point-to-point communication nature of QKD restricts the potential growth and makes it more vulnerable to **denial of service attacks**. In such attacks if Eve is not able to obtain any key, she will simply cut the communication channel. The post processing in any quantum key distribution protocol is usually done over the public channel. In addition, there is the need to have strong authentication algorithms in order to prevent **the man-in-the-middle attack.** The attack using this kind of inconsistency between the theoretical protocol and its hardware implementation is usually called side channel attacks. Thus, for any practical cryptographic implementation scheme it is important to carefully design secure sources, detectors and observe side channels for any losses or eavesdropping.

2.3 Multi-photon approach for quantum secure communication

The security of quantum cryptography is based on the inherent uncertainty in quantum phenomena. It is the only known means of providing unconditionally secure communication other than one time pad. Most of the contemporary methods of quantum communication are BB84 based. However, as seen in the previous section there are some challenges for implementing QKD with single photons in practice. The multi-photon tolerant approach to quantum cryptography provides a quantum level security while using more than a single photon per transmission. A major advantage of this multi-photon approach is by allowing more than single photon per time slot, with the photons carry polarization-encoded information at high speed and over long distances [42]. For BB84 and its variants, qubits are transmitted only in one direction, and classical information is exchanged thereafter. With multi-photon tolerant protocols data can be sent over quantum channel without the need of post-processing over classical channel. The three-stage protocol, braided single-stage protocol, Yuen's Y-00 protocol are some of the examples for multi-photon approach. Y-00 protocol is different from QKD protocol in a manner that it is used as quantum stream cipher.

2.3.1 Three stage protocol

Dr. Kak proposed the three-stage protocol in 2006 [43]. In the BB84 protocol, each transmitted qubit is in one of four different states. In the proposed protocol, the transmitted qubit can be in any arbitrary state. A method of operation for the three-stage protocol is transferring state X from Alice to Bob via qubits. The state X is one of two orthogonal states such as $|0\rangle\, and\, |1\rangle\, or\, \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)\, and\, \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)\;\; or\;\; \alpha|0\rangle + \beta|1\rangle\, and\, \alpha|0\rangle - \beta|1\rangle$.

The orthogonal states of X represent 0 and 1 by prior mutual agreement of the parties, and this is the data, or the cryptographic key, being transmitted over the public channel. Alice and Bob apply secret transformations U_A and U_B that are commutative, i.e., $U_AU_B = U_BU_A$. An example of this is $U_A = R(\theta)$ and $U_B = R(\emptyset)$, each of which is the rotation operator

$$R(\theta) = \begin{bmatrix} cos\theta & -sin\theta \\ sin\theta & cos\theta \end{bmatrix}$$

Figure 1 illustrates the operation of the three-stage protocol. A step-wise procedure is as follows:

1. Alice applies transformation U_A on X and sends the qubit to Bob.

2. Bob applies U$_B$ on the received qubit U$_A$(X) and sends it back to Alice.
3. Alice applies inverse operation$U_A^\dagger$ on the received qubit, converting it to U$_B$(X) and forwards it to Bob.
4. Bob applies $U_B^\dagger$ on the received qubit, converting it to X.

At the end of the sequence, the state X, this was chosen by Alice and transmitted over a public channel, reaches Bob. In the above steps, one can observe that though the information is sent over a public channel, it is always encoded with some transform at each leg. Eve, the eavesdropper, cannot obtain any information by intercepting the transmitted qubits, although she could disrupt the exchange by forging the communication. (The security against PNS attack is explained in [44]

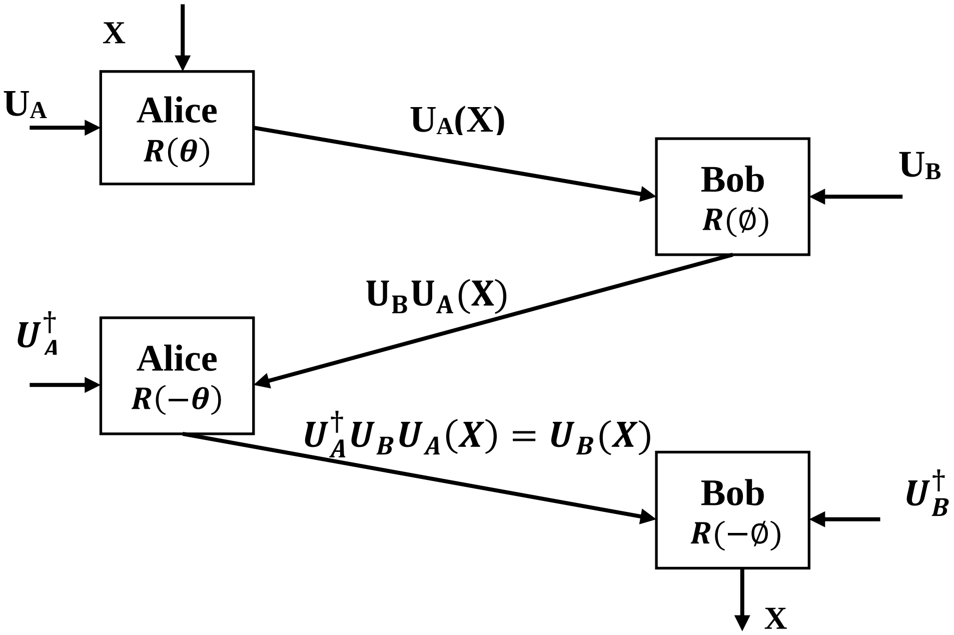

Figure 1 Operation of the three-stage protocol

Comparison of the three-stage protocol with BB84

In the BB84, the choice of polarization is limited to only four possible options as only two bases are used for encoding information on the qubit. In the three-stage protocol, there are numerous theoretical possibilities of using any of the unitary operators (e.g., Pauli matrices) because information related to operators need not be shared between sender and receiver.

2.3.2 Security aspect for multi-photon approach

The principle behind the multi-photon, multi-stage protocol is essentially the same as that of the classical double-lock cryptography. Security is given by the asymmetry in the detection strategies between the legitimate users and the eavesdropper, which is provided by the advantage creation akin to that utilized in the optimal quantum receiver in the Y00 (or αη) protocol[45] and the keyed communication in quantum noise (KCQ) method [46]. Paper [47] shows that the three-stage protocol is resilient to the photon number splitting attack, the intercept-resend attack, and the man-in-the-middle attack with the error probabilities calculated as functions of the mean number of photons in the channel. We can apply the principle to multi-photon tolerant protocols. The mean photon number of the coherent states can practically be larger than 1, in contrast to most current QKD protocols in which weak coherent pulses (mean photon number ~ 0.1 for BB84 to 0.6 for decoy-BB84) are considered.

2.4 Summary

This chapter describes the popular quantum key distribution protocols such as BB84 and the three-stage protocol. This chapter has described a detailed operation of BB84 protocol and how keys are transferred from one party to another. There are challenges associated with implementation of single photon based BB84 and its variants. These challenges are discussed in this chapter. Further, this chapter has explained the multi-photon tolerant approach for distributing keys of encryption. The detailed operation of the three-stage protocol is explained in this chapter. This chapter ends with security aspects of multi-photon tolerant protocol.

Chapter 3: The braided single-stage protocol

Bruce Schneier states that “Security is a chain: it is as strong as its weakest link” [48]. Cryptography is the success story of the information security world. If it is properly implemented, sensitive information can be transmitted securely in an insecure environment. A system failure might be due to poor key management or human failure rather than due to a cryptographic scheme failing. Considering this fact, quantum communication developments currently are dependent on practical implementations of the protocol as mentioned in previous chapter.

The three-stage protocol implemented using multi-photon tolerant approach offers many advantages over BB84 such as compatibility with existing network components. However, in the three-stage protocol, information travels over channel three times for single key or bit exchange. This leads to inefficient use of communication resources. To overcome this, braided single stage protocol was proposed [49]. This chapter explains the details of the protocol, implementation on free-space optics and advantages of the protocol considering current communication networks.

3.1 The braided single stage protocol

The braided single stage protocol includes key modifications to a single stage protocol that uses secret unitary transforms.

3.1.1 Secret unitary transforms

Unitary transformations are used to communicate information between Alice and Bob using single stage protocol. The primary idea of the protocols is to exchange key or data using rotational change in polarization. Alice and Bob can introduce any secret transformation that they are capable of generating that follows the commutative property, i.e., if U_A and U_B are Alice's and Bob's secret transformations, then,

$$U_A U_B = U_B U_A$$

for all values of U_A and U_B used for the communication. Also, the transforms when applied, should map into pure states of |0⟩ or |1⟩ with equal probability. These are basic properties on which the successful operation of the protocol relies. One of the examples of the secret transform is *a simple rotation operator* given by:

$$U_A = R(\theta) = \begin{bmatrix} cos\theta & -sin\theta \\ sin\theta & cos\theta \end{bmatrix} \text{ and } U_B = R(\phi) = \begin{bmatrix} cos\phi & -sin\phi \\ sin\phi & cos\phi \end{bmatrix}.$$

This simple rotation operator would change the plane of polarization through an angle of $\theta \; or \; \emptyset$; however, phase is not changed. We can understand this concept better with the help of Stokes' parameters [50]. Change in polarization due to simple rotation operator will affect only parameter S_1 and S_2. The Stokes' parameter S_3 will remain unchanged. The rotation operator satisfies the commutative property for any combination of $\theta \; and \; \emptyset$. The relevance of commutative operator can be understood through operation of the three-stage protocol. Another form of rotation operator which is also known as *a complex rotation operator,* is given by,

$$U_A(\theta) = \frac{1}{\sqrt{2}} \begin{bmatrix} e^{i\theta} & e^{-i\theta} \\ ie^{i\theta} & -ie^{-i\theta} \end{bmatrix}, \theta \epsilon [0,2\pi]$$

For this operator, Stokes' parameter S_1, S_2 and S_3 are changed and are considered during operation of the protocol.

3.1.2 The single stage protocol

Considering that the form of U_A (real valued or complex valued transform) is public information, and if Bob knows the value of θ used to generate U_A, then Bob has the complete knowledge of the transform by Alice. Comparing this situation with the three-stage protocol, it can be understood that Bob can forgo the subsequent two stages of the protocol and directly apply the transform $U_A^\dagger$ to obtain the unknown state X, as shown in Figure 2. So Bob will perform $U_A^\dagger U_A(X) = X$. If Eve intercepts the message, unless she knows value of θ, she cannot determine the information. The strength of this protocol depends on keeping value of θ secretly known to Alice and Bob.

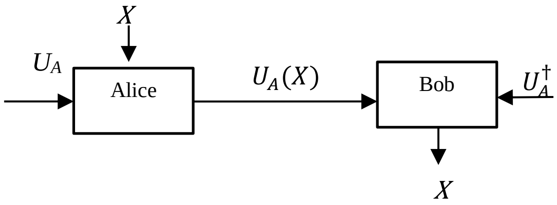

Figure 2 The single-stage protocol [51]

3.1.3 Concept of braiding

The security of this protocol is dependent on keeping the value of θ secret from everyone but Alice and Bob. One can use a secure way to communicate the initial value of θ secretly using a quantum protocol like the three-stage protocol by authenticating Alice. To enhance security of the single-stage protocol, the value of θ can be modified for the transmission of every bit. Thus, it is impossible for Eve to get the knowledge about data. The procedure can be illustrated as follows [52].

- To fulfill the precondition of sharing $\theta_{initial}$ by the secure method, the three-stage protocol is used for conveying the initial angle of transformation.
- Using the single-stage protocol $\theta_{initial}$ is used to transmit first k+n bits of information from Alice to Bob as shown in Figure 2.

- Upon mutual agreement, Alice and Bob use last n bits b$_{k+1}$ to b$_{k+n}$ from this transmission to generate a new encoding angle θ_{next} with the help mutually agreed algorithm which should include the current encoding angle θ. It is important to note that we are not transmitting extra bits in order to generate new angle. We are using some of the bits from the last transmission to generate a random angle for the next iteration.
- To do so, Alice and Bob convert last n bits to an integer value N using formula,

$$N = \sum_{i=k+1}^{k+n} b_i * 2^i$$

- Alice and Bob compute new encoding angle θ_{next} using N and previous angle θ such that,

$$U_A = \begin{bmatrix} \cos\theta_N & -\sin\theta_N \\ \sin\theta_N & \cos\theta_N \end{bmatrix} \text{ where, } \theta_N = \frac{N\pi}{2^k} + \theta_{initial}$$

The previous procedure can be repeated after a definite number of bits to calculate the new value of transform. The details about number of bits and transmission delay are given in error analysis. In this way, even if Eve attempts to attack the protocol, it would be very difficult for her to extract any information without prior knowledge of θ. The value of the new θ is derived from transmitted bits and $\theta_{initial}$; consequently, the original protocol suggested by James Thomas in [51], is renamed as *the braided single-stage protocol.* For enhancing security, mathematical one-way functions can be used. It is also suggested that the protocol can be started over, beginning with the three-stage protocol and followed by the single-stage protocol under the following conditions: a) Certain fixed amount of data is transmitted successfully, or b) the bit error rate increases suddenly because of interception of intruder. Framing of single stage protocol is shown in Figure 3.

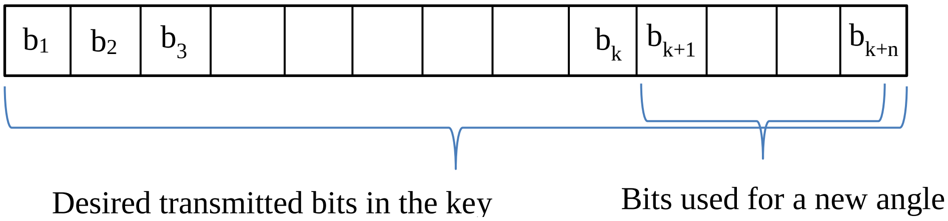
b1
b2
b3
bk
bk+1
bk+n
Desired transmitted bits in the key
Bits used for a new angle

Figure 3 Framing of bits

The braided single-stage protocol provides better security than the single-stage protocol because of interleaving of the angle of transformation and transmitted bits. Also, the new version is immune to known plaintext-cipher text attack on the single-stage protocol because of braiding concept.

The braided single-stage protocol implementation would require understanding of some of the basic of polarization of light because it is considered as one of the methods of encoding photons. Concepts like polarization of light, Stokes parameters are elaborated in the following section.

3.2 Implementation of the protocol

3.2.1 Basic of polarization

The optical field in free space is described in a Cartesian coordinate system by the three-dimensional wave equation

$$\nabla^2 E_i(r,t) = \frac{1}{c^2}\frac{\partial^2 E_i(r,t)}{\partial t^2} \qquad i = x, y \qquad (3.2.1)$$

where $\nabla^2$is the Laplacian operator, c is the velocity of light in free space, $\frac{\partial^2}{\partial t^2}$ is two-fold partial differential operator with respect to time t and *r=r(x,y,z) [53].*

Equation (3.2.1) represents two independent wave equations of two coplanar orthogonal components of light $E_x(r,t)\ and\ E_y(r,t)$. Both of these components are perpendicular to each other and travel in the direction perpendicular to the plane in which they exists. The vector nature of light as an electromagnetic wave is as shown in the Figure 4.

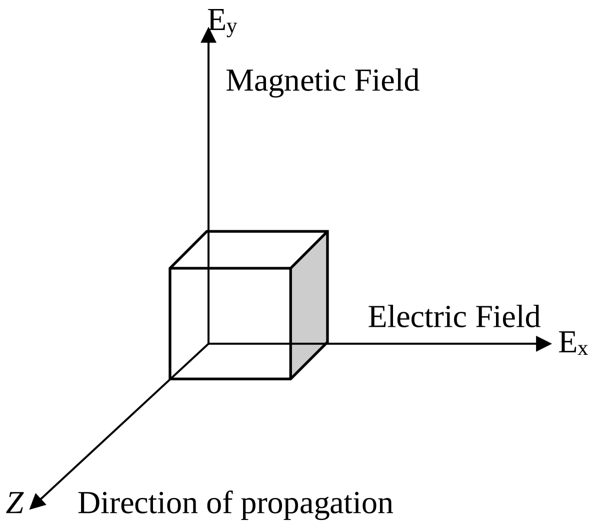

Figure 4: Relationship amongst field vectors and wave vector in electromagnetic vector [50]

Types of polarization

Light can be polarized or un-polarized. Natural light, for example, is un-polarized because instantaneous polarization fluctuates rapidly in a random manner. The projection of the electric field vector on the plane perpendicular to the traveled direction of the light describes the polarization state which can be linearly polarized, circularly polarized, or elliptically polarized [54]. Each of them can be used in optical communication depending on the application.

1. *Linear Polarization*: If the two orthogonal (perpendicular) components, $E_x\ and\ E_y$, are constant real valued and in phase, then the light is said to be *linearly polarized*. For the proposed implementation of the protocol, filtering a beam of light through polarizing filters uses linearly polarized light. Bit 0 or bit 1 is represented with the help of linear horizontal polarized and linear vertical polarized light respectively.
2. *Circular Polarization*: If the two orthogonal components, $E_x\ and\ E_y$, have exactly the same amplitude and are exactly or 90^o out of phase and one component is zero when the other component is at maximum or minimum amplitude then the light is called *circularly polarized*.
3. *Elliptical polarization*: If components $E_x\ and\ E_y$, are not in phase and either do not have the same amplitude or are out of phase, though their phase offset and their amplitude ratios are constant, the light is called *elliptically polarized*.

Stokes parameters

The Stokes parameters, was defined by George Gabriel Stokes in 1852 [55] as *a mathematically convenient alternative to the more common description of incoherent or partially polarized radiation in terms of its total intensity (I), (fractional) degree of polarization (p), and the shape parameters of the polarization ellipse*.

The relationship of the Stokes parameters to the intensity and polarization ellipse parameters is shown in the equations below and in Figure 5

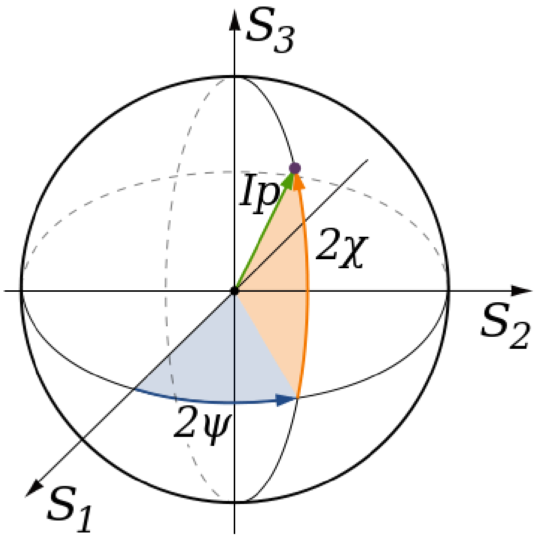

Figure 5: Stokes parameters representation [56]

Equations (3.3.2) and (3.3.3) leads to equation of polarization ellipse.

$$\frac{E_x^2(z,t)}{E_{0x}^2}+\frac{E_y^2(z,t)}{E_{0y}^2}-2\frac{E_x\ (z,t)E_y\ (z,t)}{E_{0x}E_{0y}}cos\delta = sin^2(\delta) \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots (3.3.1)$$

Applying the time average definition to the polarization ellipse then yields the following equation:

$$S_0^2 = S_1^2 + S_2^2 + S_3^2,$$

$$where\ S_0 = E_{0x}^2 + E_{0y}^2$$

$$S_1 = E_{0x}^2 - E_{0y}^2$$

$$S_2 = 2E_x\ (z,t)E_y\ (z,t)cos\delta$$

$$S_3 = 2E_{0x}E_{0y}sin\delta, \delta = \delta_y - \delta_x$$

The quantities S_0, S_1, S_2, S_3 are the observables of the polarized field. The first Stokes parameter S_0 describes the total intensity of the optical beam; the second parameter S_1 describes the preponderance of *linear horizontal polarized* (LHP) over *linear vertical polarized* (LVP) light; the third parameter S_2 describes the preponderance of L+45^{o} light over L-45° and finally, S_3 defines the preponderance of right circular polarized light over left circular polarized light.

Given the Stokes parameters, one can solve for the spherical coordinates with the following equations:

$$Intensity\ of\ polarized\ light(I) = S_0;$$

$$Degree\ of\ polarization(p) = \frac{\sqrt{S_1^2 + S_2^2 + S_3^2}}{S_0}\ where\ 0 \leq p \leq 1;$$

$$Angle\ of\ polarization\ (\Psi) = \frac{1}{2}\text{atan}\left(\frac{S_2}{S_1}\right)\ where\ 0 \leq \Psi \leq \pi$$

The Stoke vector: the four Stokes parameters can be aranged in a column matrix and written in the following form

$$\begin{bmatrix} S_0 \\ S_1 \\ S_2 \\ S_3 \end{bmatrix}$$

This representation is very useful while calculating effect of polarizing components on input beam of light and while using Mueller matrices and Jone's matrices.

