UNIVERSITY OF OKLAHOMA

GRADUATE COLLEGE

QUANTUM SECURE COMMUNICATION USING POLARIZATION HOPPING MULTI-STAGE PROTOCOLS

A DISSERTATION

SUBMITTED TO THE GRADUATE FACULTY

in partial fulfillment of the requirements for the

Degree of

DOCTOR OF PHILOSOPHY

By

MAYSSAA EL RIFAI
Norman, Oklahoma
2016

QUANTUM SECURE COMMUNICATION USING POLARIZATION HOPPING MULTI-STAGE PROTOCOLS

A DISSERTATION APPROVED FOR THE
SCHOOL OF ELECTRICAL AND COMPUTER ENGINEERING

BY

_____
Dr. Pramode K. Verma, Chair

_____
Dr. Kam Wai Clifford Chan

_____
Dr. Subhash Kak

_____
Dr. Gregory Macdonald

_____
Dr. William O. Ray

_____
Dr. James J. Sluss, Jr.

To my beloved family, my husband, and my yet unborn baby girl

ACKNOWLEDGEMENTS

This dissertation appears in its current form due to the assistance and guidance of several people. I would, therefore, like to offer my sincere thanks to all of them. First of all, I would like to express my profound appreciation toward my advisor Dr. Pramode K. Verma, who encouraged and helped me throughout the process of research and writing of this dissertation.

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

Although this dissertation mainly presents the author's own work and ideas, it contains substantial contributions by Dr. Kam Wai Clifford Chan and Dr. Majed Khodr.

I would like to thank all my friends at The University of Oklahoma for surrounding me with their kindness and support. I would like to extend my thanks to Renee Wagenblatt, Assistant to the Director, Telecommunication Engineering Program. I would also like to thank Dr. Hope Harder for her dedicated work on editing and formatting this dissertation.

This research is supported in part by the National Science Foundation (NSF) under Grants 1117179.

This dissertation is dedicated to my beloved family: my dad Jihad, mom Maha, sisters Rihab and Riham, and my husband Samer. I cannot find words to express my appreciation to them for their unceasing encouragement and love.

TABLE OF CONTENTS

LIST OF FIGURES

LIST OF TABLES

ABSTRACT

This dissertation presents a study of the security and performance of a quantum communication system using multi-stage multi-photon tolerant protocols. Multi-stage protocols are a generalization of the three-stage protocol proposed in 2006 by Subhash Kak. Multi-stage protocols use "Polarization Hopping," which is the process of changing the polarization state at each stage of transmission. During the execution of a multi-stage protocol, the message transfer always starts by encoding a bit of information in a polarization state; for example, bit 0 is encoded using state $|0\rangle$ and bit 1 is encoded using state$|1\rangle$ whereas, on the channel, the state of polarization is given by $\alpha|0\rangle + \beta|1\rangle$. In the following α and β are restricted to the real numbers i.e., the polarization stays on the equator of the Poincare sphere. A transformation applied by one communicating party at a given stage will result in new values of α and β.

This dissertation analyzes the security of multi-stage, multi-photon tolerant protocols and proposes an upper bound on the average number of photons per pulse in the cases where Fock states and the cases where coherent states are used in the implementation of the three-stage protocol. The derived average number of photons is the maximum limit at which the three-stage protocol can operate at a quantum secure level while operating in a multi-photon domain. In addition, this dissertation studies the vulnerability of the multi-stage protocol to the Trojan horse attack, Photon Number splitting attack (PNS), Amplification attack, as well as the man-in-the middle attack. Moreover, this dissertation proposes a modified version of the multi-stage protocol. This modified version uses an initialization vector and implements a chaining mode between consecutive implementations of the protocol. The modified version is proposed in the

case of the three-stage protocol and named a key/message expansion four variables three-stage protocol. The proposed nomenclature is based on the fact that an additional variable is added to secure the three-stage protocol. The introduction of this additional variable has the potential to secure the multi-stage protocol in the multi-photon regime. It results in the eavesdropper having a set of simultaneous equations where the number of variables exceeds the number of equations.

The dissertation also addresses the performance of the multi-stage, multi-photon tolerant protocol. An average photon number of 1.5 photon/stage is used to calculate the maximum achievable distance and key transfer rates while using the single-stage protocol over fiber optic cables. We compute the increase in distance as well as data transfer rate while using the single-stage protocol. Channel losses as well as the detector losses are accounted for.

Finally, an application of the multi-stage protocol in IEEE 802.11 is proposed. This application provides wireless networks with a quantum-level of security. It proposes the integration of multi-stage protocols into the four-way handshake of IEEE 802.11.

Chapter I: Introduction

I. Cryptography

The multiple human needs and desires that demand privacy among two or more people in the midst of social life must inevitably lead to cryptography wherever men thrive and wherever they write.
-David Kahn

Cryptography is the art of secret writing. It is the field of applications that provide authentication, privacy, integrity, and confidentiality to users. Cryptography has performed an important role in the history of any society that depends on information [1]. An important subfield of cryptography is that of secure communication. This field aims at protecting any message transfer between communicating parties, such that no unauthorized party can access the content of a message in transit.

Cryptography is the process of transforming information into something incomprehensible for anyone other than the intended users. The process of transformation is referred to as encryption; the reverse process is referred to as decryption. The information or message to be encrypted is referred to as plaintext; after encryption this information is called a cipher text. Along the centuries, many methods to encode messages emerged always to be broken at a later point of time.

Cryptographic methods are divided into symmetric and asymmetric key cryptography. Symmetric key cryptography is based on one secret key shared between two communicating parties. This key is used to effect both encoding and decoding of the messages to be communicated. The first provably secure cipher, the one-time pad, is based on symmetric cryptography. It was proposed around 1920 by Gilbert Vernam [2, 3]. The one-time pad cipher is relatively simple to implement; 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. The first formal proof of the security of the one-time pad was completed in 1949 by Claude Shannon. 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 [4]. The condition limiting the reusability of the key in a one-time setup makes it impractical due to the need for a constant supply of large key material at both ends.

After mid-1970s, cryptography became more widespread and it was essentially used by people in everyday life. Furthermore, cryptography became a tool not only for encryption, but also for other tasks such as digital signatures and various forms of authentication.

Two major developments happened in that decade. The first was the release of a public standard of a symmetric cipher, Data Encryption Standard (DES). DES uses relatively short keys and it encrypts a large amount of data in a quick manner. Its original version is no longer considered secure; due to its limited key length of 56 bits, a dedicated hardware can crack it in less than 24 hours. Today in use are other symmetric ciphers that have longer keys. These symmetric ciphers are called Advanced Encryption Standards (AES)[5].

The second development is the introduction of asymmetric ciphers or public key cryptography. The idea of public key cryptography was discovered by Diffie and Hellman in [6]. Rivest, Shamir, and Adleman were the first to provide a public key cryptography implementation [7]. Public key cryptography is based on a pair of keys for each

communicating party, namely, a public key for encryption and another private one for decryption. The public and private keys are connected together through a trapdoor one-way function. In this case, the encryption function is a one-way operation that can be completed using the public key; however, decryption function is cumbersome unless the trapdoor is known, i.e., the private key. Besides encryption/decryption functionalities, public key cryptography allows signature on and authentication of a message.

Most of the modern systems rely on the usage of symmetric and asymmetric cryptography in tandem. Where public cryptography is the means for key distribution, distributed keys will be used in a symmetric key cipher to encode/decode messages. Thus, the security of these systems hinges on the existence of trapdoor one-way functions and on the strength of symmetric ciphers. Nevertheless, neither of these conditions has been formally proven. Particularly, the possibility of having a quantum computer along with highly efficient factorization algorithms cannot be neglected. Then, not only cryptographic techniques in use today become insecure but the techniques become secure retroactively, thus creating a high risk for all applications where data keeps its value for a long time.

Quantum physics has changed the landscape of cryptography in the last two decades. This has been done by introducing quantum cryptography; in other words, cryptosystems that are based on quantum physic laws to provide unconditionally secure data transfer. Quantum Cryptography (QC) is mainly used for key distribution and called Quantum Key Distribution (QKD). QC and QKD are discussed throughout the next section.

II. Quantum World

Anyone who is not shocked by quantum theory has not understood it.

-Niels Bohr

Quantum information theory was established in the beginning of the last century. Its fundamental concept relies on quantum bits, or qubits, for short. Classical physics cannot be used to describe the behavior of a quantum system. The unique and counter-intuitive aspects of quantum theory are exploited to the benefit of quantum cryptography. The fundamental concepts that quantum cryptography relies on are as follows:

Information gain vs. disturbance: This aspect of quantum physics forms "the engine that powers quantum cryptography" [8]. In the simplest QC implementations, the bits of a message are encoded using photon polarization. To gain any information about the polarization of these qubits, an intruder must observe them. In other words, an intruder should measure the state of the communicated qubit. Since the polarization states used are non-orthogonal, such a measurement is destructive and disturbs the qubit's state. This phenomenon is described by the Heisenberg uncertainty principle stating that some pairs of quantum properties are complementary in a way such that measuring one of them will necessarily disturb the other. Consequently, an eavesdropper tapping on the quantum channel can be noticed in a statistically detectable way. This fundamental concept does not apply to classical cryptography where a classical bit can be read while being transmitted. In classical cryptography the security of the transmission relies solely on the security of the encryption cipher used.

An unknown quantum state cannot be copied: This fact is formalized in the no-cloning theorem [9]. The no-cloning theorem states that the unknown state of a photon cannot be copied exactly and deterministically. It is worth noting that this fact constitutes

a major security feature in quantum cryptography. It is, however, unheard of in the classical information domain.

i. Polarization Concept

Photons are the most popular carrier of quantum key bits; they have an intrinsic property called polarization [10]. Most of the QKD protocols available so far utilize the polarization states of photons to realize the key distribution [11]. The concept of polarization and its importance in quantum cryptography will be described briefly.

Light is an electromagnetic wave that bounces back and forth as it propagates in a medium. This electromagnetic wave is composed of photons, and it can be described by an electric field and a magnetic field that are perpendicular and proportional to each other. Light waves exhibit the phenomenon of polarization. Considering the polarization state of light, one need to consider only one of its components, either the magnetic or the electric field, since they are correlated and the knowledge of one fulfills the knowledge of the other. Usually the electric field is considered when talking about a polarization state.

Light may be either polarized or un-polarized. According to the projection of the electric field vector on the plane perpendicular to the travel direction of the light, polarized light can be either linearly polarized, circularly polarized or anywhere between them called elliptically polarized, as shown in Figure 1.

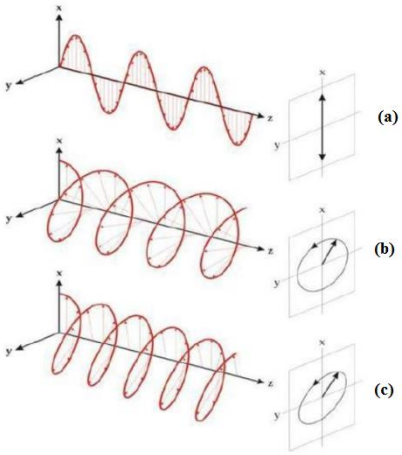


Figure 1: (a) Linear, (b) circular and (c) elliptical polarizations of light

The description of polarization of electromagnetic waves translate directly to that for a single photon. So choosing two linear orthogonal polarization axes, one can represent a vertically polarized photon by $|V\rangle$, and a horizontally polarized photon by $|H\rangle$. The general state is described by the Dirac notation,

$$|\psi\rangle = \alpha_V |V\rangle + \alpha_H |H\rangle$$

(Don't your equations need to be numbered in parentheses and positioned flush right?)

where α_V and α_H are the probability amplitudes and $|\alpha_V|^2+|\alpha_H|^2=1$ [12]. Thus, the state of the photon polarization is mathematically described by a vector of a unit length.

Any two orthogonal polarizations form a basis and the photon polarization can be expressed in terms of that basis. For example[12] , linearly polarized photons along the diagonals can be written as:

$$|D\rangle = \left|\frac{\pi}{4}\right\rangle = (|H\rangle + |V\rangle)/\sqrt{2}$$

$$|A\rangle = \left|\frac{-\pi}{4}\right\rangle = (|H\rangle - |V\rangle)/\sqrt{2}$$

In conventional quantum cryptography, we mainly use two bases: the (+) or rectilinear basis which is $\{|H\rangle, |V\rangle\}$ basis, and the (×) or diagonal basis which is $\{|D\rangle, |A\rangle\}$ basis.

Photons, individually, are completely polarized; their polarization state can be linear, circular or elliptical. Let us suppose that we want to prepare a stream of horizontally polarized photons by sending them through a horizontal polarizing filter. Furthermore, let us suppose that we want subsequently to measure the polarization of those photons by sending them through a second polarizing filter. We find that only when the measurement filter is in vertical position, no photons pass through it. For all the other orientations some photons will pass through it.

According to quantum physics laws, each photon in a stream has a certain probability to pass through the measurement filter. The probability is dependent on the orientation of the measurement filter and varies from 0 to1. Taking the same example as above when the light is horizontally polarized, each photon will have a probability 1 to pass through the measurement filter when it is in the horizontal position. This probability will decrease to $1/2$ at $\pi/4$ and 0 when the filter is vertically positioned[13].

ii. Quantum Cryptography

Quantum cryptography or quantum key distribution applies the fundamental laws of physics described earlier to guarantee unconditionally secure information transfer from a sender, Alice, to a receiver, Bob. It enables Alice and Bob to produce and share a random secret key that can be used later on for encryption and authentication functionalities. QKD promises unconditional security unlike its classical counterpart that relies on computational complexity and unproven assumptions. QKD first started with BB84 [14] . BB84 was proposed by Bennet and Brasard in 1984. They were the first to

realize that quantum states are meant to exchange information rather than storing it. The latter was first proposed by Stephen Wiesner in 1970. Wiesner proposed the idea of Quantum Money by designing bank notes and making them impossible to forge using quantum physics. That is done by assigning a series of isolated two-state quantum systems to each bank note in addition to its unique serial number[15]. An example is attaching to the bank note photons in one of four polarizations states: 0, $\frac{\pi}{4}$, $\frac{\pi}{2}$ and $\frac{2\pi}{3}$. Each of these is a two-state system in one of two bases: the rectilinear basis has states with polarizations at 0 and $\frac{\pi}{2}$ to the vertical and the diagonal basis has states at $\frac{\pi}{4}$ and $\frac{2\pi}{3}$ to the vertical.

At the bank, a record of all the polarizations and the corresponding serial numbers is present. The serial number is printed on the bank notes, meanwhile the polarizations states are kept secret. This means that the bank can always verify the polarizations without introducing any disturbance, whereas counterfeiter cannot without forging the bank note.

Later on several other protocols were proposed as alternatives to the BB84, such as B92 [16], the six-state protocol [17],BBM92 [18], and SARG04 [19]. QKD needs both a quantum channel as well as a classical channel. The quantum channel can be insecure; however, the classical one requires previous authentication. Unconditionally secure classical authentication schemes do exist and an example is Wegman-Carter authentication scheme [20, 21]. In addition, such schemes authenticate an initial key or message between Alice and Bob. QKD is referred to as key expansion protocols, which is an impossible task in the case of classical cryptography. Thus, QKD provides a solution to a problem not solvable using classical means.

The steps of the most widely known QKD protocol are as follows:

1. Alice randomly chooses one of two polarization bases to encode her bits. The bases are × or + . In other words she can choose one of two non-orthogonal states to encode each bit with. Bit 0 can be encoded with either 0 or $\frac{\pi}{4}$ polarization, whereas bit 1 can be encoded using $\frac{\pi}{2}$ or $\frac{3\pi}{4}$ polarization. After encoding Alice sends the qubit to Bob through the quantum channel.
2. Bob randomly chooses the × or + basis to measure the received qubit. Bob keeps his measurement result secret.
3. On the classical channel, Alice and Bob compare the basis they choose for encoding and measuring the exchanged qubits. This step is called reconciliation; during it half of the bits are discarded.
4. Alice and Bob implement error correction and privacy amplification to extract the final key.

iii. An Eavesdropping Example

A simple example of eavesdropping is the case where an intercept and resend attack is carried on by Eve. In this attack Eve does the exact same process done at Bob's side; she intercepts the photon coming from Alice, measures it in either + or × basis. At this point, Eve can either resend the same photon to Bob which is only possible in the case where she does her measurement in the same basis that Alice did the encoding at her side. In this case, Eve has the exact same information that Alice encoded. However, if she chooses a basis different than the one Alice prepared the state with, her result will be uncorrelated with that of Alice's. Moreover, Eve would have modified the state in such a way even if Bob uses the same basis as Alice, half of the times he will get a wrong result. Over a long keys length this attack will give Eve information on half of the bits of the

key while introducing a quantum bit error rate $Q = 0.25$. The QBER introduced by Eve makes her presence noticeable by both Alice and Bob.

iv. Unconditional Security and Its Conditions

The main reason behind the need of QKD is the fact that it can achieve unconditional security. In other words, the security of a QKD protocol can be proved without posing any constraint on the eavesdropping techniques available to Eve. QKD is said to be capable of achieving unconditional security due to its quantum physics roots. An eavesdropper, Eve, must interact with the quantum system in order to gain information about the transmitted state. Such interactions can be quantitatively measured. For instance, when Alice uses randomly chosen non-orthogonal states to encode the transmitted message, Eve's intervention will certainly modify the encoded state resulting in errors observable at both Alice's and Bob's sides. Such errors place the computation of a limit on Eve's information about the encoded state.

At this point one should mention that the term unconditional security is different from absolute security; security in its absolute sense does not exist. In reality, unconditional security claimed in QKD exists only under certain conditions. The compulsory requirements for unconditionally secure QKD are as follows [22] :

1. An eavesdropper, Eve, cannot intrude Alice's and Bob's devices. In addition, he/she cannot tamper with their setting choices, such as the basis choice.
2. The random number generator much be fully trusted by Alice and Bob. This generator is used to select the state to be sent at Alice's side and the measurement basis choice at Bob's side.

3. Unconditionally secure authentication protocols [20, 21, 23] must be used to authenticate the classical channel.
4. An eavesdropper has to obey the law of quantum physics. In other words, the security of the QKD protocols is based on a restricted set of quantum physics laws.

The failure of these requirements would compromise the security of a QKD protocol. However, it must be noted that the stated conditions only promise theoretical security; unconditional security is not guaranteed at the implementation level. For an implementation to be unconditionally secure, the theoretically described quantum states should match the signals that will be exchanged in reality. In addition, the implementation must be free of any unwanted information leakage.

v. Limitations of quantum key distribution

The notion of key distribution using quantum states is a significant development in the field of security. It is the only way of securing communication in the era of quantum computers. However, this impressive field of science is still in its immature phase and has several restrictions. The limitations associated with a system implementing the BB84 QKD protocol can be described as follows:

1. Photon Sources:

   The security of current implementations of QKD using BB84 is bound to single photon states. In other words, it is essential that Alice generates single photon states. Otherwise, in case states having more than a single photon are generated, an eavesdropper will be able to launch a photon number splitting attack (PNS). During a PNS attack, the eavesdropper will have access to the additional photon/s

generated by Alice and will analyze them and get the information he/she needs. Such an attack will go undetected.

Current implementations use faint laser pulses since it turns out achieving single photon sources is difficult. Therefore, most time slots will be empty, a few would have single photons and very few more than a single photon.

2. Distance of Communication:

   Due to detector noise and fiber losses, the range of current quantum key distribution systems is limited to 60-100 Km [24-26].In addition, this limitation can be associated with the fact that BB84 and its variants are single photon based protocols with average number of photons per pulse much less than 1.

3. Data Rates

   In today's fiber optic communication systems transmission rates on the order of Gigabits are easily attainable, but that is not the case with QKD. This is due to the limitation of no more than a single photon per pulse causing a large number of empty pulses, as well as the sifting process that truncates half of the possible key. This sets a limit in the use of QKD in conjunction with the one-time pad protocol to all but the most confidential transmissions. However, implementing QKD with AES or any other symmetric cipher is possible and can offer great improvement to the security of any system.

4. Security

   Despite the fact that QKD's unconditional security has been proven, any implementation will be susceptible to attacks at the device level. Nevertheless, a

security breach caused by a flaw in a device can be, in general, easier to deal with compared to a huge breakdown due to unproven mathematical assumptions.

III. Scope and Contributions of the Dissertation

The specific aim of this dissertation is to address the limitations associated with the current practice of QKD. As discussed earlier, BB84 and its variants are based on single photons to provide unconditionally secure communication. This dissertation presents the novel notion of multi-photon tolerant protocols, where an unconditional quantum secure key or message transfer can be established without the need for single photon based protocols.

Multi-photon tolerant protocols use what we call polarization hopping (described in the next chapters) to secure transfer data. Multi-photon tolerant protocols introduced in this dissertation are multi-stage protocols with m denoting the number of stages used for communication.

A version of the multi-photon tolerant multi-stage protocols using an initialization vector as well as chaining mode of operation is proposed. A laboratory implementation of this version of multi-stage protocols using half wave plates is presented. This implementation uses the case where $m = 3$.

This dissertation sets the physical limit at which a multi-stage, multi-photon tolerant protocol can operate in the quantum secure area. This limit is the average number of photons that can be used by Alice and Bob. The average number of photons is calculated for the cases where Alice and Bob use Fock states as well as coherent states discussed in Chapters 4 and 5. An increase in the average number of photons is realized

as compared to the BB84 protocol where the average number of photons per pulse used is $0.1 - 0.6$.

This dissertation uses the average number of photons associated with the multi-photon tolerant protocols in order to evaluate their performance Fiber Optics (FO). In addition, this dissertation proposes an application of the multi-stage protocols in the IEEE 802.11 standard.

IV. Organization of the Dissertation

This dissertation aims to address a few of the disadvantages associated with current QKD implementations. It first starts (Chapter 2) with a background on the some of the currently used QKD protocols along with their disadvantages. In addition, Chapter 2 introduces the concept of QKD networks along with descriptions of a couple of practical implementations.

The rest of this dissertation consists of three main parts. The first part (Chapter 3) deals with the concept of the multi-stage protocol. It mainly describes the three-stage protocol where $m = 3$. The details of its operation as well as its implementation are discussed. The implementation provided is an Free Space Optics laboratory implementation using half wave plates. The analytical reasoning behind the usage of the half wave plates at particular angles is provided using Mueller matrices. In addition, this part presents the three-stage protocol using an initialization vector and chaining mode to provide an extra layer of security. We call this version of the three-stage protocol the four-variable three-stage protocol. An FSO laboratory implementation of the four-variable three-stage protocol is proposed as well.

The second part of this dissertation (Chapters 4 and 5) addresses the limit on the average number of photons at which the multi-photon tolerant protocol provides quantum level security. The main basis of this work is the fact that a measurement an eavesdropper applies on a quantum state will result in an unavoidable quantum noise at the receiving end of the channel. The cases where Fock states as well as coherent states used are addressed in the context of Photon number splitting attack, Trojan horse attack, Man-in-the-middle attack and Amplification attack. It is proven that an increased average number of photons can be achieved while attaining quantum- security. In addition, in Chapter 4 a comparison between an implementation of the BB84 protocol with that of a multi-stage protocol is presented.

The third part of this dissertation (Chapters 6) provides a theoretical comparison of the performance of a multi-stage protocol where $m = 1$ with that of the BB84 protocol using FO communications (Chapter 6). An increase in the distance as well as the key generation rate is computed and presented.

Chapter 7, proposes an application of the multi-photon multi-stage protocol in the field of wireless communication. The multi-stage protocol is introduced as a means of key distribution in the IEEE 802.11 wireless standard.

Chapter 2: Quantum Key Distribution

Quantum communication is considered as the natural continuation of classical communication in the era of emerging quantum technologies. Quantum communication offers the promise of virtually unbreakable encryption; in other words, unconditional security. As discussed in Chapter 1, the main application of Quantum Key Distribution is in the field of quantum cryptography. QKD was first proposed by Bennett and Brassard in 1984; they were the first to discover that quantum states are meant to transfer information rather than store it.

The main focus of this chapter is to address three essential points in the quantum communication world. First is the discussion of a few quantum key distribution protocols proposed so far. Second is the discussion of the disadvantages of these key distribution schemes. And the third is the notion of a quantum network and its realizations. First, the BB84 protocol is described in detail along with its implementation and vulnerabilities. B92 and SARG04 are the two variants of the BB84 protocol and are discussed in this chapter as well. Second, the disadvantages of QKD are discussed. Chapter 1 did shed light on a few of these disadvantages. This chapter will discuss them in further detail. The need for QKD is addressed along with the timing when such key distribution schemes will become desirable for deployment. Third, this chapter discusses the innate point-to-point nature of quantum communication links besides the type of quantum networks that can be generated using such links. Quantum networks can be split into three major types: quantum node networks, optical node networks, and trusted relay networks. This chapter discusses the BBN DARPA QKD network [27], as well as the SECOQC network [28].

I. Quantum Key Distribution Protocols

Quantum mechanics is the basis on which quantum key distribution protocols rely to transfer and share keys. In order for this to be translated into a working cryptographic key distribution protocol, a combination of quantum processing as well as classical procedures is needed. Quantum key distribution protocols are usually subdivided into three main stages: raw key exchange, key sifting, and key distillation.

The raw key exchange is the only quantum part in the overall quantum key distribution process. It is the only stage at which quantum states are transmitted between the communicating parties. Key sifting is the direct step following the raw key exchange; it is done over the classical channel in order to agree which bits to discard and which ones to keep. This is followed by the step of key distillation where error correction and privacy amplification are performed. This section addresses the details of the BB84 along with a brief discussion of B92, and SARG04.

i. BB84

This section discusses the BB84 protocol. As mentioned earlier, it was the first proposed quantum key distribution protocol; it has been described in detail [1, 29]. Several proofs have been developed in order to show that it is unconditionally secure [30-32]. The steps of key exchange and key sifting are done as follows and depicted in Figure 2:

1. Alice encodes each photon with its corresponding polarization state. Each bit of information can be encoded either in the rectilinear (0 or $\frac{\pi}{2}$) or diagonal ($\frac{\pi}{4}$ or $\frac{-\pi}{4}$) basis. For example, if Alice chooses to encode her bit 1 in the rectilinear basis,

she will polarize her photon to $\frac{\pi}{2}$. However, if she wants to encode it in the diagonal basis she will polarize her photon to $\frac{-\pi}{4}$.

2. It is worth noting that the choice of either the rectilinear or the diagonal basis has equal probability. At this point Alice can produce a stream of photons randomly polarized. The choice of the polarization basis is done using a trusted random number generator.
3. Alice sends the stream of polarized photons over the quantum channel to Bob. Bob at his side will detect them. The BB84 protocol is referred to as a Prepare and Measure protocol (P&M).
4. At this point Bob has to detect the received photons and measure the polarizations to be able to get the encoded bit. Since Bob does not know which basis has been used by Alice, he will set the measurement basis randomly using a trusted random generator as well. If he chooses the correct basis, he will record an accurate measurement. If not, the result will be random and will not match the one sent by Alice.
5. The key exchange stage is now completed. Now the key sifting stage will start. At this point, Alice and Bob discuss their bases. No key information can be gained by an eavesdropper since the keys are not discussed publicly. 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.