3.2.2 Mode of operation

The first experimental implementation of the three-stage protocol using multiple photons was a setup over FSO [57]. The braided, single-stage protocol uses a similar setup for exchanging initial transformation angle. Concept of polarization modulation is used for encoding bits. Polarization of light for modulation can be chosen from three schemes, namely, circular polarization, linear polarization, and elliptical polarization. For the experiment, considering availability of the optical components, the linear polarizations were chosen, where 0 can be encoded as horizontal polarization and 1 can be encoded as vertical polarization. The complex transformation can be achieved through the rotations of the polarization state of the photons. .The signal processing and device control were implemented by the LabVIEW graphical programming. The overall mode of operation is as follows:

1. Alice decides the set of information to be transmitted. The data is converted in binary form through LabVIEW, and bits are encoded in horizontal polarization for 0 and vertical polarization for 1.
2. The beam of light is then passed through a beam splitter into two paths of same intensity. Using the assembly of mirrors and beam combiner, the path of beam is directed towards Alice's half wave plate.
3. Each beam is rotated through some angle θ by using half wave plates at Alice's end. On Bob's end, the received beam of light is passed through another half wave plate to inverse the transformation by Alice.
4. The light is again passed through a beam splitter and passed through polarizing filters at $0° \, or \, 90°$. This light is then detected to receive strings of 1s and 0s, which can later be converted to receive the original data or key.
5. Now, for generating a new angle of transformation θ, some of the bits from the existing bit strings are used. With help of mathematical operations, a new θ can be generated, which will be common and known to both Alice and Bob. It can be used for further communication.

Schematic for implementation

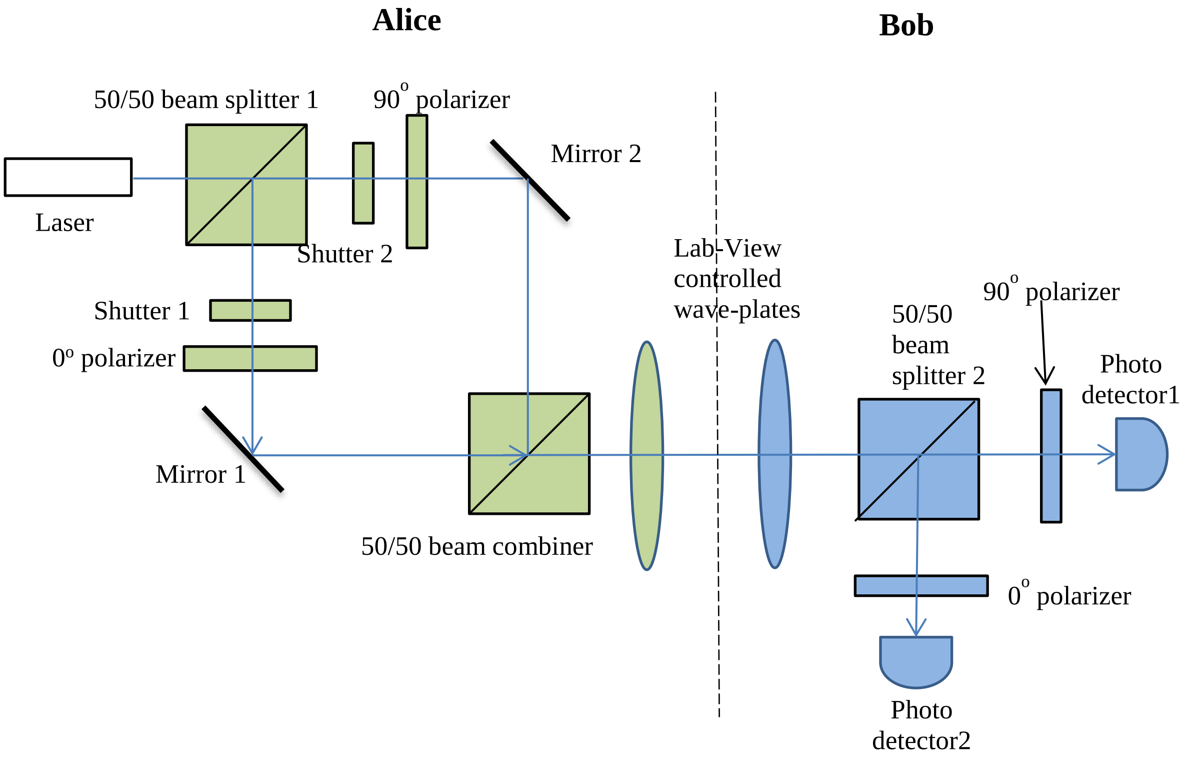

Figure 6: Schematic of operation for single-stage protocol

The schematic of operation for braided single-stage protocol is as shown in Figure 6. Hardware components used for the experimental setup are as follows:

- Beam combiner
- Beam splitter
- Laser source
- Light intensity detectors
- Mechanical beam shutters
- Motorized half wave-plates
- Plane reflecting mirrors

- Polarizing filters

LabVIEW 2010 was used for interfacing and implementing programming logic. Mechanical components like the beam shutters and motorized half wave-plates were also controlled through LabVIEW.

Hardware component description and specifications

Optical beam combiner: Optical beam combiner can combine two beams of light and operate exactly inverse as of beam splitter.

Laser: The light source is a HeNe, linearly polarized *laser* with a power higher than 0.8mW, a wavelength of 632.8nm, and an extinction ratio of 500:1. The beam of light emerging from the laser is linear polarized with random polarization.

Optical beam splitter: An optical beam splitter is a device that can split a beam of light in two different beams. In the implementation, an optical non-polarizing 50:50 cube beamsplitter from Thorlabs was used. Specified region of operation is from 400nm-700nm.

Mechanical beam shutters: An optical beam shutter is used to block the light coming from laser. The shutters help to avoid turning ON-OFF for the laser source at high speeds. The SH1 beam shutter, operating at a sustained maximum rate of 25 Hz with a minimum on time of 10 ms, utilizes a rotary, electro-mechanical actuator to provide millisecond shutter operation [58]. In general operation shutter remain closed for normal conditions and opens only when a control command is received. The assembly for beam shutters is controlled by a T-cube shutter controller, which is controlled by LabVIEW software.

Polarizing filters: A polarizing element that changes orthogonal amplitudes unequally is called a polarizer and is an anisotropic attenuator. In this experiment, polarizers are used for filtering beam to pass 0^o or 90^o polarized beam of light depending on input bit 0 or 1.

Motor controlled half wave plates: A polarizing element that introduces a *phase shift* between the orthogonal components is called *a wave plate*. A *half wave plate* essentially changes phase shift between two orthogonal components of light by phase π [56].

In the experimental set up, two of the wave-plates are mounted on automated mechanical rotators driven by APT motors from ThorLabs. The motors are controlled via LabVIEW to change the angle of polarization.

Light intensity detectors: The photo detectors converting light energy into voltage. Photo detectors from Teachspin responsive in spectral range of 400 - 1,000 nm are used in the set-up. The results in the form voltage can be displayed in Lab-View.

3.3 Error analysis

Data speed and channel utilization

In the implementation of the braided single-stage protocol, we measured the time delay involved due to the mechanical shutters and rotating half wave-plates. It was observed that the time required for the shutter to send single bit is approximately 1.56sec. The half wave plates take 20.7sec for rotating from their initial position for providing encryption. In the proof-of-principle experiment, we changed the encryption angle after each character and the total time required for sending single bit was 4.5 sec.

In the operation of the braided single-stage protocol, we can change the angle of encryption for every single bit or character to obtain the unconditional security. However, due to mechanical components involved in the lab setup, the time required to send single-bit will be limited by the time required for rotating the half wave-plates. Also, if we change encryption angle after a few hundred bits, the data rate is limited by speed of shutter operation. Figure 7 shows if we change the angle of encryption rapidly, the time required for operation of the protocol is very high as compared to changing encryption angle less frequent.

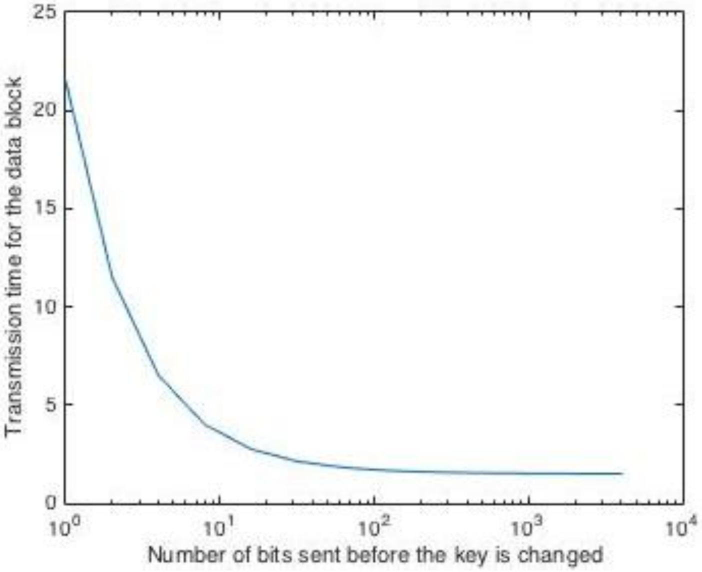

Figure 7 In the given experimental set up transmission delay increases for small blocks of data

For improving the data transfer rate, we can use a device capable of making rapid changes in polarization. We can use technique of multi-level encoding [59] for increasing data rate.

Error analysis

The purpose of error analysis is to understand the sensitivity of the devices in the experiment and to improve the accuracy in measurement. For the implementation of the braided single-stage protocol we have analyzed how the misalignments of the optical components plays a role in the accurate operation of the protocol by checking the bit error rate.

In the given experimental setup, we used motorized half wave plates for encrypting the data sent by the laser. A bit error-free operation of the protocol occurs when the polarization axes of both the half wave-plates are fully aligned. Transmission errors occur in case of misalignment. We first investigate the impact of this misalignment from a theoretical perspective.

Figure 8 represents a schematic of the system. The incident light beam characterized by its Stokes parameters is shown on the left. The light is modulated with Alice and Bob’s half wave plates to obtain output polarization.

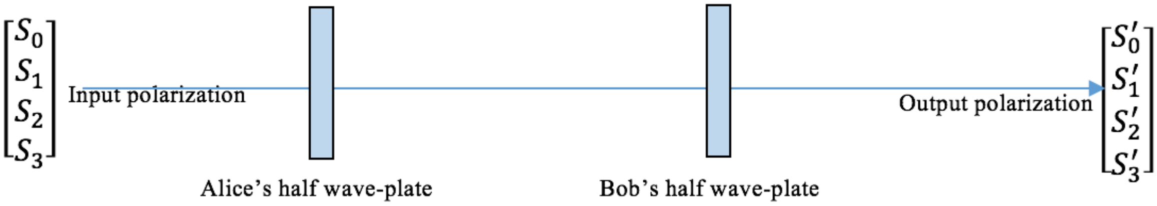
$\begin{bmatrix} S_0 \\ S_1 \\ S_2 \\ S_3 \end{bmatrix}$
Input polarization
Alice’s half wave-plate
Bob’s half wave-plate
Output polarization
$\begin{bmatrix} S_0' \\ S_1' \\ S_2' \\ S_3' \end{bmatrix}$

Figure 8: Study of misalignment between Alice's and Bob's half waveplate

When light passes through two half wave-plates, there is a change in intensity according to the changes in polarization. The Stokes parameters are mathematically convenient alternatives to more common description of the polarized radiation in terms of total intensity [50]. The Mueller matrix can help us analyze the output Stokes parameters of light when it passes through a polarizing device. The effect on light beam in the implementation is simulated using MATLAB. We keep Alice’s half wave plate aligned at

0 and Bob's half wave plate is rotated through an angle θ. It will represent the misalignment between two half wave plates.

$Alice's\ halfwave\ plate\ is\ characterized\ by\ its\ Mueller\ matrix$;

$$M1 = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & -1 & 0 \\ 0 & 0 & 0 & -1 \end{bmatrix} \tag{11}$$

$M2\ is\ Mueller\ matrix\ of\ Bob's\ half\ waveplate$;

$$M2 = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & \cos(2\theta) & \sin(2\theta) & 0 \\ 0 & -\sin(2\theta) & \cos(2\theta) & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix} \tag{12}$$

$Input\ polarization\ state, S_{input} = \begin{bmatrix} S_0 \\ S_1 \\ S_2 \\ S_3 \end{bmatrix}$ then,

$Output\ polarization\ state, S_{output} = \begin{bmatrix} S_0' \\ S_1' \\ S_2' \\ S_3' \end{bmatrix}$; is given by

$$S_{output} = M2 * M1 * S_{input} \tag{13}$$

The angle of polarization of light (α) after passing through the polarizing device is given by

$$\alpha = \frac{1}{2} tan^{-1}(\frac{s_2'}{s_1'}) \qquad (14)$$

where, $s_1' and\ s_2'$ are the Stokes parameters of the output light. . Since the output Stokes parameter are dependent on the misalignment angle θ, the angle of the polarization of light (α) is varied according to the misalignment θ. According to Malus's law, the intensity of polarized light is directly proportional to the square of the cosine of the angle between the input polarization state and the fast axis of the polarizing medium. In other words,

$$I_{output} = I_{input} * cos^2(\alpha) \qquad (5)$$

In Figure 9, first plot shows variation in angle of polarization with misalignment θ while second plot shows variation in the intensity with misalignment θ

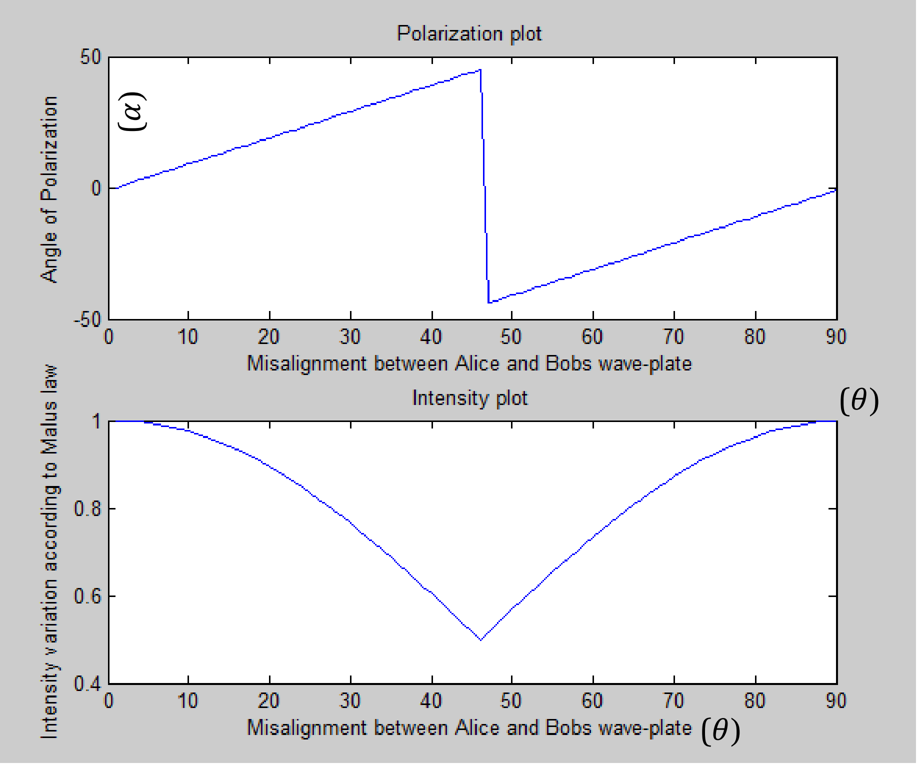

Figure 9 With increse in misalignment between Alice and Bob's waveplates, the intensity of light is minimum at 45º of misalignment

From the intensity plot shown in Figure 9 the following observations are made:

- The plot is symmetric with the high intensity from 0° to 10° and 80° to 90° and lowest at $45°$
- For 0° to 10° and 80° to 90° of misalignment, we observe that the intensity is close to 95% of the total intensity of light. Hence we can expect accurate determination of bit 0 or 1 at the detectors.
- When the misalignment of the wave plates is in between range 10^{o} to 40^{o}, the intensity of the light decreases rapidly.
- At $45°$ of misalignment, the intensity of light drops to a level less than 50% of the intensity of the incident light. This will decrease the amount of light received by the detectors. This will make it difficult to distinguish the bit 0 from bit 1.

During the correct alignment of the component, we observe error-free operation. The practical experiment is conducted as follows: Alice's wave-plate is kept at 0^{o} position and Bob's wave-plate is rotated in steps of 5^{o} to observe the impact caused by angular displacement of Bob's wave-plate on decoding. This procedure is repeated from 0^{o} to 90^{o} in steps of 5^{o} and a graph of bit error rate versus the degree of misalignment is plotted. The bit error rate (BER) is calculated using the formula,

$$\mathrm{BER} = \frac{\text{Number of erroneous bits recieved}}{\text{Total number of bits received}}$$

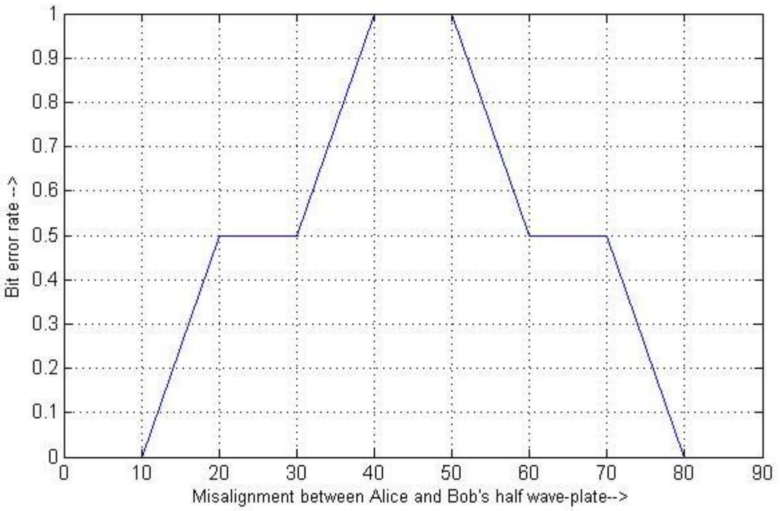

Figure 10 Impact of misalignment of half wave-plates on bit error rate

Observations from the graph are as follows:

1. The graph is symmetric about the angle of 45°. For the range of misalignment 0° to 10° and 80° to 90°, we observe error free operation. This is justified with the help of the intensity curve in Figure 9.
2. We observe a rapid increase in BER with misalignment 10^{o} to 40^{o}. BER reaches 50% which means Bob is not receiving correct information bits at all.
3. For a range of misalignment from 40° to 50°, we get 100% BER which can result in error free data recovery by inverting each received bit.

The experimental plot does not show a smooth curve as in case of theoretical approach because of the quantization errors of the detectors used in the experiment.

From the experimental results and theoretical studies, we conclude that in lab conditions, for error free operation of the braided single stage protocol over FSO, the misalignment of the half wave plates affects intensity which in turn affects BER. Hence for improving accuracy in measurement and sensitivity in performance, the intensity at the receiver should always be more than 95% of the total intensity. In case of practical real world implementation to maintain a BER with industry standards, the intensity of the light will definitely play a significant role as stated from above experimental results.

3.4 Application for optical burst switching networks

Basics of optical burst switching (OBS)

The rapid expansion of the Internet, evolution of smart phones and tremendous increase in demand of multimedia data are continuously testing the limits of existing telecommunication backbone technologies. The benefits of optical networking have been known for a while now; however, for current optical networks, the speed is limited to electronic router capacities due to optical-electrical-optical (O-E-O) conversions [60]. Optical burst switched network has emerged as a hybrid between optical packet switched networks (all-optical networks) and optical circuit switched networks (existing network technology) [61]. An OBS network consists of optical burst switching nodes interconnected with fiber links. The development of OBS technology lies in the successful design and implementation of the core architecture. In an OBS network, a data burst consisting of all IP packets is switched through all optical networks. There are two approaches doing this: one is distributed with link-based reservations, and the other is centralized with end-to-end reservations [62]. In both approaches, data and control signals within the core of the OBS architecture are separated as shown in Figure 11. It uses out-of-band signaling for a separate control network with a dedicated wavelength [63]. That means a control packet is transmitted ahead of the burst to configure the switches along the burst’s route and to set up the light-path for data transmission.

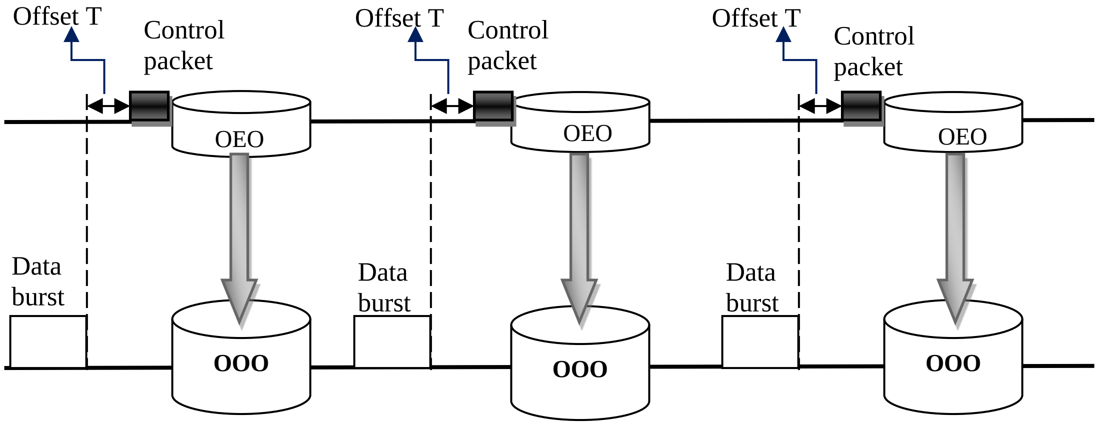

Figure 11 Separated transmissions of data and control signal

OBS architecture needs some fundamental research in the field of network security. The generation and distribution of the keys, authentication techniques for the burst headers, and data confidentiality methods for data burst are few of the research areas. Embedded secure framework using strengths of both classical cryptography and quantum cryptography is proposed in [64].

Quantum cryptography for OBS networks

Considering the real-world application of quantum key distribution protocols, three-stage protocol and single-stage protocol are best suited for OBS networks. The reasons is that both are invulnerable to photon siphoning attacks, both use multi-photon sources like lasers that are easily available and data can be sent over longer distances than BB84 due to multi-photon polarization modulation techniques. As mentioned earlier, the data bursts pass through all-optical paths. OBS preserves photonic modality of information within its domain. Additionally with the help of optical passivity within the

OBS boundary, quantum data can be sent on a proposed *Q-channel* created between two edge nodes. It is possible to preserve end-to-end polarization of photons over this *Q-channel* [65].

A subsystem developed to implement quantum key distribution over OBS network

A *Q-channel* is proposed for carrying all quantum key information. An optical switch can be used for switching between a classical channel, which will carry encrypted data, and a quantum channel, which will carry keys for encryption. The proposed setup is illustrated in Figure 12.

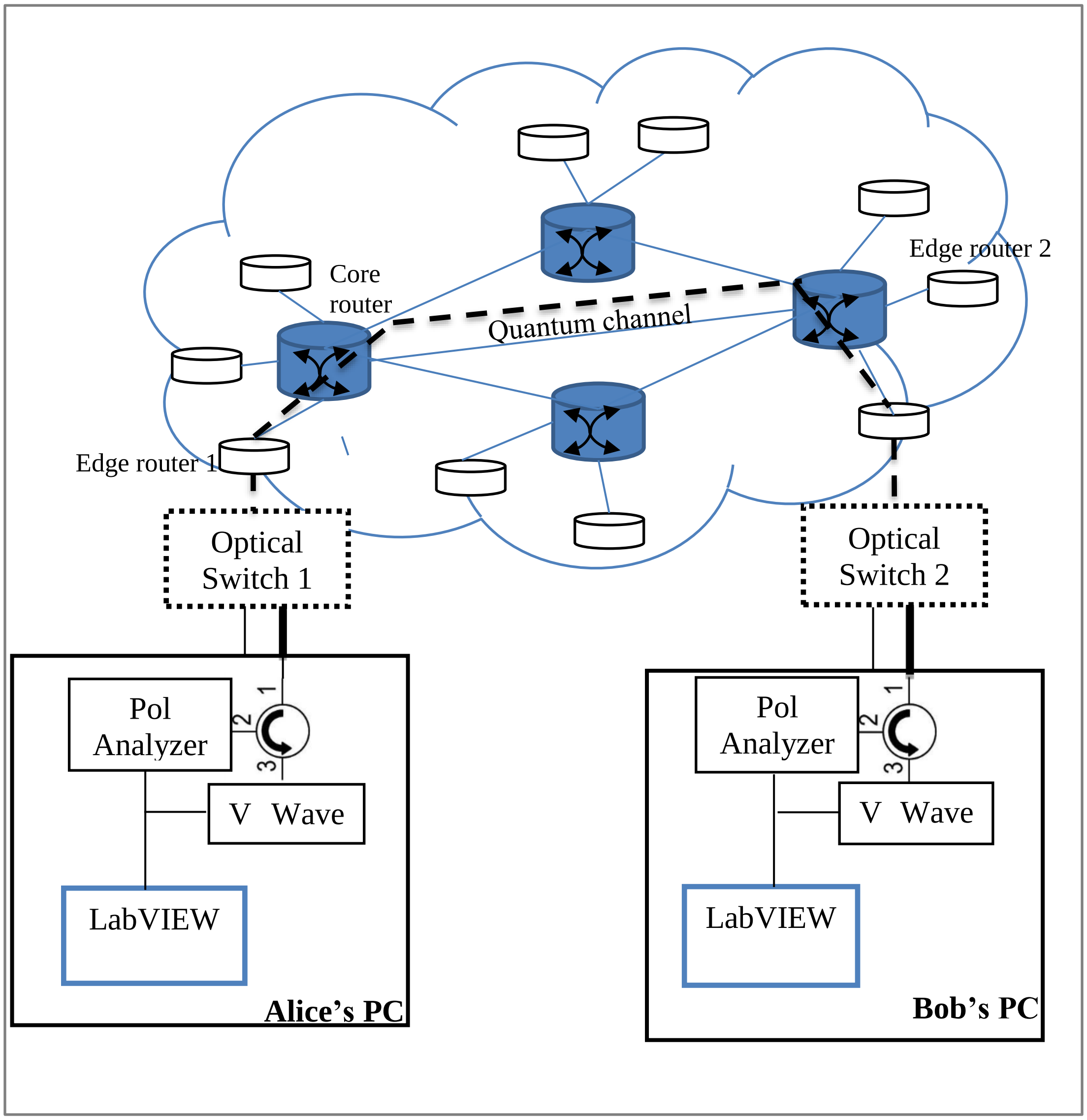

Figure 12 Subsystem proposed for quantum key distribution

In Figure 12, V Waves represent Versawave devices. It is a device design to change the polarization in fiber. It acts as a half wave plate. Alice PC and Bob PC are the black boxes considered to be totally secured. Bold channels between optical switches and PCs represent a quantum channel, whereas the other link represents a classical channel. The aim of this system is to exchange keys between Alice and Bob, where Alice initiates a communication. A circulator is used to direct the flow of photons from the edge router to the polarization analyzer to identify the *state of polarization* (SOP) of the incoming photons, followed by the Versawave device to generate newly calculated SOP and send it to the router through port 3 and onto port 1 of the circulator. This enables a seamless operation of the protocol. The general procedure can be stated as follows:

1. The edge router acting as Alice initiates a communication request with another edge router acting as Bob through a classical channel. In this step, Alice authenticates Bob and gets ready for key exchange.
2. An optical switch is used to switch between a quantum channel and a classical channel. For default condition of a switch (i.e. OFF condition), classical channel is active. When the optical switch is turned ON, the quantum channel gets connected between the two edge routers
3. Next, the switch position is changed, and the quantum channel is connected to the edge router at both ends. Alice and Bob send known states of polarization one after the other to characterize the channel, *e.g.* Alice sends a horizontal polarization (0°) for some time, and Bob receives, say, δ_b° polarization. Similarly Bob sends a horizontal polarization, and Alice receives δ_a° polarization state. Ideally, δ_b°= δ_a°. This change in angle of polarization of beam of light can be compensated while sending a particular angle. This procedure is called as a polarization compensation procedure.
4. Now that Alice and Bob have authenticated each other as well as found out the compensation angle for the channel, Alice will start sending the key.

5. Upon mutual agreement between Alice and Bob to represent bit ‘0’ as 0° SOP and bit ‘1’ as 90° SOP, Alice will compute $90°+x_a°+\delta_a°$, where $x_a°$ is Alice’s encoding angle. (In this case, the assumption is that Alice wants to send bit ‘1’.)

6. $\delta_a°$ angle will be nullified over the channel, and Bob will receive $90°+x_a°$ to which he will add $x_b°$, which is his encoding angle, and sends $90°+x_a° + x_b° + \delta_b°$ to Alice.

7. $\delta_b°$ angle will be nullified over the channel, and Alice will receive $90°+x_a° + x_b°$ to which she will subtract $x_a°$ and will send $90° + x_b° + \delta_a°$ to Bob.

8. $\delta_a°$ angle will be nullified over the channel, and Bob will receive $90°+x_b°$ from which Bob will subtract $x_b°$ to get 90° angle, which was sent by Alice, representing bit ‘1’.

9. This procedure is carried out until the required number of bits in the key is exchanged between Alice and Bob.

10. Now, using the bits transferred during this key exchange, a new angle of transformation (x_{new}) is generated and this is known to both Alice and Bob. In this case, Alice can send $90°+x_{new}°+\delta_a°$ and since Bob will already know value of new transform say, $x_{\text{new}},$ he will just subtract that angle to obtain the information bit i.e. 0 or 1.

11. When the key exchange procedure is completed, using an optical switch, both Alice and Bob will switch to a classical channel (default condition) and will start encoding data using the key exchanged using one of the agreed methods of encryption.

3.5 Summary

This chapter presents the concept and implementation of the braided single stage protocol. There are three section of this chapter first explains the theory, second explains the implementation details with error analysis and the third part provides the detailed application over optical burst switched network. The proof of concepts has been validated with lab implementation using passive optical components. The error analysis is based on the implementation might provide useful information for future design ideas. The detailed application over OBS network helps to realize the real world scenarios of the protocol for ground segment of the proposed global communication.

Chapter 4: Multi-photon approach for satellite communication

Communication today has become an intimate part of our personal, social, business and professional lives. With increasing dependency of the world's economy on information, it becomes crucially important to secure the communication. When it comes to secure communication, quantum cryptography is the only known solution that provides unconditional security [66]. Considering the global access of information, the satellite network has progressed a lot in recent years. The satellite technology has brought a revolutionary change in the field of communication with conveying information at faster data rate over long distances. With state-of-the-art RF links proving inefficient to travel inter-planetary distances, Free Space Optics (FSO) is emerging as a giant leap forward in space communication [67]. Experimental quantum cryptography is mainly divided into two categories: free space optics (FSO) and fiber optics [68]. Due to propagation losses along optical fibers, quantum key distribution over fibers can only reach a few hundreds of kilometers [69]. It appears prudent to utilize satellite technology to increase the distance of quantum communication using FSO. In this chapter we will see some of the experiments done for applying quantum cryptographic techniques for satellite communications serving dual purpose of securing satellite communications as well as transferring quantum keys over longer distances.

4.1 Overview of use of FSO in satellite communication

The ever increasing demand for carrying larger volumes of data over satellite links are pushing the demand for using higher electromagnetic frequencies bands (S, X and Ka) [67]. Through its inherently narrow beam-width and high carrier frequencies, optical technology shows much promise in the quest to increase data rates. Ever since the discovery of lasers, the use of optical frequencies for communication has been pursued.

4.1.1 Advantages of lasers over microwaves

The following subsection states the advantages of laser over traditional RF techniques emphasizing the higher bandwidth, narrower beamwidth, and smaller equipment size and weight.

Narrow beamwidth: The maximum narrowness of the laser beam is achieved with diffraction limited optics, providing a beam-width of $\theta = 2.24 * \frac{\lambda}{D}$;

where $\lambda =$ wavelength of laser transmission and D= diameter of aperture of transmitting telescope. Comparing the laser beam-width (e.g. $\lambda = 1.0\, micron\ with\ D = 10cm\ yields\ \theta = 22.4\, \mu\, rad$) with that of RF signal at 10GHz ($\lambda = 3\, cm\ with\ D = 1\, m$), the beamwidth will be $\theta = 67.2\, m\, rad$. Lesser beamwidth ensures maintenance of privacy to the intended callee’s platform.

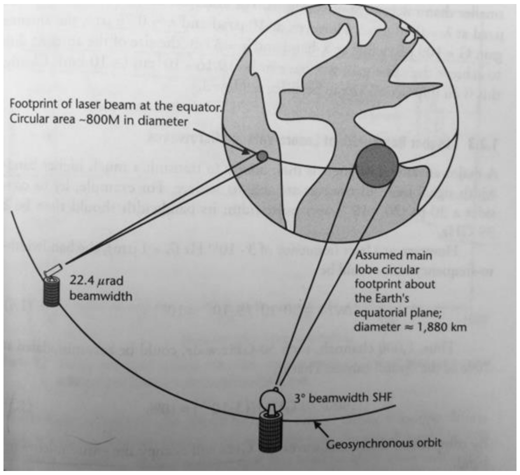
Footprint of laser beam at the equator.
Circular area ~800M in diameter
22.4 μrad beamwidth
Assumed main lobe circular footprint about the Earth's equatorial plane; diameter ≈ 1,880 km
3° beamwidth SHF
Geosynchronous orbit

Figure 13: Privacy comparison between microwaves versus laser footprints [70]

Large directivity: Because of very short wavelength (0.48-0.78μm) for FSO, very high directivity is attainable with small-aperture telescopes. As the beam is narrower for lasers, power efficiency is observed for long distances.

Higher bandwidth: Lasers are able to transmit a much higher bandwidth signal than microwaves. The channel bandwidth must be consistent with the carrier frequency for accurate signal detection.

Privacy comparison: An indication of the privacy comparison is shown in Figure 13. It shows that the field of view on the ground for optical signal is lesser than that of RF signal. For optical signal, one must be quite close to the center of the beam to be able to listen without requiring a sensitive receiver. For the case of the microwave signal of 35GHz, the signal could easily be picked up at roughly less than 40miles [70]. For mobile ground stations, a combined system with laser and microwaves proves to be beneficial.

4.1.2 Optical communication links

Besides the standard links from Low Earth orbit (LEO), Geosynchronous Earth orbit (GEO), and deep-space spacecraft to ground, multi Gigabit links between LEO and GEO spacecraft, earth observation and communications spacecraft are also required. Fig. 2 shows several possible point-to-point optical links from Earth to space [71].

Near-Earth Links: They include lower Earth orbit (LEO, Geocentric orbits ranging in altitude from 160 km (100 miles) to 2,000 km (1,200 mi) above mean sea level), medium-Earth orbit (MEO, orbits with altitudes at apogee ranging between 2,000 km (1,200 mi) and that of the geosynchronous orbit at 35,786 km (22,236 mi), geo-stationary orbit, GEO. The ground telescopes with approximately, 1-2m diameter are needed to receive data at high-rates [72]. Near-earth links such as LEO and MEO have proven to be suitable for building a satellite interconnection network to reach from one point to another point on the Earth [73].

Deep-space links: Optical links from “deep-space” that extend from the Sun-Earth Lagrange points [74] to planetary distances. The increased distances in deep-space communication causes new link considerations such as higher power lasers and larger diameter transmitting optics, larger effective diameter for collecting; and implementing signaling and detection scheme to capture faint laser pulses [75].

Space-to-space: Inter-satellite or space-to-space links are at an advantage due to their non-vulnerability to weather or cloud outages. Using various advanced lasers, link capacity can be increased and as stated in [76], LEO-LEO links can go up to 5.6 Gb/s. For establishing space-to-space satellite links, there needs to be an orbiting receiver. However, the cost of maintaining such orbiting receivers is very high. Furthermore, orbiting assets may have single point of failure.

4.1.3 Weather and clouds effects

For free space optics, atmospheric turbulences and attenuations are the major sources of increasing BER. In satellite communication networks, ground-to-space links are affected the most for both uplinks and downlinks due to weather conditions and cloud blockage. Various strategies are developed to ameliorate the signal loss and distortion problems. One of the scheme relies on a global network of ground based receivers that, due to weather diversity, will ensure the ability to deliver data back to the Earth [77].

4.2 Current QKD methods for satellite communication

In this section we will review some of the QKD based experiments carried out for satellite communications. The BB’84 protocol is implemented in practice using single photons, decoy state method and phase encoding methods. Other than the BB’84 protocol, entanglement is widely used for QKD [78]. Satellite aided QKD using entanglement and decoy state is explained further.

4.2.1 Using entangled photons

The use of satellite for distributing entangled photons provides unique solution to the problem of distance in global QKD [78]. One can share quantum keys over free space optics medium and use traditional RF or free space channel for actual transmission of data. Thus, this set up involves two separate channels between ground station and transceiver. There can be three cases to allow distribution of entangled photons: a satellite is used to carry either i) a transmitter, or ii) a receiver or, iii) a relay station. These scenarios permit different applications as shown in Figure 14.

Earth-based Transmitter terminal: The entanglement can be shared between a transmitter and a receiver in air, or with a receiver on ground via relay, or between two or more ground stations via relay. It is possible to develop a global QKD network with possible applications like QKD or entanglement-enhanced communication protocols [79].

Space-Based Transmitter Terminal: This method allows less influence to atmospheric turbulence as compared previous one [78]. Only the use of entangled states sent to two separate ground stations allows instantaneous key exchange between two communicating Earth-bound parties.

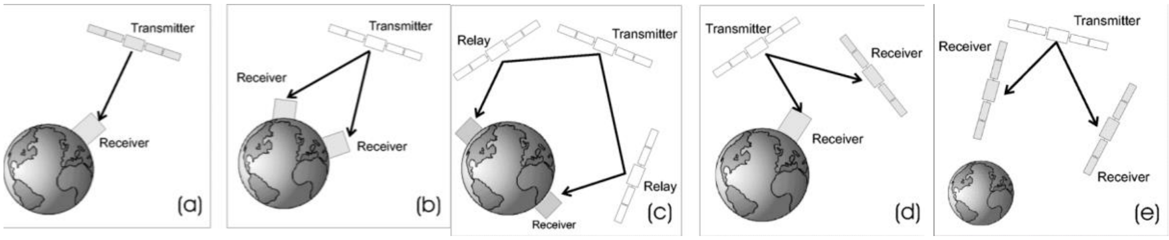

Figure 14: Scenarios for quantum communication with a space based transmitter terminal

Procedure for entanglement sharing: The experimental steps needs to be followed are as follows: Step I: Creation and detection of qubits, Step II: Establishment of the entanglement, Step III: Bell-state analysis for of independent qubits. The important consideration factors are link attenuation and experimental flexibility. The total link attenuation should not exceed 60dB. Hence, entanglement can be sent over LEO but it is very difficult to share entanglement using GEO satellite due to higher loss and attenuation. The speed of transmission of data is limited due to methods of preparation and detection of entangled photons.

4.2.2 Implementing BB'84 protocol

Using Decoy state: Experimentally, for implementing QKD, single photon sources are developed from faint laser pulses, which may have more than one photon per pulse. To overcome the Photon Number Splitting attack (PNS) for BB84 protocol in the presence of high loss, decoy-state method was proposed in 2003 [31]. This method proved useful for improving distances for QKD. The key point for decoy state idea is that Alice prepares a set of additional states, i.e. decoy states along with the standard BB'84 states. These decoy states are meant for frustrating Eve and detect presence of Eve on communication channel. If Eve tries to attack with photon number splitting method, it is easily captured with the help of decoy state. The only difference between standard states and decoy state is their intensities [80]. Experimental demonstration of free-space decoy-state quantum key distribution over 144km is explained in [81]. Use of decoy state enabled to distribute a secure key at a rate 12.8 bit/s at an attenuation of about 35dB. This experiment utilizes simple transmitter setup and an optical ground station capable of tracking a spacecraft in low earth orbit.

Using single-photons: Another experiment based on the exchange of single-photons between a LEO transmitter (at a perigee height of 1458km) and ground station is reported in [82]. The systems used are devised for geodynamical monitoring by means of an optical pulse from a station on the Earth and the retro reflectors on the satellite. This is called as satellite laser ranging (SLR). According to the link budget analysis presented in [82], about $1.2 * 10^5$photons are sent and only 0.4 photons are directed in the channel. This experiment demonstrates the feasibility of existence of quantum channel.