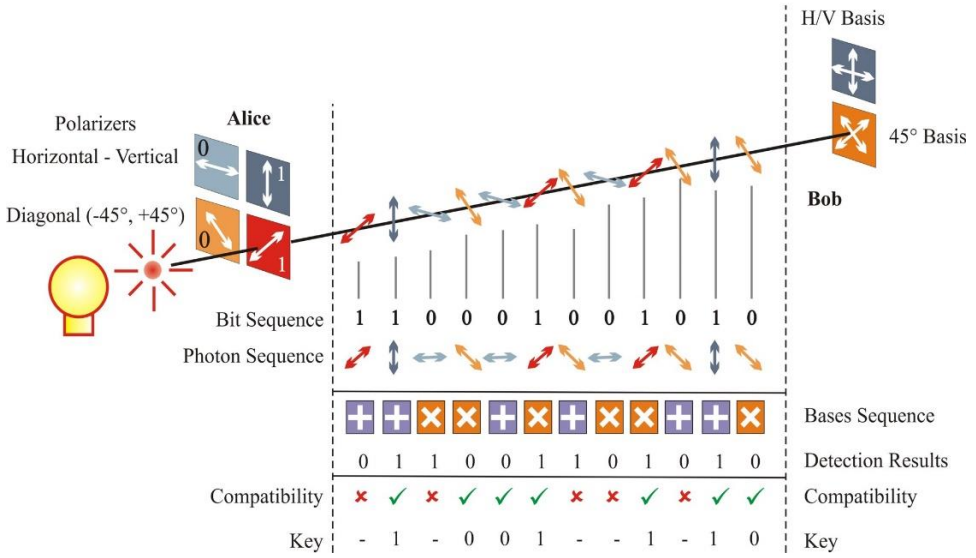


Figure 2: Alice and Bob using the BB84 protocol for raw key exchange and sifting. Source: [33]

Alice and Bob can identify the presence of an eavesdropper on the channel by calculating the QBER introduced over the channel. This has been explained in detail in Chapter 1. However, Table 1 shows how the presence of Eve on the quantum channel can be known.

Alice's random bit	0	1	1	0	1	0	0	1
Alice's random sending basis	+	+	×	+	×	×	×	+
Photon polarisation Alice sends	↑	→	↘	↑	↘	↗	↗	→
Eve's random measuring basis	+	×	+	+	×	+	×	+
Polarisation Eve measures and sends	↑	↗	→	↑	↘	→	↗	→
Bob's random measuring basis	+	×	×	×	+	×		+
Photon polarisation Bob measures	↑	↗	↗	↘	→	↗	↑	→
PUBLIC DISCUSSION OF BASIS	+							
Shared secret key	0		0			0		1
Errors in key	✓		✘			✓		✓

Table 1: BB84 exchange during the presence of an Eavesdropper

At this point, both Alice and Bob have in their possession a sifted key. They will start the step of key distillation; it is a one-way post-processing procedure consisting of two steps: error correction (EC) and privacy amplification (PA). During this procedure if the sender is the same as the one who sent the quantum states during the raw key exchange, one can speak of a direct reconciliation. Otherwise, the post-processing procedure is referred to as reverse reconciliation.

The error correction step is also called information reconciliation. During this step Alice and Bob will generate a corrected sifted key. The corrected sifted key is shorter than the raw key and has perfectly correlated bits. According to Claude Shannon, the mutual information given by $I(A:B) = H(A) + H(B) - H(AB)$ is the fraction of perfectly correlated keys that can be extracted from the partially correlated sifted keys. This means that the sender must reveal an amount of information at least as large as the uncertainty the receiver has on the sifted key in order to be able to extract the perfectly correlated keys.

The privacy amplification step is the second step of the post-processing procedure. The aim behind PA is to destroy any information Eve has on the sifted key. 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. PA was first addressed in [34]; however after the introduction of the notion of universally composable security [35, 36] it was replaced by a more general version [36]. 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:

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

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 portion can be significantly improved [37-39]. In addition, pre-processing has been introduced to improve these bounds. Pre-processing is a procedure that can be completed before post-processing, in order to increase the randomness of the data possessed by Alice and Bob. This procedure can be either one-way or two-way. By adding local randomness to the data shared between Alice and Bob, a decrease in the correlations between them can be seen. However, this procedure decreases Eve's information as well and can have an overall positive effect [40, 41]. Both pre-processing and two-way processing are relatively simple to implement and allows extraction of a fraction of the keys in regions where one-way post-processing fails.

Photon Number Splitting Attack

It might appear that Eve has no options for obtaining useful information from the key exchange without being detected. However, the BB84 protocol has several underlying assumptions about the operation of the protocol in addition to the conditions described in Chapter 1, Section *II. iv* regarding the capabilities of Alice, Bob, and Eve.

It is assumed that Alice has in her possession a perfect single-photon source capable of generating on demand polarized single photons. Practical implementations of BB84 use unreliable photon sources that cannot achieve this requirement. Weak coherent pulses are used in such implementations, they generate with a finite probability empty pulses, pulses with single photons, and pulses with multi-photons. Having pulses with more than a single photon is a major weakness in the implementation of the BB84. It gives Eve the opportunity to siphon off surplus photons and measure them. This attack is

known as the Photon Number Splitting Attack (PNS) and was first identified by Brassard et *al*. in 2000 [42].

During a PNS attack, Eve effects a quantum non-demolition measurement. After siphoning off the photon successfully, Eve will have to wait until the communication of the bases over the classical channel happens and then she can measure the siphoned photons with 100% accuracy. During this attack, Eve's presence will go unnoticed since it does not contribute to the QBER.

Counteracting PNS Attacks

To counteract a PNS attack the communicating parties can choose to use one of the following two methods:

Using reference pulses: In general reference pulses are signal pulses stronger than the message pulses sent at regular intervals by Alice [16]. Reference pulses contain multiple photons. In case reference pulses are used while Eve tries to launch a PNS attack, she will intercept a genuine single photon pulse or the reference pulse and record an error at Bob's side. Thus, using reference pulses the presence of Eve can be detected.

Using decoy states: Decoy pulses can be used to counter a PNS attack in the cases where the quantum channel is characterized with high losses. A noisy channel is the ideal condition for Eve to launch an extended photon number splitting attack [43].Decoy states were first proposed in [44].

ii. B92

The B92 protocol was introduced by Bennet in 1992 as a variant of the BB84 protocol [16]. The B92 results in a lower key efficiency than that of the BB84; however,

only half of the state preparation hardware is required. Compared to BB84, B92 has the following differences [45]:

1) B92 requires only two non-orthogonal states instead of the four required in BB84.
2) Alice on her side prepares a string of random bits A_i; she encodes the photons in two non- orthogonal states. Let us say bit 0 is encoded using $|H\rangle$ and bit 1 is encoded using $\left|\frac{\pi}{4}\right\rangle$. Alice now sends her photons to Bob.
3) On his side Bob prepares a random binary string B_i and chooses his measurement basis accordingly. For example, bit 0 represents the rectilinear basis and bit 1 represents the diagonal basis. Now Bob measures each quantum state received from Alice with the basis he chose.
4) Now if Bob detects $|H\rangle$ he will register bit 0; however, if he detects $\left|\frac{\pi}{4}\right\rangle$ he will register bit 1. These bits are registered in a string T_i; this string will be sent to Alice and only the bits where $T_i = 1$ are kept.

iii. SARG04

The SARG04 protocol was proposed in 2004 [19] as an alternative of the BB84 protocol. SARG04 can be considered as a generalization of the BB84 protocol using B92 to become more robust to the photon number splitting attack. In its original version SARG04 uses polarization states to transfer quantum bits from Alice to Bob; however, there exists a version of SARG04 which uses entangled photons[46].

Alice encodes her states in one of four non-orthogonal states and sends them to Bob. On his side, Bob selects one of two bases in order to measure them. Looking at the

operation of the protocol over the quantum channel, SARG04 operates in the same way as BB84. However, the fundamental difference between the two protocols lies in the key sifting process. During the sifting stage, Alice reveals the states she has used and one of the states that code to the other value of the bit. The second state revealed is not orthogonal to the first. If there are no errors in Bob's guessing, the sifting process will result in a key with a length equal to $^3/_4$ that of the raw key.

Now, let us consider the case where Eve carries out a PNS attack on a SARG04 setup. If she siphons off a photon she can only know that the state is in one of two non-orthogonal states, which is not the case with BB84 where she will gain full information after public key discussion. However, Eve's best bet is to perform measurements on three-photon pulses; in this case her success probability is limited to$^1/_2$.

The SARG04 protocol provides the same level of security as that of the BB84 only when perfect single-photon sources are available. In the cases where PNS attacks are a threat to BB84, SARRG04 provides a higher level of security compared to BB84. However, BB84's performance in a noisy environment is more efficient since at a given channel visibility the QBER of SARG04 is twice that of BB84.

II. Challenges to Quantum Key Distribution

As mentioned earlier, QKD is still in its immature phases. A mass of issues are restricting its appeal within the cryptography community. Some of the problems with QKD were discussed in Chapter 1; this section will discuss them in more detail along with a few additions.

i. Denial of Service

The point-to-point nature of the quantum channel results in it having unique characteristics. During quantum communication, Alice and Bob should be online and available at both ends of the communication channel equipped with sources and detectors in order for the exchange to take place. This is the opposite to the collection of connections of which the Internet is formed. The refined small world architecture of the Internet described in [47] allows distant regions to be connected. Using QKD only point-to-point communication is possible; this 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. This attack is at the heart of motivations to develop a quantum key distribution network.

ii. Photon sources and detectors

As discussed earlier, the quality of photon sources and detectors have a significant impact on the performance of the implementation of the QKD protocol. Less than perfect single photon sources in single-photon based protocols raise the vulnerability to PNS attacks. In addition, the detectors have several practical issues such as dark counts and dead time which can be exploited by an attacker. The criteria of ideal detectors are as follows [24]:

1. High efficiency over a large spectral range
2. Low dark counts probability
3. Constant time between detection of a photon and the corresponding electric signal
4. Small dead time after photon detection

Detectors are always different; a mismatch in the dead time of rectilinear and diagonal basis will always be present. Eve can observe this and control the arrival time of photons at Bob's side and give higher probability of a reading on one of Bob's detectors. She can then make a reasonable guess of the qubit sent [48]. In addition, Eve can always launch an attack on the implementation called the Trojan horse attack. During this procedure, she will shine a bright light into Bob's detector and analyze its backscattering. This process is called reflectometry [49].

iii. Losses in the Quantum Channel

Quantum properties are adversely affected by the distance that a pulse is traveling. Free-space optical channels incur losses on the quantum signal due to atmospheric as well as equipment dependent geometric losses. On the other hand, in fiber optics the pulses suffer from decoherence, chromatic dispersion, and polarization mode dispersion. This type of loss affects the quantum signal irreversibly. They introduce security weaknesses as well as limit the distance and rate of quantum communication.

iv. Security Proofs

Security proofs are not equal to proven security since all security poofs make major assumptions. Some of these assumptions are not realistic and cannot be accurately translated in implementation setup. Most significant assumptions are about Alice and Bob's capabilities [50]. These capabilities are idealized in some security proofs. Examples of these instances are provided in [22].

v. *Classical Authentication*

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. This means that the overall security of the QKD protocol can be reduced to only the security of the authentication algorithm used at the onset of the protocol. However the use of Carter Wegman algorithms [20, 21] give unconditionally secure authentication.

vi. *Side Channel Attacks*

The attack using this kind of inconsistency between the theoretical protocol and its hardware implementation is usually called side channel attacks. This type of attacks occurs when an eavesdropper can extract information from a cryptosystem indirectly. Since QKD is still in its immature phases, it did not have the chance to have rigorous research in this type of information leakage. An example of such instances in QKD is when photon detectors in the receiver are controlled by sending tailored optical pulses through the quantum channel. This was not considered to take place in the security proofs. Among various side channel attacks, those related to photon detectors are serious because they are usually common to most of the QKD schemes. An example is the blinding attack with bright light [51, 52] , the implementations of its countermeasures were reported [53, 54].

vii. *Key management*

To be effective, QKD must employ an overall key management scheme. This scheme should deal with key storage, maintenance, and destruction once the useful lifetime of the key is up. This is a challenging task especially when QKD is to be used

with a one-time pad scheme since key management is often difficult. This is due to the fact that the key should be the same at both the sending and receiving ends as well as the fact that it should be totally random and never reused. In addition, a classically authenticated channel for the implementation of a QKD protocol can itself present a challenge and an overhead.

Thus, key management is not only important but it is crucial for any cryptosystem to succeed. Key management is the hardest aspect of a system based on QKD since it should meet the organizational challenges to ensure that the key remains secure at any point of time in its life-cycle.

viii. Need for QKD Based Crypto-systems

One of the most important issues facing QKD is whether it is actually needed at all! Researchers have a range of different opinions. Some of them consider QKD as a solution looking for a problem with no existing or forthcoming use [55-57]; the rest regard QKD as the rescuer because cryptography as we know it is destined to fail [58].

Cryptography is the success story of the information security world. If it is properly implemented, it can enable sensitive information to be transmitted securely in an insecure environment. For practical purposes security as known today can prove to be an extremely strong defense mechanism. A system failure might be due to poor key management or human failure rather than due to a cryptographic scheme failing.

The promise of unconditional security through QKD can be ideal for certain applications e.g., banking. However, for it to have an industrial appeal, it must be directed into solving a business problem, save money and/or make a procedure more efficient.

Research and development continues to increase the efficiency of QKD algorithms as well as reduce the cost of the equipment needed for deployment of such technology.

Bruce Schneier states that “Security is a chain: it is as strong as its weakest link”[55].This is why he described QKD “as awesome as it is pointless” [55]. Strengthening the strongest link will prompt hackers to look somewhere else in the network for vulnerabilities. With this in mind, a QKD proponent’s claims should be analyzed carefully. The events that will influence the adoption of QKD are major points to be set. We summarize them as follows:

1. The event where current used cryptographic technics are considered ineffective and not secure enough.
2. The event where advances in mathematical techniques constitute a threat to currently used cryptographic techniques. This advancement mainly can address the speed of factoring large numbers.
3. The event where a fully functional quantum computer is practical and available for use.

Cryptographic techniques cannot be absolutely secure; this is the case with QKD as well. But QKD may be the way to provide the highest level of security. The main purpose of this dissertation is to provide a quantum level of security while efficiently addressing a few problems that current QKD protocols have. This is addressed in the next chapters; however, one can note that this dissertation also addresses the problem of the need of sifting, public channel, and the need of single photon pulses. All of these in turn affect the distances and data rates of the quantum transmission.

III. Quantum Networks

In its innate nature, QKD is a point-to-point key distribution technique. However, only a tiny fraction of all communication uses dedicated channels to insure safe information transfer. Most of the communication relies on networks where multiply interconnected users can operate and exchange information using a multitude of techniques and algorithms. In addition, the discussion of the disadvantages of QKD in Chapters 1 and 2 did shed light on a very important problem; that is the problem of the relatively short communication distance achieved by QKD. QKD implementations have what we call a "quadratic curse" [59], where a signal undergoes steep attenuation at a critical distance before totally disappearing as shown in Figure 3.

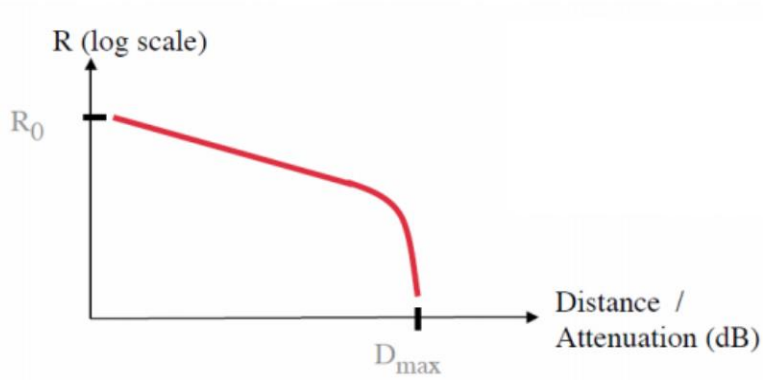


Figure 3:Point-to-point QKD link performance. Source:[60]

To be suitable for practical communication, QKD links should be part of an overall network. This solution will alleviate the point-to-point nature of QKD and improve the distance of the key transfer by having a cascaded nodes scheme. The design of such a network should take into consideration having enough redundancy to cope with single or multiple link failure while insuring any two nodes in the network can exchange keys with unconditional security. QKD networks where each link inhibits the same

unconditional level of security is the only way proponents of QKD can thrust aside the claims of their opponents described in Section *II.viii*. Currently, increased research has been devoted to design and implementing various QKD networks. Quantum networks are described through the rest of this section.

Quantum networks can be divided into three main types: quantum node networks, optical node networks, and trusted relay networks. Each of them has strengths and weaknesses; they are described in detail in [61].

i. Quantum Node Networks

Quantum nodes are used to combat the process of decoherence [62]. This phenomenon is typically the reason behind the degradation of the signal over a quantum channel. Since decoherence is a quantum phenomenon, it can only be fixed by using nodes which can perform active transformations on quantum signals. Such nodes are called quantum nodes; they all rely on entanglement. As explained in [63], a network consisting of quantum memories where each of them stores a share of multipartite entangled states can be used for quantum cryptography. According to them, the challenge of quantum nodes is in the distribution entangled states over long distances. The most elaborate quantum nodes proposed so far are quantum repeaters [64]. The authors of [64] use entangled photon sources along with quantum memories and purification of entanglement in order to achieve perfect entangled quantum states. These states are stored in nodes over quantum channel links. These links are chained using entanglement swapping.

ii. Optical Node Networks

Optical QKD nodes use classical optical processes on a quantum signal such as: beam splitting, multiplexing, de-multiplexing, switching, etc. These optical networking functionalities allow the creation of one to many QKD links. In other words, it permits going beyond 2-user QKD. One-to-many connectivity between four QKD devices is presented in [65] . With active optical switching, selective connection of any two QKD nodes with a direct quantum channel is allowed. The BBN DARPA quantum network [66, 67] is the first network to use the multi-user QKD feature. It has been deployed between Boston University, Harvard, and BBN. The optical nodes used in this type of network do not need to be trusted, since quantum signals are transmitted over a quantum channel with no disruption. An optical node QKD network model cannot be used as a way to extend the distance of key distribution. Undeniably, the extra optical losses introduced in the nodes will actually reduce the maximum length of quantum channels.

iii. Trusted Relay Networks

The QKD network types described above both have major disadvantages. Quantum node networks have the promise of increasing the distance; however, they are only achievable theoretically. On the other hand, the optical node networks are practically possible but they have an adverse effect on the maximum achievable distance. Trusted relay networks is the third type and it is somewhere in between the two types. Trusted relays use classical technology but a relay node is trusted implicitly to forward the quantum signal without tampering or eavesdropping.

Trusted relay QKD networks follow the following principle: local keys are generated over QKD links and then stored in nodes at both ends of each link. Global key

distribution is performed over a QKD path. One chain of trusted relays is connected by QKD links, as shown in Figure 4, to establish a connection between two end nodes. Hop-by-hop fashion along QKD paths is used to distribute secret keys. End-to-end security is guaranteed between the end nodes, given that the nodes in the middle can be trusted. Trusted relay networks can be used to build a long-distance QKD network.

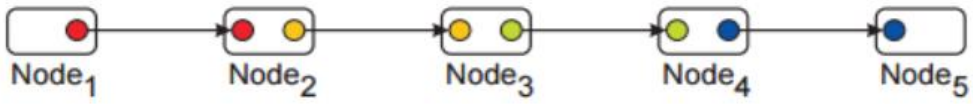


Figure 4:Hop by Hop QKD path. Source:[59]

IV. Practical QKD Networks Implementation

This section aims at describing a couple of QKD network implementations. The first implementation is that of BBN DARPA QKD network and the second is that of SECOQC network.

i. BBN DARPA QKD Network

As discussed earlier, the limitations associated with QKD can be mitigated by forming QKD networks to replace stand-alone QKD nodes. Therefore, 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) [68]. This network is referred to as DARPA Quantum Network; it became fully operational on October 23, 2003 in BBN's laboratories, and in June 2004 it was fielded through dark fiber under the roads of Cambridge, Massachusetts. It is the first metro-area QKD network in continuous operation.

As of December 2004, DARPA QKD network constituted of six QKD nodes. Four of these nodes are used at BBN and are weak-coherent QKD systems operating at 5-MHz pulse rate and are inter-connected using a photonic switch. The other two are built by the National Institute of Standards and Technology (NIST).

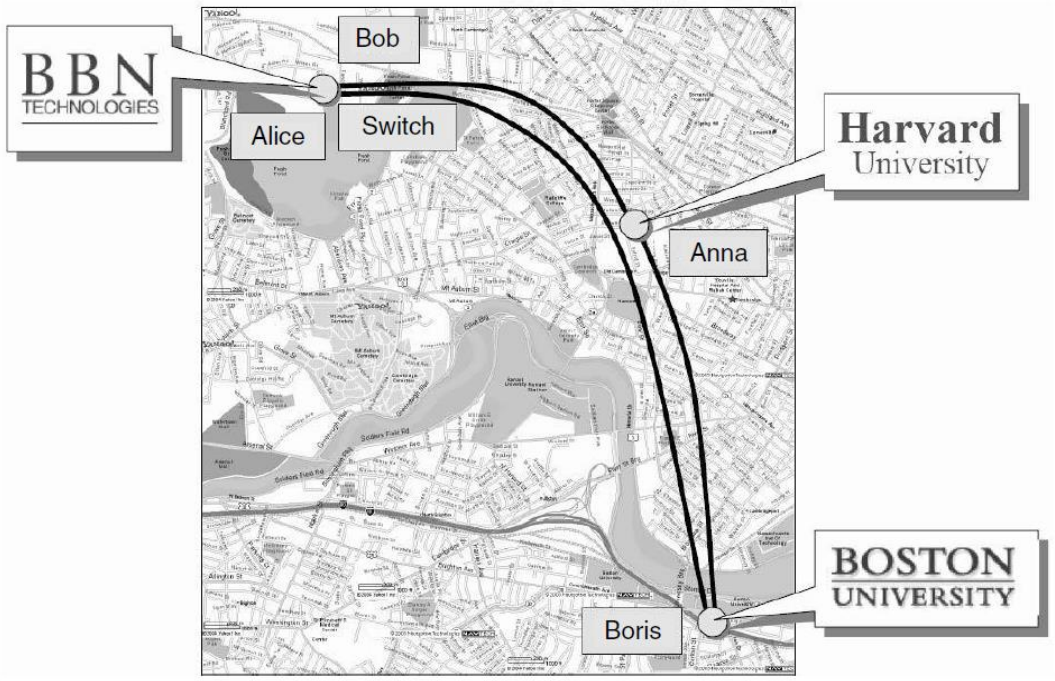


Figure 5: Metro-Fiber DARPA Quantum Network. Source: [68]

The span of the DARPA QKD network is shown in Figure 5 (as of December 2004). Figure 6 shows the connectivity schematic of the network. Alice and Anna are two weak-coherent BB84 transmitters. Bob and Boris are two receivers; along with a 2×2 switch they can couple any transmitter to any receiver. Alice, Bob, and the switch reside at BBN's laboratories, whereas Boris is in Boston University and Anna is at Harvard.

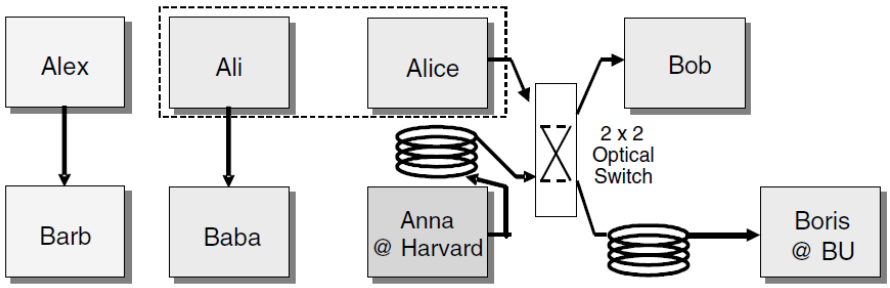


Figure 6: Connectivity schematic of the DARPA QKD network. Source:[68]

The part spanning from Harvard to BBN is around 10 Km long. The part from Boston University to BBN is almost 19 Km. This gives a total of 29 Km QKD distance from Harvard to Boston University. The network uses SMF-28 telecommunication fiber, with an average number of photons from Anna of 0.5 and an average of 1 at Boris. Anna-Bob link delivers about 1000 secret bits/second with an average QBER of 3%.

The network also contains Ali and Baba running the BBN QKD system protocols linked to the overall network by key relay between Alice and Ali. Furthermore, the network contains two other nodes that are entanglement based. These links are Alex and Barb and they are built jointly by Boston University and BBN.

ii. SECOQC

The SECOQC network is formed of two types of nodes:

- Access Nodes or QAN: These nodes are essentially a point-to-point link from an end user into the backbone of the quantum network.
- Backbone Nodes or QBB: These nodes are more complex and are in the form of building blocks where each four of them are connected via six quantum channels.

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.

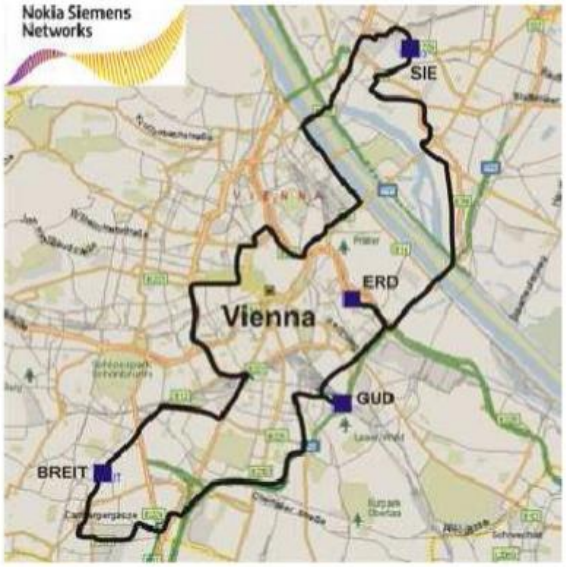


Figure 7: Stations SIE, ERD, GUD, and BREIT. Source:[59]

Figure 7 shows the geographical span of the network. Six nodes are connected via eight QKD links. BREIT, SIE, ERD, FRM and GUD are located in various premises belonging to Siemens and use Siemens' internal fiber optic communications ring. Another node (STP) is a repeater station near St Polten.

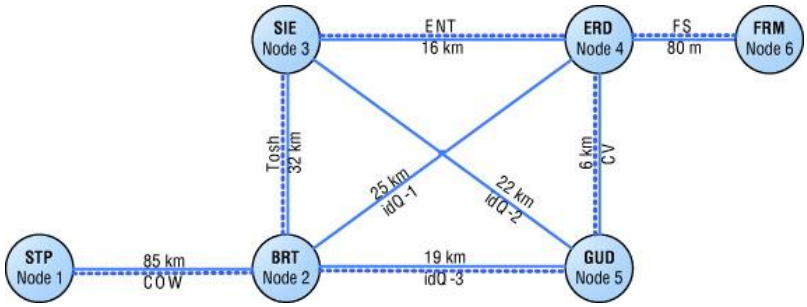


Figure 8: Connectivity schematic of SECOQC ring via Vienna. Source: [59]

Figure 8 shows the network topology of the SECOQC QKD. (Solid lines represent quantum communication channels; dotted lines denote classical communication channels). Various QKD technologies are used:

- STP – BRT use a Coherent One-Way protocol (COW)
- BRT – GUD, BRT – ERD and SIE – GUD use Plug and Play, which use BB84 and SARG04 (BRT – ERD)
- BRT- SIE use a Toshiba system via Weak Coherent Pulses plus decoy states in BB84
- ERD – FRM use a free space Quantum optical link, via BB84 and decoy states
- SIE – ERD use an entanglement based scheme, in the BBM92 protocol
- GUD – ERD employed a CV system

The results are shown in Table 2.