4.2.3 Technological challenges for entangled or single photon approach

Various experiments reported in [78], [83], [81], [82] demonstrates the feasibility of global QKD with the help of satellites. These experiments are however, face certain practical limitations such as use of two separate communication channel, compatibility with the state-of-the-art technology used for satellite communication, speed and distance limitations due to use of single photons, etc. According to the concept of QKD, only keys are exchanged using satellite rest of the secure communication must take place over another satellite communication channel, which in turn means more resource utilization for secure communication. This can be considered as a major disadvantage since the resources in space communication are very limited. For QKD, popular wavelength used is 800nm because the best single-photon detectors exist at 800nm [83]. However, the most widely used wavelength in telecom equipment is 1550nm. Thus we can see that problem of compatibility arises due to the use of single photons. Furthermore, rate of information transfer is limited by maximal number of photons or entangled pairs generated or detected. Typical standard repetition rate for pulsed laser (used in generating entangled photons) are of the order of $10^6 - 10^7\ s^{-1}$, and detector system have a maximal detection rate of few MHz [78]. Number of photons limits the distances of QKD to LEO and, under certain circumstances to MEO. However, GEO communication is not possible with single or decoy state methods [84]. Table 2 shows the distances covered for the BB'84 protocol using a single photon and a decoy state approach.

Scenarios	**BB'84 single photons (distance in km)**	**BB'84 decoy state (distance in km)**
Uplink (Turbulence attenuation 5 dB)	460	4650
Uplink (Turbulence attenuation 11 dB)	-	2200
Downlink	1540	9450
Inter-satellite	430	2660

Table 2 Critical distances in km for each method from [84]

4.3 Multi-photon approach can reach the heights of GEO satellite

Moving towards a goal of global QKD, satellite-aided communication has overcome the distance limitations up to certain extend. The use of multiple photons in quantum implementations has potential to improve speed and distance of communication. In the following section, implementation of the three-stage protocol and its extension, the braided single stage protocol for satellite communication is explained.

Advantages of using the multi-photon approach

Efficient use of channel resources: The multi-photon tolerant protocols are used not only for distribution of quantum keys but for actual communication at data rates comparable to today's data rates. Thus, we can achieve quantum secure communication using multi-photon tolerant protocols. Other methods of quantum cryptography such as BB'84 protocol, key distribution using entangled pairs require two communication channel between sender and receiver [78]. For multi-photon protocols, only one optical (quantum) channel is required for data transmission. Thus, resources are used efficiently in this proposed approach.

Photon generation and detection: For use of entangled pair of photons, one transmitter terminal and two simultaneous analyzing receiver terminals which individually can vary their measurement basis and store the arrival time of single-photon detection events, are required [85]. Given the state-of-the art technologies present in today's quantum devices, the rate of information transfer is limited by the maximal number of pairs that can be created and detected [78]. Similar is the case with single photons, where maximum detector rate is restricted by the operation in Geiger mode up to some tens of kHz in case of InGaAs detectors. The proposed multi-photon approach uses full beam laser pulse as a source and hence it is compatible with the lasercom technology used in contemporary satellite devices, which produce data rates up to few gigabits per sec. The limitation in speed in our approach is possible due to mechanical shutter operations to send bit ‘0’ or ‘1’.

Number of photons and Possibility of achieving GEO communication

In contemporary quantum cryptography techniques, use of single photons or entangled photons limits the distance of communication. If number of photons per pulse is increased for BB’84 protocol, Eve can easily perform photon number splitting attack and security of the protocol is cracked. From the performance analysis discussions in [86], simulations for the key generation rate as a function of the link distance are shown in Figure 15.

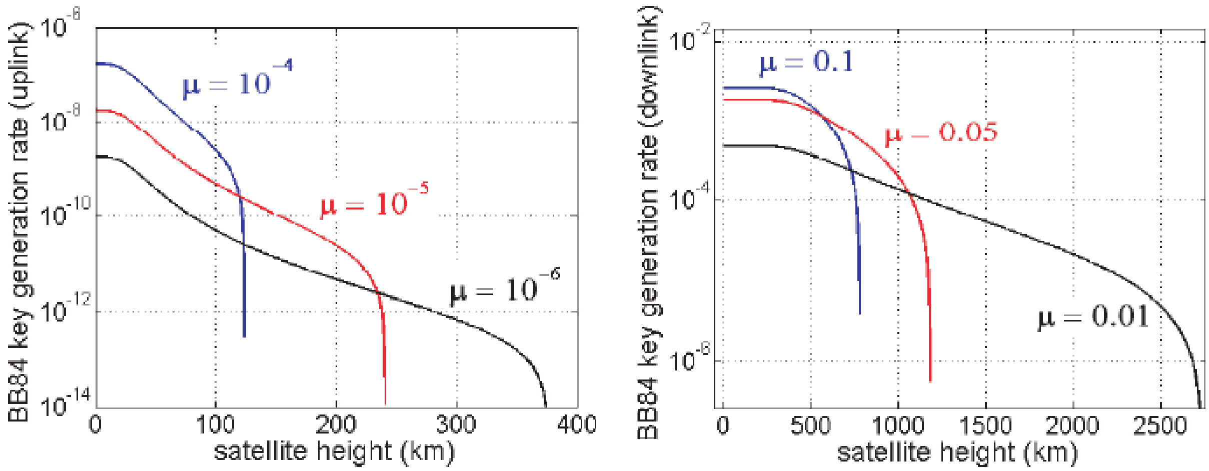

Figure 15: Simulations of key generation rate as a function of distance

In the case of the uplink the attenuation is so high that the secure key generation rate is extremely low (of the order of 10^{-12}, on the other hand it is not possible to increase the value of μ in order to avoid photon number splitting attack. When the attenuation grows, Eve’s attacks are more difficult to be detected. From Table 2, it can be realized that improvement in distance is due to increase in number of photons per pulse.

Also following specifications can support our deduction of increase in distance with increase in number of photons. Link power budget for lasercom systems explained in [70], provides the relation of number of photons required per bit to detect accurately at the detector. The mathematical equation is given by $n' = \frac{(P_T * d_r^2 * F_L * Q * \Gamma_t')}{M * R^2 * \theta_T^2 * (hv) f}$ where,

n' = required number of signal photons per bit (counted at the receiver)
P_T = transmit power in W, $d_r =$ diameter of the receiver aperture in m,
F_L = combined efficiency of transmitter and receiver, Q = quantum efficiency,
Γ_t' = the coupling efficiency of the uplink signal given by $\frac{1}{1+(\frac{d_r}{\rho_0})^2}$, where ρ_0 is coherence length in cm,
M = safety factor of the design of the communication link,
R = distance between transmitter and receiver in km, $\theta_t =$ optical beam width in rad,
hv = energy per photon in J/Hz/photon, f = data rate in bits per second

For fixed transmit power of 10 W and at a fixed data rate of 1 Gbps, the number of photons that are received at the receiver (n') are inversely proportional to the distance between transmitter and receiver (R), i.e., $n' \propto \frac{1}{R^2}$. For a laser communication using wavelength (λ) of 1550 nm, we used a quantum efficiency (Q) to be 0.5, diameter of the receiver aperture (d_r) of 0.5 m, coherence length (ρ_0) of 0.08m, an optical beamwidth (θ_t) of 5 µrad, Plank's constant (h) of $6.625\, X\, 10^{-34}$ J/Hz/photon, we plotted the number of received photons (n') as a function of the distance between transmitter and the receiver (R) as shown in Figure 16.

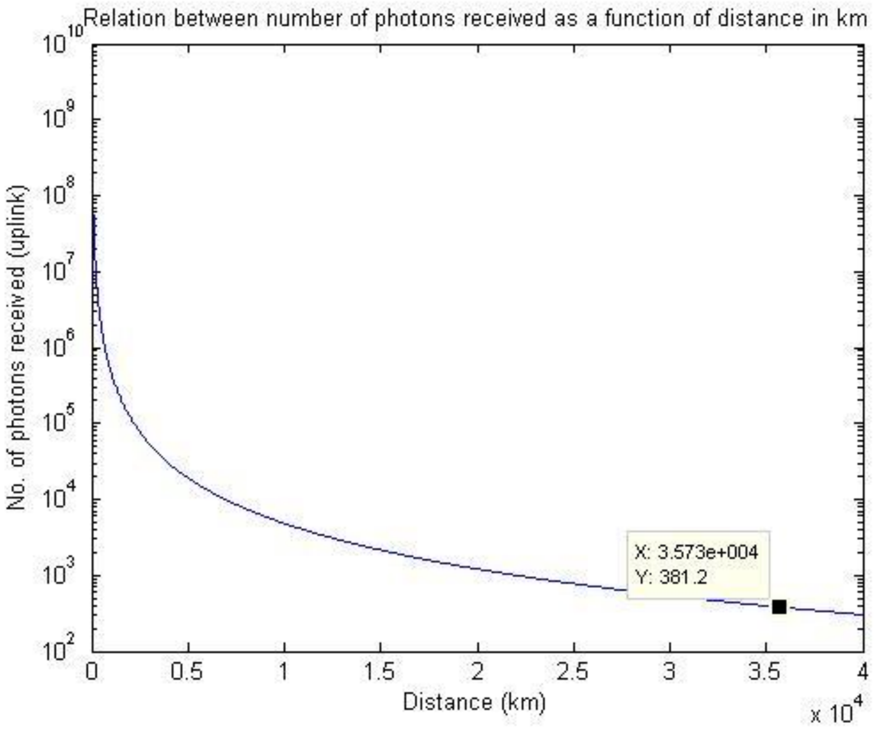

Figure 16: Plot of the relation between numbers of photons received as a function of distance in km

We can see that at a distance of around 35730 km, we will be able to receive around 380 photons on an average to complete the polarization state measurements, which is a sufficient number of photons to perform the task.

4.4 Scheme for implementation of braided single stage protocol for satellite communication

4.4.1 Technical challenges for implementation:

Point ahead angle: One of the important aspect for FSO satellite communication with narrow laser beams is consideration of point ahead angle. Because of the finite velocity of light (c) and the relative angular velocity of communication terminals moving in space, the transmit beam must be directed towards the receiver's position it will have at some *later time. This point ahead angle is given by* $\beta = 2 * \frac{V_R}{c}$ *where,* V_R *is the relative velocity between transmitter and receiver as illustrated in Figure 17 [87].*

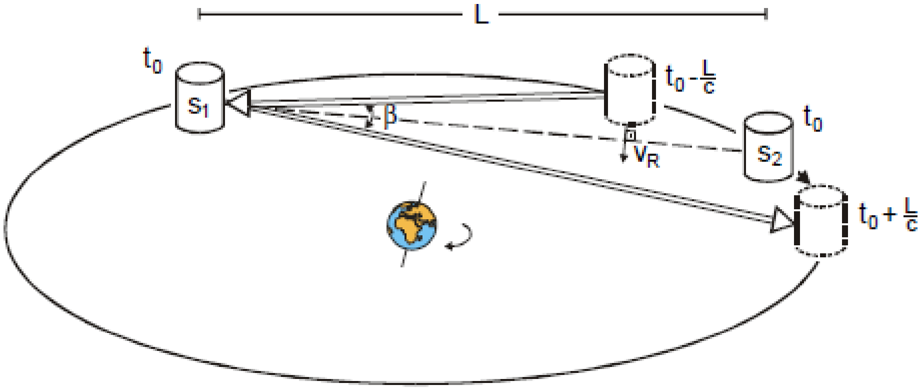

Figure 17: Point ahead angle β for space craft S1 and S2 that have a relative velocity component V_R orthogonal to the line of sight. Shown with dotted lines: position of S2 at time instants indicated (L: distance, c: velocity of light)

For inter-satellite communications, point-ahead angle is required from both sides. It amounts up to 40 μrad for a GEO-GEO link and up to 70 μrad for a LEO-GEO link and may thus be appreciably larger than the beam width. While implementing the three-stage protocol, we have to consider calculations of point ahead angle at each stage. For the three-stage protocol, information traverse back and forth three times and this traversing can be considered as a drawback in satellite communication. Also, one has to consider the fact that if Alice is on the ground and Bob is in the space, there will be two uplinks and one downlink set up for single bit of information transfer. The power link budget for implementing the three-stage protocol should consider the directions of photon travel.

Influence of satellite motion on polarization of qubits: As mentioned in previous subsection, in satellite transceivers, a pointing system is required to send the photons from sender to receiver accurately. This pointing system consist of mirrors assembly, hence effect of these assembly on satellite motion is studied in [88]. Mirrors are used to provide a constant offset, hence they introduce time-dependent modification which can be compensated by proper calibration. One of the solutions discussed in [88], is to deterministically calculate the actual polarization rotation by theoretical calculations given the satellite trajectory and pointing angles are known. But this requires knowledge of the refractive indices of all the mirrors in the satellite system. The change in polarization over satellite can also be detected by polarization compensation process. The polarization compensation process is described as follows:

Step 1: Alice and Bob will require a set of known polarization states (say $0°, 30°, 45°, 60° \dots 180°$ predetermined amongst them. Since the channel used is bidirectional, we characterize channel from Alice to Bob and Bob to Alice.

Step 2: Alice sends a horizontal polarization (0°) for some time, and Bob receives, say, $\delta_b°$ change in polarization. Similarly Bob sends a horizontal polarization, and Alice receives $\delta_a°$ change in polarization state. Ideally, $\delta_b°= \delta_a°$, but it might not be the case. This change in angle of polarization of beam of light can be compensated while modulating with a particular angle.

Step 3: Add the compensation during operation of the protocol, i.e., suppose Alice wants to send bit '0' with angular transform in polarization of $\theta_A°$, then resulting polarization angle sent by Alice would be ($\theta_A° + \delta_b°$). Similarly, Bob will send his polarization angle $\theta_B + \delta_a$ for communication.

This procedure can be implemented at the beginning of the data transfer only once and can be repeated if drastic change in atmospheric turbulences is expected. One important thing to note is, values of compensation angle differ for uplink and downlink for obvious effects of atmospheric turbulence.

4.4.2 Implementation of the braided single-stage protocol for satellite communication

For satellite-aided communication, different scenarios where point-to-point quantum communication can be implemented are described as follows: Ground-to-space communication, inter-satellite communication and ground-to-ground communication with satellite relay. All of these scenarios can be explained with typical quantum analogy, where Alice is sender of information and Bob is the receiver of information. Unlike other quantum cryptography methods, the multi-photon tolerant approach requires only one quantum channel for communication. The distances to be bridged may extend anywhere from a few hundred kilometers to thousands of kilometers.

Ground-to-space communication: In this setup, a transmitter can be ground station or a transmitter can be spacecraft. The main limiting factor is atmospheric turbulence. The smaller-scale turbulence causes beam width broadening whereas large-scale turbulences might cause beam deflection (beam wondering) [89]. Usually, uplinks face more broadening because they first propagate through turbulent atmosphere.

Inter-satellite communication: In this set-up both Alice and Bob are in space and hence the effect of atmospheric turbulence is very low. We can achieve maximum bit rate in this scenario.

Ground-to-ground communication: In this set-up two ground stations can be connected with a satellite relay system. Geostationary orbits are useful for this type of implementation.

Terminals for optical communication links are mostly designed for bi-directional links. The major design parameter in a transceiver system are laser wavelength, modulation format, data rate and reception technique [78]. The proposed transceiver system block diagram for multi-photon approach is as shown in Figure 18. The encoding scheme used is polarization encoding where 0° polarization indicate bit '0' and 90° polarization indicate bit '1'. Laser is the light source for transmitting data, popularly 1550 nm wavelength is chosen.

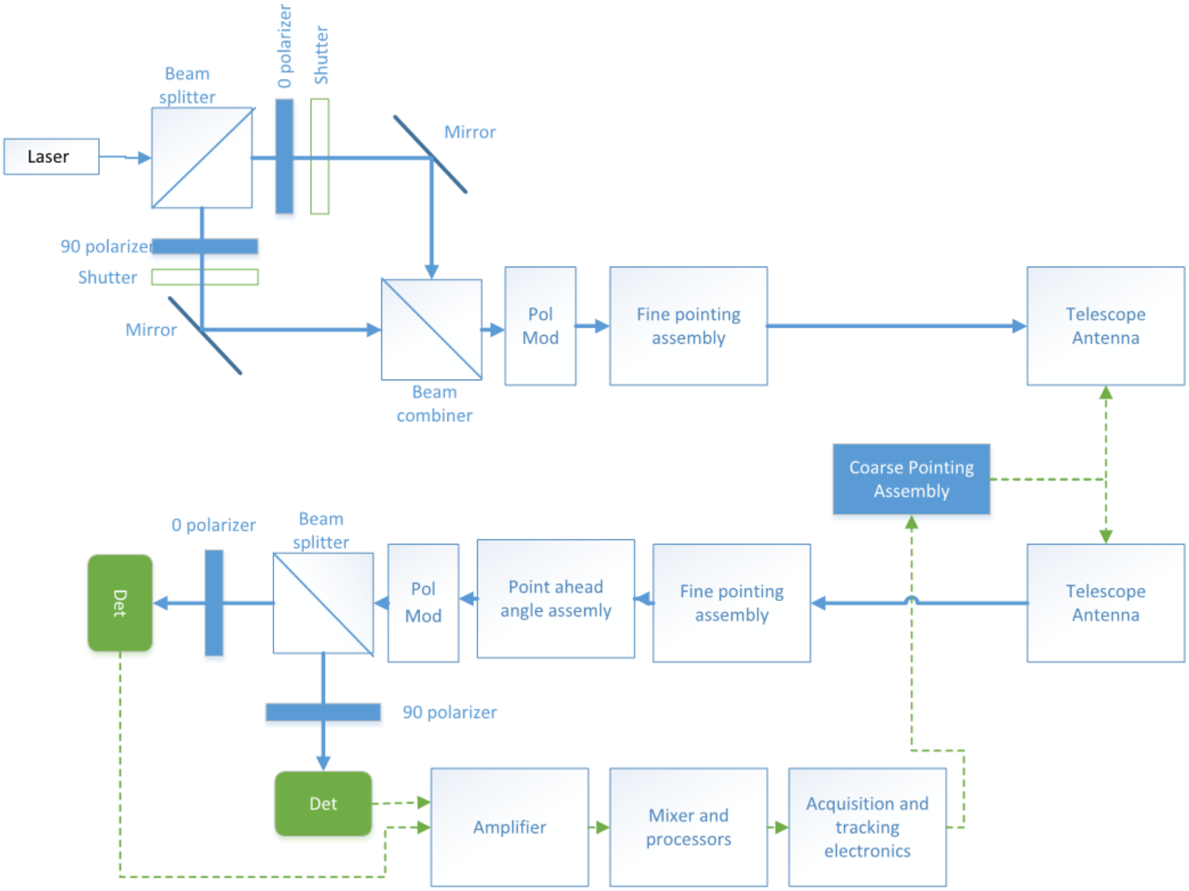

Figure 18: Proposed block diagram of transceiver for implementing multi-photon tolerant protocol

Steps of operation are as follows:

1. Laser beam is passed through a beam splitter to split in two paths one of which passes through $0°$ polarizer and other through $90°$ polarizer. Alice depending upon whether the bit sent is’0 ‘or’1’ operates shutters. Using mirrors and beam combiner assembly, beam is then directed towards polarization modulator.
2. A polarization modulator is a device that will change plane of polarization through some angle θ. In proof of experiment of the braided single-stage protocol, half wave plates are used [90].
3. The optical beam passes a fine pointing assembly before it enters telescope that is acting as a transmitting antenna. The functions of telescope include increasing beam diameter and thus reducing divergence. A coarse pointing assembly provides for steering the antenna.

   Thus, Alice transmits data to be sent ‘X’ in the form of linearly polarized light ($U_A(X)$) to Bob with the help of telescoping antenna. In the experiments reported in [91] proves that degree of polarization was maintained up to 99.4% in the satellite communication.
4. Now, at Bob’s station, received light beam passes the telescopic antenna and the fine pointing assembly and directed towards a polarization modulator. A point-ahead-angle assembly (PAA) has to be inserted in the receiver path to allow electronic control of the internal angular alignment between transmission and reception. Bob applies his transform and sends linearly polarized light ($U_B U_A(X)$) back to Alice.