QKD Technology	**Protocol**	**Key Generation Rate (Kbits per second)** *SECOQC objective =1kbits^{-1}*	**Distance** *SECOQC objective = 25 km*
idQuantique Plug and Play	BB84 with decoy states and SARG04	27 18 11 5.7 3.1	1 km 10 km 20 km 25 km 33 km
GAP (University of Geneva)	COW	0.6	82 km
Ent QKD (Austrian-Swedish Consortium)	BBM92	2.5	16 km
CV (Thales research, et al)	CV QKD	8	6 km
FS QKD (University of Munich)	BB84 with decoy states	17	80 metres

Table 2: Key rate generation for SECOQC links. Source:[59]

V. Conclusion

The chapter was divided into three main topics. First, this chapter discussed the details of a few QKD distribution protocols. Beginning with the BB84 protocol, this chapter presented a detailed description of its principle of operation. A description was given of how a quantum key is generated and exchanged between two communicating parties and the use of this protocol was provided. In addition, this chapter presented two variants of the BB84 protocol. The first one was the B92 protocol; it was shown that the only difference lies in the number of states used to distribute the raw key. The second one was the SARG04 protocol; here the only difference lies in the key sifting process. Both of the discussed variants have advantages and disadvantages compared to the original BB84 protocol.

Second, this chapter discussed the disadvantages associated with the QKD protocols. The disadvantages are: vulnerability to denial of service attack, problems of realization of single photon sources and detectors, losses a quantum signal undergoes over the quantum channel, unrealistic assumptions in the current security proofs, need for classical authentication, vulnerability to side channel attacks, need for proper key management, and need for QKD based crypto-systems.

Third, this chapter addressed the topic of QKD networks. QKD networks are considered as the way to make suitable use of the QKD technology and a way to the make use of it on a large scale basis. Three different types of QKD networks were presented: Quantum nodes network, Optical nodes networks, and trusted relays networks. Furthermore, this chapter discussed the actual realization of two quantum networks: the BBN DARPA QKD network as well as the SECOQC network.

Chapter 3: Multi-Stage Protocols Using Polarization Hopping

Securing information in transit is an increasingly important need of modern society. As discussed in the previous chapters, given sufficient computational power, all cryptography techniques in commercial use today can be rendered ineffective. This has led to quantum cryptography which is the only known mechanism to provide unconditional security.

BB84 and its variants [16, 69-72] are deployed for quantum key exchange and based on single photon implementations which have their own set of drawbacks. These drawbacks were discussed in detail in Chapters 1 and 2. We mention the fact that current contemporary QKD implementations rely on weak optical beams that produce much less than one photon per time slot on average. Therefore, most time slots will be empty; a few would have single photons and very few more than a single photon. The BB84 configuration thus limits the distance, the speed, and the security of quantum communication.

Currently, attention is being directed into establishing quantum secure protocols that use multiple photons in order to overcome the limitations associated with single photon approaches [73, 74]. This chapter proposes a multi-stage protocol related to the three-stage protocol initially introduced in 2006 [11, 75, 76]. This chapter generalizes the three-stage protocol to an m -stage protocol where m defines the number of stages in the protocol. The multi-stage protocol is based on the usage of unitary transformations known only to Alice and Bob, individually. Alice and Bob need not communicate information about the transformations they use to anyone, even to each other. The only condition on these transformations is being commutative. In the following, the encoding of the

information bits and the transformation operations are taken to be performed in the polarizations of the photons.

In this chapter, a modified version of the multi-stage protocol is proposed in order to counteract the man-in-the middle attack [77]. The proposed version adds one more dimension to the multi-stage protocol, where the number of variables used is equal or larger than $m+1$, m being the number of stages. This modification is called a key/message expansion multi-stage protocol where an initial random string of bits known to both Alice and Bob is used in order fully to secure the next message to be transferred.

I. The Multi-stage Protocol Polarization Hopping

This section presents the multi-stage protocol as a quantum secure protocol that makes use of linearly polarized light to encode classical bits of information to be shared. During the execution of a multi-stage protocol with an odd number of stages, one of the communicating parties (Alice) starts the communication by encoding the data to be sent into one of two orthogonal states, then applies its unitary transformation and sends it to Bob. Bob applies his own unitary transformation and sends the resulting state back to Alice. Alice now removes the first unitary transformation she applied and applies a new unitary transformation before sending it back to Bob who will repeat the process. This process will be executed in the same way until the last stage of the protocol where Alice will remove all the transformations she made and return the data, with only Bob's transformations back to Bob. Since Bob knows exactly the transformations he made to the encoded data, he removes his transformations and recovers the data.

In case m is even, the communication will start at the receiver (Bob). He starts the communication using a random polarization state representing his first unitary

transformation. He sends this polarization state to Alice who in turn encodes the information to be shared and applies her transformation. The communication will proceed in this manner as in the case where m is odd but with Bob being the entity who decodes the information at the last stage. In the cases where $m = 1, 2$ are special cases. For security purposes, the use of the key/message expansion protocol proposed later in this chapter is required.

As explained above, the encoded polarization states of the information to be transferred are never sent directly on the channel. At each stage of transmission, a unitary transformation is applied in order to change the state of the polarization sent over the channel. The unitary transformation applied is only known to the party applying it. Polarization hopping is the process of changing the polarization state at each stage of the protocol. The message transfer always starts by encoding a bit of information in a polarization state; for example, bit 0 is encoded using state $|0\rangle$ and bit 1 is encoded using state $|1\rangle$, whereas on the channel the state of polarization is given by $\alpha|0\rangle + \beta|1\rangle$. A transformation applied by one communicating party at a given stage will result in new values of α and β. Note that in the following we will restrict to the case with real α and β, i.e., the polarization stays on the equator of the Poincare sphere.

We designate the polarization state as a value of a linear polarization angle, e.g., 0 is bit 0 and $\frac{\pi}{2}$ is bit 1. When the transfer is initiated on Alice's side, she performs her unitary transformation by changing the value of the polarization angle and sends it to Bob, who in turn will do the same. The next steps of the protocol will be carried out the same way until the last stage where Alice removes her transformations and sends them to

Bob who in turn removes his transformations and recovers the original state. While in transit, the value of the polarization angle will be in the following form:

$$\phi_i = \begin{cases} 0° + \frac{b_i\pi}{M} + \frac{a_i\pi}{M}, & \text{encoded angle is } 0° \\ 90° + \frac{b_i\pi}{M} + \frac{a_i\pi}{M}, & \text{encoded angle is } 90° \end{cases}$$

where b_i denotes Bob's transformation and a_i denotes Alice's transformation in the *i*th stage with $a_i, b_i \in \{0, 1, \cdots, M-1\}$. The total number of angles that can be used over the channel is$M$, which is derived by dividing the full polarization circle into $2M$ equal parts. Alice's and Bob's transformations are multiples of $\frac{\pi}{M}$ changes to the polarization angle. We wish to have M as large as possible for a higher degree of security, with the ideal limit $M \to \infty$. Figure 9 represents one example of the extraction of possible polarization angles.

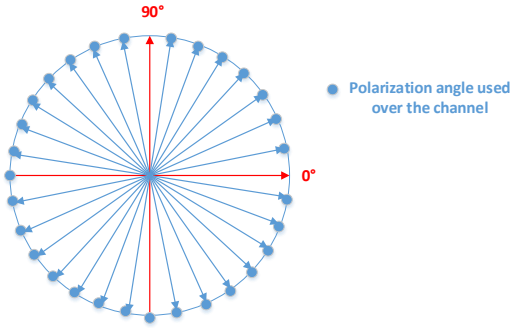


Figure 9: Representation of the choices of encoding angles and the angles used over the channel for $\boldsymbol{2M = 32}$

The advantage that the intended receiver has over an intruder is that while the intruder has to distinguish between one of the M polarization angles, the receiver only needs to distinguish between two orthogonal polarization angles. While the receiver would need only one photon to do so, the intruder Eve would need N photons per leg.

When Eve attempts to measure ϕ_i she will be confronted with quantum noise; this is addressed in detail in Chapter 4.

Throughout this chapter, we use the multi-stage protocol with $m = 3$ stages. However, the discussion can be generalized to any value of *m*. It is important to note that the multi-stage protocols fall into two categories. The first category is the case when $m < 3$. In this case, the protocol needs an initialization vector to be shared before the onset of the transmission and thus can only be used as a key/message expansion protocol (discussed in section V for$m = 3$). The second category is when$m \geq 3$. In this case, the protocol can be used for direct quantum communication or can be used as a key/message expansion protocol. It is important to note that an increased number of stages m means that an eavesdropper is faced with the problem of measuring the states of polarization of more stages .In addition, using more stages means that the sender can use more photons per pulse to encode each bit of information, mN photons. However, an increase in the number of stages poses an overhead on the sender and the receiver with an increase of the losses that the beam of light will experience. As stated previously, when m is odd, the communication begins at Alice's side and ends at Bob's side and when m is even, the communication begins and ends both at Bob.

II. The Three-stage Protocol

i. Operation

The three-stage protocol shown in Figure 10 was first proposed in [75], and implemented as a multi-photon tolerant protocol in [11]. It is an alternative to the BB84 protocol which is the most widely used QKD protocol.

The mode of operation of the three-stage protocol can be described as follows: a sender, Alice, wants to convey a message X to a receiver, Bob. Alice can encode each bit of her message using orthogonal polarization angles; she can encode bit 0 with 0° polarization and bit 1 with $\frac{\pi}{2}$ polarization. In order to secure the information transfer over the channel, Alice and Bob apply secret unitary transformations U_A and U_B respectively. These transformation should commute, i.e., $U_A U_B = U_B U_A$. The steps of the three-stage protocol are as follows:

Step 1: Alice applies a unitary transformation U_A on the quantum information X and sends the qubits to Bob.

Step 2: Bob applies $U_B(X)$ on the received photons $U_A(X)$, giving $U_B U_A(X)$ and sends them back to Alice. As mentioned above U_A and U_B should be commutative transformations.

Step 3: Alice applies $U_A^\dagger$ (transpose complex conjugate of U_A) on the received photons to get $U_A^\dagger U_B U_A(X) = U_B(X)$ and sends them back to Bob.

Step 4: Then Bob applies $U_B^\dagger$ on $U_B(X)$ to get the information X.

The operation of the three-stage protocol is shown in Figure 10.

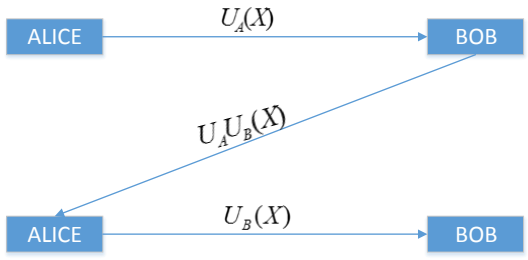


Figure 10: Three-stage protocol operation

ii. Implementation of the Protocol

The first implementation of the three-stage protocol depicted in Figure 11 was reported in [11, 76, 78]. The implementation of the protocol is divided into three main stages: encoding, polarization transformation or key application , and decoding. At the first stage, each bit of the message is encoded using one of two orthogonal polarization angles; bit 0 is encoded with 0° polarization and bit 1 is encoded with $\frac{\pi}{2}$ polarization. At this stage an optical beam polarized at $\frac{\pi}{4}$ is directed into a polarizing beam splitter (beam splitter 1), where it will be divided into two equal intensity beams. Now the bits are encoded using LabView programmed shutters. Shutters are programmed in a way such that shutter 1 will open when bit 1 is to be sent; the optical beam will then pass through a $\frac{\pi}{2}$ polarizer (pol-1). On the other hand, if bit 0 is to be sent, shutter 2 will open and the optical beam will pass through a 0° polarizer (pol-2). After encoding each bit with the respective polarization, the optical beam will be redirected using a mirror (mirror 1 in the first path and mirror 2 in the second path) and a combiner.

During the second stage the transformations U_A and U_B are applied using half wave plates. Alice will have two half wave plates mounted on rotators controlled by a computer. Half wave plate 1 (HWP-1) will be rotated to a random angle θ_A (angle of the fast axis) chosen by Alice and known only to her; meanwhile half wave plate 2 (HWP-2) will be rotated to an angle$-\theta_A$. At Bob's side two half wave plates are fixed at opposite angle θ_B and $-\theta_B$ (HWP-3 and HWP-4 respectively). It is important to note that the half wave plates at Bob's side are also mounted on rotators and the value of θ_B can be

randomly chosen and known only to Bob. The formalism of how the angles of the fast axis are chosen is discussed in the next section using the Mueller matrices.

In the last stage of this implementation, the decoding stage, the optical beam is passed through a polarization beam splitter. The horizontal polarization component of the optical beam will pass the beam splitter while the vertical component is reflected. Decoding is done according to the light intensity received at the detectors D1 and D2.

It is worth noting that the implementation presented in this section is a laboratory proof of concept of an implementation of a multi-stage protocol with $m = 3$. The data rates achieved are of the order of a few bits per second due to the fact that the implementation uses mechanically driven hardware to encode and effect the polarization rotations. The distance at which the implementation was done is 30cm.

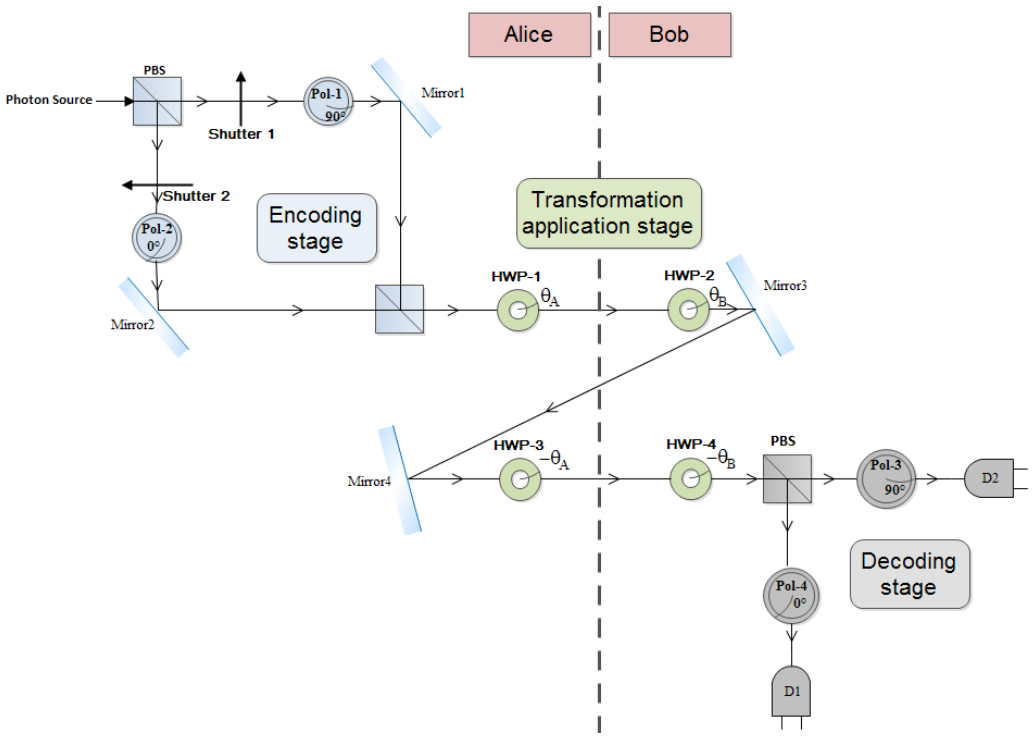


Figure 11: Implementation of the three-stage protocol

iii. Rotation Transformations:

In this section the setup of the unitary transformations applied using half wave plates is discussed along with the choice of the rotation angle (θ) of the half wave plates with respect to the horizontal axis. This choice is based on the Mueller matrix formalism to ensure that a polarization angle input to the setup of the half wave plate is equal to that at the output of the setup.

Half Wave Plate Operation

A half wave plate produces a polarization shift of 180° between the fast and slow axes of a wave plate [79]. The Mueller matrix of a half wave plate is given by:

$$\mathrm{M_{HWP}} = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & -1 & 0 \\ 0 & 0 & 0 & -1 \end{bmatrix}.$$

The implementation described in the previous section uses rotating half wave plates. The Mueller matrix of a rotating half wave plate with an angle θ with respect to the horizontal direction is given by [79]:

$$\mathrm{M}(\theta)_{\mathrm{HWP}} = \mathrm{M_{ROT}}(-\theta) \cdot \mathrm{M_{HWP}} \cdot \mathrm{M_{ROT}}(\theta),$$

where $\mathrm{M_{ROT}}(\theta)$ is the Mueller matrix for rotation and is given by:

$$\mathrm{M}_{\mathrm{ROT}}(\theta) = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & \cos(2\theta) & \sin(2\theta) & 0 \\ 0 & -\sin(2\theta) & \cos(2\theta) & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix}.$$

Then the Mueller matrix of a rotating half wave plate is given by:

$$\mathrm{M}_{\mathrm{HWP}}(\theta) = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & \cos(4\theta) & \sin(4\theta) & 0 \\ 0 & \sin(4\theta) & -\cos(4\theta) & 0 \\ 0 & 0 & 0 & -1 \end{bmatrix}.$$

Choice of the Rotation Angle

It is important to note that the requirement imposed on the transformations used in the three-stage protocol is to be commutative while being only known to the entity applying them. In the case where only the setup of Alice's half wave plates are considered, one can see that when Alice applies a transformation $\mathrm{M}_{\mathrm{HWP}}(\theta_A)$ using her first half wave plate (HWP-1 in Figure 11), she should apply $\mathrm{M}_{\mathrm{HWP}}(\theta_A)$ using her second half wave plate (HWP-3 in Figure 11) in order to remove the effect of her first transformation on the input polarization angle. It can be observed that

$$\mathrm{M}_{\mathrm{HWP}}(\theta_A) \cdot \mathrm{M}_{\mathrm{HWP}}(\theta_A) = \mathrm{I}, \qquad (1)$$

where I is the identity matrix.

However, once the half wave plates of Bob are considered, one can see that the polarization of the input beam is not equal to the polarization of the output beam even if the same angles are used, *viz.*,

$$\mathrm{M}_{\mathrm{HWP}}(\theta_B) \cdot \mathrm{M}_{\mathrm{HWP}}(\theta_A) \cdot \mathrm{M}_{\mathrm{HWP}}(\theta_B) \cdot \mathrm{M}_{\mathrm{HWP}}(\theta_A) \neq \mathrm{I}. \qquad (2)$$

This is due to the fact that the operation of the half wave plates is not commutative, i.e.,

$$\mathrm{M_{HWP}}(\theta_B) \cdot \mathrm{M_{HWP}}(\theta_A) \neq \mathrm{M_{HWP}}(\theta_A) \cdot \mathrm{M_{HWP}}(\theta_B). \qquad (3)$$

One can note from the Mueller matrix representation of half wave plates that

$$\mathrm{M_{HWP}}(\theta_B) \cdot \mathrm{M_{HWP}}(\theta_A) = \mathrm{M_{HWP}}(-\theta_A) \cdot \mathrm{M_{HWP}}(-\theta_B). \qquad (4)$$

Thus,

$$\mathrm{M_{HWP}}(-\theta_B) \cdot \mathrm{M_{HWP}}(-\theta_A) \cdot \mathrm{M_{HWP}}(\theta_B) \cdot \mathrm{M_{HWP}}(\theta_A) = \mathrm{M_{HWP}}(-\theta_B) \cdot \mathrm{M_{HWP}}(-\theta_B) \cdot$$
$$\mathrm{M_{HWP}}(\theta_A) \cdot \mathrm{M_{HWP}}(\theta_A) = \mathrm{I}, \qquad (5)$$

where $0 < \theta_A < \pi$ and $0 < \theta_B < \pi$.

Equation (5) shows the choice of the angles that will insure that the transformations used by Alice and Bob commute without the need of sharing any information about the actual angles. Therefore, we choose the angles of the transformation in such a way that in case Alice applies $\mathrm{M_{HWP}}(\theta_A)$ first she will apply $\mathrm{M_{HWP}}(-\theta_A)$ in order to cancel her transformation and Bob does the same as well using his own randomly chosen angles.

III. Key/Message Expansion Multi-stage Protocol

In this section a key/message expansion algorithm using a multi-stage protocol is proposed. We call a key expansion algorithm a key distribution method that requires having a shared initialization vector at the onset of the communication. In the meanwhile, we call a message expansion algorithm a message sharing scheme that requires having a shared initialization vector at the onset of the communication. The initialization vector

used is updated using the message or the key shared in the case of message expansion or key expansion respectively.

i. Multi-stage Protocol Using an Initialization Vector

In this section we present the multi-stage protocol using $m + 1$ variables. It is well known that it is impossible to obtain a unique solution for an undetermined system. In this approach we make sure our system satisfies this fact by adding the requirement of an initialization vector to any version of the multi-stage protocol. We call IV the initialization vector shared between the sender and receiver at the onset of the communication. The initialization vector IV along with the message/key shared will be used in order to create a new IV to be used during the next communication.

In the next section we discuss the four-variable three-stage protocol. It should be noted that the same logic is followed to generalize the proposed approach for different values of m. As mentioned earlier, if m is even the communication would start and end at the receiver's end. Whereas, if m is odd the communication starts at the sender and ends at the receiver.

ii. Operation of the Four-variables Three-stage Protocol

In this chapter we propose an implementation of a the key/message expansion four-variable three-stage protocol reported in [77]. The four-variable three-stage protocol adds one more dimension to the three-stage protocol to enhance its security while keeping its mode of operation intact. The dimension added is presented as an initialization vector IV that Alice and Bob are assumed to possess at the beginning of the first iteration of the protocol. The initialization vector IV is a string of unitary transformations; we call

a cycle of the protocol a complete execution of the three-stage protocol that results in one bit shared between Alice and Bob. It is important to note that the number of cycles per iteration is equal to the length of the string IV. The initialization vector IV is updated to a new value at the end of eachiteration using the message shared between Alice and Bob as well as the initialization vector used in the last iteration. This can be observed as chaining between iterations of the protocol implementation. One can use any non-linear function to relate between IV_0 and X_0 and generate the new value IV_1. The operation of the four-variable three-stage protocol is discussed below and depicted in Figure 12.

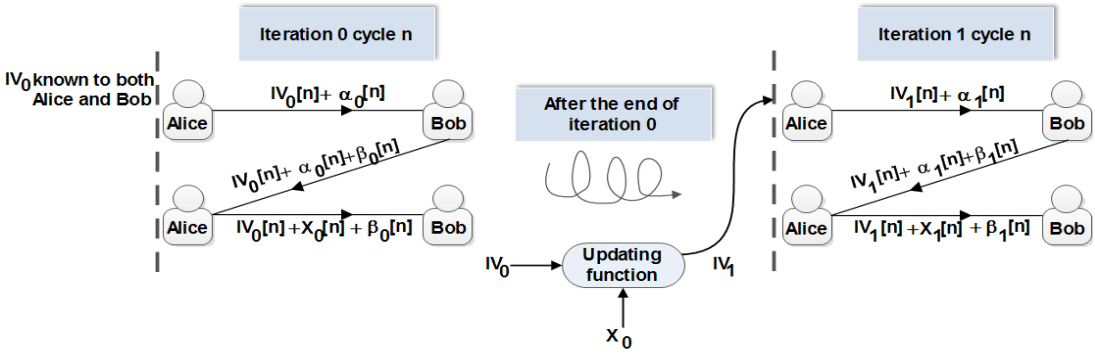


Figure 12: Operation of the three-stage protocol using four variables

We call $IV_0[n]$ the initialization vector at iteration 0 cycle number n; $X_0[n]$ is the bit value of the message being transferred, and $\alpha_0[n]$ and $\beta_0[n]$ are the values of the unitary transformations at iteration 0 cycle number n of Alice and Bob respectively.

Step 1: Alice applies a unitary transformation $\alpha_0[n]$ on the on $IV_0[n]$ and sends the optical beam to Bob.

Step 2: Bob applies $\beta_0[n]$ on the received optical beam and sends it back to Alice.

Step 3: Alice applies $\alpha_0^{\dagger}[n]$ (transpose complex conjugate of $\alpha_0[n]$) on the received qubit to get and then encodes the value of $X_0[n]$ and sends it to Bob.

Step 4: Then Bob applies $IV_0^{\dagger}[n]$ (transpose complex conjugate of $IV_0[n]$) then applies $\beta_0^{\dagger}[n]$ and gets the information $X_0[n]$.

At the next cycle Alice will use a new transformation set $\alpha_0[n+1]$ and Bob should use $\beta_0[n+1]$ and a next value in the string of the initialization vector $IV_0[n+1]$ will be used. When the number of cycles is equal to the length of IV, a new IV_1 of the same length as IV_0 will be generated. It should be noted that Alice and Bob do not have any restrictions on the transformations associated with IV, and it does not need to commute with α and β. Furthermore, the updated initialization vector will be in the binary form of 0's and 1's. Alice and Bob can associate these bits with variable transformation values depending on a prior agreement.

Adding an extra dimension to the three-stage protocol makes it possible to consider it as a one-time pad since at each stage of the protocol one new variable is added in order to secure the outcome of the previous stage. An eavesdropper having simultaneous access to the three stages of the protocol will not be able to compute the value of the sent bit, since he/she will be faced with the problem of solving an undetermined system of equations. In addition, such an approach makes it impossible to launch a man-in-the-middle attack.

The addition of an initialization vector to the three-stage protocol can be regarded as a door function to protect the message sent over the channel. Any illegitimate user is denied from the ability of retrieving the value of the bit sent over the channel as long as he/she does not have in his/her possession the key for the door function, with the angle θ at which the half wave plate in the next section is set.

iii. Implementation of the Four-variables Three-stage Protocol

In this section we discuss the implementation of a four-variable three-stage protocol over free-space optics (FSO) using passive optical components. The setup of the implementation is depicted in Figure 13. The setup proposed is as follows: Alice will have four half wave plates in her possession meanwhile Bob has only three half wave plates. At the beginning of the protocol Alice generates a state with a 0° linear polarization using a 0° polarizer. Then she will apply a transformation $IV[n]$ using a half wave plate (HWP-1) set at an angle θ and the unitary transformation $\alpha[n]$ using her second half wave(HWP-2) plate at an angle θ_A. Then she will send the optical beam to Bob. Bob will apply his unitary transformation $\beta[n]$ using his first half wave plate (HWP-3) at an angle θ_B and send the optical beam to Alice using mirror 1. Alice will remove her transformation by setting her third half wave plate (HWP-4) at the angle $\alpha[n] = -\theta_A$. Then she will apply the transformation associated with the encoded bit using her fourth half wave plate (HWP-5) that will be set at angle $\theta_x = 0°$ in the case of bit 0 is being sent and $\theta_x = 45°$ if bit 1 is being sent. Now Alice will send the optical beam containing the message to Bob who will first pass it through a half wave plate (HWP-6) at angle θ to remove the transformation induced by the initialization vector. Then he will remove his transformation using a half wave plate (HWP-7) set at the angle $-\theta_B$. At this stage Bob will have a beam polarized at either 0° or 90°. He will pass it through a polarization beam splitter to detect whether bit 0 or 1 has been received.