5. At Alice’s end, she will use polarization modulator to remove her transform and send the optical beam back to Bob. Eventually, Bob applies polarization modulator to remove his transform and beam is passed through beam splitter.
6. After splitting the beam, it is passed through $0°$ polarizer and $90°$ polarizer to detect bit ‘0’ or ‘1’.
7. The output of the detector is used as an input for acquisition and tracking electronics to calculate the coarse adjustments.
8. Now that Alice and Bob has shared a message ‘X’ completely securely, a new angle of transform is calculated at both Alice and Bob’s end by the formula mentioned. So for next iteration, whenever Alice send a message with her transform U_A(X), Bob already knows value of U_A and hence applies $U_A^\dagger$ to get information directly.

   Thus, the three-stage protocol and its extension, the braided single-stage protocol can be implemented over satellite communication.

4.5 Summary

This chapter has provided the details of the ground to satellite segment in the global network. With development in free space optics technology it has become feasible to communicate over longer distances in space communication. This chapter proves that quantum key distribution protocols can be implemented at the heights of GEO communications. The details of challenges in implementation, procedure of implementation and block diagram of the transceiver has been provided in this chapter.

Chapter 5: Multi-photon based threshold quantum cryptography

The science of cryptography was developed to achieve secure communication between multiple parties. Traditionally, cryptography only deals with the communication between one sender and one receiver. However, more commonly, a communication is required between an individual and an organization or between different organizations. Moreover, many crucial decisions in an organization are made by a group of people and not an individual. Therefore, there is the requirement to guarantee the authenticity of messages sent by a group of individuals to another group or a person. Hence, the threshold cryptography based on secret sharing was developed.

Some classical threshold encryption schemes were developed based on some popular public key encryption schemes such as RSA, ElGamal cryptosystems. While secure distributed computation has a more general scope, many of these schemes are not practical. Classical threshold cryptography faces certain drawbacks such as, a) the resulting cipher text becomes very large which affects the efficiency of the schemes, b) the shared keys can be used only once, c) it is not possible to detect the presence of eavesdropper on any of the communication channel, and hence the shared secrets cannot be used. Moreover, the classical methods are only conditionally secure.

On the other hand, quantum cryptography provides unconditional security. Quantum communication is the most promising application of quantum information theory. Quantum Key Distribution (QKD) allows two legitimate parties to communicate secretly over communication channel in the presence of an adversary. Various QKD protocols have been proposed since the pioneering works of Bennett and Brassard. However, the applications of BB84 and its variants are limited to point-to-point communication. Recently, there is the necessity of secure point-to-multipoint communication. The purpose of threshold cryptography is to develop a technique to deal with multi-sender/multi-receiver scenario. In this dissertation, we propose *a multi-photon approach* for quantum threshold cryptography. The multi-photon approach uses Shamir's secret sharing method to generate shares of the classical secret and uses *threshold collaborative unitary transformation* for distribution of those shares. Multi-photon tolerant approach was discussed in [42] . The advantages provided by multi-photon approach are ease of implementation, increase in speed of communication and longer distances of communication as compared to single photon approach.

5.1 Background

The concept of threshold cryptography evolves from the idea: Instead of giving the key for the encrypted secret to an individual, it may be desirable to distribute information in such a way that no single party alone has the whole knowledge of the key, but a few of them can jointly determine the key.

Mathematical Logic of Sharing the Secret

The mathematical logic for making shares of the secret is based on Shamir's secret sharing method as mentioned in [92]. The goal is to divide secret S (e.g., a safe combination) into n pieces of data $S_1, S_2, \dots, S_n$ in such a way that:

i. Knowledge of any t or more S_i pieces makes S easily computable, where $i = 1, 2, \dots, n$.

ii. Knowledge of any $t - 1$ or fewer S_i pieces leaves S completely undetermined (in the sense that all its possible values are equally likely).

This scheme above is called (t, n) threshold scheme. If $t = n$, then all participants are required in order to reconstruct the secret. We will explain how this scheme works with the following example. Let F be a finite field. We want to share the secret S using Shamir's secret share amongst n users.

$$S \rightarrow (S_1, S_2, \dots, S_n)$$

The secret can be retrieved when t users collaborate in three steps:

i. Choose arbitrary positive integers $f_1, f_2, \dots, f_{t-1}$, which are to be coefficients of $t - 1$ degree polynomial $f(z)$ as in the next step and $f_0 = S$.

ii. Build a polynomial $f(z) = f_0 + f_1 \times z + \cdots + f_{t-1} \times z^{t-1}$, where $f(0) = f_0 = S$.

iii. Calculate and share the points on that polynomial $(z_i, f(z_i))$where $f(z_i) = f(i)$ with party index $i = 1, 2, \dots, n$.

For recovery, when t parties out of n have a part of the secret, i.e. any subset of t pairs, then we have t points on the curve of $(t - 1)$ degree polynomial, so by this fact, we get unique coefficients to a $(t - 1)$ degree polynomial. We use Lagrange Interpolation over a finite field. The details of the method are given section 5.2. Solving the linear systems, we can find out the coefficient f_0. The secrecy of the shared secret is guaranteed based on the following explanation. Suppose we have only $t - 1$ parties contributing shares. This corresponds to knowing only $t - 1$ point on $t - 1$ degree polynomial. It turns out we cannot find out coefficient f_0 using this partial information. Given $t - 1$ pairs of $(i, f(i))$, we need point $(0, S)$. If we just know $t - 1$ points, none of which has input 0, the conditional distribution on these points on having a point $(0, S)$ is still uniform. Thus, all values of the secret S are equally likely and the secret holds.

Quantum secret sharing

This subsection explains another method for sharing secret and how it is different from the proposed approach. The pioneering work in quantum secret sharing (QSS) is presented in [93]. It allows a secret quantum state to be shared among many participants in such a way that only the authorized groups can reconstruct it. A method for sharing classical secret using quantum information to transmit the shares securely in presence of an eavesdropper using three-particle and four-particle GHZ states was proposed in [18]. In [94], the concept of threshold cryptography was discussed and it claimed that the only constraint on the existence of threshold schemes comes from the quantum 'no-cloning theorem', which requires the total number of parties $n \leq 2t$ where t is threshold number. This work led to many theoretical and experimental researches, mainly divided into two categories: QSS of classical messages [94-96] and QSS of quantum information where the secret is an arbitrary unknown qubit [95] [93] [97]. Entangled states are used in [94-96]. The proposed multi-photon approach differs from QSS because the shared secrets are *classical* information and we use collaborative quantum unitary transform.

In 2005, a (n, n) threshold scheme of multiparty quantum secret sharing of classical messages (QSSCM) using only single photons was proposed in [98]. One of the shortcomings of this protocol is all the members have to be present in order to decrypt a secret. Thus, in case of interrupted communication when any one of the n parties is not available, the secret cannot be accessed by anyone else. The proposed approach requires only t users with $t < n$ for reconstructing the secret and hence more efficient in practice.

5.2 Threshold quantum cryptography with single photon

Threshold quantum cryptography combines secret sharing schemes with several quantum cryptographic functions. The threshold version of quantum cryptography based on conjugate coding was proposed in [99]. It takes an example of quantum money proposed in [9] to show that when classical secret is shared by using quantum unitary transforms, the constraint of no cloning theorem does not apply on the protocol. In the concept of *t out of n* threshold quantum cryptography scheme suggested by [99].

$K = (a_1, b_1, a_2, b_2, \dots, a_m, b_m)$

where, m=log$_2$L is the binary representation of the original secret with ; where L is bitwise length of secret; a_i, b_i are chosen uniformly from {0,1} then bits $a_1, a_{2..}$ are encoded with bases b_1, b_2 ... b_m respectively. The bases are chosen from

$|0\rangle\ or\ |1\rangle\ and\ |+\rangle\ or\ |-\rangle$

In this protocol, the dealer makes shares of the secret and distributes it among *n* authorized users. Now *t out of n* users can collaborate to obtain the original secret. The scheme is based on Shamir's secret sharing method. There are 3 phases in the *t* out of *n* threshold quantum cryptography protocol, distribution phase, pre-computation phase, and issuing phase. In this section, we will explain in detail the first two phases as it is from [99] and issuing phase in more general form so these steps can be applied into our proposed protocol.

Distribution phase

Following is procedure for distributing the secret among n users:

- Dealer choose secret K

$$K = (a_1, b_1, a_2, b_2, \dots, a_m, b_m)$$

- Dealer makes shares of the secret $S_1, S_2, \dots, S_n$ using Shamirs secret sharing method over finite field F_2^{2m}.
- The dealer choses $x_j\ for\ j = 1,2, \dots n$ which are in n distinct non-zero elements over F_2^{2m}.
- The dealer randomly chooses a secret (t-1)th degree polynomial $f(x) over\ F_2^{2m}\ where\ f(0) = \widetilde{K}$, here is the polynomial representation of K. Then dealer computes $S_j\ = f(x_j)$ and secretly sends it to $P_j\ where\ j = 1,2..n$

Precomputation phase

In this phase, the centers compute the preliminary information for collaborative procedure. The preliminary information depends on which centers are collaborating. Let us assume there are *t* centers that collaborate to get the secret. For each $j = 1,2, \dots t$, P_j calculates and stores following value given by the Lagrange interpolation formula over F_2^{2m}.

$$K_j = S_j \prod_{1 \leq l \leq t, l \neq t} \frac{x_l}{x_l - x_j} \tag{1}$$

Let $K^{[j]} = a_1^{[j]}, b_1^{[j]} \dots , a_m^{[j]} b_m^{[j]}$ be representation of each K_j. Each share of the secret is kept locally and not shared with other parties. The values of Kj follow property

$$K = \sum_{j=1}^{t} K_j\ (Mod\ 2) \tag{2}$$

Issuing phase

In the issuing phase, we understand how each center contributes to create the original secret. The sequence of operation is as follows though order is not important.

- The center P1 generates the quantum state and sends it to P2

$$|\phi^{[1]}\rangle = |\psi_{a_1^{[1]},b_1^{[1]}}\rangle \otimes |\psi_{a_2^{[1]},b_2^{[1]}}\rangle \ldots \otimes |\psi_{a_m^{[1]},b_m^{[1]}}\rangle \tag{3}$$

- For each $j = 1,2,\ldots t$, P_j receives $|\phi^{[1]}\rangle$ $from\ P_{j-1}$ and applies following transform

$$W^{[j]} = U_1^{[j]}V_1^{[j]} \otimes U_2^{[j]}V_2^{[j]} \otimes \ldots U_m^{[j]}V_m^{[j]} \tag{4}$$

where, U and V are the unitary operators of rotations. They perform the required quantum operation on the photons so that data transferred between two parties is always in quantum state. They are given by

$$U_i^{[j]} = U_{a_i^{[j]}}$$

$$V_i^{[j]} = V_{b_i^{[j]}} \tag{5}$$

- For each $j = 1,2,\ldots t$, P_j obtains the transform $|\phi^{[j]}\rangle$ using $W^{[j]}$ i.e.

$$W^{[j]}: |\phi^{[j-1]}\rangle \rightarrow |\phi^{[j]}\rangle \tag{6}$$

and send it to P_{j+1}

Consider, $W^{[2]}$ operating on $|\phi^{[1]}\rangle$ to yield $|\phi^{[2]}\rangle$

$$\begin{aligned} W^{[2]} \otimes |\phi^{[1]}\rangle &= (U_1^{[2]}V_1^{[2]} \otimes U_2^{[2]}V_2^{[2]} \cdots \otimes U_m^{[2]}V_m^{[2]}) \otimes (|\psi_{a_1^{[1]},b_1^{[1]}}\rangle \otimes |\psi_{a_2^{[1]},b_2^{[1]}}\rangle \otimes ..|\psi_{a_m^{[1]},b_m^{[1]}}\rangle) \\ &= U_{a_1^{[2]}}V_{b_1^{[2]}}|\psi_{a_1^{[1]},b_1^{[1]}}\rangle \otimes U_{a_2^{[2]}}V_{b_2^{[2]}}|\psi_{a_2^{[1]},b_2^{[1]}}\rangle .. \otimes U_{a_m^{[2]}}V_{b_m^{[2]}}|\psi_{a_m^{[1]},b_m^{[1]}}\rangle \end{aligned} \tag{7}$$

We use following property which will be proved in the next section

$$U_{a'}V_{b'}|\psi_{a,b}\rangle = |\psi_{a+a',b+b'}\rangle \tag{8}$$

By using unitary transformation $W^{[2]}$, $|\phi^{[1]}\rangle$ is transformed to $|\phi^{[2]}\rangle$ which encodes

$(a_1^{[1]} \oplus a_1^{[2]}, a_2^{[1]} \oplus a_2^{[2]}, \cdots a_m^{[1]} \oplus a_m^{[2]})$

using bases $(b_1^{[1]} \oplus b_1^{[2]}, b_2^{[1]} \oplus b_2^{[2]}, \cdots b_m^{[1]} \oplus b_m^{[2]})$

The procedure continues till $j = t$ and $|\phi^{[t]}\rangle$ finally encodes

$(a_1^{[1]} \oplus a_1^{[2]}, a_2^{[1]} \oplus a_2^{[2]}, \cdots a_m^{[1]} \oplus a_m^{[2]} .. a_m^{[t]} \oplus a_m^{[t]})$

using bases $(b_1^{[1]} \oplus b_1^{[2]}, b_2^{[1]} \oplus b_2^{[2]}, \cdots b_m^{[1]} \oplus b_m^{[2]} .. b_m^{[t]} \oplus b_m^{[t]})$

Now from equation above $(a_1^{[1]} \oplus a_1^{[2]}, a_2^{[1]} \oplus a_2^{[2]}, \cdots a_m^{[1]} \oplus a_m^{[2]} .. a_m^{[t]} \oplus a_m^{[t]}) = (a_1, a_2 .. a_m)$ is encoded

using bases

$(b_1^{[1]} \oplus b_1^{[2]}, b_2^{[1]} \oplus b_2^{[2]}, \cdots b_m^{[1]} \oplus b_m^{[2]} .. b_m^{[t]} \oplus b_m^{[t]}) = (b_1, b_2, .. b_m)$

Thus, t *out of* n parties collaborate to create the secret. For recovery, any t center can collaborate to recover the secret. For each $j = 1, 2, \cdots, (t-1), P'_j$ receives $|\phi'_{j-1}\rangle$ from P'_{j-1} and applies W'_J to receive $|\phi'_j\rangle$ by unitary transformation,

$$W^{[j]'} : |\phi^{[j-1]'}\rangle \to |\phi^{[j]'}\rangle \tag{9}$$

Finally, P'_t applies $W^{[t]'}$ to $|\phi^{[t-1]'}\rangle$ to obtain $|\phi^{[t]'}$ measure it in bases $(0, 0 \cdots 0)$ and gets the string $(c_1, c_2 \cdots c_m)$.

P'_t then checks if $c_i = 0$ for all $i = 1, 2 \cdots m$. Thus, the secret is shared and recovered

5.3 Multi-photon based quantum threshold cryptography scheme

In multi-photon approach, for achieving the security of the protocol and to limit the eavesdropper performance number of coherent states must be higher than the mean photon number. Consider the following scheme in which each data bit is encoded into coherent state of M possible states. Using maximum likelihood positive operated value measurement technique, a lower bound between the number of non-orthogonal coherent states (M) and mean photon number ($|\alpha|^2$)is calculated for a given probability of measurement error.

$$M \geq -\frac{|\alpha|^2 + 1}{\ln(P_e)}$$

Multiple basis approach

A dealer constructs n shares of a secret and distributes it to n users, which are authenticated via some classical method of authentication. Any t parties out of n then collaborate to encode the classical secret on the quantum state by a sequence of unitary transformations. The unitary transformations used in this operation are based on the secret shared between the parties. Each party changes both the basis of the bits and encodes the classical secret in the form of quantum state. While decoding, any of the t parties can again collaborate to apply the reverse of the unitary transformation to get the original secret back.

Consider K is the original secret which is represented as the sequence of bits

$K = (a_1, b_1, a_2, b_2, \cdot \cdot \cdot , a_m, b_m)$

where, bits $a_1, a_2, a_3, \cdot \cdot \cdot , a_m$ are uniformly chosen from 1, 0 and encoded with basis $b_1, b_2, \cdot \cdot \cdot , b_m$

where $b_i = 0, 1, \cdot \cdot \cdot , M -1$, We consider a scheme where each data bit is encoded into coherent state of M possible states known as qumode. This is very similar to the qumode scheme chosen in Y- 00 protocol.

There are two approaches for implementing the protocol, phase encoding and polarization encoding. There will be M pairs of coherent states with phase or polarization given by

$$\theta_m = \frac{2m\pi}{2M} \tag{10}$$

The pairs are given with angle basis

$$\theta_m \; and \; \theta_{m+M} = \theta_m + \pi \tag{11}$$

Each pair is opposite to each other on the polar coordinates and can be used to represent 0 and 1. Now for each pair, one can flip 0 to 1 or 1 to 0 by making a π rotation.

On the other hand, encoding on the m^{th} basis is the same as rotating the state with $\theta = 0$ with an angle θ_m.

In the Fock basis, a polarized single photon is given by $|1\rangle_r = a_r^\dagger|0\rangle$, where

$$a_r^\dagger = \cos\frac{\theta}{2} a_H^\dagger + e^{i\phi} \sin\frac{\theta}{2} a_V^\dagger \tag{12}$$

In which θ and ϕ are the spherical coordinates of the polarization vector **r** on the Block sphere, and a_H and a_V are the annihilation operators for the north pole and the south pole, which we designate as the horizontal and vertical polarizations respectively. We consider greater circle of polarization on Block sphere for our calculation. That means $\phi = \frac{\pi}{2}$.

The multiphoton coherent quantum state can be expressed in terms of the superposition of photon number state $|n\rangle$.

For polarization,

$$|a\rangle_r = e^{\frac{-\alpha^2}{2}} \sum_{n=0}^{\infty} \frac{a_r^{\dagger n}}{\sqrt{n!}} |0\rangle \tag{13}$$

For phase,

$$\left|\alpha e^{i\theta}\right\rangle = e^{\frac{-\alpha^2}{2}} \sum_{n=0}^{\infty} \frac{(\alpha e^{i\theta})^n}{n!} |n\rangle \tag{14}$$

Now, consider quantum state for the given secret K represented as,

$$|\phi\rangle = \left|\psi_{a_1,b_1}\right\rangle \otimes \left|\psi_{a_2,b_2}\right\rangle \ldots \otimes \left|\psi_{a_m,b_m}\right\rangle \tag{15}$$

Multi-photon t out of n quantum threshold protocol

In this paper we assume that the dealer and the participating parties are authenticated and honest. We further assume that the communication channels between the parties are secure and error free. The detailed steps of the protocol for distributing the shares of the secret amongst users and pre- computation steps that user needs to complete are explained in previous section. For multi-photon and multiple bases approach, equation 2 is changed to

$$K = \bigoplus_{i=1}^{t} K_j \; mod \; M \tag{16}$$

The issuing phase described in the previous section is the generalized procedure for sharing and recovering the secret. The key equation for the multi-photon scheme to be successful is

$$U_{a'}V_{b'}|\psi_{a,b}\rangle = |\psi_{a+a',b+b'}\rangle$$

As mentioned previously, there are two approaches for implementing the proposed protocol namely, polarization and phase encoding.

In case of polarization encoding, the rotations can be realized by the polarization rotator operator

$$U_a = e^{i\frac{\pi^a}{2}(a_H a_V^\dagger + a_V a_H^\dagger)}$$

where, $a = 0, 1$ representing the bit value and

$$V_b = e^{i(\theta_b + \pi(-1)^{P_b})(a_H a_V^\dagger + a_V a_H^\dagger)} \tag{17}$$

where, $b = 0, 1, \cdots, M-1$ representing basis Here, P_b is the parity operator $P_b = 0$ if b is even and $P_b = 1$ if b is odd.