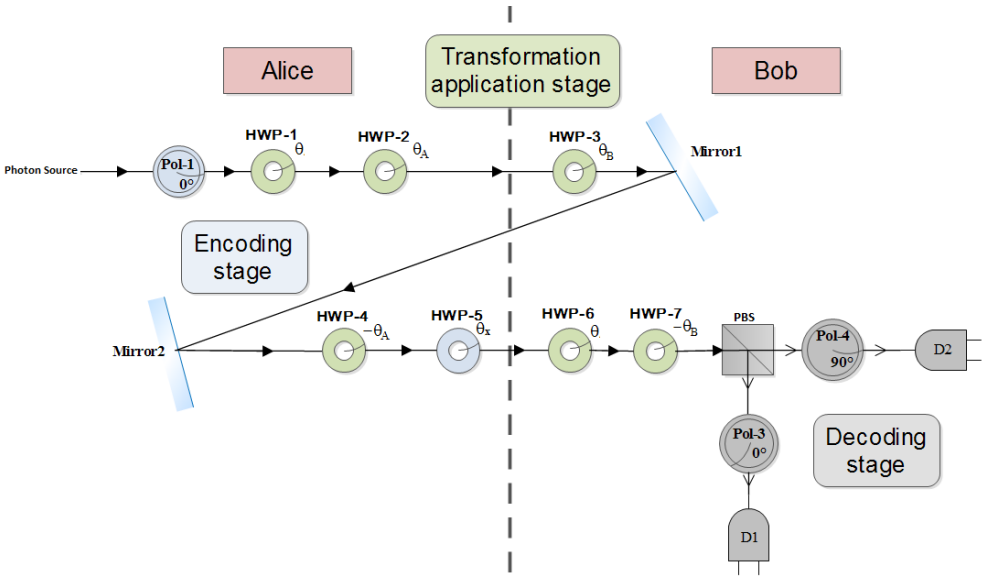


Figure 13: Implementation of the four variables three-stage protocol

The choice of the angles for the setup described above is made according to the same formalism described in section *II. iii* of Chapter 2. For the implementation of the four-variable three-stage protocol we can write the Mueller matrices of the half wave plates operation as follows:

$$\mathrm{M_{HWP}}(-\theta_B)\cdot \mathrm{M_{HWP}}(\theta)\cdot \mathrm{M_{HWP}}(\theta_x)\cdot \mathrm{M_{HWP}}(-\theta_A)\cdot \mathrm{M_{HWP}}(\theta_B)\cdot \mathrm{M_{HWP}}(\theta_A)$$
$$\cdot \mathrm{M_{HWP}}(\theta) = \mathrm{M_{HWP}}(\theta_x).$$

Since the input state is a 0° polarized state it can be represented using the Stokes parameters:

$$\mathrm{S_{in}} = \begin{bmatrix} 1 \\ 1 \\ 0 \\ 0 \end{bmatrix}.$$

Thus the Stokes parameters of the output of the proposed setup are given by:

$$\mathrm{S_{out}} = \mathrm{M_{HWP}}(\theta_x)\cdot \mathrm{S_{in}}. \qquad (14)$$

This means that in the case $\theta_x = 0°$, the output light will be horizontally polarized; otherwise if $\theta_x = \frac{\pi}{4}$, the output light will be vertically polarized.

IV. Conclusion

This chapter has proposed a generalized multi-stage multi-photon tolerant protocol for quantum secure communication. The security of the multi-stage protocol is based on the fact that while a legitimate receiver only needs to distinguish between two orthogonal polarization states, an intruder has to distinguish among an infinite number of possible polarization states. In other words, while the receiver would need only one photon to do so, an intruder would need to siphon off a minimum number N of photons per stage. This chapter has also proposed a key/message expansion scheme associated with the multi-stage protocol which has been proposed. The key/message expansion scheme provides a countermeasure to any man-in-the-middle attack that can be launched on the system. The proposed multi-stage multi-photon protocol provides higher data rates as well as longer communication distances compared to its single-photon counterparts. In addition, in this chapter an implementation of the generalized multi-stage multi-photon tolerant protocol as well as its key/message expansion scheme has been proposed. These implementations have been done in a laboratory setup using passive optical components. In this chapter, the theory behind the use of half wave plates in this implementation has been explained in detail based on the Mueller matrices formalism.

Chapter 4: Preliminary Security Analysis of the Multi-stage Protocol

A generalized multi-stage, multi-photon tolerant protocol was proposed in Chapter 3. Multi-stage protocols use arbitrary polarization states to communicate data securely between a sender and a receiver. It is well known that since the polarization measurement of an arbitrarily unknown polarized state results in altering the state in an irreversible way, any such measurement produces noise in the measured state. The proposed multi-stage protocol exploits this phenomenon to provide quantum secure communication. This chapter assesses the vulnerability of the multi-stage protocol to a photon number splitting attack and a Trojan horse attack.

In addition, this chapter presents two approaches to calculating an upper bound on the average number of photons that can be used per pulse to exchange information while maintaining quantum-level security. The first approach is through the assumption that an eavesdropper is faced with the problem of discriminating between two polarization states. This results in an inaccurate state estimation. The second approach is through the assumption that a certain amount of noise will be introduced to the measurement of the state in each stage. The noise introduced may result in an undetermined value of the measured bit, or a flip in the value of the bit. The assumption we make through the second approach is that Alice and Bob are using Fock states.

Determination of an upper bound on the number of photons is an extremely important task for the multi-stage protocol. It allows the multi-stage protocol to operate in the multi-photon domain while maintaining quantum-level security. It is shown that the average number of photons that can be used per stage of a multi-stage protocol is

larger than that of its single photon counterpart. In the latter case, in BB84 and its decoy state version an average of less than 0.5 photons per pulse is used [32, 80-85]. Increasing the average number of photons will result in a better performance of the QC protocols, as shown in Chapter 6.

I. Background Knowledge

i. Helstrom discrimination

The Helstrom formula was derived in the mid-70s to describe the minimum error probability for the case where two quantum states are used [86]. These quantum states can be either pure or mixed states, and the error probability is denoted by P_E.

This section summarizes the derivation of the probability of the correct state discrimination P_C [87]. P_C is used later in this chapter to compute the number of photons that Alice and Bob can use while achieving quantum secure communication. It is instructive to start by analyzing the two-state minimum-error measurement with the help of the method in [88, 89]. Starting from,

$$P_{err} = 1 - \sum_{j=1}^{m} \eta_j Tr(\rho_j \Pi_j)$$

where η_j and Π_j are the priori probabilities and detection operators respectively and ρ_j is the density operator of a given quantum system. They should satisfy the following relations

$$\eta_1 + \eta_2 = 1 \text{ and } \Pi_1 + \Pi_2 = I_{D_s}$$

Then, the probability of getting an erroneous result in the measurement is given by [87]

$$P_{err} = 1 - \sum_{j=1}^{2} \eta_j Tr(\rho_j \Pi_j) = \eta_1 Tr(\rho_1 \Pi_2) + \eta_2 Tr(\rho_2 \Pi_1)$$

This can be alternatively expressed as

$$P_{err} = \eta_1 + Tr(\Lambda\Pi_1) = \eta_2 - Tr(\Lambda\Pi_2)$$

where we introduced the Hermitian operator,

$$\Lambda = \eta_1\rho_1 + \eta_2\rho_2 = \sum_{k=1}^{D_s} \lambda_k |\emptyset_k\rangle\langle\emptyset_k|$$

Here the states $|\emptyset_k\rangle$ denote the orthonormal eigenstates belonging to the eigenvalues λ_k of the operator Λ. By using the spectral decomposition of Λ, we get the representations:

$$P_{err} = \eta_1 + \sum_{k=1}^{D_s} \lambda_k \langle\emptyset_k|\Pi_1|\emptyset_k\rangle = \eta_2 + \sum_{k=1}^{D_s} \lambda_k \langle\emptyset_k|\Pi_2|\emptyset_k\rangle \qquad (4.1)$$

Now the optimization task consists of determining the specific operators Π_1, or Π_2, respectively, that minimize the right-hand side of (4.1) under the constraint that

$$0 \leq \langle\emptyset_k|\Pi_j|\emptyset_k\rangle \leq 1 \qquad (j = 1,2)$$

for all eigenstates $|\emptyset_k\rangle$. The latter requirement is because $Tr(\rho\Pi_j)$ denotes a probability for any ρ. From this constraint and from (4.1), it follows that the smallest possible error probability, $P_{err}^{min} = P_E$, can be achieved when the detection operators are selected in such a way $\langle\emptyset_k|\Pi_1|\emptyset_k\rangle = 1$ and $\langle\emptyset_k|\Pi_2|\emptyset_k\rangle = 0$ are fulfilled for eigenstates belonging to negative eigenvalues. Meanwhile eigenstates corresponding to positive eigenvalues obey the equations $\langle\emptyset_k|\Pi_1|\emptyset_k\rangle = 0$ and $\langle\emptyset_k|\Pi_2|\emptyset_k\rangle = 1$. Thus, the optimum detection operators can be written as

$$\Pi_1 = \sum_{k=1}^{k_0-1} |\emptyset_k\rangle\langle\emptyset_k| \qquad \Pi_1 = \sum_{k=k_0}^{D_s} |\emptyset_k\rangle\langle\emptyset_k|$$

By inserting the optimum detection operators into the minimum error probability is found to be [89]

$$P_E = \eta_1 - \sum_{k=1}^{k_0-1} |\lambda_k| = \eta_2 - \sum_{k_0}^{D_s} |\lambda_k| \qquad (4.2)$$

Taking the sum of these two alternative representations and using $\eta_1 + \eta_2 = 1$, P_E is represented by

$$P_E = \frac{1}{2}(1 - \sum_k |\lambda_k|) = \frac{1}{2}(1 - Tr(|\Lambda|)$$

where $|\Lambda| = \sqrt{\Lambda^{\dagger}\Lambda}$. Together with (4.1) this yields the well-known Helstrom formula [86] for the minimum error probability in discriminating ρ_1 and ρ_2,

$$P_E = \frac{1}{2}(1 - Tr|\eta_2 \rho_2 - \eta_1 \rho_1|)$$

In the special case that the states to be distinguished are the pure states $|\emptyset_1\rangle$ and $|\emptyset_2\rangle$, this expression reduces to [86]

$$P_E = \frac{1}{2}(1 - \sqrt{1 - 4\eta_1 \eta_2 |\langle \emptyset_1 | \emptyset_2 \rangle|^2}$$

Giving rise to a probability of correct measurement given by

$$P_C = \frac{1}{2}(1 + \sqrt{1 - 4\eta_1 \eta_2 |\langle \emptyset_1 | \emptyset_2 \rangle|^2} \qquad (4.3)$$

Equation (4.3) is used in Section *II.i* to derive the number of photons needed if Eve was to carry a PNS attack on the three-stage protocol. In this case we consider the capability of Eve to distinguish between two quantum states. It is worth noting that section *II.i* uses the condition $\eta_1 = \eta_2 = \frac{1}{2}$ that denotes the optimum discrimination strategy[87].

ii. Fock states

In quantum mechanics, a Fock state or number state is a quantum state that is an element of a Fock space. A Fock state is a state with a well-defined number of particles. This type of state is named after the Soviet physicist Vladimir Fock. This section presents the derivations of the definition of the N^{th} Fock state [90]. We start by considering the eigenvalue problem for $\hat{H} = h\omega\left(\hat{N} + \frac{1}{2}\right)$. It is solved by considering the eigenvalue problem for the number operator since $\left[\hat{H}, \hat{N}\right] = 0$. The eigenvalue equation reads

$$\hat{N}|\emptyset_N\rangle = N|\emptyset_N\rangle$$

where n is the eigenvalue of $\widehat{N}$ and $|\psi_N\rangle$ is the matching eigenvector. The number operator $\widehat{N} = \hat{b}^{+}\hat{b}$ is a Hermitian operator; therefore its eigenvalues N are real and its eigenvectors $|\emptyset_N\rangle$ form a complete set of orthogonal states. From the following

$$\langle\emptyset_N|\widehat{N}|\emptyset_N\rangle = \langle\emptyset_N|\hat{b}^{+}\hat{b}|\emptyset_N\rangle = N\langle\emptyset_N|\emptyset_N\rangle$$

it can be seen that n must be non-negative. This is due to the fact that $|\psi_N\rangle$ and $\hat{b}|\psi_N\rangle$ are both Hilbert-space vectors with non-negative norms. Applying$\left[\hat{b}, \hat{b}^{+}\right] = 1$, it can be found that $\left[\hat{b}, \widehat{N}\right] = \left[\hat{b}, \hat{b}^{+}\hat{b}\right] = \hat{b}\left[\hat{b}, \hat{b}^{+}\right] = \hat{b}$; hereafter $\widehat{N}\hat{b}|\emptyset_N\rangle = \left(\hat{b}\widehat{N} - \left[\hat{b}, \widehat{N}\right]\right)|\emptyset_N\rangle = (N-1)\hat{b}|\emptyset_N\rangle$.This means $\hat{b}|\emptyset_N\rangle$ is an eigenvector of the number operator with eigenvalue $N-1$ which it can be called $|\emptyset_{N-1}\rangle$. However, since all eigenvalues of $\widehat{N}$ s are non-negative, a state $|\emptyset_0\rangle$ with $\hat{b}|\emptyset_N\rangle = 0$ should be available. This state is referred to as the ground state. It contains no excitation, and thus cannot be further annihilated. Similarly, it can be found that

$$\widehat{N}\hat{b}|\emptyset_N\rangle = (N+1)\hat{b}^{+}|\emptyset_N\rangle$$

It can be seen that $\hat{b}$ and $\hat{b}^{+}$ lower and raise the number of excitations by one; hence their names, annihilation and creation operators. The action of $\hat{b}$ and $\hat{b}^{+}$ are shown in Figure 14.

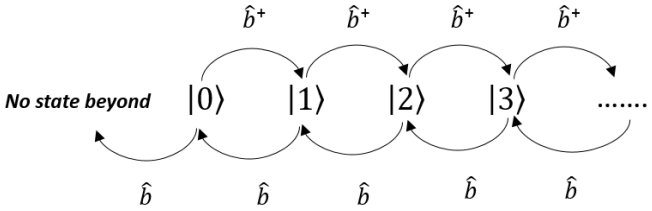


Figure 14: The action of b^and b^+ on a given Fock state

Starting from the ground state $|\emptyset_0\rangle$ all other states can be generated by successive application of the creation operator, $|\emptyset_N\rangle = (\hat{b}^{+})^N|\emptyset_0\rangle$. If we normalize these states

according to $|\emptyset_N\rangle/\langle\emptyset_N|\emptyset_N\rangle$, we arrive at the definition of the number states or Fock states. If we assume that the ground state (or vacuum state) $|0\rangle = |\emptyset_0\rangle$ is already normalized, then the N^{th} Fock state is given by

$$|\emptyset_N\rangle = c_N(b^\dagger)^N|0\rangle$$

where c_n is the normalization constant given by $c_N = \frac{1}{\sqrt{N!}}$.

II. Photon Number Splitting Attack (PNS)

A photon number splitting attack in the context of a multi-stage, multi-photon protocol would require an eavesdropper to siphon off a certain number of photons at each leg of the protocol in order to be able to recover the message sent over that leg (stage). In the case of the three-stage protocol, Eve would siphon off n photons at each of the three legs. The PNS attack in the case of a three-stage protocol is shown in Figure 15. Furthermore, the angles of polarization at each stage of the protocol should be measured or estimated since the information from only one stage will not be sufficient to get the original encoded polarization angle.

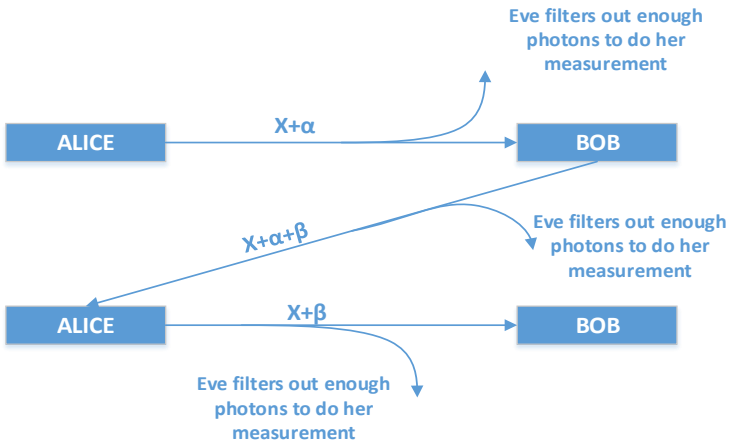


Figure 15: Photon number splitting attack on the three-stage protocol

It is well known that as the number of photons in the optical beam increases, Eve's ability to measure the polarization of the beam increases, and vice versa. In particular, this is due to the fact that the fidelity with which Eve can measure the state of polarization increases with the number of photons split from the beam. In other words, one can say that the three-stage protocol is theoretically secure as long as the number of photons in the beam launched by Alice is less than a certain threshold. We call this threshold N. So, in case y is the total number of photons in the beam, the security of the three-stage protocol is theoretically guaranteed as long as $y < N$ [78].

Assume that Eve successfully siphoned an equal number of photons off each of the three legs of the protocol. Knowing that a measurement of the value of the polarization angle would introduce noise, Eve will not be able to deduce the exact value of the incoming polarization state from the measured state of polarization. If the measurement on each leg introduces an equal amount of uncertainty to the actual angle of polarization sent over the channel, Eve will have in her possession, in the worst case scenario, $\phi + 3\Delta\phi$, where $\Delta\phi$ is the uncertainty added by the measurement on one leg. This logic can be applied to both the cases of state discrimination as well as Fock state measurement.

Eve will have no precise information about ϕ in case [91]:

$$3\langle\Delta\phi\rangle \geq \frac{\pi}{4}, \quad \text{or} \quad \langle\Delta\phi\rangle \geq \frac{\pi}{12} .$$

i. Helstrom Discrimination

As the number of photons in a beam increases, the level of vulnerability of the protocol towards a PNS attack increases. In this section, we use the probability P_C calculated in section *I.i* in order to calculate the minimum average number of photons Eve needs to siphon off for her measurement. This number of photons per stage is the

maximum number per stage that should be used in the three-stage protocol to provide quantum secure communication. It is calculated in terms of the probability P_C, in such a way that at each stage $\langle \Delta\phi \rangle \geq \frac{\pi}{12}$ is introduced giving rise to a total difference of more than or equal to $\frac{\pi}{4}$ between the original angle sent over the channel and the angle Eve has by the end of the protocol execution.

Figure 16 illustrates the interplay between the number of photons per stage in the beam and P_C. The three-stage protocol is unconditionally secure as long as the number of photons per stage used is less than depicted by the blue curve in Figure 16. We assume y is the actual number of photons per stage sent over the channel.

The interplay between the number of photons needed by Eve and M can be derived usingP_C. We call M the number of achievable polarization states at angle $\frac{k\pi}{M}$ with $k \in [0 \ldots . N-1]$. The possible states of y photons can be written as follows [92]

$$\left|\phi_k\right\rangle = |k, y\rangle = \left(\frac{|0> + e^{2ik\pi/M}|1>}{\sqrt{2}}\right)^{\otimes y} \qquad (4.4)$$

The probability of confusing two different angles k and $k'$is the scalar product given by:

$$\langle k', y|k, y\rangle = \left(\cos\left([k-k']\frac{\pi}{M}\right)\right)^y \qquad (4.5)$$

If the problem is restricted to discrimination between two angles k and $k+1$ the probability of success of a Helstrom discrimination is given by [93]

$$P_C = \frac{1}{2}[1 + \sqrt{1 - |< k', y|k, y >|^2}] \qquad (4.6)$$

$P_c \geq 1-\epsilon$ where $\epsilon \ll 1$, thus

$$(cos\frac{\pi}{M})^y \leq 2\sqrt{\epsilon(1-\epsilon)}$$

$$y \geq \frac{\frac{1}{2}log\epsilon + log2 + \frac{1}{2}log(1-\epsilon)}{log(cos\frac{\pi}{M})} \qquad (4.7)$$

When $M \gg 1$ we have $cos\frac{\pi}{M} \cong 1-\frac{1}{2}(\frac{\pi}{M})^2$ and therefore,

$$log\left(cos\frac{\pi}{M}\right) \cong -\frac{loge}{2}(\frac{\pi}{M})^2$$

$$y \geq M^2\frac{2}{\pi^2}(-ln\epsilon - ln2 - ln(1-\epsilon))$$

In other words, this implies that the number of photons needed to discriminate between two polarization states is of the order M^2.

The calculations above are meant to distinguish between two states of a $\frac{\pi}{M}$ difference. In order to be applicable in the case of the three-stage protocol, the uncertainty introduced by the state discrimination used by should be equal to $\frac{\pi}{12}$ at least. Setting $M = 12$ we get the following relation

$$y \geq 12^2\frac{2}{\pi^2}(-ln\epsilon - ln2 - ln(1-\epsilon))$$

Once again y in this equation is the minimum number of photons needed by Eve and in the meanwhile it is the maximum number of photons that should be sent over the channel. This in turn means

$$y < 12^2\frac{2}{\pi^2}(-ln\epsilon - ln2 - ln(1-\epsilon)) \qquad (4.8)$$

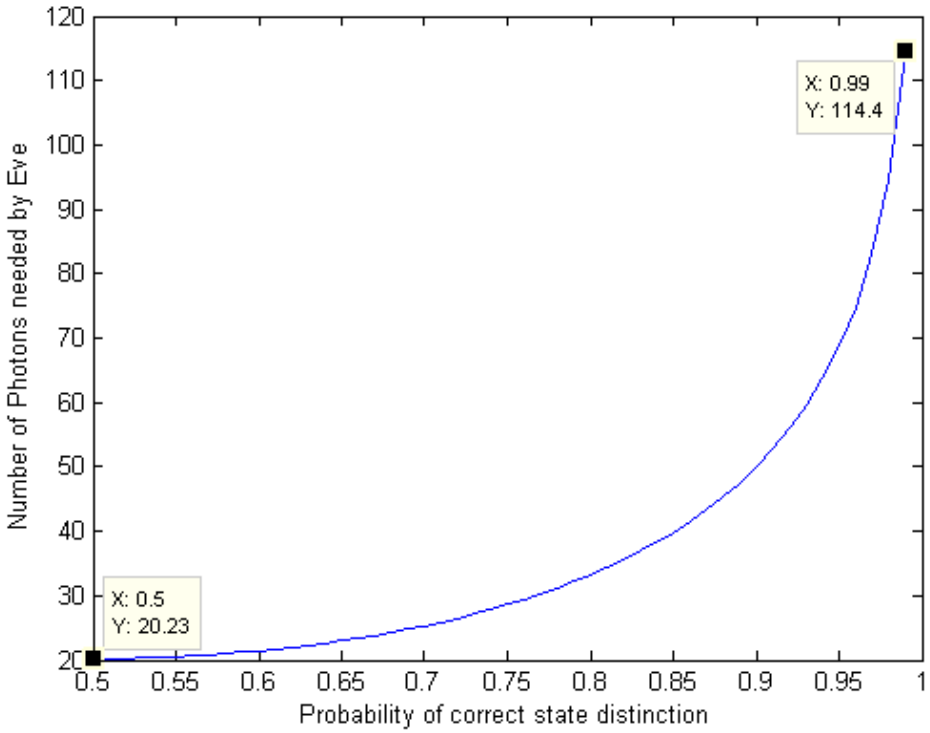


Figure 16: Interplay between the number of photons needed by Eve and P_C

ii. Fock states

In this section, the following calculations are used to find a generalized relation between $\langle \Delta\phi \rangle$, the average angular deviation that a measurement done at Eve's side has, and the minimum number of photons n Eve needs for her measurement. We consider the case of Fock states or number states discussed in section *I.ii* [94] to find the variance induced while measuring the polarization state using *H*-mode and *V*-mode. *H*-mode and *V*-mode represent measurements with respect to a horizontal or a vertical reference, respectively.

In our analysis, we represent our states as number states or Fock states. We assume that the vacuum state $|\emptyset_0\rangle = |0\rangle$ is already normalized. Then the N^{th} Fock state is given by

$$|\emptyset_N\rangle = c_N (b^\dagger)^N |0\rangle, \qquad (4.9)$$

where $b^\dagger = \cos\phi \ a_H^\dagger + \sin\phi \ a_V^\dagger$ with a_H and a_V being the field operators for horizontal and vertical polarizations respectively, and the normalization constant $c_N = 1/\sqrt{N!}$. The binomial expansion of $|\emptyset_N\rangle$ is given by

$$|\emptyset_N\rangle = \sum_{k=0}^{N} \sqrt{\frac{N!}{k!(N-k)!}} \cos^k\phi \sin^{(N-k)}\phi \, |k\rangle_H |N-k\rangle_V \qquad (4.10)$$

Since our decoding scheme is based on intensity detection, we derive Malus' Law for our analysis. The average photon number in *H*-mode is given by the mean intensity distribution:

$$\langle I_H\rangle = \sum_{k=0}^{\infty} k |\langle k|\emptyset\rangle_H|^2 = \sum_{k=0}^{N} k \left[\frac{N!}{k!(N-k)!}\right] (\cos^2\phi)^k (\sin^2\phi)^{N-k} = N\cos^2\phi \quad (4.11)$$

Similarly, $\langle I_V\rangle = N\sin^2\phi$. Then we find that the normalized intensities become

$$\frac{I_H}{I_H+I_V} = \cos^2\phi, \qquad (4.12)$$

and

$$\frac{I_V}{I_H+I_V} = \sin^2\phi. \qquad (4.13)$$

The variance in the intensity measurement in *H*-mode done by Eve can be found as follows:

$$\langle I_H^2\rangle - \langle I_H\rangle^2 = \frac{N}{4}\sin^2 2\phi. \qquad (4.14)$$

Thus the normalized deviation of the H-mode is given by:

$$\frac{\sqrt{\langle I_H^2\rangle - \langle I_H\rangle^2}}{I_H+I_V} = \frac{|\sin 2\phi|}{2\sqrt{N}} \qquad (4.15)$$

It can be shown that the normalized deviation of the *V*-mode is identical to that of the *H*-mode.

In order to find $\langle \Delta\phi \rangle$ we take derivative of both sides of (4.15) as follows:

$$\Delta\left(\cos^2\phi\right) = \Delta\left(\frac{I_H}{I_H + I_V}\right)$$

$$\text{or} \qquad -\sin(2\phi)\Delta\phi = \frac{\Delta I_H}{I_H + I_V} - \frac{I_H}{(I_H + I_V)^2}(\Delta I_H + \Delta I_V)$$

$$\text{giving} \qquad \Delta\phi = \frac{\cos(2\phi)}{2\sqrt{N}}.$$

We now find the average angular deviation that a measurement done at Eve's side as

$$\langle \Delta\phi \rangle = \left| \frac{\langle \cos(2\theta) \rangle}{2\sqrt{N}} \right|$$

$$\text{Thus, } \langle \Delta\phi \rangle = \frac{1}{\pi\sqrt{N}}$$

Thus, to have $\langle \Delta\phi \rangle \geq \frac{\pi}{12}$, the number of photons $N \leq 1.48$. Therefore, the total number of photons in the beam should be $3N \leq 4.5$.

III. Trojan Horse Attack

A Trojan horse attack [49] that can be launched by Eve is shown in Figure 17. During this attack, Eve can inject an optical beam with a known state of polarization right

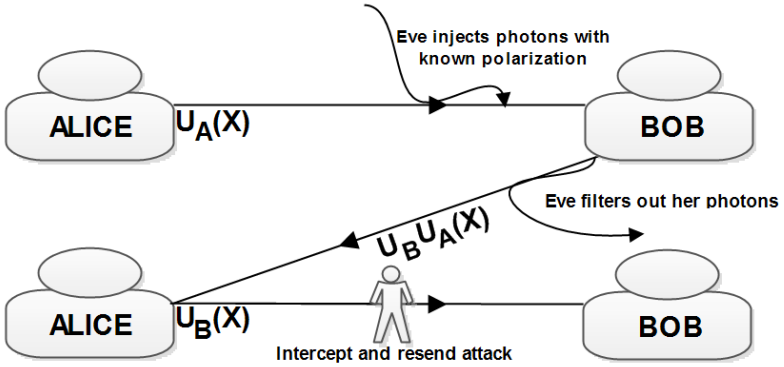


Figure 17 : Diagram of a Trojan horse attack on the three-stage protocol

before Bob applies his transformation U_B. Then Eve will filter out her photons at the second stage of the protocol. By measuring and comparing the polarization states of the injected and the recovered photons, Eve can now estimate the polarization transformation introduced by Bob (U_B). During the execution of the protocol in the third stage, Eve can launch an intercept and resend attack. Having a prior knowledge of the transformation U_B, she will be able to recover the value of X being sent.

To defeat a Trojan horse attack, Alice and Bob should actively monitor the intensity of the optical beam at each end. This can be implemented using auxiliary detectors and active monitoring of any incoming beam. Furthermore, one can use an "optical fuse" to monitor any increase in the beam intensity over the channel. An increase in the beam intensity takes place in case Eve injects an optical beam with a slightly higher intensity than the one she siphoned off. It is worth noting that the intensity threshold at which the protocol is operating is preset before the onset of the implementation and is mainly determined by the number of photons used by Alice and Bob. Furthermore, the noise on the channel can be characterized prior to any data exchange; thus Alice and Bob can know whether the intensity fluctuations were due to eavesdropping or to noise.

IV. Hardware Countermeasures

In order to limit the vulnerability of a system implementing the three-stage protocol to the attacks discussed above, one can implement the following hardware countermeasures:

1. Limit the maximum number of photons to a value less than that proposed earlier. We call this method the multi-photon tolerant approach. Using this approach one can guarantee that an eavesdropper cannot measure the actual polarization state

over a given leg of the protocol; thus, the message X is transmitted at a quantum secure level while using multiple photons in each pulse. The use of a single photon to encode each bit maintains the security level of the BB84 protocol while removing its major limitations. It loosens the limits on the distance, data rates, and single photon generation and detection. It is worth noting that we use the value $3N \leq 4.5$ found in section *II.ii*; this is due to the assumption that Eve will use the method where she needs the least number of photons in order to launch her attack.

2. Actively monitor the intensity of the optical beam at each receiving end. This can be implemented using auxiliary detectors and active monitoring of any incoming light. Furthermore, one can use an optical fuse to monitor any increase in the beam intensity over the channel. An increase in the beam intensity takes place in case Eve injects an optical beam with slightly higher intensity than the one she siphoned.
3. A "door" function can be applied as well; this is an effective countermeasure against a Trojan horse attack. This door can be thought of as a narrow band filter that will disallow Eve from injecting light at a wavelength different than that used during communication. Therefore, Eve's presence can be detected through intensity measurements that can be carried out as proposed in 2. Furthermore, the door function can open access to the channel only once a legitimate signal has been sent through the channel. In other words, the system will be in an idle state as long as Alice and Bob are not sending any information over the channel.
4. Alice and Bob must implement a *QBER* check at the end of the execution of the protocol. Once the *QBER* measured is higher than a certain threshold, the presence

of an eavesdropper on the channel is detected. The communicated message should be discarded. The *QBER* threshold varies from one medium to another since it depends highly on the noise and environmental changes.

V. Comparison with Single-photon Protocols

The multi-stage protocol is a multi-photon tolerant protocol that differs from the single-photon protocols in many aspects. We now compare it with the BB84 protocol which is the prime example of a single photon protocol:

1) Multi-stage protocols use pulses of photonic beams consisting of mN photons per pulse. The BB84 protocol uses a single photon per pulse.
2) The underlying physical principles used to prove security are the same, yet emphasized differently. The multi-stage protocol is based on the Heisenberg uncertainty principle mainly by the fact that measuring a state of polarization with fewer numbers of photons than needed will generate quantum noise that an eavesdropper cannot overcome. On the other hand, the BB84 is mainly based on the no-cloning theorem and its underlying fact that a copy of a photon cannot be generated with accuracy.
3) It should be noted that the operation of the multi-stage protocol is comparable to that of the BB84 if the number of photons mN is restricted to no more than one. In this case the multi-stage protocol can operate with only two different polarization transformations at each end of the communication. In other words the protocol will be using only four different polarization angles to secure the transmission of a single photon.

4) It might seem that in BB84 no prior secret string (initialization vector) is needed to start the communication. This is not the case since in order to authenticate the messages sent through the public channel, Alice and Bob need a common secret string to start with. Thus, the assumption is made in the key/message expansion multi-stage protocol that Alice and Bob share some random string (initialization vector); this is implicitly made in BB84 as well [74].

5) In the BB84 protocol, the receiver as well as the intruder is required to distinguish among four different polarization angles. Thus, both the receiver and the intruder measurements are probabilistic. In the case of a multi-stage protocol, an intruder Eve will be faced with identifying from among an infinite number of polarization angles. In contrast, the intended receiver only needs to distinguish between two orthogonal polarization angles.

VI. Conclusion

This chapter has analyzed the security of the multi-stage, multi-photon tolerant protocol for quantum secure communication. The security of the multi-stage protocol is based on the fact that while a legitimate receiver only needs to distinguish between two orthogonal polarization states, an intruder has to distinguish among an infinite number of possible polarization states. In other words, while the receiver would need only one photon to do so, an intruder would need to siphon off a minimum number n of photons per stage. The results presented in this chapter set an upper bound on the number of photons at $3N \leq 4.5$ in the case of the three-stage protocol. As long as the average number of photons that Eve can siphon off from each leg is less than N, the

communication between the parties is expected to be secure from a photon number splitting attack. The chapter has also assessed the security of the generalized multi-stage protocol to the Trojan horse attack and the additional measures for defying such attacks have been proposed. The proposed security analysis is discussed in the case of the three-stage multi-photon protocol; however, it should be noted that this analysis can be generalized to any case of the multi-stage protocol. Furthermore, a comparison between the BB84 protocol and the multi-stage protocol has been presented. The proposed security analysis discussed demonstrates that a multi-photon protocol can provide quantum secure communication while using a larger average number of photons. This in turn enhances the performance of the multi-stage protocol compared to its single-photon counterparts.

Chapter 5: Security Analysis of the Multi-stage Protocol

The previous chapters presented a multi-stage, multi-photon quantum cryptography protocol based on the double-lock cryptography. As mentioned earlier, the multi-stage protocol exploits the asymmetry in the detection strategies between the legitimate users and the eavesdropper. In this chapter, we study the security of the multi-photon protocol using coherent states by demonstrating its security against the intercept-resend (IR) attack, the photon-number-splitting (PNS) attack, and the man-in-the-middle (MIM) attack. It is found that the mean photon number of the coherent pulses can generally be greater than 1. The protocol thus has the potential to allow QC using detectors that may not be very efficient.

The principle behind the multi-photon, multi-stage protocol discussed earlier 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 [73] and the keyed communication in quantum noise (KCQ) method [95].

This chapter calculates the secure key rate in terms of the optimal error probability of eavesdropping. In addition, it devises an authentication method to check for the potential man-in-the-middle attack that could be launched by the eavesdropper and determined the modified secure key rate achievable in the presence of such an attack. It is worth noting that in case the key/message expansion protocol proposed in Chapter 3 is used, the three-stage protocol acts as a quantum communication protocol rather than key

distribution protocol. However, in the authentication method developed in this chapter the three-stage protocol is assumed to be a QKD protocol. In addition, an estimate of the maximal mean photon number when the channel loss is taken into account is calculated. This chapter also provides a detailed analysis of the security of the simplest form of the multi-stage protocol, the three-stage protocol. The dependence of the error probabilities in terms of the number of photons utilized in the channel is studied.

The amount of polarization rotations that both sides (Alice and Bob) select to give to the information bits is an arbitrary and independent value which varies from 0 to π degrees. It should be noted that practically one must also take into account the difficulties with maintaining fidelity in the presence of noise. In the following analysis, such a requirement is ignored and it is assumed that Alice and Bob can maintain perfect alignment in their basis for simplicity.

I. Intercept-Resend (IR) and Photon Number Splitting (PNS) Attacks

First, consider the situation that the communication between Alice and Bob is "authenticated", i.e., Alice knows that the information she sends out passes through Bob in the intermediate step and vice versa. Under this assumption, Eve can launch intercept-resend (IR) attacks, or more importantly, the photon-number-splitting (PNS) attack.

The main difference between IR and PNS is that, in IR all the photons are being taken out by Eve and she then resends any photon state to Bob. On the other hand, under PNS attack, the number of photons Bob receives is less than that in the original pulse. Such

a loss of photons practically could be due to the channel loss, but in this analysis it is attributed to the action of the intruder.

If we further restrict ourselves to the situation of incoherent attacks, Eve is required to perform measurements before the classical post processing. Therefore, under the IR attack, the polarization states of the pulses resent by Eve usually are different from those she intercepts because of the measurement process, with the difference depending on the number of photons she receives. The security against the IR attack can be estimated by assuming the polarization states of the resent pulses are the same as those before the pulses are intercepted by Eve. This is an overestimation of the ability of Eve. Nevertheless, it enables us to analyze IR and PNS attacks using the same formalism. In addition, Eve's information I_{EA} and I_{EB} become identical, where $I_{EA} = \max_{\text{Eve}} I(E:A)$ is the maximal mutual information between Eve and Alice with a similar expression for $I\ (E:B)$.

For the IR and PNS attacks on the three-stage protocol, Eve only needs to measure the polarization angles of any two stages. Then she can extract the bit value by orienting her measurement device in the third stage according to the angles of the first and second stages.

More definitely, suppose the polarization angles of the three stages of the protocol are denoted by $\phi_1 = X + \alpha$, $\phi_2 = X + \alpha + \beta$ and $\phi_3 = X + \beta$, where X is the information bit angle (0 or $\frac{\pi}{2}$), and α and β are the angles associated with Alice's and Bob's unitary transformations. Then the corresponding angles estimated by Eve for the first two stages are written as $\hat{\phi}_1 = \hat{X} + \hat{\alpha}$ and $\hat{\phi}_2 = \hat{X} + \hat{\alpha} + \hat{\beta}$. As a result, the estimate of the polarization

rotation applied by Bob is $\hat{\beta} = \hat{\phi}_2 - \hat{\phi}_1$. In order for Eve to obtain useful information, she requires that the error in determining β should not be too large. Since X is a binary random number of either 0 or $\frac{\pi}{2}$, Eve will determine the bit value erroneously if $\left|\hat{\beta} - \beta\right| = \left|(\hat{\phi}_2 - \hat{\phi}_1) - (\phi_2 - \phi_1)\right| > \pi/4$. The error probability of Eve is then given by

$$P_e(N_1, N_2) = \int_S d\hat{\phi}_1 \, d\hat{\phi}_2 \, d\phi_1 d\phi_2 \; P(\phi_1) P_1(\hat{\phi}_1 \mid \phi_1, N_1) P(\phi_2) P_2(\hat{\phi}_2 \mid \phi_2, N_2) \quad (5.1)$$

where $P(\phi) = 1/2\pi$ is the prior distribution of Alice's (Bob's) rotation angle and $P_i(\hat{\phi}_i \mid \phi_i, N_i)$ is the conditional probability of determining $\hat{\phi}_i$ given the angle ϕ_i and the mean photon number N_i that is accessible by Eve. The integration domain S corresponds to the region where the condition $\left|(\hat{\phi}_2 - \hat{\phi}_1) - (\phi_2 - \phi_1)\right| > \pi/4$ is satisfied. The mutual information $I\,(E:A)$ is given by $I(E:A) = 1 - h(P_e)$.

Consider a three-stage protocol using coherent states of mean photon number N. First of all, Alice should randomize the phases of the coherent states to avoid Eve exploiting the phase information [96]. In this case, the quantum state is described by a density matrix with photon number following the Poisson distribution with parameter N.

To obtain a bound of the secure key rate, one has to estimate Eve's maximal information. This involves an optimal measurement strategy to obtain the conditional probability $P_i(\hat{\phi}_i \mid \phi_i, N_i)$. Bagan et al. [97] gave a detailed comparison of the estimation of the polarization state of a finite number of photons using the collective and local measurements. Instead of an optimal polarization measurement, in the following we

consider a simple strategy that Eve performs polarization analysis with a fixed basis, denoted as horizontal and vertical, that is the same as Alice and Bob's basis. Such a fixed basis measurement is generally not optimal. Nevertheless, we additionally assume that Eve can determine the polarization angle correctly using a single basis only, instead of two bases that are required for the polarization states on a circle of the Poincaré sphere. This is accomplished by attributing Eve's measured polarization in the correct quadrant as the original polarization in the numerical calculations below. This procedure effectively doubles the number of photons available to Eve for the estimation, and the fidelity obtained is generally even better than that using optimal collective measurements

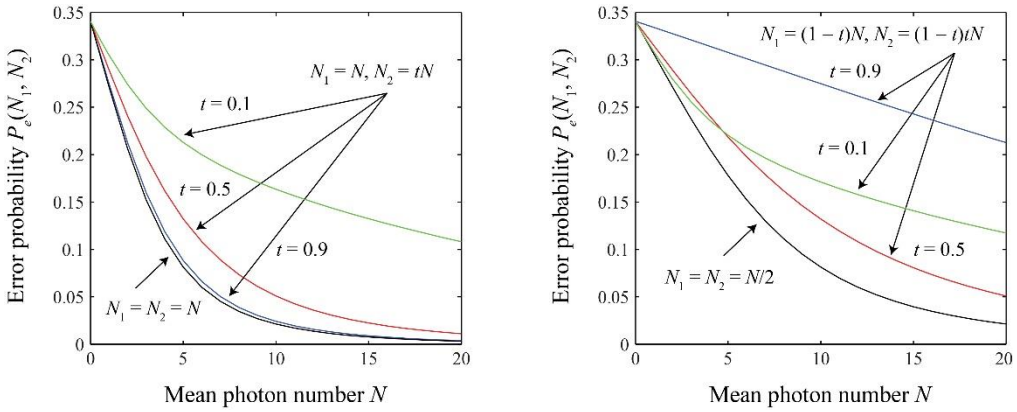
With the measurement strategy mentioned above, the probability distributions of Eve's numbers of horizontal and vertical photons in the three stages are given by

$$P_i\left(n_{H,i}, n_{V,i} \mid \phi_i, N_i\right) = \frac{e^{-N_i}}{1-e^{-N_i}} \frac{\left(N_i \cos^2 \phi_i\right)^{n_{H,i}} \left(N_i \sin^2 \phi_i\right)^{n_{V,i}}}{n_{H,i}! n_{V,i}!} \qquad (5.2)$$

for $i = 1, 2, 3$, where N_i is the mean number of photons in stage i that is accessible by Eve. Here the continuous variable $\hat{\phi}_i$ in (5.1) is replaced by the discrete variables $n_{H,i}$ and $n_{V,i}$. Then ϕ_i can be estimated from the numbers of photons detected in the vertical port ($n_{V,i}$) and the horizontal port ($n_{H,i}$) of the polarization analyzer by $\tan^2 \hat{\phi}_i = n_{V,i} / n_{H,i}$. Note that in (5.2), $n_{H,i}$ and $n_{V,i}$ cannot be zero simultaneously, for this gives no information to Eve about the angle ϕ_i. Also we assume N_i is known to Eve.

For the PNS attack, Eve's best strategy without causing errors to Bob's received bits will be to take $N_1 = N_2 \sim \frac{N}{2}$ if Bob did not monitor the photon statistics. Nevertheless,

we require that Bob monitors the number of incoming photons so that Eve cannot probe Alice and his devices with very bright pulses. For the IR attack, we can consider $N_1 = N_2 \sim N$. This corresponds to the optimal situation for Eve when the channel is assumed to be lossless. For a lossy channel with transmittance t, we consider $N_1 = N$ and $N_2 = tN$ for IR and $N_1 = (1-t)N$ and $N_1 = (1-t)tN$ for PNS. Figure 18 gives the plots of P_e as a function of the mean photon number N. It is seen in Figure 18 that even at the mean photon number $N = 10$, there is considerable error in Eve's estimated values of the true bit values.



(a) (b)

Figure 18: Plots of the (a) IR and (b) PNS error probabilities of Eve as functions of the mean number of photons N.

As mentioned previously, Alice and Bob need to monitor the number of incoming photons to deny Eve from injecting a very bright beam to probe their encoding devices. The presence of Eve is revealed if Alice and Bob also check the photon number distribution and detect any loss or change of the distribution. Eve could compensate the photon loss in the channel by injecting photons of arbitrary polarizations or at the angles $\hat{\phi}_i$, as in the IR attack. Nevertheless, this introduces extra error in her determination of $\hat{X}$ as well as error in Bob's bits. In addition, the IR attack in fact induces errors to the bit

values obtained by Bob. The estimation of the rotation angle error is addressed by the authentication process which specifically handles the man-in-the-middle attack in the next section.

II. Authentication

The three-stage protocol can be compromised entirely if Eve launches the man-in-middle (MIM) attack as depicted in Figure 19. Here Eve impersonates Bob to extract the true bit value perfectly. She also impersonates Alice to send the bit angle X together with the unperturbed angle β back to Bob, so that Bob receives the bit without error and hence cannot catch Eve. In such an MIM attack, Eve totally separates the quantum communication between Alice and Bob. Therefore the attack could be revealed if authentications are made by Alice and Bob to guarantee the locks are legitimate, i.e., they are the true users who applied the rotation angles on the pulses they received in the three stages.

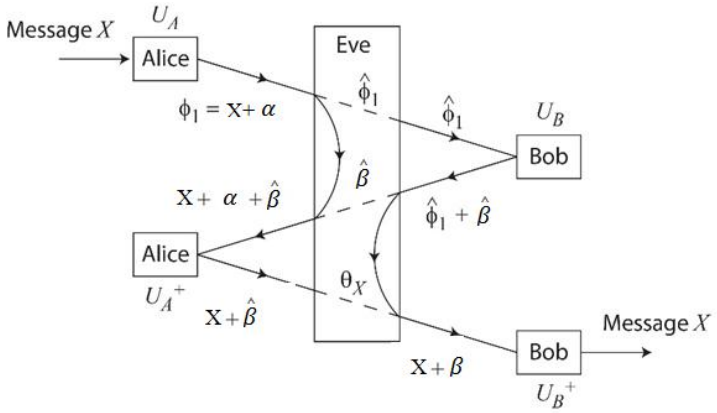


Figure 19: Schematic diagram of the three-stage protocol under the man-in-the-middle (MIM) attack

In principle, authentication can be performed perfectly if Alice and Bob could retain the photons in steps 2 and 3 of the protocol above until the end of the key exchange,

which can be accomplished by using quantum memories [98, 99] or slow light technologies [100]. More practically they need to perform measurements to determine the parameters of the transformations during the key exchange. At the end of the key exchange, they check their measured values against the true values (step 6). It should be noted that we assume Alice and Bob are authenticated for exchanging classical information on a public channel. This will rule out the chance that Eve is also in the middle when Alice and Bob try to compare the measurements.

We consider that the transmittance of the quantum channel is t. If Alice sends pulses with a mean photon number of N, Bob expects to receive pulses with mean photon number tN in the first stage and t^3N in the third stage, and Alice expects to receive pulses with mean photon number t^2N in the second stage. Therefore, for the MIM attack, Eve can extract a mean photon number of $t(1-t^2)N$ to obtain the estimate $\hat{\phi}_1$ and a mean photon number of $t(1-t^2)N$ to obtain the estimate $\hat{\beta}$. Eve then uses these two angles to impersonate Alice and Bob simultaneously. If Bob uses the pulse for authentication instead of the normal three-stage, the angle $\tilde{\phi}_1$ he measures conditioned on ϕ_1 will have a distribution given by $P(\tilde{\phi}_1 \mid \hat{\phi}_1, tN)P(\hat{\phi}_1 \mid \phi_1, (1-t^2)N)$. Here ϕ_1 is announced to Bob by Alice at the end of the protocol. Using this angle, Bob can guess X with an error probability of

$$P_e^{\text{Auth,MIM}}(t,N) = \int_{|\phi_1-\tilde{\phi}_1|>\pi/4} d\phi_1 d\hat{\phi}_1 d\tilde{\phi}_1 \; P(\tilde{\phi}_1 \mid \hat{\phi}_1, tN)P(\hat{\phi}_1 \mid \phi_1, (1-t^2)N)\; P(\phi_1) \qquad (5.3)$$

On the other hand, in the normal operation when the MIM attack is not present, Bob's error probability is instead given by

$$P_e^{\text{Auth, normal}}(t,N) = \int_{|\phi_1-\tilde{\phi}_1|>\pi/4} d\phi_1 d\tilde{\phi}_1 \; P(\tilde{\phi}_1 \mid \phi_1, tN) P(\phi_1) \qquad (5.4)$$

It is remarked that (5.3) and (5.4) manifest the fact that, like Eve, Bob and Alice cannot estimate the polarization angles with certainty in the middle of the three-stage protocol because the photons are not in orthogonal states.

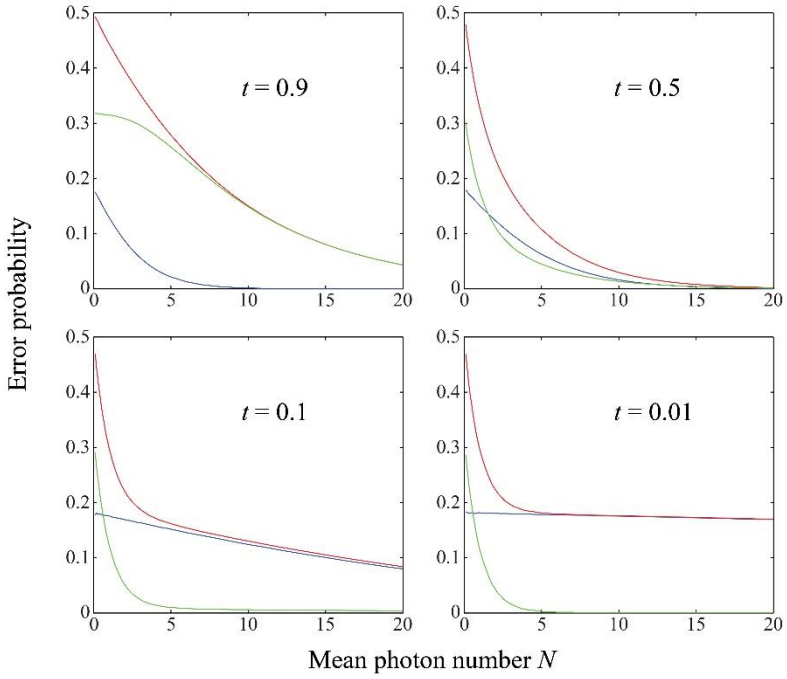


Figure 20: Bob's error probabilities in the estimation of X for the normal three-stage operation (blue lines) and under the MIM attack (red lines) at different values of the channel transmittance t. The green lines denote the differences between the two error probabilities

Numerical simulations were performed using the measurement scheme described in the last section. Figure 20 shows the two error probabilities as functions of the mean photon number N for different values of the transmittance t. In addition, $P_e^{\text{Auth, normal}}(t,N)$ is found analytically to be

$$P_e^{\text{Auth, normal}}(t,N) \approx \frac{2}{\pi\left(1-e^{-N}\right)}\left[\int_{\frac{\pi}{4}}^{\frac{\pi}{2}} \sum_{n_H=1}^{\infty} P_1(n_H,0 \mid \phi_1, tN) d\phi_1 + \int_0^{\frac{\pi}{4}} \sum_{n_V=1}^{\infty} P_1(0,n_V \mid \phi_1, tN) d\phi_1\right]$$

$$= \frac{4}{\pi}\int_0^{\frac{\pi}{4}} \frac{1-e^{tN\sin^2\phi_1}}{1-e^{tN}}\,d\phi_1 = \frac{e^{\frac{tN}{2}}\left[I_0\left(\frac{tN}{2}\right)-L_0\left(\frac{tN}{2}\right)\right]-1}{e^{tN}-1}, \quad (5.5)$$

where In(x) is the modified Bessel function of the first kind and Ln(x) is the modified Struve function.

It is noted in Figure 20 that at small N the error probabilities tend to the constant values $P_e^{\text{Auth, norm}} \to 2^{-1} - \pi^{-1}$ and $P_e^{\text{Auth, MIM}} \to 0.5$ whereas both probabilities tend to zero at large N. When the transmittance decreases, the two error probabilities converge to each other at a smaller N. In addition, the difference $P_e^{\text{Auth, MIM}} - P_e^{\text{Auth, norm}}$ approaches an asymptotic form when $t \to 0$, which is non-negligibly greater than zero for $N < 4$.

III. Amplification Attack

So far we have only focused on the situation where Eve makes direct measurement using the photons that she siphons off from the quantum channel. Generally she can do more with her photons. An important class of attacks is the one that Eve amplifies the quantum states that she extracts from the channel. This kind of attack is linked to the foundation of the three-stage protocol, that is whether she can find out the angles α and β, which are open to her eavesdropping, with high precision. In fact, the purpose of using a finite number of photons in the channel is to limit Eve's precision of measurement.

It is well known that the amplification of a quantum state must also accompany with the amplification of the noise [101]. For the implementation with coherent states discussed in this chapter, Eve does not gain anything by amplifying the signal. Even with

the use of squeezed states, Fock states or entangled states to resend pulses to Bob and Alice, the intensity check by Alice and Bob will introduce vacuum noise to Eve's probes, and Eve's information gain may only be modest.

On the other hand, it has recently been shown that noiseless amplification of a quantum state is possible if a perfect guarantee of success is not required, unlike the usual deterministic linear amplification mentioned above [102, 103] .Experiments of amplifying coherent states noiselessly have already been demonstrated [104, 105]. This apparently imposes a significant drawback to the three-stage protocol. Nevertheless, it should be noted that the probabilistic nature of the amplification means that Eve's bit rate will further decrease. More importantly, the implementations of the amplification of coherent states operate with high fidelity only when the mean photon number after the gain is around unity [104, 105]. The amplification attack works well essentially for very weak coherent states but not for the regime of $N > 1$ that we consider in our protocol. The distortion of the quantum states at larger N introduces noise to the determination of the polarization. Further work is needed to quantify the effects of the amplification attack to the security of the protocol.

Another issue related to the amplification attack on the three-stage protocol is that, in the actual implementation, the polarization rotations U_A and U_A nevertheless have to be confined to a finite set because of the noise and stability of the experimental setup. Such limitation may open up the unambiguous state discrimination (USD) attack [106, 107] . Fortunately, the polarization rotations are local information that is secret to Alice and Bob independently; they can change their sets of the rotations frequently without disclosing their actions. This results in an extremely large set of the polarization rotations and

effectively mitigates the threat of the USD attack, which requires that the number of photons needed must be greater than or equal to the number of polarization states in the middle of the three-stage protocol.

IV. Security and Key Rate Efficiency

With error correction and privacy amplification, the expression for the secret key rate extractable using one-way classical post processing is [22]

$$K = R\left[I(A:B) - \min\left(I_{EA}, I_{EB}\right)\right], \quad (5.6)$$

where R is the raw key rate, $I(A:B)$ is the mutual information between Alice and Bob, and I_{EA} and I_{EB} are Eve's information about the raw key of Alice and Bob respectively. We consider the case when $H(A) = H(B) = 1$ and $H(A \mid B) = H(B \mid A) = h(Q)$, where $h(Q)$ is the binary entropy function and Q is quantum bit error rate (QBER). For the three-stage protocol, the raw key rate is given by the total bit that Bob measured minus the bits for authentication.