Now,

$$\begin{aligned} \hat{U}_a a_H^\dagger \hat{U}_a^\dagger &= \cos\frac{\pi^a}{2} a_H^\dagger + i\sin\frac{\pi^a}{2} a_V^\dagger \\ \hat{U}_a a_V^\dagger \hat{U}_a^\dagger &= \cos\frac{\pi^a}{2} a_V^\dagger + i\sin\frac{\pi^a}{2} a_H^\dagger \end{aligned} \tag{18}$$

Similarly,

$$\begin{aligned} \hat{V}_b a_H^\dagger \hat{V}_b^\dagger &= \cos\frac{\theta_b + \pi^{P_b}}{2} a_H^\dagger + i\sin\frac{\theta_b + \pi^{P_b}}{2} a_V^\dagger \\ \hat{V}_b a_V^\dagger \hat{V}_b^\dagger &= \cos\frac{\theta_b + \pi^{P_b}}{2} a_V^\dagger + i\sin\frac{\theta_b + \pi^{P_b}}{2} a_H^\dagger \end{aligned} \tag{19}$$

Operations of the unitary operators are given as follows:

$$\begin{aligned} \hat{U}_a f(a_H^\dagger, a_V^\dagger)|0\rangle &= \hat{U}_a f(a_H^\dagger, a_V^\dagger)\hat{U}_a^\dagger \hat{U}_a|0\rangle \\ &= \hat{U}_a f(a_H^\dagger, a_V^\dagger)\hat{U}_a^\dagger|0\rangle \\ &= f(\hat{U}_a a_H^\dagger \hat{U}_a^\dagger, \hat{U}_a a_V^\dagger \hat{U}_a^\dagger)|0\rangle \end{aligned}$$

One can see that,

$$\begin{aligned} |\psi_{a,b}\rangle &= U_a V_b |n\rangle_{\mathbf{r}} \\ &= U_a V_b e^{-\frac{\alpha^2}{2}} \sum_{n=0}^{\infty} \frac{a_{\mathbf{r}}^{\dagger n}}{\sqrt{n!}} |0\rangle \\ &= f(U_a V_b a_{\mathbf{r}}^{\dagger} V_b^{\dagger} U_a^{\dagger}) |0\rangle \end{aligned} \qquad (20)$$

Substituting values from equation 19,

$$\begin{aligned} V_b a_{\mathbf{r}}^{\dagger} V_b^{\dagger} &= \cos\frac{\theta}{2}(\cos\frac{\theta_b + \pi^{P_b}}{2} a_H^{\dagger} + i \sin\frac{\theta_b + \pi^{P_b}}{2} a_V^{\dagger}) + i * \sin\frac{\theta}{2}(\cos\frac{\theta_b + \pi^{P_b}}{2} a_V^{\dagger} + i \sin\frac{\theta_b + \pi^{P_b}}{2} a_H^{\dagger}) \\ &= (\cos\frac{\theta}{2}\cos\frac{\theta_b + \pi^{P_b}}{2} - \sin\frac{\theta}{2}\sin\frac{\theta_b + \pi^{P_b}}{2}) a_H^{\dagger} + i(\cos\frac{\theta}{2}\sin\frac{\theta_b + \pi^{P_b}}{2} + \sin\frac{\theta}{2}\cos\frac{\theta_b + \pi^{P_b}}{2}) a_V^{\dagger} \end{aligned}$$

Using trignomatric identities we get,

$$V_b a_{\mathbf{r}}^{\dagger} V_b^{\dagger} = \cos(\frac{\theta + \theta_b + \pi^{P_b}}{2}) a_H^{\dagger} + i \sin(\frac{\theta + \theta_b + \pi^{P_b}}{2}) a_V^{\dagger} \qquad (21)$$

Substituting equation 21 in equation 20 for simplification of calculations we substitute $\frac{\theta + \theta_b + \pi^{P_b}}{2} = X$

$$\begin{aligned} |\psi_{a,b}\rangle &= f(U_a \cos(X) a_H^{\dagger} + i \sin(X) a_V^{\dagger} U_a^{\dagger}) |0\rangle \\ &= f(\cos(X) U_a a_H^{\dagger} U_a^{\dagger} + i \sin(X) U_a a_V^{\dagger} U_a^{\dagger}) |0\rangle \\ &= f(\cos(X)(\cos\frac{\pi^a}{2} a_H^{\dagger} + i \sin\frac{\pi^a}{2} a_V^{\dagger}) + i \sin(X)(\cos\frac{\pi^a}{2} a_V^{\dagger} + i \sin\frac{\pi^a}{2} a_H^{\dagger})) |0\rangle \\ &= f((\cos(X)\cos\frac{\pi^a}{2} - \sin(X)\sin\frac{\pi^a}{2}) a_H^{\dagger} + i(\cos(X)\sin\frac{\pi^a}{2} + \sin(X)\cos\frac{\pi^a}{2}) a_V^{\dagger}) |0\rangle \end{aligned}$$

Using trignometric identities and substituting the value of X,

$$|\psi_{a,b}\rangle = f(\cos(\frac{\theta + \theta_b + \pi^{P_b} + \pi^a}{2}) a_H^{\dagger} + i \sin(\frac{\theta + \theta_b + \pi^{P_b} + \pi^a}{2}) a_V^{\dagger}) |0\rangle$$

Now consider,

$$\hat{U}_{a'}\hat{V}_{b'}|\psi_{a,b}\rangle = \hat{U}_{a'}\hat{V}_{b'}(\cos(\frac{\theta+\theta_b+\pi^{P_b}+\pi^a}{2})a_H^\dagger + i\sin(\frac{\theta+\theta_b+\pi^{P_b}+\pi^a}{2})a_V^\dagger) \tag{22}$$

Following similar calculations we can show that,

$$\begin{aligned}
U_{a'}V_{b'}|\psi_{a,b}\rangle &= \cos(\frac{\theta+\theta_b+\theta_{b'}+\pi_b^P+\pi_{b'}^P+\pi^a+\pi^{a'}}{2})a_H^\dagger + i\sin(\frac{\theta+\theta_b+\theta_{b'}+\pi^{P_b}+\pi^{P_{b'}}+\pi^a+\pi^{a'}}{2})a_V^\dagger) \\
&= \cos(\frac{\theta+\theta_b+_{b'}+\pi^{P_b}+^{P_{b'}}+\pi^a+^{a'}}{2})a_H^\dagger + i\sin(\frac{\theta+\theta_b+_{b'}+\pi^{P_b}+^{P_{b'}}+\pi^a+^{a'}}{2})a_V^\dagger) \\
&= |\psi_{a+a',b+b'}\rangle
\end{aligned}$$

For phase encoding we can show similar calculations, The M pairs in phase encoding can be written as $|\alpha e^{i\theta_m}\rangle$ and $|\alpha e^{i(\theta_m+\pi)}\rangle$ Precisely, rotation can be realized by the phase shift operations,

$U_a = e^{i\pi^a a^\dagger a}$ and $V_b = e^{i(\theta_b+\pi^{P_b})a^\dagger a}$ where, P_b is the parity operator. $a^\dagger$ and a are the creation and the annihilation operators, and together $a^\dagger a$ is just the number operator, i.e., $a^\dagger a|n\rangle = n|n\rangle$.

Then one can see that,

$$\begin{aligned}
|\psi_{a,b}]\rangle &= U_aV_b|\alpha e^{i\theta_0}\rangle \\
&= [e^{i\pi^a a^\dagger a}e^{i(\theta_b+\pi^{P_b})a^\dagger a}]e^{-\frac{\alpha^2}{2}}\sum_{n=0}^{\infty}\frac{(\alpha e^{i\theta_0})^n}{n!}|n\rangle \\
&= e^{i(\theta_b+\pi^{P_b}+\pi^a)a^\dagger a}e^{-\frac{\alpha^2}{2}}\sum_{n=0}^{\infty}\frac{(\alpha e^{i\theta_0})^n}{n!}|n\rangle \\
&= e^{-\frac{\alpha^2}{2}}\sum_{n=0}^{\infty}\frac{(\alpha e^{i\theta_0})^n}{n!}e^{i(\theta_b+\pi^{P_b}+\pi^a)a^\dagger a}|n\rangle \\
&= e^{-\frac{\alpha^2}{2}}\sum_{n=0}^{\infty}\frac{(\alpha e^{i\theta_0})^n}{n!}e^{i(\theta_b+\pi^{P_b}+\pi^a)n}|n\rangle \\
&= |\alpha e^{i(\theta_0+\theta_b+\pi^{P_b}+\pi^a)}\rangle \\
&= |\alpha e^{i(\theta_b+\pi^{P_b}+\pi^a)}\rangle
\end{aligned} \tag{23}$$

Now consider,

$$\begin{aligned} U_{a'}V_{b'}|\psi_{a,b}\rangle = U_{a'}V_{b'}|\alpha e^{i(\theta_b+\pi^a)}\rangle &= |\alpha e^{i(\theta_b+\theta_{b'}+\pi^a+\pi^{a'}+\pi^{P_b}+\pi^{P_{b'}}}\rangle \\ &= |\alpha e^{i(\theta_{b+b'}+\pi^{a+a'}+\pi^{P_b+P_{b'})}}\rangle \\ &= |\psi_{a+a',b+b'}\rangle \end{aligned} \qquad (24)$$

Hence, we see that both phase encoding and polarization encoding can be successfully implemented with multi-photon based threshold quantum cryptography. Next, we see a derivative of this protocol without a dealer.

5.4 Multi-photon based threshold protocol with multiple trusted dealer

Distribution phase: In this phase, w centers ($P_1, P_2, \cdots P_w$) distribute their shares. For all P_j in w centers,

i P_j chooses $\sigma_j = (a_{j,1}, b_{j,1}, \cdots, a_{j,m}, b_{j,m})$ as a secret where $a_{j,1}, a_{j,2}, \cdots, a_{j,m}$ are uniformly chosen from $1, 0$ and encoded with basis $b_{j,1}, b_{j,2}, \cdots, b_{j,m}$ where $b_{j,i} = 0, 1, \cdots, M-1$.

ii P_j makes n shares of the secret $S_{j,1}, S_{j,2}, \cdots, S_{j,n}$ of σ_j using Shamir's secret sharing method over finite field F_2^{2m} such that $S_{j,l} = f_j(x_{j,l})$ for each $l = 1, 2, \cdots n$.

iii P_j secretly sends $S_{j,l}$ to P_l for each $l = 1, 2, ..n$

Pre-computation phase: Consider, t centers $P_1, ..P_t$ collaborate to encrypt the secret.

i For each $l = 1, 2, ..n$, P_l calculates and secretly stores the following value given by Lagrange interpolation formula:

$$K_l = \sum_{j=1}^{w} S_{j,l} \prod_{l \leq k \leq t, k \neq l} \frac{x_{j,k}}{(x_{j,k} - x_{j,i})} \tag{25}$$

over F^{2m}. Let $K^{[l]} = (a_1^{[l]}, b_1^{[l]}, \cdots, a_m^{[l]}, b_m^{[l]})$ be the representation of K_l The whole secret can be written as

$$\tilde{K} = \sum_{l=1}^{t} K_l = \sum_{j=1}^{w} \sigma_j \tag{26}$$

over F^{2m}. The issuing phase is same as that of protocol 1.

5.5 Application of the quantum threshold scheme

Use of quantum communication prevents the shares from copying and they can be reused for future communication. Any organization with very valuable secrets, such as certificate authorities, military, and governments, would make use of this technology. The multi-photon based approach using polarization helps in experimental realization of the protocol. An implementation scheme based on photon polarization is practically suitable for the proposed multi-photon quantum threshold cryptography. Real valued or complex valued unitary transforms can be used for rotation of polarization. The real valued transforms are commutative and hence the sequence of operation on the photon does not matter. Hence the general threshold quantum cryptography scheme can be easily implemented without paying attention to the sequence.

We consider a military application as an example of implementation based on multilevel-shared control schemes, where the lower level of authority (and hence responsibility) at a lower level of command could be satisfactorily compensated for by requiring a higher level of concurrence for the action to be initiated. Consider a missile launching system that requires a secret code to initiate the operation. The consequences of a missile being launched without proper authorization would be so adverse that in normal times (peacetime or in lower levels of alert) the capability to initiate such an action should be held at a higher level of command, perhaps by the president. In other words, the policy is that even if all of the officers in the house believe that a missile should be launched, they should not be able to do so without requesting an authorization from the superior commander (and more importantly, could not do so without being given the launch enable codes).

The missile activation code is protected by quantum secret. Per this protocol, this code is encoded using different shares which are given to the responsible parties in the cabinet. When the quantum state matches with a missile activation code, then the missile gets activated. There are *t* out of *n* officers needed in order to activate the system. In case of operation of the activation, the person in command will send request to *(t-1)* officers to contribute to generate the shared secret. The procedure is mentioned in the proposed protocol in this paper is followed and quantum state is sent from one user to another until it reaches the person in command who will contribute to t^{th} share of the secret and gets secret quantum state. When he applies his unitary transform to the secret quantum state, the outcome is sequence that matches the secret code and the missile is activated.

Similarly, threshold quantum cryptography can be used in corporate scenarios while implementing high-level business decisions. Protecting a bank account by multiple shares is also one such example. There are certainly many areas where a similar situation can arise for which the proposed multilevel scheme provides a means of solution.

5.6 Summary

This chapter presents a quantum version of threshold cryptography based on multi-photon approach. This approach has advantages over single-photon approach in the sense of experimental implementation. The level of security is better than that provided by classical threshold schemes because of the use of quantum states for actual communication between parties. The advantage of this approach is: although the secret is classical, the shares are in quantum states, which cannot be copied and hence can be reused even if needed. The approach of threshold cryptography without trusted dealer is a good practical approach that can be implemented in practice.

Chapter 6: Toward secured global communication

Quantum communication has developed with notable progression in devices, techniques, and implementation. This pace of progression is likely to be maintained, if not increased, in the near future. Hence it will be prudent to look into the possibility of securing a network with a quantum approach. In this chapter, we propose a quantum key distribution (QKD) network underlying the existing communication network to secure global communication.

A QKD-network is an infrastructure for distributing the secret keys between nodes on a many-to-many basis over potentially unlimited distances. Under the assumption that the nodes can be trusted, it utilizes the information-theoretic security of QKD and achieves unconditional key distribution across the network. There have been a couple of experiments for developing a QKD-network based on the single photon-based protocols with limitations on distances as discussed later in the chapter. A team from BBN Technologies, Boston University, and Harvard University built and operated the first QKD network under the sponsorship of the Defense Advanced Research Projects Agency (DARPA) [100]. The network contains two nodes running the BBN QKD system protocols linked to the overall network by key relay. The network also contains two other nodes that are entanglement based. Another network developed in Vienna, Austria, is called SECOQC. The implementation strategy of the SECOQC is to use different types of QKD equipment to maximize the effectiveness of the experiment. The specific performance objective is to establish a QKD link that spans over 25 Km and operates at a rate higher than 1 Kbit/sec [101]. These implementations inspired to use multi-photon tolerant protocols with their advantages for designing global communication network.

This chapter explains the layered framework for QKD, the possibility of implementing QKD multicasting with satellites, and key management using threshold quantum cryptography.

6.1 Layered framework for quantum key distribution

We propose a layered framework inspired by existing optical backbone networks for the Internet. Currently, with single-photon QKD protocols, it is difficult to visualize a near future development in *quantum networks* because of special requirements of single photon-based sources and detectors. Also, the communication is point-to-point with distant limitations. Hence, we looked into the possibility of multi-photon-based protocols for *quantum secure* communication. The proposed layered framework consists of three layers—user layer, layer of secrets, and physical layer—as shown in Figure 19. The logical concept of actual operations is as follows: Upon the user's request to securely connect with another user, the encryption keys are transferred over a layer of secrets with the help of the physical layer. Then the user data in its encrypted form is transferred from User 1 to User 2. Now, the users can keep communicating over a secure channel; and incorporating the concept of braiding, the underlying keys on encryption can be updated at a particular interval to avoid any eavesdropping.

User Layer

Compared to a 7-layer Open Systems Interconnect (OSI) model, the *user layer* serves as an application layer. Through the proposed architecture, the user has a sense of security while using any form of communication without worrying about the protocols or devices used. The secured architecture will facilitate in further development of Internet communication[102].

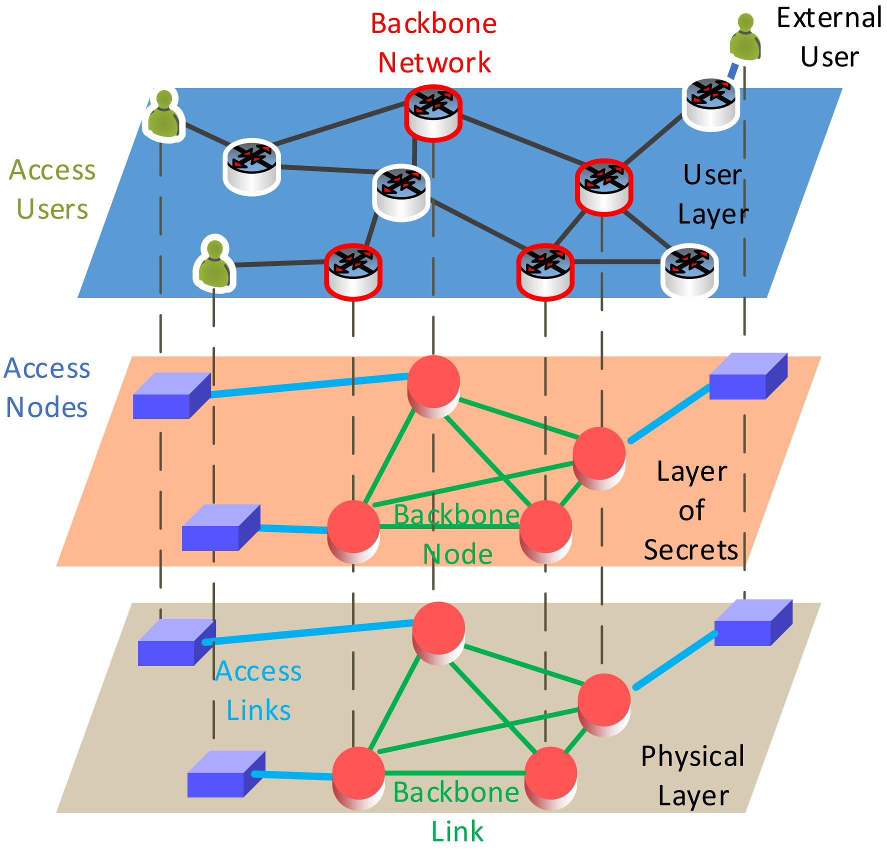

Figure 19 Layered architecture for distributing the secret keys [103]

Layer of Secrets

In current networking situations, data is carried in the form of encrypted packets of information through a gigantic unsecured optical network. Nodes on the networks are points where more than one optical link come together. Essentially, a communication between two nodes can be a single link or multiple links of point-to-point connections. Hence, quantum cryptographic protocol can work for the interconnection of nodes. However, because quantum protocols need to use very few photons, traffic may slow down, hence throughput may also be slow. Thus, we propose a separate layer, *layer of secrets*, for distributing the keys of encryption. The underlying idea is to build up a network for distributing secrets out of single point-to-point QKD-Links. The corresponding QKD-Link end points (i.e., the QKD devices) are situated in network nodes. Point-to-multipoint QKD-Links can be formed as described as multicasting later in this chapter. For operation of the QKD scheme on the *layer of secrets,* we propose a quantum protocol suite consisting of three parts: a) quantum protocols, b) optical process control, and c) optical transmission. The quantum protocol defines the multi-photon-tolerant protocols used in transmission, e.g., braided single-stage, three-stage, or Y00 protocol. The optical process control coordinates signals between the physical transmission and logical steps of the protocol. Optical transmission deals with carrying keys using photons on a FSO channel for satellite or fiber optics channel in case of ground communication. As the development happens in case of quantum cryptography, this protocol suite can be developed to correlate to an existing seven-layer architecture of the OSI model [104] as shown in Figure 20. There are prospects of standardization in the future related to using quantum protocol suite.

Physical Transmission Layer

This layer is comprised of an existing transmission network for carrying data around the globe. All communication between fixed points will take place over fiber optics. A second world of untethered radio and infrared communication involving portable devices will be working from this backbone infrastructure. Fiber optics provides high throughput and largest capacity for carrying the data as radio frequencies provide mobility. With the development in optical technology, we can envision all optical networks with very few delays and huge data capacity.

The layered architecture explains how keys can be transferred over network. Further, the question of managing the key and possibility of multicasting using the multi-photon approach is explained in the following section.