Assuming the error correction is carried out perfectly and using a very conservative estimate for the PNS/IR attack mentioned in Section I with mutual information $I(E:A) = 1 - h\left(P_e(N, tN)\right)$, the security key rate then becomes

$$K = R\left[(1-f)h\left(P_e(N, tN)\right) - h\left(Q\right)\right], \quad (5.7)$$

where f is the fraction of the MIM attacks launched by Eve, which is estimated by the ratio of the measured authentication error probability difference and the expected measured authentication error probability difference, i.e.,

$$f = \frac{P_e^{\text{Auth, measured}}(t,N) - P_e^{\text{Auth, norm}}(tN)}{P_e^{\text{Auth, MIM}}(t,N) - P_e^{\text{Auth, norm}}(tN)}. \qquad (5.8)$$

The threshold for the QBER is then determined by the condition $K > 0$ for some given $f < 1$ and N.

A potentially significant drawback of the three-stage protocol compared to other QKD protocols is that it requires multiple quantum communications between Alice and Bob, effectively increasing the photon loss of the channel. On the other hand, the multiple-photon resilient nature of the protocol allows a larger mean photon number to start with. As an estimate, we consider the ratio of the raw bit rates between the three stage protocol and the weak-coherent state BB84 with mean photon number 0.5. The ratio is given by

$$E = \frac{1 - e^{-Nt(3l)}}{1 - e^{-0.5t(l)}}, \qquad (5.9)$$

V. Conclusion

This chapter has given a detailed security analysis to a form of quantum cryptography protocol, the three-stage multi-photon quantum cryptography system, using coherent states to encode qubits. It is important to note that a three-stage protocol can be used as a quantum communication protocol if authentication between Alice and Bob is established before the onset of the protocol. In case this condition is not met, the three-stage protocol may be used as a QKD protocol and operate as section *II* of this chapter has described. In particular, this chapter has showed 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 certain error probability thresholds. In addition this chapter has

obtained the secure key rate in terms of the error probabilities under the attacks considered. Importantly, it has been found that 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 are considered. The multi-photon multi-stage QKD scheme presented does not require pre-sharing of a key between the legitimate users like the Y00 protocol. Hence it can be used to complement such multi-photon quantum communication protocols. This chapter has also discussed the amplification and unambiguous state discrimination attacks and argued that such attacks do not impose significant threat to the multi-stage protocol.

Chapter 6: Multi-photon Tolerant Protocols over Fiber Optics

This chapter investigates the performance aspects of practical quantum secure communication over Fiber Optics using multi-photon tolerant protocols [11, 75, 78]. As discussed earlier, multi-photon tolerant protocols weaken the limit on the number of photons imposed by currently used single photon based quantum key distribution protocols. This chapter calculates the secret raw key generation and quantum bit error rates as a function of distance over a fiber optic channel for several optimum average photon numbers μ (referred to as N in the previous calculations).

Multi-photon tolerant protocols can be either used in order to share a key, i.e. for QKD, or for direct quantum communication. In addition, multi-stage protocols can be used to share a key between Alice and Bob, followed by using the shared key as a seed key to a single-stage protocol. We call this process the braiding concept [108]. Security aspects of the multi-stage protocol were discussed earlier in Chapters 3-5.

This chapter particularly addresses the performance of the single-stage multi-photon tolerant protocol over fiber optics (FO).The secret raw key generation rates are calculated with respect to distance over a fiber optical channel. It is well-known that raw key generation rates decrease with the increase in distances. Coherent non-decoying quantum states are used in this chapter in order to transfer the encoded bits from Alice to Bob. Raw key generation rates are calculated for different optimum average photon numbers μ_{opt}, and with respect to distances over a fiber optical channel. As discussed in Chapters 4 and 5, we consider that μ_{opt}corresponding to the single-stage protocol is around 1.5 which is one third of the average number of photons derived for the three-stage protocol.

I. Multi-photon Tolerant Protocol Secret Key Rate Formulation

In this section, the secret and raw key rate formulation for the multi-stage protocol is introduced. These formulations are used in the rest of the chapter to evaluate the performance of the multi-stage protocol over fiber optics. A sender Alice has in her possession a list of M' symbols. She wishes to share them with Bob using a quantum protocol. In the case where Alice and Bob use the BB84, due to the sifting step, they will eventually end up with a list of $m' \leq M'$ symbols even when the channel loss is not considered. These raw keys are only partially correlated. If a multi-stage protocol is used, the sifting step is omitted. The keys shared between Alice and Bob will be of $m' = M'$ symbols.

To extract a short secret key K from the raw key of length $l \leq m'$, classical post-processing is required. The length of the final secret key depends on Eve's information about the raw keys. One way post processing is the most studied and characterized procedures and consists of two steps. The first step is error correction (EC), also called information reconciliation. At the end of which m' becomes shorter and perfectly correlated. The second step is privacy amplification (PA) and it is aimed at diminishing Eve's knowledge of the reference raw key.

In the asymptotic case where $M' \to \infty$, the meaningful quantity is the secret fraction:

$$r = \lim_{M \to \infty} \frac{l}{m'}$$

r is the quantity for which the security proofs in [22] provide an explicit expression. However, a more practical parameter must also be taken into account as well: namely the

raw-key rate R, i.e., the length of the raw key that can be produced per unit time. These rates depend on the protocol used and on the details of the implementation setup such as the source used, losses in the channel, and efficiency and type of detectors. In conclusion, to assess the performance of practical single-stage protocol, the secret key rate is defined as:

$$K = Rr \qquad (6.1)$$

i. Raw Key Rate (R) formulation

The raw key rate *R* is given by (6.2)

$$R = \nu_s P_{Bob}(N_{max}) = \nu_s \sum_{n=1}^{N_{max}} p_A(n)\left[1 - \left(1 - \eta_{det}\eta_{qc}\right)^n\right] \qquad (6.2)$$

The factor ν_s is the repetition rate of the source used and $P_{Bob}(N_{max})$ is Bob's detection probability. The number of photons n' is distributed according to the Poissonian statistics of mean $\mu = \langle n' \rangle$, $p_A(n) = \frac{\mu^{n'}}{n!}e^{-\mu}$. Alice encodes her bit in one photon with frequency $p_A(n' = 1)$, in two photons with frequency $p_A(n' = 2)$, and so on, and does nothing with frequency $p_A(n' = 0)$. η_{det} is the quantum efficiency of the detector (typically 10% at telecom wavelengths) and η_{qc} is the attenuation due to losses in the quantum channel. For fiber optics links with length D, η_{qc} is given by

$$\eta_{qc} = 10^{\frac{-\alpha_1 D}{10}}, \qquad (6.3)$$

where α_1 is the attenuation coefficient in dB/km at telecom wavelengths of interest.

ii. Secret fraction (r) formulation

The observed perturbations in the quantum channel due to Eve's intervention allow computation of a bound on the information that Eve might have access to during the transmission. Such a lower bound for security has been proven for many protocols in the uncalibrated-device scenario. In this chapter the derivation and analysis in [22] is followed in order to determine the lower bound respective to the three-stage protocol.

The secret fraction using one-way post-processing is given by (6.4):

$$r = [1 - h(Q) - I_E], \qquad (6.4)$$

where $h(x)$the binary entropy is function, and Q is the quantum bit error rate (QBER). Eve's information about the raw key shared between Alice and Bob is represented by I_E. Eve's information about the raw key must be kept at a minimum and should be less than the mutual information shared between Alice and Bob. Therefore, Alice and Bob should remove from the raw key a fraction equal to Eve's information about the raw key.

Hence (6.1) can be written as follows

$$K = R[1 - h(Q) - I_E] \qquad (6.5)$$

iii. Secret Key Rate (K) formulation

For a practical single-stage system, the secret key K should contain only quantities that are known from calibration or from the parameter estimation of the protocol (R, Q). Therefore, it is important to find an expression for I_E in terms of these quantities.

During the operation of the single-stage protocol, Alice and Bob need not to affect a sifting process due to the fact that the same basis is used during the encoding and the measurement procedure. Therefore, the detection rate for the events R_n, for the single-stage protocol does not include the sifting probability. Hence,

$$R_n = \nu_s \, p_A(n') \, f_{n'}, \qquad (6.6)$$

where $f_{n'}$ is the probability that Eve forwards some signal to Bob for n-photon pulses. Eve's attack must be optimized over the possibility $\{f_{n'}\}_{n'} \geq 0$ compatible with $\sum_{n'} R_{n'} = R$.

Based on the formulation in [22], the quantity to be subtracted in privacy amplification (PA) I_E is given in (6.7) [22, 32, 81, 82, 109, 110] . For simplicity we consider:

$$I_E = 1 - Y_1[1 - h(\varepsilon_1)] = 1 - Y_1\left[1 - h\left(Q/Y_1\right)\right], \qquad (6.7)$$

where Y_1 is given by [22]:

$$Y_1 = 1 - \frac{\nu_s}{R} p_A(n' \geq 2) = 1 - \frac{\mu}{2\eta_{det}\eta_{qc}}. \qquad (6.8)$$

The corresponding achievable secret key rate K in (6.5) can be written as

$$K = R\left\{Y_1\left[1 - h\left(Q/Y_1\right)\right] - h(Q)\right\}. \qquad (6.9)$$

iv. Optimizing The Secret Key rate K

Alice and Bob can optimize K by changing the parameters of the source, typically the intensity. There exists an optimum value for the intensity $\mu = \langle n' \rangle$ or the average number of photons. However, this optimum value cannot be estimated exactly in general, because Y_1 in (6.8) depends on μ. Using the approximate expressions and formulations for Y_1 from [22], the secret key rate K can be written as,

$$K = R\left\{\left(1 - \frac{\mu}{2\eta_{det}\eta_{qc}}\right)\{1 - h(2Q)\} - h(Q)\right\}. \qquad (6.10)$$

By calculating the secret key rate K as a function of μ at a fixed channel length, an optimum K value can be obtained at an optimum value of intensity referred to in this chapter as μ_{opt}. In Section *II*, we specifically use a short optical fiber ($D \approx 0$) for the calculation of μ_{opt}.This short distance represents a lossless channel.

To find an expression for Q one needs to include the contributions of dark counts and the above definition for R in (6.2). The raw key rate can then be written as

$$R = v_s(P_{Bob} + P_d) \qquad (6.11)$$

P_{Bob} is given by

$$P_{Bob}(N_{max}) = \sum_{n'=1}^{N_{max}} p_A(n)\left[1 - \left(1 - \eta_{det}\eta_{qc}\right)^{n'}\right] \qquad (6.12)$$

P_d is the dark count rate given by

$$P_d = 2p_d \sum_{n' \geq 0} p_A(n')[1 - \eta_{det}\eta_{qc}]^{n'} \qquad (6.13)$$

where $p_d = 10^{-5}$ is the dark count. The expected error rate Q or QBER can be written as follows [111]

$$Q = \frac{\varepsilon P_{Bob} + \frac{1}{2}P_d}{P_{Bob} + P_d}, \qquad (6.14)$$

where the error rate on the channel is given by $\varepsilon = \frac{1 - Visibility}{2}$ and the dark counts always gives an error of $\frac{1}{2}$.

The number of photons n' that Alice encodes her bit can vary as $n' \geq 1$ for $P_{Bob}(N_{max})$ and $n' \geq 0$ for P_d. Finally, using the optimum value of μ_{opt}, one can

calculate the secret key rate K from (6.10) as a function of distance. Also, one can calculate Q as a function of distance.

II. Secret Key Rate, Error Rate Data and Results

First, to find μ_{opt} that corresponds to the optimum secret key rate K from (6.10), we assume the following: 1) a maximum number of photons N_{max} that Alice can use to encode her bit, which is to represent a multi-photon beam with a specific number of emitted photons; 2) a lossless fiber optics channel which corresponds to a channel of length $D \approx 0$; 3) operating wavelength of $\lambda = 1550$ nm ; and 4) a typical quantum efficiency of the detector $\eta_{det} = 0.1$ and the dark count $p_d = 10^{-5}$.

To shed light onto the relationship between the maximum number of photons and μ_{opt}, we varied the maximum number of photons from $N_{max} = 1$ to $N_{max} = 12$ and found μ_{opt}. The results are shown in Figure 21 below. Figure 22 plots the relationship between maximum key rate and μ_{opt}. By examining the relationship shown in Figure 22, one notices that the relationship is far from linear and K reaches a saturation limit at around 8-10 photons.

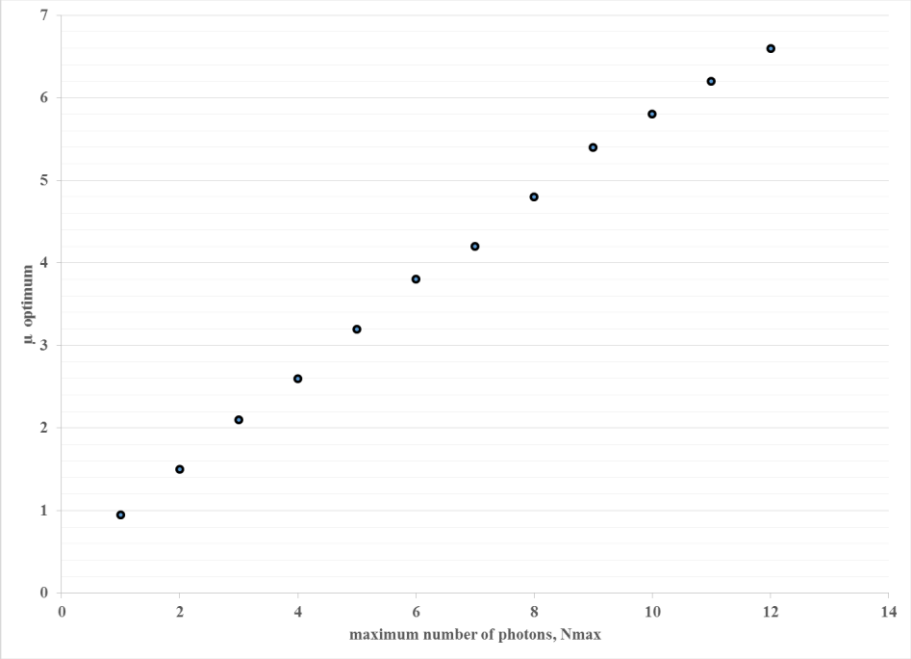


Figure 21: Plot of the optimum average number of photons $\boldsymbol{\mu_{opt}}$ as the function of the maximum number of photons $\boldsymbol{N_{max}}$ that Alice can used to encode her bits

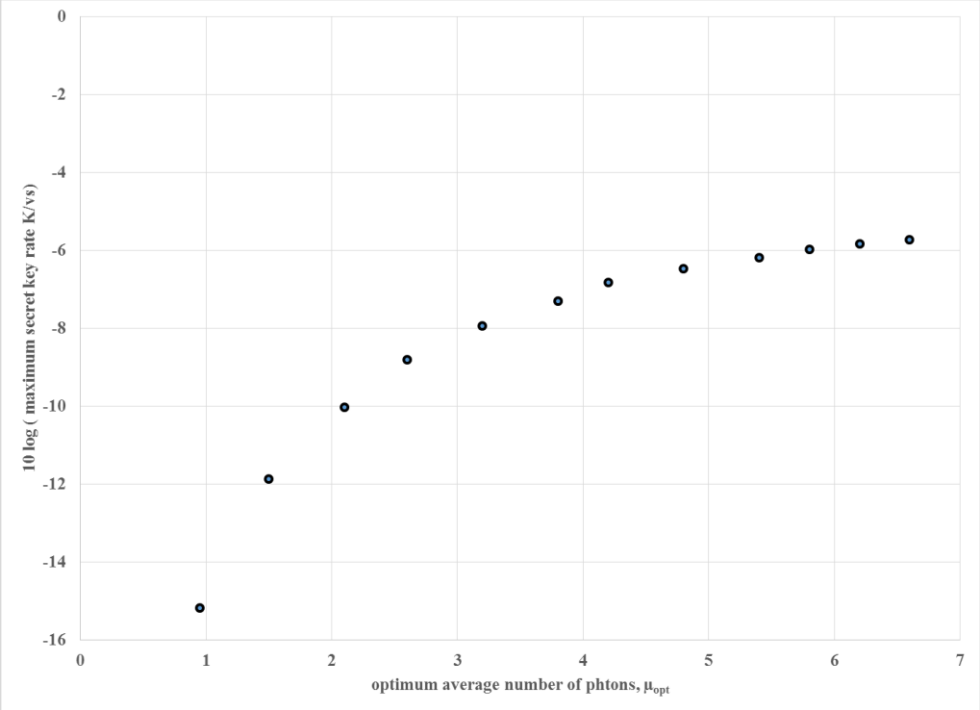


Figure 22: Plot of the maximum key rate as a function of the optimum average number of photons $\boldsymbol{\mu_{opt}}$ for a lossless fiber optics length

In Figure 23 we used the optimum average of photons values: μ_{opt} = 0.95, 1.5, 2.1 and 2.6 that corresponding to N_{max} = 1, 2, 3, and 4 respectively (as shown in Figure 21) to calculate the secret key as a function of distance and channel losses. As mentioned before, the inset of Figure 23 shows the secret key rate from (6.10) as a function of μ, and the maximum K value occurs at $\mu_{opt} = 2.6$ for $N_{max} = 4$ photons. This result falls within the security proofs of the three-stage protocol established in [112]; in other words the three-stage protocol can achieve a maximum key rate while providing a quantum secure communication. Using (6.12), (6.13) and (6.14), the secret key values from (6.10) can be calculated as a function of distance with μ_{opt} as a parameter. These calculations are plotted in Figure 23 where error correction (EC) and private amplifications (PA) are included for a non-decoying coherent state. It can be seen that an increase in the average number of photons means an increase in the achievable distance while maintaining a higher key rate. As is the case in μ_{opt} where a longer distance is achieved while having a key rate higher than the cases were μ_{opt} = 0.95, 1.5, 2.1, and 2.6.

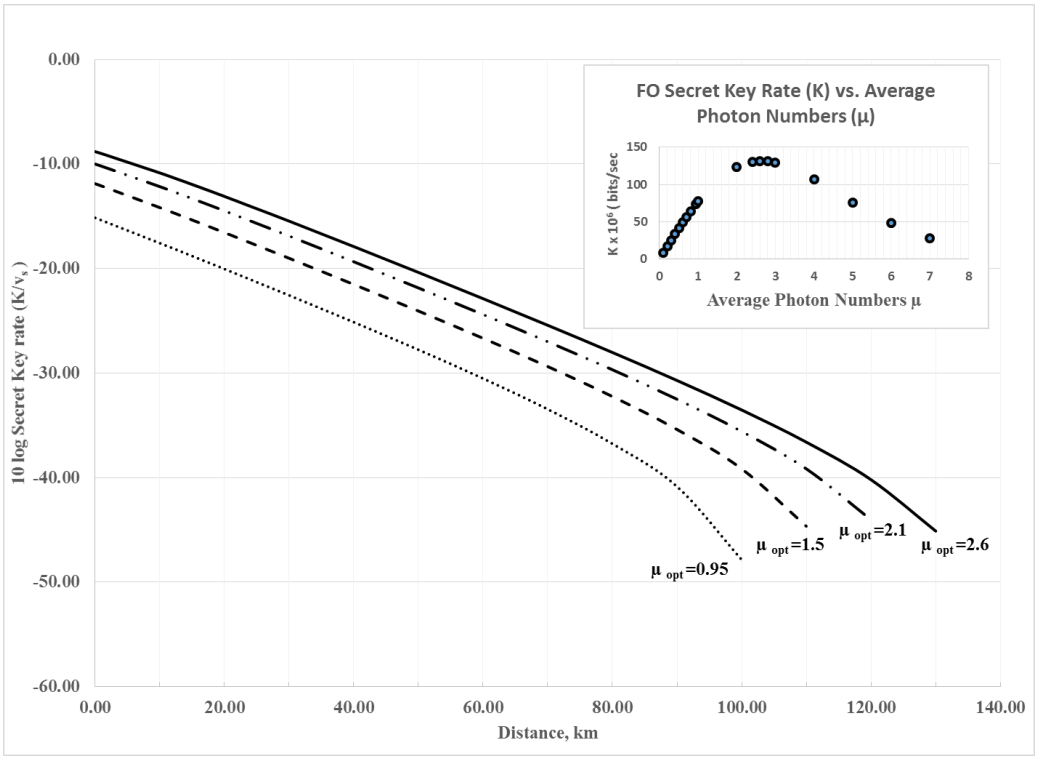


Figure 23: Plot of the maximum achievable key rate as the function of the distance for $\boldsymbol{\mu_{opt}}$= 0.95, 1.5, 2.1, and 2.6

The maximum possible distances (D_{max}) that can be achieved at the four values of μ_{opt} can be found from Figure 23 at the fall off *K* values. Similarly, we can find the maximum possible distances for the remaining μ_{opt} values found in Figure 21 above. The relationship between these maximum distances and μ_{opt} are shown in Figure 24. This relationship can be used to estimate the maximum possible distance that can be achieved for any value of μ_{opt}.

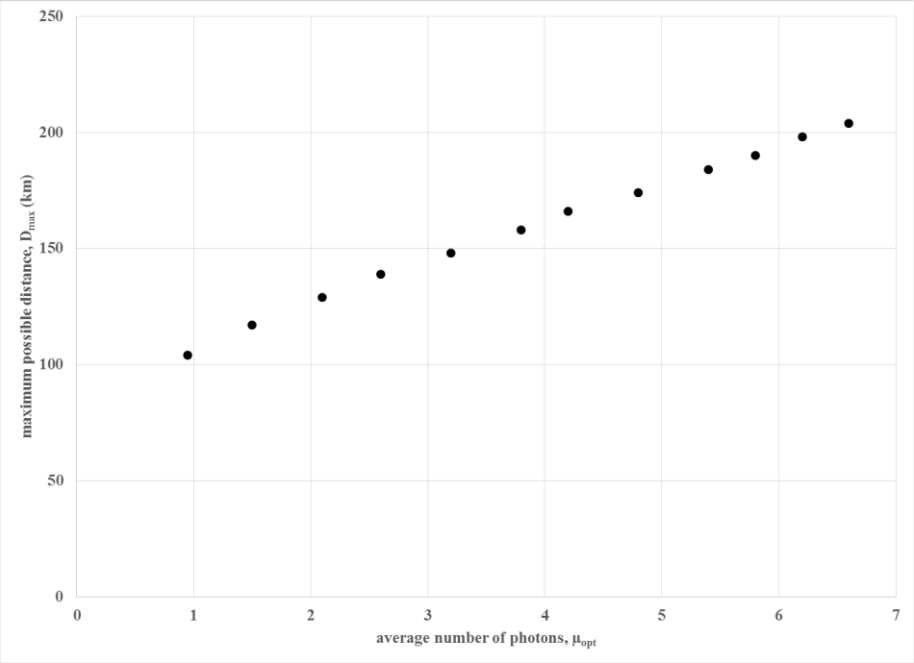


Figure 24: Plot of the maximum achievable distance as function of the optimum average number of photons $\boldsymbol{\mu_{opt}}$

Figure 25 shows the effects of error correction (EC) and privacy amplifications (PA) for a non-decoy state at μ_{opt} = 2.6 as a function of distance and channel losses (inset). It can be noted that these effects are small for short distances and losses values. However as we approach the maximum possible distance the channel loses increase thus EC and PA have more severe effects on the key rate. This leads to a sharp drop in the secret key rate at the distance of about 120 km (or the loss of about 30 dB).

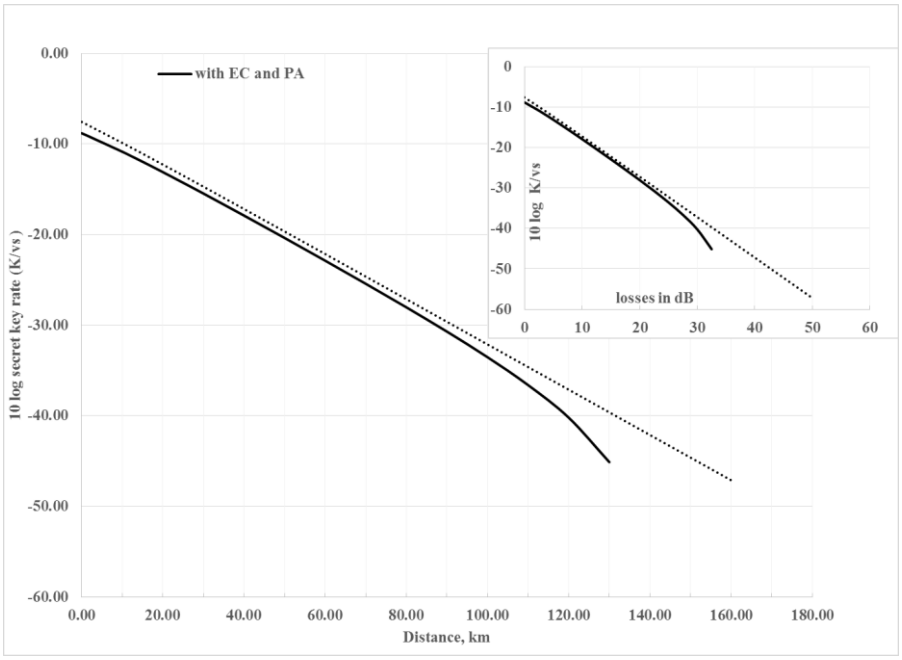


Figure 25: Plot of the secret key rate as a function of the distance (Km) and losses (dB) for $\boldsymbol{\mu_{opt}}$=2.6

Figure 26 shows the influence of the wavelength used on the secret key rate values for μ_{opt} = 2.6 at λ = 1550 nm, 1300 nm, and 800 nm with attenuation coefficients of 0.25, 0.35, 2 dB/km, and detector efficiencies of 0.9, 0.1, and 0.1, respectively. The achievable distance is higher at λ = 1550 nm that is due to the low attenuation of the medium at this wavelength. The attenuation coefficient affects the secret key rate through the variable η_{qc} as seen from (6.3).

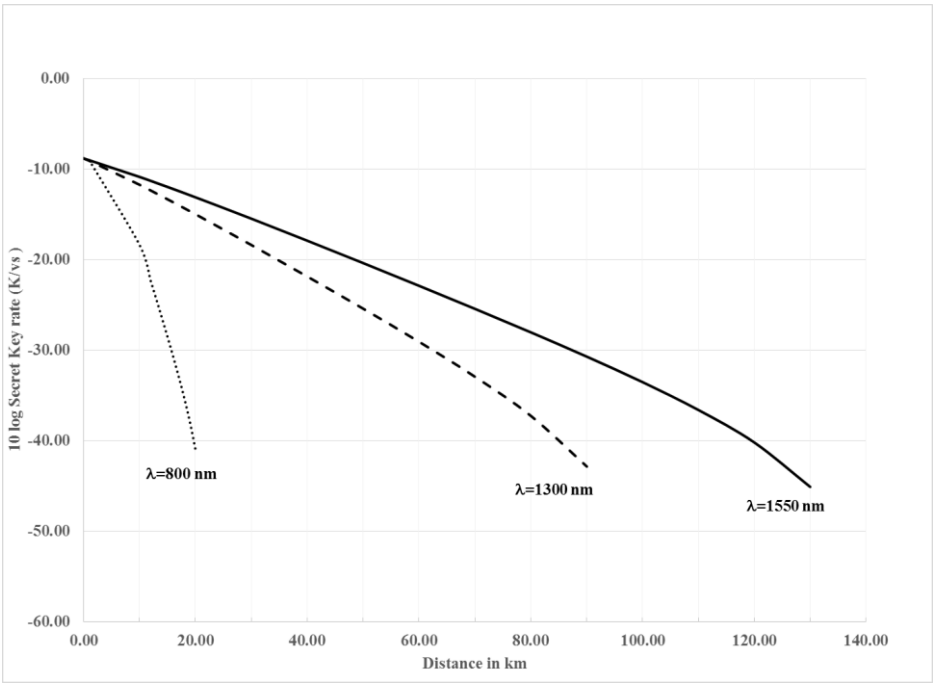


Figure 26: Plot of the key rate as a function of the distance (Km)

Using (6.12) and (6.13), the error rate Q or QBER in (6.14) can be calculated as a function of distance. Figure 27 shows the variation of the QBER as a function of the distance for μ_{opt} = 0.95, 1.5, 2.1, and 2.6. The QBER at μ_{opt} = 2.6 which is the optimum value derived from Figure 23 exerts the same increasing pattern as in the cases of μ_{opt} = 0.95, 1.5, and 2.1. The only difference is the distance at which the value of QBER increases sharply.

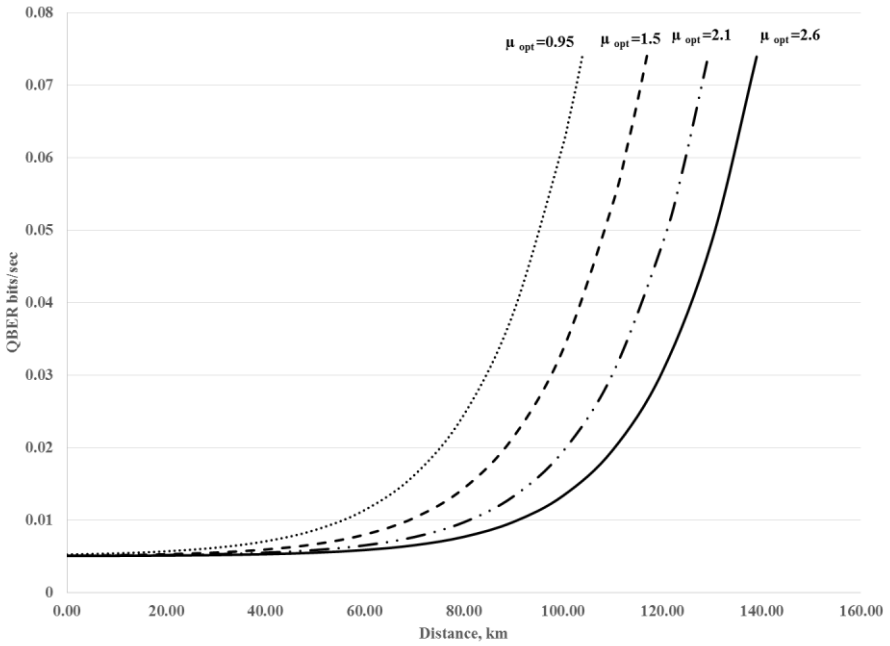


Figure 27: Plot of the QBER as a function of the distance (Km) for μ_{opt} = 0.95, 1.5, 2.1, and 2.6

III. Conclusion

This chapter has investigated the performance aspects of a practical quantum secure communication using multi-photon tolerant protocols. The security of such protocols stems from the fact that the optimal detection strategies of the legitimate user and the eavesdropper are asymmetrical, allowing Bob to obtain measurement results deterministically, while imposing unavoidable quantum noise to the eavesdropper Eve's measurement. This chapter has also presented the results of a study of multi-photon tolerant multi-stage protocols, security aspects as well as challenges to the practical implementation. In this chapter, coherent non-decoying quantum states have been used to transfer the encoded bits from Alice to Bob. The maximum number of photons that Alice can use to encode her bit was varied from N_{max} = 1 to N_{max} = 12. An optimum value μ_{opt} has been found for each N_{max} and as a result a relationship between both

values has been derived. Also, a linear relationship has been obtained between the maximum distance that can be achieved and μ_{opt}. However, by examining the relationship between the maximum key rate as a function of μ_{opt}, one notices that the relationship is far from linear and *K* reaches a saturation limit at around μ_{opt} = 4.8 – 5.8 that corresponds to $N_{max} = 8 - 10$ photons.

The relationship between the secret key generation rates for μ_{opt} = 0.95, 1.5, 2.1, and 2.6 has been calculated with respect to both losses and distances over a fiber optical channel. This chapter has shown that at μ_{opt} = 2.6, the key generation rates are higher than the cases were μ_{opt} = 0.95, 1.5, and 2.1. It is worth noting that the BB84 operates at μ = 0.1, which is much less than the case of the multi-stage protocol. The QKD multi-stage protocol using a coherent state uses an average of 1.5 photons per stage. However, in case it is used as a communication protocol the average number of photon number per stage is 3.3. Furthermore, this chapter has shown that the QBER in case of μ_{opt} = 2.6 exerts the same characteristics as in the cases of μ_{opt} = 0.95, 1.5, and 2.1; the only difference is the distance at which the value of QBER increases sharply. The calculations derived in this chapter can be generalized to evaluate the performance of any multi-stage QKD or communication protocol.

Chapter 7: Application of the Multi-stage Protocol in IEEE 802.11i

The dynamics of the work force environment has evolved substantively by the introduction of wireless communication. Professionals nowadays can work without being tied to a certain location. In addition to the advantages of mobility, wireless networks gained popularity due to various other benefits such as: convenience, productivity, deployment, and expandability. While wireless networks are becoming more popular day after day, related security issues are expanding in unison. Due to their nature, snooping and modifying a transmitted wireless signal is easier compared to its wired counterpart.

The focus of this chapter is to present a model of integration of the multi-stage quantum cryptography protocol into the IEEE 802.11 wireless communication standard. It proposes a method to integrate the three-stage quantum cryptography protocol and its variants into the key distribution scheme of the IEEE 802.11 standard. Integrating the three-stage protocol with the IEEE 802.11 standard offers several benefits compared to the utilization of its single-photon counterpart. These benefits are: enhanced data rates, longer distance, and an increased number of photons that can be used during the transmission process. Integrating the multi-stage protocol and the three-stage protocol into the IEEE 802.11 network will provide such networks with a security level comparable to that of quantum cryptography.

I. IEEE 802.11i

The IEEE 802.11i standard defines a Robust Security Network Association (RSNA) based on IEEE 802.1X [113] authentication. RSNA is defined in order to provide better authentication and confidentiality in 802.11 networks compared to that of WEP.

Three entities are involved in the authentication process: the Supplicant, the Authenticator, and the Authentication Server. In general, a supplicant and an authenticator have successful authentication after they verify each other's identity and generate a secret key that can be used in following data transmissions.

The process of authentication in the IEEE 802.11i consists of handshakes between the authenticator and the authentication server, between the supplicant and the authentication server, and between the supplicant and the authenticator. The handshakes used in the process of authentication result in the generation of a common secret key called the Master Session Key (MSK). The MSK key is shared between the supplicant and the authentication server and is used by the supplicant to derive a Pairwise Master Key (PMK). The authenticator derives the same PMK using the Authentication, Authorization and Accounting (AAA) key material on the server side that is securely transferred to it. In other cases, the supplicant and the authenticator may be configured using a static Pre-Shared Key (PSK) to generate the PMK. In some other cases such as re-association, a cached PMK can be used in order to reduce the overhead employed on the authentication server when the same user undergoes repeated authentication processes.

After the establishment of a PMK, a four-way handshake protocol is executed. The four-way handshake key management protocol confirms the existence of the PMK, and the protocol generates a Pairwise Transient Key (PTK) for each subsequent session, synchronizes its installation into the MAC, and transfers the Group Transient Key (GTK) from the authenticator to the supplicants. Successful implementation of the four-way handshake means that a secure communication channel can be constructed between the

authenticator and the supplicant during the following data transmissions. The same PMK can be used in different four-way handshakes.

i. The four way handshake

Once the key between the authenticator and supplicant has been shared, the four-way handshake process will be started either by the authenticator itself or after a request from the supplicant. The message exchange is shown in Figure 28.

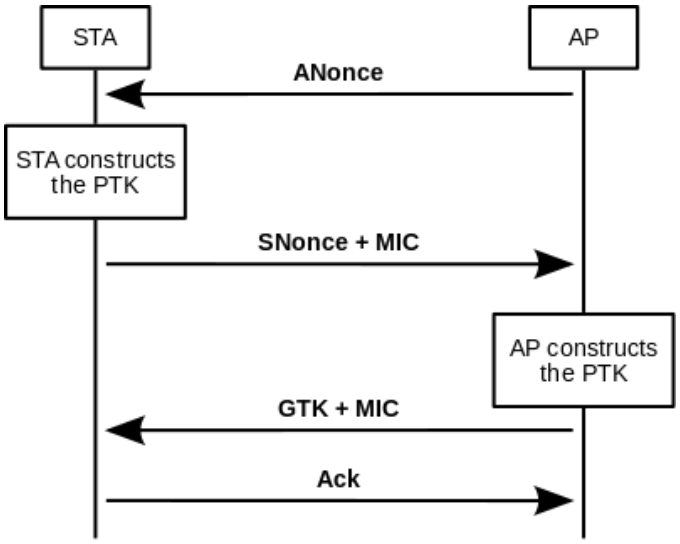


Figure 28: four-way handshake message exchange between an Access Point AP and a Station STA

The EAP exchange performed prior to the four-way handshake provides the shared PMK secret key. This key should be exposed as little as possible since it is intended to last for the complete session. The four-way handshake is actually used to establish another key called the PTK which is generated by concatenating the following attributes: PMK, ANonce, SNonce, AP MAC address, and STA MAC address. The product is then passed through a cryptographic hash function.

The messages exchanged during the handshake represented in Figure 28 are explained below [114]:

1. The Access Point (AP) sends a nonce-value to the Station STA (ANonce). The STA now has all the elements needed to construct the PTK.
2. The STA sends its own nonce-value (SNonce) to the AP together with a MIC (message integrity code).
3. The AP sends the GTK and a sequence number together with another MIC to be used in the next multicast or broadcast frame. In this way, the STA can perform basic replay detection.
4. The STA sends an acknowledgement to the AP.

The PTK is then subdivided into three main parts: Key Confirmation Key (KCK), Key Encryption Key (KEK), and Temporal Key (TK). Figure 29 depicts the pairwise key hierarchy:

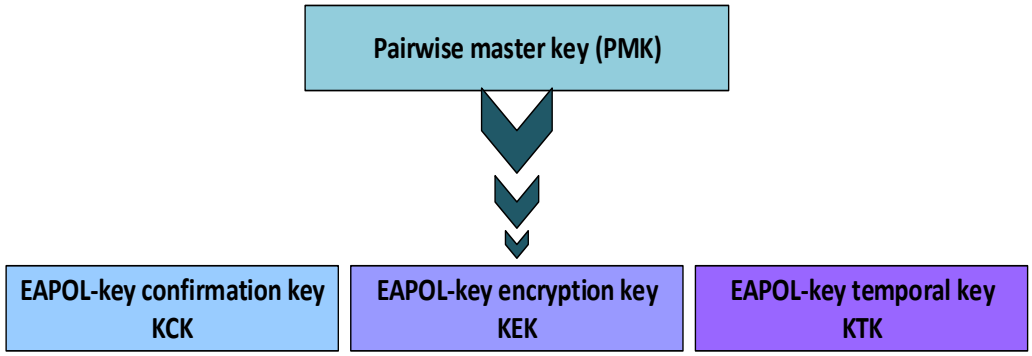


Figure 29: Pairwise key hierarchy

Some of the flaws of four-way handshake are explored in [114-118]. In addition, the tool Aircrack-ng is a 802.11 WEP and WPA-PSK keys cracking program that can recover keys once enough data packets have been captured. To prevent such attacks and

provide theoretically proved secure communication, the authors [119] proposed the integration of the BB84 protocol into the four-way handshake. The four-way handshake with integrated QKD is called the quantum handshake. Quantum handshake is discussed in the rest of the chapter.

II. Integration of QKD for key distribution in IEEE 802.11i

IEEE 802.11 wireless local area networks are a suitable candidate to be used in conjunction with quantum key distribution protocols. That is due to its limited coverage area of around 200 meters. Wi-Fi networks can offer a line-of-sight path, which is a major requirement for QKD. Furthermore, the sum of users of Wi-Fi is increasing significantly. Currently, all laptops are equipped with a Wi-Fi interface by default. This indicates that Wi-Fi networks must provide secured connections for the users of their services. As discussed in the previous chapters, QKD has the ability of providing unconditional security, thus it can offer Wi-Fi networks with the highest level of security that can be achieved.

The mode of integrating QKD into the key distribution process in Wi-Fi networks has been done with minimal modifications to the existing IEEE 802.11 and IEEE 802.1X protocols. The communication process implementing the four-way handshake and the initial exchange of capability parameters are the only key areas impacted when integrating QKD in the IEEE 802.11i standard.

In IEEE 802.11 standard, during the first flows of the communication, association between STA and AP is established. These initial flows involve Beacon, Probe Request and Probe Response frames. The beacon frame enables stations to establish and maintain communications in an arranged method. STA and AP use the initial flow messages to

agree on the set of parameters used for following communications. When QKD is integrated in the process, it is necessary that the STA and the AP agree on all QKD related parameters at the beginning. These key parameters include: QKD protocol, reconciliation method, hash function used in privacy amplification, and quantum transmission rate. QKD parameters should be negotiated via Beacon, Probe Request, and Probe Response messages. Since the Beacon and the Probe Response frames contain Capability information fields, AP will inform prospective STAs of its capabilities of supporting QKD via the Capability information field. In addition STA, on its side, informs a prospective AP of its capabilities of supporting QKD via the Request Information and Vendor Specific fields. The information capability elements are used to transfer all the QKD specifics. It is worth noting that when any STA or AP does not support QKD, it can still proceed with the original IEEE 802.11i protocol.

The protocol proposed to integrate the QKD process in the IEEE 802.11i networks is shown in Figure 30 below and described as follows[119, 120]:

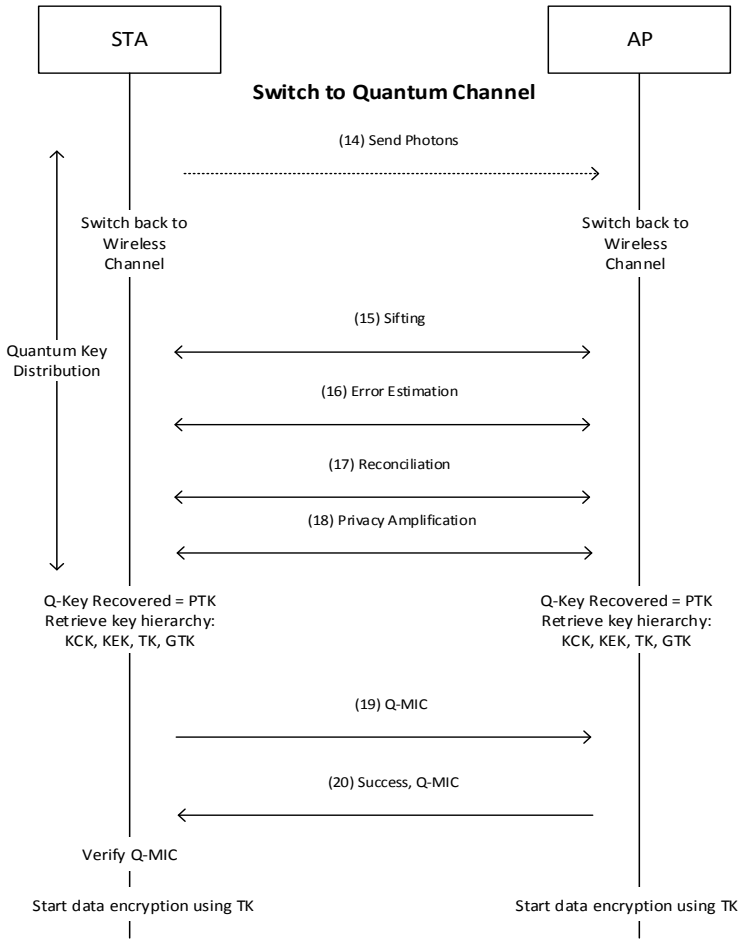


Figure 30: Quantum handshake procedure

The overall communication is hybrid and is done via two channels: Quantum Channel and Classical Channel. The quantum channel is used to transmit polarized photons that represent the key bits only at the beginning of the quantum handshake. After the PMK has been shared, both STA and AP switch to the quantum channel. On the other hand, the classical channel is then used later on to retrieve the final secret key by implementing the proposed quantum handshake protocol.

After EAP Key message, both STA and AP start the QKD protocol by switching to the quantum channel. In flow (14) of Figure 30 the STA sends a sequence of polarized photons representing the random key that STA intends to share with the AP. Flow (14)

corresponds to the first three steps of the BB84 protocol. The number of photons that an STA sends depends on the length of the PTK, the QKD protocol used, and the privacy amplification algorithm. Sufficient number of photons should be sent, since during the communication over the classical channel, some of these bits conveyed over the quantum channel get discarded. Bits are eliminated due to: sifting, dark counts of apparatus, error estimation, reconciliation, privacy amplification, errors introduced due to noise, and environmental conditions.

When the AP receives the photons it affects step 4 of the BB84 protocol. Then AP and STA switch back to the classical channel. From this point forwards, the key recovery process based on the BB84 protocol takes place. Using EAPOL frames for communication, AP and STA remove the bits that are in error and end up with identical and secured key. During flow (15) of Figure 30 they affect the sifting process of the BB84 protocol. Using flow (16) of Figure 30 STA and AP effect the step of error estimation of the BB84 protocol.

Using flow (17) of Figure 30, STA and AP effect the most crucial phase of the quantum handshake corresponding to the reconciliation process. This is step in the BB84 protocol is done to correct the errors in their keys and recover identical keys. The error correction algorithm that the STA and AP will follow at this stage has already been decided by the Beacon, Probe Request and Probe Response messages at the beginning of the communication. The STA and AP implement the reconciliation protocol agreed on via EAPOL message communications. At the end of the reconciliation phase both STA and AP have identical copies of an error free key. The next step is the privacy amplification implemented using flow (18) of Figure 30.

The final key recovery process of the quantum handshake involves removing some bits from their position in the raw key. In this case, the quantum transmission must ensure sending a sufficient number of photons in order to recover the final key that contains a number of bits at least equal or greater than that of PMK. Any extra bits of the final key will be removed so that it will have the same length as PTK.

Using flow (19) of Figure 30, STA sends Q-MIC to AP. AP calculates its own version of Q-MIC and upon receiving Q-MIC from STA, it compares it with the Q-MIC version it has calculated. If they match, the STA is authenticated and AP will send a success message using flow 20.Since the PTK is shared by performing QKD, PTK is unconditionally secure. Thus the rest of the key structure of 802.11 comprising KCK, KEK and TK inherit the same level of security as PTK.

i. Disadvantages of the approach described to integrate QKD into IEEE 802.11i

Integrating the BB84 into the four-way handshake of the IEEE 802.11i protocol has several limitations:

1. The AP and STA might not be able to have a direct line of sight even in an environment where an AP and STA are only distant by few meters. In such cases the solution is to use the original IEEE 802.11i protocol.
2. A single photon generator and single photon detectors are required on both AP and STA sides. Due to the Heisenberg uncertainty principle, we cannot have any device that can reliably generate a single photon per time slot. Current QKD systems rely on attenuated laser pulse that may generate less than one photon per time slot, thus all but guaranteeing that most time slots will be either empty or carry no more than a single photon per pulse. Therefore, an STA will need much

more time to send the required number of photons, and in addition photon pulses containing more than one photon per pulse will make the system vulnerable to the photon number splitting attacks. On the other hand, avalanche photodetectors are used at the AP side. APDs require a cooling temperature of -50 C to reduce the dark counts. Also in a wireless environment, vulnerability of a signal containing a single photon to environmental noise will be higher than its wired counterpart. This is why it is important to look into solutions where different QKD multi photon tolerant protocols can be used.

3. The requirement of a single photon per pulse for BB84 limits the distance and the data rate at which the PTK can be shared. Thus solutions provided by using multi-photon protocol are proposed in the next chapter of this report.
4. Furthermore, the BB84 has several steps after the quantum transmission process. These steps include: sifting, error estimation, error correction, and privacy amplification. Compared to the cases using a multi-photon tolerant protocol, these steps are seen as an overhead associated with the BB84 protocol execution in addition to the associated cost of implementing them, where a shorter key will be derived. Furthermore, multiple agents should be present to implement these steps. A multi-agent based approach with a lesser number of needed agents will be discussed later in this chapter.

The first proposed multi-photon tolerant protocol is the three-stage protocol. It was first proposed by Subhash Kak in 2006; this protocol can obviate some of the known limitations of the BB84 protocol such as the distance, data rate, and single photon requirement. One can think of the three-stage protocol as a candidate to replace the BB84

in the quantum handshake discussed in the precious chapter. The three-stage protocol described in Chapter 3 has two other variants: the three-stage protocol using an initialization vector and implementing a chaining mode between the keys agreed on (three-stage protocol using four variables) discussed in Chapter 3, and the single-stage protocol where an initialization vector is used as the set of initial transformations to be applied on the message transmitted. In the case of the single-stage protocol one transmission only is needed to convey a message. The next part of this chapter will present a discussion of the integration the three-stage protocol and its variants into the IEEE 802.11 quantum handshake.

III. Hybrid three-stage protocol

The three-stage protocol is composed of three consecutive quantum communications that require a line-of-sight between the STA and the AP. One can think of implementing a hybrid approach where a reduced number of transmissions requiring a line of sight can be used.

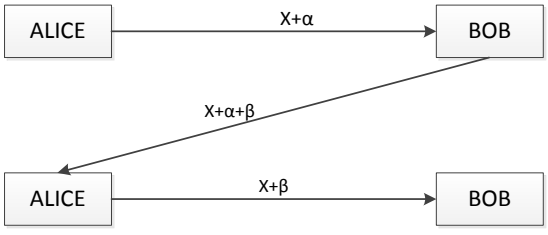


Figure 31: The three-stage protocol

Form Figure 31 one can see that in case the second transmission of the three-stage protocol is made on a multi-photon level the protocol can be said to be unconditionally secure. In this case, an intruder will not be able to measure the value of $X + \alpha + \beta$, thus cannot calculate the value of the message even if the first and last transmissions are made

over the classical channel. In addition, one must observe that in case the second transmission is done over a quantum channel the third one should be done on a quantum channel as well. Since Alice will not have enough photon to measure the polarization sent over the second channel she cannot continue with the communication unless it is still using the quantum channel. So in this case the three-stage protocol proceeds as follows:

Step 1: Alice sends the polarization value of the first transmission using the classical channel. The value of the polarization is equal to $X + \alpha$, where X is the value of the corresponding bit of the key (90° for bit value 1 and 0° for bit value 0) and α is the rotation applied by Alice.

Step 2: Bob receives the value of the polarization, generates a number of photons having the corresponding polarization and applies his rotation transformation and sends using the quantum channel the set of photons having a polarization of $X + \alpha + \beta$ back to Alice, where β is the polarization rotation applied by Bob.

Step 3: Alice removes her transformation and sends using the quantum channel the set of photons of polarization equal to $X + \beta$.

Step 4: Bob will receive the set of photons from Alice removes his transformation and measure the initial value of X.

i. Quantum handshake using the three-stage protocol

If we replace the BB84 protocol in the IEEE 802.11i protocol (described in the previous section) by the three-stage protocol the only part affected will be the quantum handshake. The quantum handshake using the three-stage protocol is as shown in Figure 32.

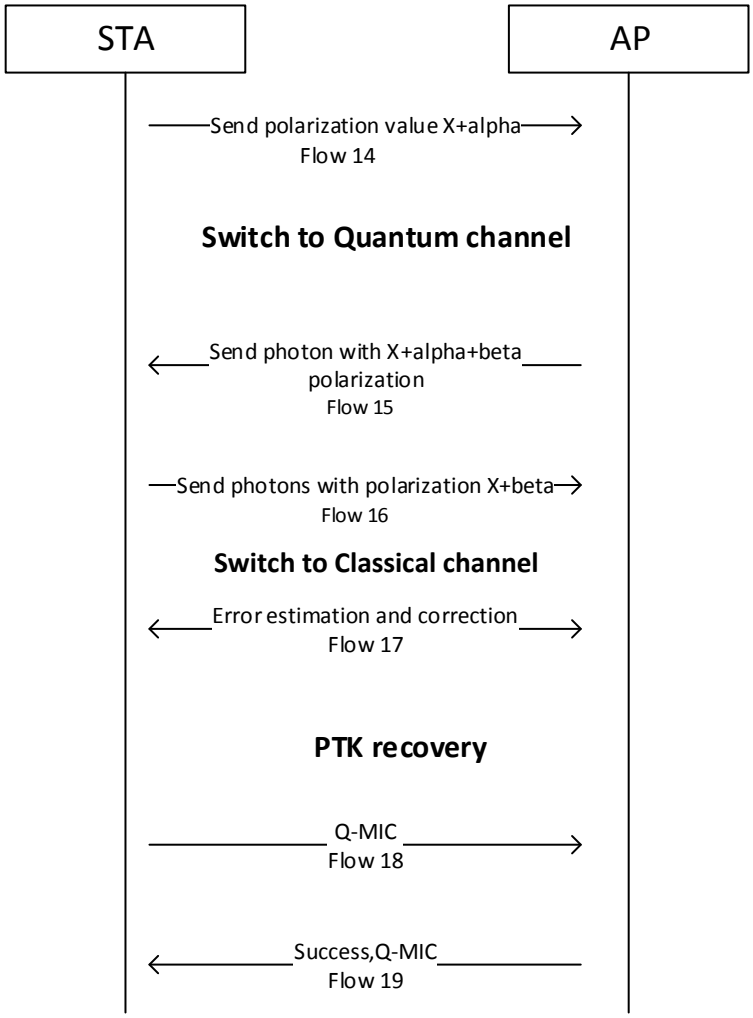


Figure 32: Quantum handshake using the three-stage protocol

As shown in the Figure 32 the quantum handshake using the three-stage protocol requires fewer message flows between the AP and the STA.

ii. Quantum handshake using the four-variable three-stage protocol

The three-stage protocol using four-variable is described in [77]. In this protocol an initialization vector *IV* is used to enhance the security of the three-stage protocol. Then a chaining mode is implemented in order to update the value of the polarization vector. In this case the PMK can be used as an initialization vector and for later transmission, the

PTK can be used to update the value of the initialization vector. The three-stage protocol using four variables was described in details in Chapter 3.The integration of this variation of the three-stage protocol into the quantum handshake is shown in Figure 33.