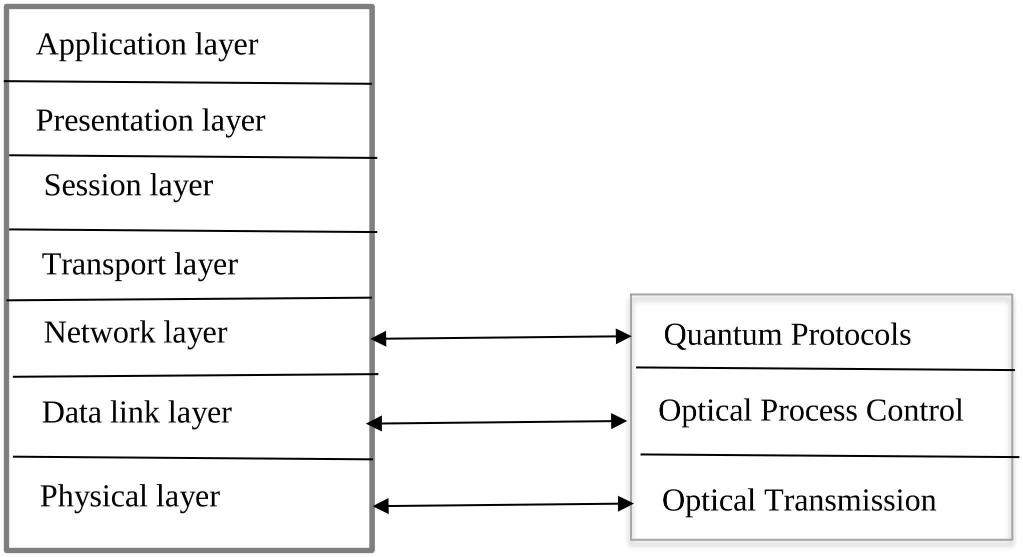

Figure 20 Resemblance of proposed quantum suite with OSI layers

Key management and multicasting communications Key Management:

Multicast communication is an efficient means of transmitting information over the Internet such as audio and video conferencing, computer–supported, co-operative work (CSCW), distributed databases, video and audio distribution, e-learning, and broadcasting stock quotes. Applying security for a multicast network is challenging due to the huge number of users over a network that can participate or leave dynamically. Hence, it is important to manage the keys over networks [105]. Another requirement for designing a secure, scalable key management procedure is to implement an access control mechanism to guarantee that only valid users can access the group communication content. The fundamental principle here is to allow the authorized entities to obtain valid keys. Hence, we propose a hierarchy-based scalable framework supported by threshold quantum cryptography as explained in chapter 5.

The secure framework consists of a secure distribution tree composed of small subgroups arranged in a hierarchy and subgroups that are relatively independent. The members of the tree include the group security controller (GSC) that manages the top-level subgroups, and group security agent (GSA) that manages members in the group.

Forming a Group Request:

- When an end user wants to form a group, s/he will send a *Form a group request* to GSA. The GSA will validate all the parties that are forming a group.
- Once validation is completed, GSA will ping all the parties with a *join the group invitation* that will hold the shares for keys to generate the initial group key.
- GSA will monitor the shared keys and further act as a moderator to the ongoing session.

Join the Group Request:

- When a new member sends request to join the group or when parties in a group send a request to add a member to the ongoing session, GSA checks the database for valid IDs for the new member.
- GSA then sends a part (out of *n*) of group key to the new member and other shares (*n-1*) to already existing members.
- The new member requests other (*t-1*) members for their share. Upon validation, the existing members send their shares to the new member.

- The new member now has sufficient shares to generate the quantum key for that group.

Leaving the Group:

- Whenever a member leaves the group, GSA updates the number of members and the threshold number of members required to allow a join request.

Refresh or re-keying:

As soon as a member joins or leaves, the number of members changes, hence for future communications, the shares of the secret key changes. GSA will control this situation and send new keys for further communication. The advantage of using threshold quantum cryptography in this case is that no one person has full access to the key used for encryption except GSA. Hence there will not be eavesdropping by a member who has left the group. Since the new member has to take permission from *t* out of *n* people in the group before joining, the chances of an unauthenticated user entering the group are reduced. Thus, in a quantum environment, the key can be managed over a multicast network. We further looked into technology for sending data to multiple user using quantum-based protocol.

Multicast Communication

Network topologies for satellite quantum communication can be a) point-to-point, b) point-to-multipoint (broadcast), or c) multi-point to multi-point (multicast). Here, we explain different methods with which multi-photon tolerant quantum protocols like three-stage or braided single-stage can be implemented for the multipoint-to-multipoint scenario.

Method 1: Choosing different basis for encoding

For different users, a sender can choose a different pair of basis to convey the information in a secured manner, i.e., user 1 gets data encrypted with horizontal or vertical polarization pair of basis whereas user 2 gets data with diagonal or antidiagonal polarization pair of basis. The details about the selected basis are kept with GSA and the end user only. Hence, only the user with accurate basis information is able to decrypt the information. The basis selection can be further made more complicated by moving from linear polarization to elliptic and circular polarizations, thus allowing the sender to communicate with multiple parties when s/he intends to.

Method 2: Choosing different wavelength

Considering the access through the FSO channel, a technique such as coarse wavelength division multiplexing (**CWDM**) in which multiple signals at various wavelengths can be used for transmission. For inter-satellite network implementation, there are different criteria used to choose the wavelength:

- Availability of compact, efficient and tunable laser source
- Adequate available peak power
- Adequate electrical to optical conversion and overall power consumption
- Detectors availability with sufficient sensitivity and noise level

A simple schematic of lab implementation of CWDM is shown in Figure 21. The wavelengths that we chose for lab implementation purposes are 670 nm and 632.8 nm.

The procedure for implementation to demonstrate coarse wavelength division multiplexing over FSO with multi-photon tolerant quantum communication protocol is the following. We considered a scenario where Alice is sending secured data to Bob and Charlie simultaneously using different frequencies. There can be more than one sender here who can be easily modified by adding an assembly of beam combiner and laser source.

1. The implementation set up uses frequency beam combiner to combine light from two different sources.
2. The light is then split into two beams with 50-50 intensity beam splitter such that one beam passes through an assembly of shutter and polarizer kept at 0° and another beam passes through a similar assembly of a shutter and 90° polarizer. Both beams are then combined and sent over the channel. Bits are encoded as 0 or 1 depending on the polarizer it passes through.
3. A set of LabView-controlled rotating half-wave plates are used for encrypting the data.
4. At the receiver end of Bob or Charlie, a frequency beam splitter splits the light beam into two parts that Bob's and Charlie's locations receive. There is a frequency filter kept at λ_1 at Bob's end and λ_2 at Charlie's end. The filter is followed by a detection assembly as discussed in the implementation of the braided single-stage protocol on FSO that is used for detection of bits.

In this way, we can demonstrate implementation of CWDM over FSO using lab components.

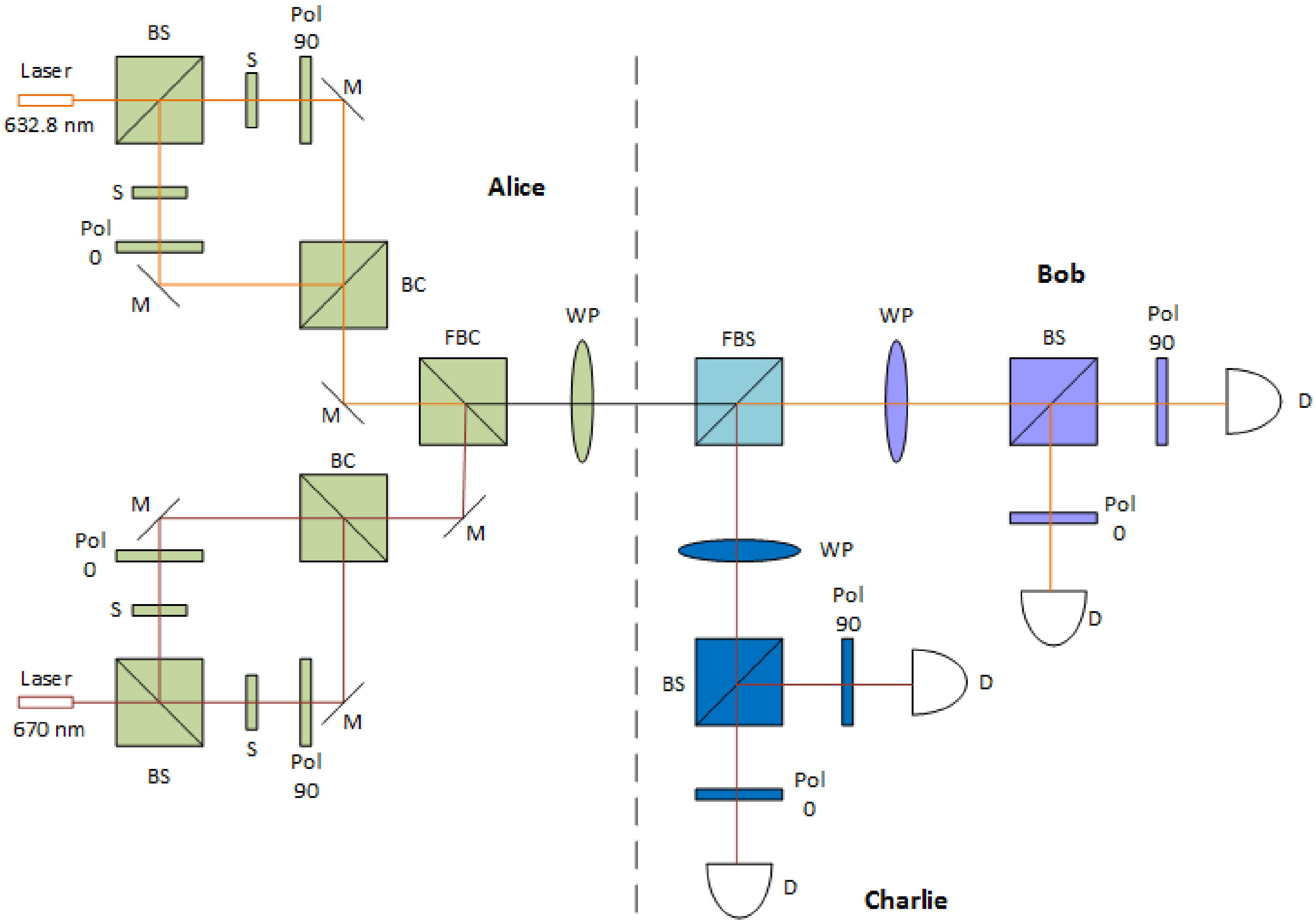

Figure 21 Proposed experimental set up for proof of concept of wavelength based multicasting

In Figure 21, BS is a beam splitter, M are mirrors, S is a shutter, Pol 90 is 90^0 polarizer, Pol 0 is 0^0 polarizer, WP are waveplates, FBC is a frequency beam combiner, FBS is a frequency beam splitter, and D are the detectors. Though lab implementation seems pretty simple and straightforward; for actual implementation on satellite network, there will be many considerations for choosing the appropriate source and respective antenna, the range of frequencies for communication, the performance of the detector in response to frequencies, and beam widening.

6.3 Global Quantum Key Distribution Network Using Satellites

For increasing the distances during the initial key transfer, we used satellite communication. The proposed global QKD system is a composite network consisting of space elements, i.e., satellite-to-satellite links; connect elements. i.e., ground-to-satellite links; and ground elements, i.e., optical node-to-node links.

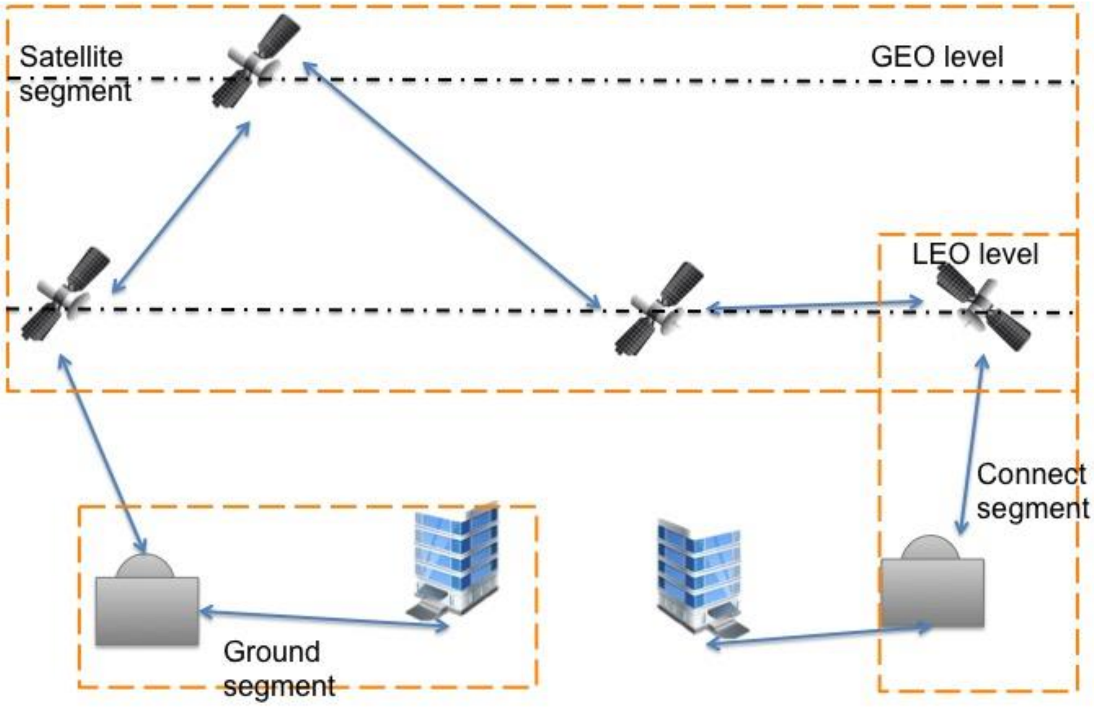

Figure 22 Segments of global network

Space segment:

The optical free-space link could provide a unique solution to the globe quantum communication since it allows in principle for larger propagation distances of photons due to its low absorption into the atmosphere in certain wavelength ranges. The types of links that we can consider are LEO-LEO links, LEO-GEO links and GEO-GEO links. Paper [78] studied the attenuation on these links and showed the feasibility of quantum communication. One of the challenges in satellite security is handling the multicast network for key distribution. The key management used was that explained in the earlier section of this paper.

Connect segment

This segment interconnects the space and ground segments via satellite–to-ground links. The development in free space optics technology has offered benefits of reaching the longer distances in satellite communications. Considering implementation of quantum communication network, single-photon-based protocols limit the distances that can be reached at LEO satellites; however, with proposed multi-photon approach, the heights of GEO can be achieved as shown in Chapter 4.

Space segment:

The optical free-space link could provide a unique solution to the globe quantum communication since they allow in principle for larger propagation distances of photons due to the low absorption of the atmosphere in certain wavelength ranges. The types of links that we can consider are LEO-LEO links, LEO-GEO links and GEO-GEO links. Paper [78] studies the attenuation on these links and shows the feasibility of quantum communication. One of the challenges in satellite security is handling the multicast network for key distribution. The key management is as explained in earlier section.

Connect segment

This segment interconnects the space and ground segments via satellite to ground links. The development in free space optics technology has offered benefits of reaching the longer distances in satellite communications. Considering implementation of quantum communication network, single-photon based protocols limits the distances that can be reached at LEO satellites however, with proposed multi-photon approach the heights of GEO can be achieved as shown in Chapter 4.

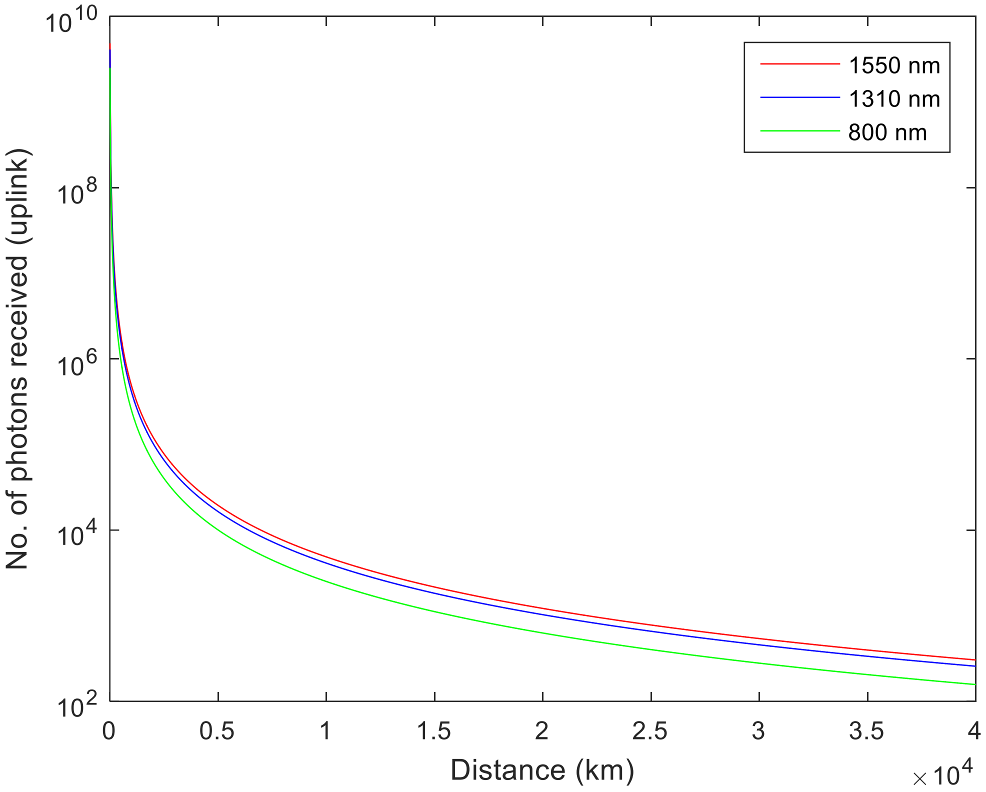

Figure 23: Relation between number of photons received as a function of distance in km and wavelength in nm

The figure shows the received number of photons at GEO satellite as a function of a wavelength used for the communication. It can be seen that the attenuation is higher during first 500 km of the link since during this time, the channel passes through earth's ionosphere experiencing higher losses. These losses are also due to the pollutant particles and clouds. The attenuation caused by these factors is found predominant on the uplink as compared to the downlink since in case of uplink, the transmitter itself is surrounded by these factors as against the downlink. Also, at a distance of 35,730 km where the GEO satellites revolve around the earth, received number of photons for wavelengths 1550 nm, 1310 nm, and 800 nm are found to be 381, 322, and 197 respectively, which are still sufficient to measure and get the required throughput of 1 Gbps on the uplink. It is general trend that, as the wavelength decreases; attenuation increases, which is again highlighted here in Figure 23. Approximately 1–2-m diameter ground telescopes are needed to receive the high-rate downlink from near earth distances such as LEO, MEO and GEO [106]. Near-infrared wavelength lasers at discrete wavelengths around 800, 1310, and 1550 nm can be used. The ground stations in this segment are usually located in remote areas from the city for avoiding the ambient light noise due to city lights.

By providing end-to-end encryption via ground to satellite links the current threats in satellite communication sabotaging the links with spoofing and hacking can be taken care. Also, use of optical frequencies eliminates signal jamming.

Ground segment

The ground segment consists of different ground stations interconnected in a communication network. The implementation of multi-photon-based protocol in optical fiber has been successfully demonstrated in [107]. The method of intrusion detection using polarization has been described in [108]. In addition to that, formation of quantum channel for transferring keys on OBS network was explained in chapter 3.

In this way the communication around the globe can be secured from device to ground station to satellite and from satellite back to ground station and then to other user device.

6.4 Summary

This chapter has provided a complete scenario for a secured global communication network with the multi-photon tolerant quantum protocols used for key distribution. The implementation details of each segment can be further studied and developed. The considerations for proposed design are authenticated nodes and the security of a multi-photon-tolerant protocol. The framework for QKD includes a separate layer of secrets for transferring keys from point–to-point or point-to-multipoint. We used the quantum threshold cryptography protocol for key management of in-group communication. For point-to-multipoint quantum key distribution, we used a multicasting method. This chapter proposes the lab experimental set up for multicasting. The final section explained the flow of keys from ground to satellite, over satellite relay and back to the ground. In this way, global secure communication is achieved.

Chapter 7: Conclusion and Future Work

This dissertation has investigated the potential of multi-photon tolerant protocols for secured global communication. This dissertation has proposed satellite-based network configuration and its operation that uses multi-photon tolerant protocols. The two main protocols discussed here are the three-stage protocol and its variant the braided single-stage protocol. Both the protocols have been implanted in lab successfully over FSO [42, 49] and in fiber [107]. The security aspects of the protocols have been studied in [44].

The proposed network configuration uses communication satellites at Lower Earth Orbits (LEO), Medium Earth Orbit (MEO) and Geostationary Earth Orbit (GEO) for carrying the keys at long distances. The reach of quantum key distribution to the heights of GEO by virtue of multi-photon tolerant protocols has been presented in this dissertation. This dissertation further proposes multicasting in QKD with two different methods first with different basis and second with different wavelength. In multicast communication managing the key for communication is a difficult task. This dissertation has proposed the concept of quantum threshold cryptography. The primary idea for threshold cryptography is that for encryption or decryption more than threshold number of users is required to agree upon mutual connection. This can be considered as a step towards multiparty quantum communication.

The dissertation has proposed domestic and global network configurations using satellites and fiber optic links that can form a composite system for carrying the information payload and distributing quantum-secure keys for encrypting information in transit. The layered network architecture for distributing quantum keys globally has been proposed. Also a quantum protocol suite based on the OSI 7 layered structure has been proposed in this dissertation.

For future work for this research, first of all there is room for standardizing the quantum cryptography protocols on network. A systematic protocol suite and packet distribution system or quantum communication can be looked in more details in future. There is lot of potential for research in quantum threshold cryptography. There is a need to bring this protocol in real world implementations. Quantum multicasting proposed in this dissertation seems like a simple concept but the future prospects of developing this area is very important from quantum network prospective.

Overall, this dissertation can be seen as stepping stone in developing a secure global network of future.

References

[1] S. Singh, *The code book: the science of secrecy from ancient Egypt to quantum cryptography*: Anchor, 2011.

[2] T. Kelly, "The myth of the skytale," *Cryptologia*, vol. 22, pp. 244-260, 1998.

[3] L. Accardi, Y. G. Lu, and I. Volovich, *Quantum theory and its stochastic limit*: Springer Science & Business Media, 2013.

[4] G. S. Vernam, "Cipher printing telegraph systems: For secret wire and radio telegraphic communications," *Journal of the AIEE,* vol. 45, pp. 109-115, 1926.

[5] C. E. Shannon, "Communication theory of secrecy systems*," *Bell system technical journal,* vol. 28, pp. 656-715, 1949.

[6] J. L. Massey, "Contemporary cryptology: an introduction," 1992.

[7] W. Diffie and M. Hellman, "New directions in cryptography," *IEEE transactions on Information Theory,* vol. 22, pp. 644-654, 1976.

[8] R. L. Rivest, A. Shamir, and L. Adleman, "A method for obtaining digital signatures and public-key cryptosystems," *Communications of the ACM,* vol. 21, pp. 120-126, 1978.

[9] S. Wiesner, "Conjugate coding," *ACM Sigact News,* vol. 15, pp. 78-88, 1983.

[10] V. Bužek and M. Hillery, "Quantum copying: Beyond the no-cloning theorem," *Physical Review A,* vol. 54, p. 1844, 1996.

[11] M. M. Wilde, "From classical to quantum Shannon theory," *arXiv preprint arXiv:1106.1445,* 2011.

[12] P. J. J. Binney, "Introduction to Quantum Mechanics, Probablity ampplitude and Quantum states," ed. Youtube: University of Oxford, Nov 2009.

[13] G. Brassard and C. Crépeau, "25 years of quantum cryptography," *ACM Sigact News*, vol. 27, pp. 13-24, 1996.

[14] I. quantique. Available: http://marketing.idquantique.com/acton/attachment/11868/f-00a0/1/-/-/-/-/Clavis%20QKD%20Datasheet.pdf

[15] M. technologies. Available: http://www.magiqtech.com/Products_files/QBox%20Datasheet-2011.pdf

[16] G. Zeng. (2010). *Quantum private communication*. Available: http://dx.doi.org/10.1007/978-3-642-03296-7

[17] S. Song and C. Wang, "Recent development in quantum communication," *Chinese Science Bulletin*, vol. 57, pp. 4694-4700, 2012.

[18] M. Hillery, V. Bužek, and A. Berthiaume, "Quantum secret sharing," *Physical Review A*, vol. 59, p. 1829, 1999.

[19] D. Gottesman and I. L. Chuang, "Demonstrating the viability of universal quantum computation using teleportation and single-qubit operations," *Nature*, vol. 402, pp. 390-393, 1999.

[20] A. J. Menezes, P. C. Van Oorschot, and S. A. Vanstone, *Handbook of applied cryptography*: CRC press, 1996.

[21] L. Lizama, J. M. Lopez, E. D. C. López, and S. E. Venegas-Andraca, "Enhancing Quantum Key Distribution (QKD) to address quantum hacking," *Procedia Technology*, vol. 3, pp. 80-88, 2012.

[22] M. Dušek, N. Lütkenhaus, and M. Hendrych, "Quantum cryptography," *Progress in Optics*, vol. 49, pp. 381-454, 2006.

[23] C. H. Bennett and G. Brassard, "Quantum cryptography: Public key distribution and coin tossing," in *Proceedings of IEEE International Conference on Computers, Systems and Signal Processing*, 1984, p. 8.

[24] P. W. Shor and J. Preskill, "Simple proof of security of the BB84 quantum key distribution protocol," *Physical review letters*, vol. 85, p. 441, 2000.

[25] S. Goldwater, "Quantum Cryptography and Privacy Amplification," ed, 1996.

[26] C. H. Bennett, G. Brassard, C. Crépeau, and U. M. Maurer, "Generalized privacy amplification," *Information Theory, IEEE Transactions on*, vol. 41, pp. 1915-1923, 1995.

[27] H. F. Chau, "Practical scheme to share a secret key through a quantum channel with a 27.6% bit error rate," *Physical Review A*, vol. 66, p. 060302, 2002.

[28] N. Gisin and S. Wolf, "Quantum cryptography on noisy channels: quantum versus classical key-agreement protocols," *Physical Review Letters*, vol. 83, p. 4200, 1999.

[29] D. Gottesman and H.-K. Lo, "Proof of security of quantum key distribution with two-way classical communications," *IEEE Transactions on Information Theory*, vol. 49, pp. 457-475, 2003.

[30] C. H. Bennett, F. Bessette, G. Brassard, L. Salvail, and J. Smolin, "Experimental quantum cryptography," *Journal of cryptology*, vol. 5, pp. 3-28, 1992.

[31] W.-Y. Hwang, "Quantum key distribution with high loss: Toward global secure communication," *Physical Review Letters*, vol. 91, p. 057901, 2003.

[32] V. Scarani, A. Acin, G. Ribordy, and N. Gisin, "Quantum cryptography protocols robust against photon number splitting attacks for weak laser pulse implementations," *Physical review letters*, vol. 92, p. 057901, 2004.

[33] C. H. Bennett, "Quantum cryptography using any two nonorthogonal states," *Physical Review Letters*, vol. 68, p. 3121, 1992.

[34] A. K. Ekert, "Quantum cryptography based on Bell's theorem," *Physical review letters*, vol. 67, p. 661, 1991.

[35] S. Cova, M. Ghioni, A. Lacaita, C. Samori, and F. Zappa, "Avalanche photodiodes and quenching circuits for single-photon detection," *Applied Optics*, vol. 35, pp. 1956-1976, 1996/04/20 1996.

[36] S. Bahrani, M. Razavi, and J. A. Salehi, "Orthogonal frequency-division multiplexed quantum key distribution," *Journal of Lightwave Technology*, vol. 33, pp. 4687-4698, 2015.

[37] E. Diamanti, H.-K. Lo, B. Qi, and Z. Yuan, "Practical challenges in quantum key distribution," *arXiv preprint arXiv:1606.05853*, 2016.

[38] K. Patel, J. Dynes, M. Lucamarini, I. Choi, A. Sharpe, Z. Yuan*, et al.*, "Quantum key distribution for 10 Gb/s dense wavelength division multiplexing networks," *Applied Physics Letters*, vol. 104, p. 051123, 2014.

[39] I. Choi, Y. R. Zhou, J. F. Dynes, Z. Yuan, A. Klar, A. Sharpe, *et al.*, "Field trial of a quantum secured 10 Gb/s DWDM transmission system over a single installed fiber," *Optics express*, vol. 22, pp. 23121-23128, 2014.

[40] L. Lydersen, C. Wiechers, C. Wittmann, D. Elser, J. Skaar, and V. Makarov, "Hacking commercial quantum cryptography systems by tailored bright illumination," *Nature photonics*, vol. 4, pp. 686-689, 2010.

[41] N. Jain, E. Anisimova, I. Khan, V. Makarov, C. Marquardt, and G. Leuchs, "Trojan-horse attacks threaten the security of practical quantum cryptography," *New Journal of Physics*, vol. 16, p. 123030, 2014.

[42] Y. Chen, S. Kak, P. K. Verma, G. Macdonald, M. El Rifai, and N. Punekar, "Multi-photon tolerant secure quantum communication—From theory to practice," in *Communications (ICC), 2013 IEEE International Conference on*, 2013, pp. 2111-2116.

[43] S. Kak, "A three-stage quantum cryptography protocol," *Foundations of Physics Letters*, vol. 19, pp. 293-296, 2006.

[44] M. El Rifai, "QUANTUM SECURE COMMUNICATION USING POLARIZATION HOPPING MULTI-STAGE PROTOCOLS," 2016.

[45] O. Hirota, M. Sohma, M. Fuse, and K. Kato, "Quantum stream cipher by the Yuen 2000 protocol: Design and experiment by an intensity-modulation scheme," *Physical Review A*, vol. 72, p. 022335, 2005.

[46] O. Hirota, "Practical security analysis of a quantum stream cipher by the Yuen 2000 protocol," *Physical Review A*, vol. 76, p. 032307, 2007.

[47] K. W. C. Chan, M. El Rifai, P. Verma, S. Kak, and Y. Chen, "SECURITY ANALYSIS OF THE MULTI-PHOTON THREE-STAGE QUANTUM KEY DISTRIBUTION."

[48] B. Schneier, "Quantum cryptography: As awesome as it is pointless," *Wired (October 2008),* 2008.

[49] B. Darunkar and P. Verma, "The braided single-stage protocol for quantum secure communication," in *SPIE Sensing Technology+ Applications*, 2014, pp. 912308-912308-8.

[50] E. Collett, *Polarized light in fiber optics*: SPIE Press, 2003.

[51] J. H. Thomas, "Variations on Kak's Three Stage Quantum Cryptography Protocol," *arXiv preprint arXiv:0706.2888*, 2007.

[52] P. Verma, B. Darunkar, and N. Punekar, "Optical cryptography systems and methods," ed: Google Patents, 2014.

[53] G. R. Fowles, *Introduction to modern optics*, 2d ed. New York: Holt, Rinehart and Winston, 1975.

[54] S. Chandrasekhar, *Selected Papers, Volume 3: Stochastic, Statistical, and Hydromagnetic Problems in Physics and Astronomy* vol. 3: University of Chicago Press, 1989.

[55] S. Chandrasekhar, *Radiative transfer*: Dover publications, 1960.

[56] E. Collett, "Field guide to polarization," 2005.

[57] S. Mandal, G. Macdonald, M. E. Rifai, N. Punekar, F. Zamani, Y. Chen, *et al.*, "Implementation of Secure Quantum Protocol using Multiple Photons for Communication," *arXiv preprint arXiv:1208.6198,* 2012.

[58] ThorLabs. *Beam Shutters*. Available: http://www.thorlabs.com/newgrouppage9.cfm?objectgroup_id=927

[59] M. El Rifai, N. Punekar, and P. K. Verma, "Implementation of an m-ary three-stage quantum cryptography protocol," in *SPIE Optical Engineering+ Applications*, 2013, pp. 88750S-88750S-13.

[60] T. Battestilli and H. Perros, "An introduction to optical burst switching," *Communications Magazine, IEEE,* vol. 41, pp. S10-S15, 2003.

[61] Y. Chen, C. Qiao, and X. Yu, "Optical burst switching: a new area in optical networking research," *Network, IEEE,* vol. 18, pp. 16-23, 2004.

[62] M. A. Raza, W. Mahmood, and A. Ali, "Hybrid control and reservation architecture for multidomain burst switched network," *Journal of Lightwave Technology,* vol. 26, pp. 2013-2028, 2008.

[63] C. Qiao and M. Yoo, "Optical burst switching (OBS)-a new paradigm for an optical Internet," *Journal of high speed networks,* vol. 8, p. 69, 1999.

[64] Y. Chen, P. K. Verma, and S. Kak, "Embedded security framework for integrated classical and quantum cryptography services in optical burst switching networks," *Security and Communication Networks,* vol. 2, pp. 546-554, 2009.

[65] C. Yuhua and P. K. Verma, "Secure Optical Burst Switching: Framework and Research Directions," *Communications Magazine, IEEE,* vol. 46, pp. 40-45, 2008.

[66] N. Gisin and R. Thew, "Quantum communication," *Nature Photonics,* vol. 1, pp. 165-171, 2007.

[67] H. Hemmati, *Deep space optical communications* vol. 11: John Wiley & Sons, 2006.

[68] D. J. Rogers, "Broadband Quantum Cryptography," *Synthesis Lectures on Quantum Computing*, vol. 2, pp. 1-97, 2010.

[69] N. Gisin, G. Ribordy, and H. Zbinden, "Quantum cryptography," *arXiv preprint quant-ph/0101098,* 2001.

[70] D. G. Aviv, *Laser Space Communications*: Artech House Publishers, 2006.

[71] H. Hamid, "Introduction," in *Near-Earth Laser Communications*, ed: CRC Press, 2009.

[72] R. H. Czichy, Z. Sodnik, and B. Furch, "Design of an optical ground station for in-orbit checkout of free-space laser communication payloads," in *Photonics West'95*, 1995, pp. 26-37.

[73] B. Patnaik and P. K. Sahu, "Inter-satellite optical wireless communication system design and simulation," *Communications, IET,* vol. 6, pp. 2561-2567, 2012.

[74] N. J. Cornish. [Online]. Available: http://map.gsfc.nasa.gov/mission/observatory_l2.html

[75] H. Hemmati, A. Biswas, and I. B. Djordjevic, "Deep-space optical communications: future perspectives and applications," *Proceedings of the IEEE*, vol. 99, pp. 2020-2039, 2011.

[76] B. Smutny, R. Lange, H. Kämpfner, D. Dallmann, G. Mühlnikel, M. Reinhardt, *et al.*, "In-orbit verification of optical inter-satellite communication links based on homodyne BPSK," in *Lasers and Applications in Science and Engineering*, 2008, pp. 687702-687702-6.

[77] G. S. Wojcik, H. L. Szymczak, R. J. Alliss, R. P. Link, M. E. Craddock, and M. L. Mason, "Deep-space to ground laser communications in a cloudy world," in *Optics & Photonics 2005*, 2005, pp. 589203-589203-11.

[78] M. Aspelmeyer, T. Jennewein, M. Pfennigbauer, W. Leeb, and A. Zeilinger, "Long-distance quantum communication with entangled photons using satellites," *arXiv preprint quant-ph/0305105,* 2003.

[79] C. H. Bennett, C. A. Fuchs, and J. A. Smolin, "Entanglement-enhanced classical communication on a noisy quantum channel," in *Quantum Communication, Computing, and Measurement*, ed: Springer, 1997, pp. 79-88.

[80] H.-K. Lo, X. Ma, and K. Chen, "Decoy state quantum key distribution," *Physical Review Letters,* vol. 94, p. 230504, 2005.

[81] T. Schmitt-Manderbach, H. Weier, M. Fürst, R. Ursin, F. Tiefenbacher, T. Scheidl*, et al.*, "Experimental demonstration of free-space decoy-state quantum key distribution over 144 km," *Physical Review Letters,* vol. 98, p. 010504, 2007.

[82] P. Villoresi, T. Jennewein, F. Tamburini, M. Aspelmeyer, C. Bonato, R. Ursin*, et al.*, "Experimental verification of the feasibility of a quantum channel between space and Earth," *New Journal of Physics,* vol. 10, p. 033038, 2008.

[83] C.-Z. Peng, T. Yang, X.-H. Bao, J. Zhang, X.-M. Jin, F.-Y. Feng*, et al.*, "Experimental free-space distribution of entangled photon pairs over 13 km: towards satellite-based global quantum communication," *Physical review letters,* vol. 94, p. 150501, 2005.

[84] L. Moli-Sanchez, A. Rodriguez-Alonso, and G. Seco-Granados, "Performance analysis of quantum cryptography protocols in optical earth-satellite and intersatellite links," *Selected Areas in Communications, IEEE Journal on,* vol. 27, pp. 1582-1590, 2009.

[85] R. Kaltenbaek, M. Aspelmeyer, T. Jennewein, C. Brukner, A. Zeilinger, M. Pfennigbauer*, et al.*, "Proof-of-concept experiments for quantum physics in space," in *Optical Science and Technology, SPIE's 48th Annual Meeting*, 2004, pp. 252-268.

[86] C. Bonato, A. Tomaello, V. Da Deppo, G. Naletto, and P. Villoresi, "Feasibility of satellite quantum key distribution," *New Journal of Physics,* vol. 11, p. 045017, 2009.

[87] R. Walter, "Space Laser Communications: Systems, Technologies, and Applications."

[88] C. Bonato, M. Aspelmeyer, T. Jennewein, C. Pernechele, P. Villoresi, and A. Zeilinger, "Influence of satellite motion on polarization qubits in a Space-Earth quantum communication link," *Optics express*, vol. 14, pp. 10050-10059, 2006.

[89] C. Bonato, A. Tomaello, V. Da Deppo, G. Naletto, and P. Villoresi, "Study of the quantum channel between earth and space for satellite quantum communications," in *Personal Satellite Services*, ed: Springer, 2009, pp. 37-40.

[90] B. Darunkar, "The Braided Single-Stage Protocol and its Application in Quantum Communication," Master of science in Telecommunication Engineering, Telecommunication Engineering, University of Oklahoma, 2013.

[91] M. Toyoshima, H. Takenaka, Y. Shoji, Y. Takayama, Y. Koyama, and H. Kunimori, "Polarization measurements through space-to-ground atmospheric propagation paths by using a highly polarized laser source in space," *Optics express*, vol. 17, pp. 22333-22340, 2009.

[92] A. Shamir, "How to share a secret," *Communications of the ACM*, vol. 22, pp. 612-613, 1979.

[93] R. Cleve, D. Gottesman, and H.-K. Lo, "How to share a quantum secret," *Physical Review Letters*, vol. 83, p. 648, 1999.

[94] D. Gottesman, "Theory of quantum secret sharing," *Physical Review A*, vol. 61, p. 042311, 2000.

[95] A. Karlsson, M. Koashi, and N. Imoto, "Quantum entanglement for secret sharing and secret splitting," *Physical Review A*, vol. 59, p. 162, 1999.

[96] W. Tittel, H. Zbinden, and N. Gisin, "Experimental demonstration of quantum secret sharing," *Physical Review A*, vol. 63, p. 042301, 2001.

[97] L.-Y. Hsu, "Quantum secret-sharing protocol based on Grover’s algorithm," *Physical Review A*, vol. 68, p. 022306, 2003.

[98] Z.-J. Zhang, "Multiparty quantum secret sharing of secure direct communication," *Physics Letters A*, vol. 342, pp. 60-66, 2005.

[99] Y. Tokunaga, T. Okamoto, and N. Imoto, "Threshold quantum cryptography," *Physical Review A,* vol. 71, p. 012314, 2005.

[100] C. Elliott, A. Colvin, D. Pearson, O. Pikalo, J. Schlafer, and H. Yeh, "Current status of the DARPA quantum network," *arXiv preprint quant-ph/0503058,* 2005.

[101] A. Poppe, M. Peev, and O. Maurhart, "Outline of the SECOQC quantum-key-distribution network in Vienna," *International Journal of Quantum Information,* vol. 6, pp. 209-218, 2008.

[102] L. Atzori, A. Iera, and G. Morabito, "The internet of things: A survey," *Computer networks,* vol. 54, pp. 2787-2805, 2010.

[103] R. Alleaume, F. Roueff, O. Maurhart, and N. Lutkenhaus, "Architecture, security and topology of a global Quantum Key Distribution network," in *2006 Digest of the LEOS Summer Topical Meetings*, 2006, pp. 38-39.

[104] H. Zimmermann, "OSI reference model--The ISO model of architecture for open systems interconnection," *IEEE Transactions on communications,* vol. 28, pp. 425-432, 1980.

[105] S. Ali, O. Mahmoud, and A. A. Hasan, "Multicast network security using quantum key distribution (QKD)," in *Computer and Communication Engineering (ICCCE), 2012 International Conference on*, 2012, pp. 941-947.

[106] M. Toyoshima, T. Takahashi, K. Suzuki, S. Kimura, K. Takizawa, T. Kuri, *et al.,* "Results from phase-1, phase-2 and phase-3 Kirari optical communication demonstration experiments with the NICT optical ground station (KODEN)," in *24th International Communications Satellite Systems Conference of AIAA*, 2007.

[107] N. Punekar, B. Darunkar, and P. Verma, "Secured optical fiber communication using polarization restoration technique and channel characterization," in *Proc. of SPIE Vol*, 2016, pp. 97740F-1.

[108] G. G. MacDonald and J. J. Sluss Jr, "Method for polarization-based intrusion monitoring in fiberoptic links," ed: Google Patents, 2011.