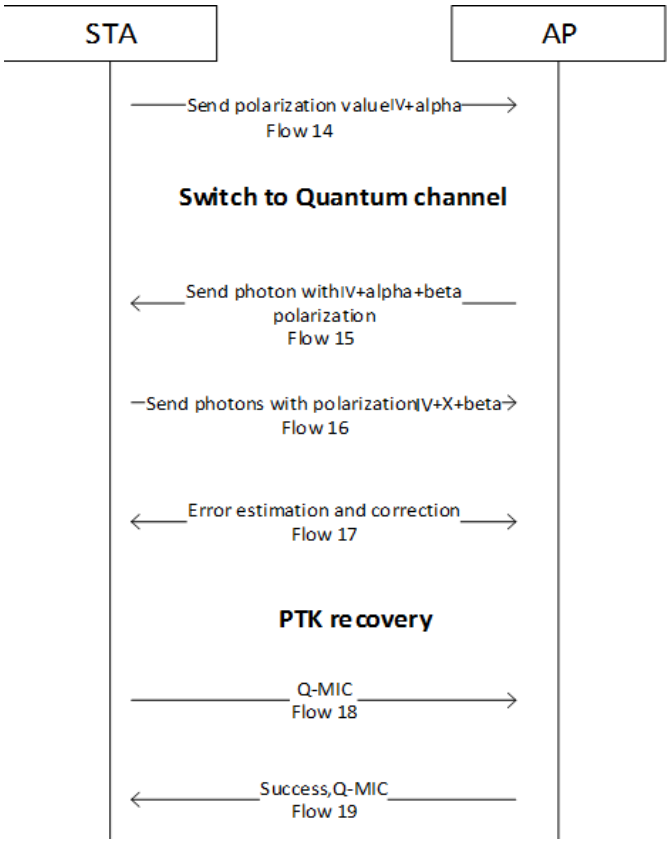


Figure 33: Quantum handshake using the four variable three-stage protocols

iii. Quantum handshake using the single-stage protocol

In the single-stage protocol, it is assumed that Alice and Bob use complex transformations known to both Alice and Bob (in our case STA and AP). Thus, rather than using three transmissions to convey the key STA and AP can share the key using one transmission. Prior to the communication Alice and Bob should have a set of transformations that they will be applying to the messages exchanged among them. This

set of transformation in this case can be derived from the PMK and updated according to the value of the shared PTK.

The steps of the single-stage protocol are as follows [121]:

Step 1: Alice applies her complex transformation on the message and sends $U_A(X)$ to Bob.

Step 2: Bob removes the transformation applied by Alice, by applying its transpose complex conjugate since he has a prior knowledge of this transformation.

Figure 34 shows the quantum handshake of the IEEE 802.11i protocol using the one-stage protocol.

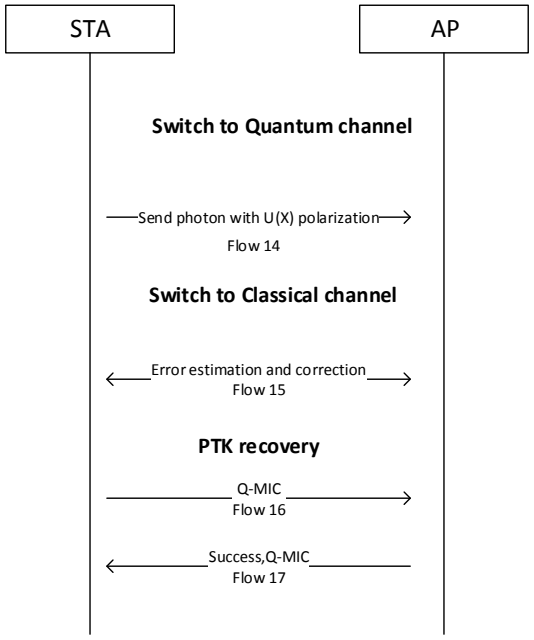


Figure 34:The quantum handshake of the IEEE 802.11i using the one-stage protocol

iv. Hardware Implementation

Currently there are no commercially available Wi-Fi specific wireless devices that support quantum transmission. Thus the quantum transmission in [119] has been established as a separate project aligned to an existing QKD research [122-124] where

the quantum transmissions have been practically implemented over free space. The setup between AP and STA is shown in Figure 35.

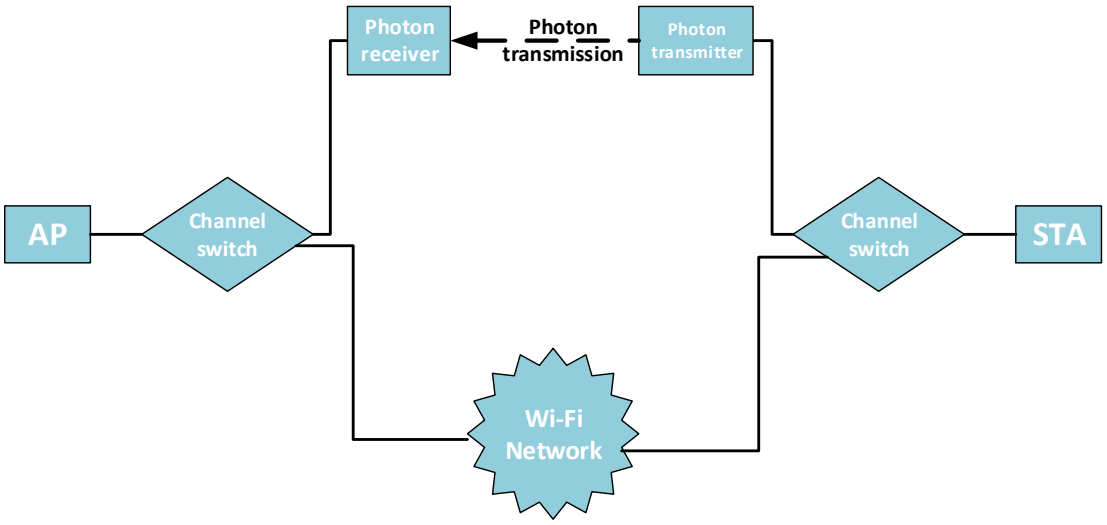


Figure 35: Implementation setup of the IEEE 802.11i integrated with QKD

IV. Software implementation

The implementation was done using a multi agent system. An agent is a sophisticated computer program capable of acting autonomously to accomplish tasks on behalf of its users, across open and distributed environments [125, 126]. It has the following characteristics: autonomy, mobility, rationality, reactivity, inferential capability, pro-activeness, and social ability… etc.

Together multiple agents form a Multi-agent System (MAS) which offer several advantages over a centralized approach. They can distribute computational resources and capabilities across a network. Multiple agents enhance overall system performance, efficiency, reliability, extensibility, robustness, maintainability, responsiveness, flexibility, and reuse.

ii. Multi-agent Approach in BB84

The QKD based IEEE 802.11i using BB84 can be represented using the agents shown in Figure 36.

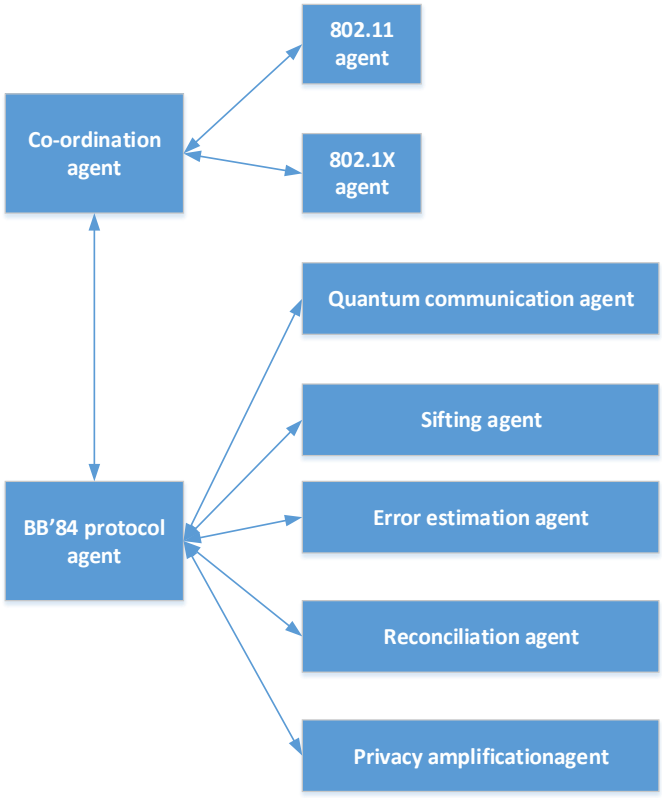


Figure 36: Multi-agent approach to BB84 in IEEE 802.11i. Source: [119]

The functionalities of each agent can be described as follows [119]:

802.11 Agent: This agent performs the 802.11 Association and Authentication.

802.1X Agent: This agent carries out the 802.1X authentication. It is also capable of making decisions on suspicious messages from adversaries similar to what 802.11 Agent does.

BB84 Agent: This agent is to act as the coordinating agent to execute the BB84 QKD protocol. It communicates with 4 other agents to execute the BB84 protocol.

Sifting Agent: This agent effectuates the sifting stage of the BB84 protocol.

Error Estimation Agent: This agent verifies if the error level of the quantum transmission is acceptable or not.

Reconciliation Agent: This agent executes the reconciliation process of the BB84 protocol to remove incorrect bits and obtain an error free key at either end.

Privacy Amplification Agent: This agent effectuates the Privacy amplification of the BB84 protocol. The key obtained by this agent is the "unconditionally secured" PTK key used to derive the rest of the key hierarchy.

Coordination Agent: The coordination agent communicates with all other agents and assures that monitoring efforts and management of internal requests with other agents are handled consistently within a specific transmission. In other words, the coordination agent offers an outline of all communications performed between agents.

The operational procedure of the multi-agent approach is shown in the Figure 37.

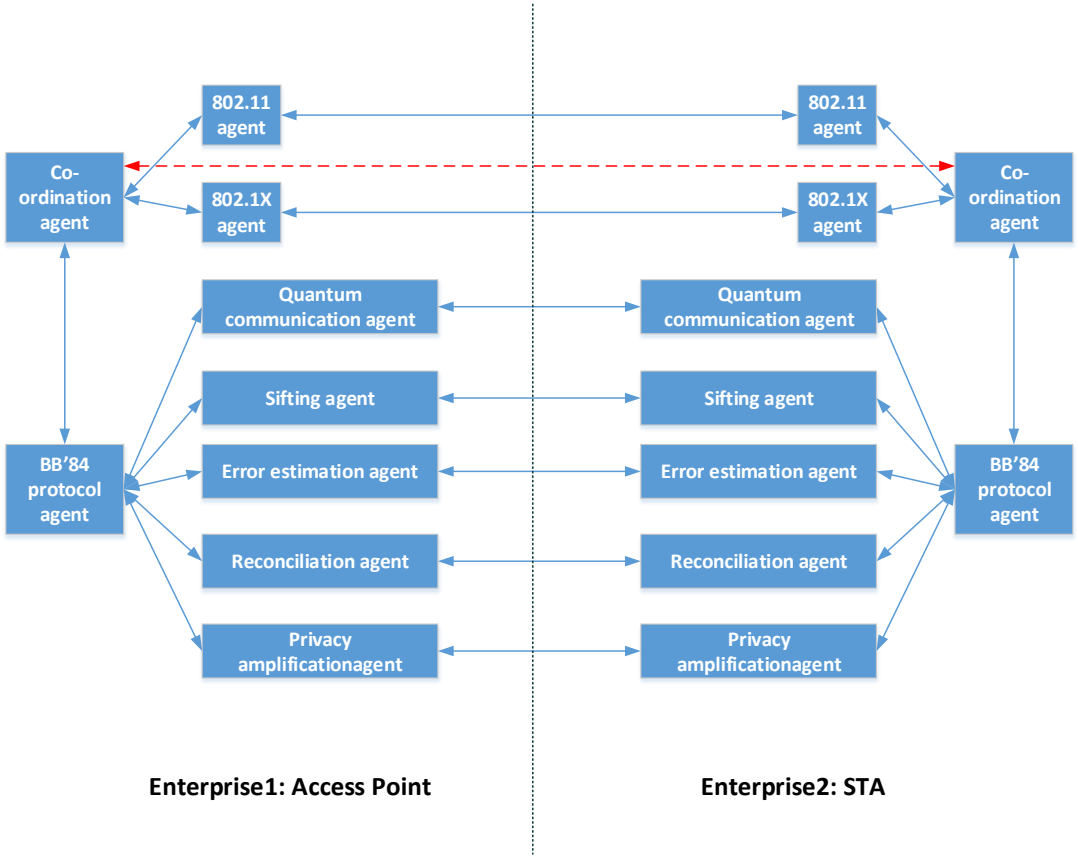


Figure 37: Operation of a multi-agent approach

Each time a new STA enters into the network, AP creates an enterprise corresponding to the new STA in order to facilitate the communication. On the other hand the STA also creates an instance of this enterprise. Since the STA communicates with only one AP at a time, it will only have one enterprise; however, the AP's side will contain many enterprises according to how many STA it is dealing with. The two enterprises that make and the communication procedure are shown in Figure 36.

iii. Multi-agent approach in Multi-photon Tolerant Protocols

One can use a multi-agent approach to implement the three-stage protocol and its variant in an IEEE 802.11i network. Compared to its BB84 counterpart, such

implementation will need fewer agents to perform the actions required in order to share a PTK between AP and STA. The agents are shown in Figure 38:

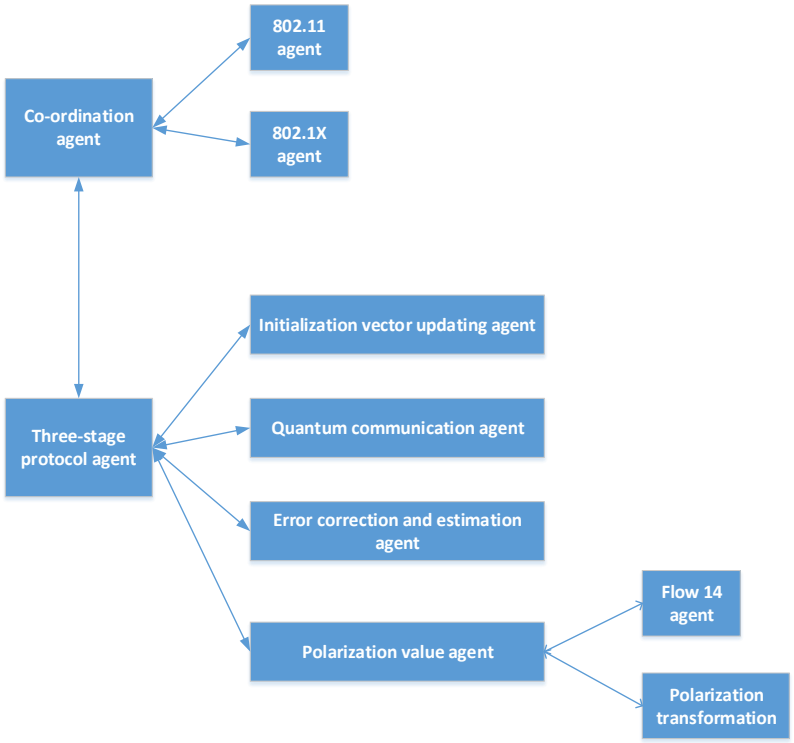


Figure 38: Agents used for the three-stage (and its variants)

As we can see the three-stage protocol and its variants do not need the presence of: sifting agent, reconciliation agent, and privacy amplification agent. On the other hand, it is useful for the software implementation of the three-stage protocol and its variants to have an initialization vector updating agent that will compute the value of the new initialization vector to be used at the next session. In addition to a polarization value agent, this agent has two wrapper agents; the first is for sending the value of the polarization of the flow 14 of figures 32 and 33 and the second is for applying the polarization transformation on each side of the communication. It is worth noting that the

polarization value agent of the AP and STA need not to communicate at any point in the session.

iv. Analysis of the quantum handshake using three-stage protocol and its variants

Compared to the quantum handshake using BB84, the quantum handshake using three-stage and its variants offers the following advantages:

1. On the positive side, the three-stage protocol and its variants are multi-photon tolerant protocols. Thus, AP and STA do not need to be equipped with single photon generators and detectors. However, the proposed approach requires the presence of a high speed polarization modulator at both AP and STA sides.
2. On the positive side, the three-stage protocol offers a higher data rate and a longer communication distance between AP and STA. Since the three-stage protocol is a multi-photon tolerant protocol it can offer a longer distance of communication since a light pulse containing several photons can travel for a longer time. Furthermore, the three-stage protocol doesn't require sifting thus the data rate will be higher compared to that of the BB84 and one can have a better assumption of how many bits should be sent to retrieve the final key.
3. Compared to BB84, three-stage protocol and three-stage protocol using four variables will require two flows to be sent over the quantum channel (flows 15 and 16 of figures 32 and 33). However, the single-stage protocol does not impose this requirement.

V. Conclusion

Security risks are inherent in wireless network; the major source of risks in such networks is the communication medium, which is open to intruders. Till date, many efforts have been put in to address security issues in wireless networks. This chapter has presented a method to provide wireless networks with a security level comparable to that of QKD. This chapter has discussed the integration of the BB84 protocol into the four-way handshake of the IEEE 802.11i protocol along with its shortcomings. On the positive side, quantum handshake provides the Wi-Fi networks with unconditional security. On the other hand, quantum handshake using the BB84 imposes several limitations such as short distances, low data rates etc. This chapter has proposed the integration of multi-stage protocols into the four-way handshake of IEEE 802.11i. Multi-stage protocols offer several advantages compared to its BB84 counterpart. The mode of operation of the proposed quantum handshake (using multi-stage protocol) has been discussed along with its multi-agent implementation approach. Providing the four-way handshake with the capability of implementing the multi-stage protocol offers a quantum level of security meanwhile achieving higher data rates, longer distances, while using a larger average number of photons per pulse. The only disadvantage of such an approach is the requirement of at least a single line-of-sight between AP and STA. Furthermore, one can think of implementing QKD in the key distribution of Wi-Max networks [127], since such networks use keys hierarchy similar to that in IEEE 802.11i.

Chapter 8: Conclusion and Future Work

This dissertation has presented a study of the security and performance of a quantum communication system using multi-stage, multi-photon tolerant protocols. This dissertation has been divided into three main parts. The first part has analyzed the security of multi-stage protocols and proposed several approaches to secure these protocols in order to provide quantum-secure communication. The second part has discussed the performance of the single-stage protocol in a fiber optics medium and shown the effect of an increase in the average photon number to be used on the QBER, the key rate, and the distance of communication. The third part has introduced an application of the multi-stage protocol in the four-way handshake of the IEEE 802.11.

First, this dissertation has proposed a generalized multi-stage multi-photon tolerant protocol for quantum secure communication. The security of the multi-stage protocol is based on the fact that while a legitimate receiver only needs to distinguish between two orthogonal polarization states, an intruder has to distinguish among an infinite number of possible polarization states. In other words, while the receiver would need only one photon to do so, an intruder would need to siphon off a minimum number N of photons per stage. This dissertation has also proposed a key/message expansion scheme associated with the multi-stage protocol which has been proposed. The key/message expansion scheme provides a countermeasure to any man-in-the-middle attack that can be launched on the system. In addition, in an implementation of the generalized multi-stage multi-photon tolerant protocol as well as its key/message expansion scheme has been proposed. These implementations have been done in a laboratory setup using passive optical components. Furthermore, the results presented in

this dissertation set an upper bound on the number of photons at $3N \leq 4.5$ in the case of the three-stage protocol using Fock states. And $N \approx 10$ when coherent states are used in conjunction with the key/message expansion protocol; however, $N < 4$ is the limit when coherent states are used without any prior authentication. Several attacks have been analyzed. These are Trojan horse attack, man-in-the-middle attack, PNS attack through measurement and Helstrom discrimination, amplification attack.

Second, this dissertation has investigated the performance aspects of a practical quantum secure communication using multi-photon tolerant protocols. It has also presented the results of a study of multi-photon tolerant multi-stage protocols, security aspects as well as challenges to the practical implementation. In this dissertation, coherent non-decoying quantum states have been used to transfer the encoded bits from Alice to Bob. The maximum number of photons that Alice can use to encode her bit was varied from N_{max} = 1 to N_{max} = 12. An optimum value μ_{opt} has been found for each N_{max} and as a result a relationship between both values has been derived. Also, a linear relationship has been obtained between the maximum distance that can be achieved and μ_{opt}. However, by examining the relationship between the maximum key rate as a function of μ_{opt}, one notices that the relationship is far from linear and *K* reaches a saturation limit at around μ_{opt} = 4.8 – 5.8 that corresponds to $N_{max} = 8 - 10$ photons.

The relationship between the secret key generation rates for μ_{opt} = 0.95, 1.5, 2.1, and 2.6 has been calculated with respect to both losses and distances over a fiber optical channel. This dissertation has shown that at μ_{opt} = 2.6, the key generation rates are higher than the cases were μ_{opt} = 0.95, 1.5, and 2.1. It is worth noting that the BB84 operates at

μ = 0.1, which is much less than the case of the multi-stage protocol. The QKD multi-stage protocol using coherent state uses an average of 1.5 photons per stage. However, in case it is used as a communication protocol the average number of photon number per stage is 3.3. Furthermore, this dissertation has shown that the QBER in case of μ_{opt} = 2.6 exerts same characteristics as in the cases of μ_{opt} = 0.95, 1.5, and 2.1; the only difference is the distance at which the value of QBER increases sharply. The calculations derived in this dissertation can be generalized to evaluate the performance of any multi-stage QKD or communication protocol.

Third, this dissertation has addressed the security risks inherent in the IEEE 802.11 wireless network by presenting a method to provide wireless networks with a security level comparable to that of QKD. This dissertation has discussed the integration of the BB84 protocol into the four-way handshake of the IEEE 802.11i protocol along with its shortcomings. On the positive side, quantum handshake provides the Wi-Fi networks with unconditional security. On the other hand, quantum handshake using the BB84 imposes several limitations such as short distances, low data rates etc. This dissertation has proposed the integration of multi-stage protocols into the four-way handshake of IEEE 802.11i. Multi-stage protocols offer several advantages compared to its BB84 counterpart. The mode of operation of the proposed quantum handshake (using multi-stage protocol) has been discussed along with its multi-agent implementation approach. Providing the four-way handshake with the capability of implementing the multi-stage protocol offers a quantum level of security meanwhile achieving higher data rates, longer distances, while using a larger average number of photons per pulse. The

only disadvantage of such an approach is the requirement of at least a single line-of-sight between AP and STA.

Future work would potentially expand on two different aspects of the multi-stage protocol proposed in this dissertation: the theoretical aspect as well as the implementation and applications aspect. On the theoretical aspect, a further generalization of the study of the performance of the multi-stage protocol over Fiber optics as well as Free Space Optics can be addressed. The performance over FSO is expected to follow the same patterns of the investigation presented in Chapter 7. However, the distance of communication over FSO is expected to be less than that of FO due to the introduction of geometrical losses in the case of FSO. In addition, implementation over FO as well as FSO using the calculated secure average photon number can be designed and executed in a laboratory environment as a start. Then such implementations can be conducted in more realistic environments where random noise affects the transmission. Furthermore, other applications of the multi-stage protocol such as terrestrial ground FSO links, FO networks, FSO space transmission can be theoretically studied as well as implemented in the context of future work based on the results presented in this dissertation.

References

[1] S. Singh.*The Code Book: The Secret History of Codes and Code-breaking*. 1st edition Great Britain: Fourth Estate.

[2] G. Vernam. "Secret signaling system," Patent No. 1310719, 1919.

[3] G. Vernam. "Cipher printing telegraph systems: For secret wire and radio telegraphic communications," *Journal of the A.I.E.E.,* vol. 45, p. 109, 1926.

[4] C. E. Shannon. "Communication Theory of Secrecy Systems*," *Bell System Technical Journal,* vol. 28, pp. 656-715, 1949.

[5] S. William and W. Stallings. *Cryptography and Network Security,*, Prentice Hall ed.: Pearson Education India, 2006.

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

[7] 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.

[8] C. A. Fuchs, "Information gain vs. state disturbance in quantum theory," *arXiv preprint quant-ph/9611010,* 1996.

[9] W. K. Wootters and W. H. Zurek, "A single quantum cannot be cloned," *Nature,* vol. 299, pp. 802-803, 1982.

[10] S. Huard, "Polarization of light," ISBN 0-471-96536-7, Wiley-VCH ,1997.

[11] 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.

[12] G. Brassard and L. Salvail, "Secret-key reconciliation by public discussion," in *Advances in Cryptology—EUROCRYPT'93*, 1994, pp. 410-423.

[13] antenna-theory.com. (September 28). *http://www.antenna-theory.com/basics/polarization.php*.

[14] C. H. Bennett and G. Brassard, "Quantum cryptography: Public key distribution and coin tossing," *Theoretical Computer Science,* vol. 560, pp. 7-11, 2014.

[15] H.-K. Lo, T. Spiller, and S. Popescu. *Introduction to quantum computation and information*: World Scientific, 1998.

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

[17] D. Bruss. "Optimal eavesdropping in quantum cryptography with six states," *Physical Review Letters,* vol. 81, p. 3018, 1998.

[18] C. H. Bennett, G. Brassard, and N. D. Mermin. "Quantum cryptography without Bell's theorem," *Physical Review Letters,* vol. 68, p. 557, 1992.

[19] 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.

[20] J. L. Carter and M. N. Wegman. "Universal classes of hash functions," in *Proceedings of the ninth annual ACM symposium on Theory of computing*, 1977, pp. 106-112.

[21] M. N. Wegman and J. L. Carter. "New hash functions and their use in authentication and set equality," *Journal of computer and system sciences,* vol. 22, pp. 265-279, 1981.

[22] V. Scarani, H. Bechmann-Pasquinucci, N. J. Cerf, M. Dušek, N. Lütkenhaus, and M. Peev,. "The security of practical quantum key distribution," *Reviews of modern physics,* vol. 81, p. 1301, 2009.

[23] D. R. Stinson, "Cryptography Theory and Practice," Third edition: CRC press.

[24] N. Gisin, G. Ribordy, W. Tittel, and H. Zbinden.. "Quantum cryptography," *Reviews of Modern Physics,* vol. 74, p. 145, 2002.

[25] idQuantique (September 28). *http://www.idquantique.com/qkd.html*.

[26] I. MagiQ Technologies. (September 28). *http://www.magiqtech.com*.

[27] C. Elliott, "The DARPA quantum network," *Quantum Communications and Cryptography*, pp. 83-102, 2006.

[28] 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.

[29] S. Vittorio, "Quantum cryptography: Privacy through uncertainty," *Retrieved from CSA information company: http://www. csa. com,* 2002.

[30] E. Biham, M. Boyer, P. O. Boykin, T. Mor, and V. Roychowdhury. "A proof of the security of quantum key distribution," *Journal of Cryptology,* vol. 19, pp. 381-439, 2006.

[31] D. Mayers. "Unconditional security in quantum cryptography," *Journal of the ACM (JACM),* vol. 48, pp. 351-406, 2001.

[32] 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.

[33] Swiss Quantum. (2009). *KEY SIFTING*. Available: http://swissquantum.idquantique.com/?Key-Sifting

[34] C. H. Bennett, G. Brassard, and J.-M. Robert. "Privacy Amplification by Public discussion," *SIAM Journal on Computing,* vol. 17, pp. 210-229, 1988.

[35] M. Ben-Or, M. Horodecki, D. W. Leung, D. Mayers, and J. Oppenheim. "The universal composable security of quantum key distribution," in *Theory of Cryptography*, ed: Springer, 2005, pp. 386-406.

[36] R. Renner and R. König. "Universally composable privacy amplification against quantum adversaries," in *Theory of Cryptography*, ed: Springer, 2005, pp. 407-425.

[37] 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.

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

[39] D. Gottesman and H.-K. Lo. "Proof of Security of Quantum Key Distribution with Two-way Classical Communications," *Information Theory, IEEE Transactions on,* vol. 49, pp. 457-475, 2003.

[40] B. Kraus, N. Gisin, and R. Renner. "Lower and Upper Bounds on the Secret-Key Rate for Quantum Key Distribution Protocols Using One-way Classical Communication," *Physical Review Letters,* vol. 95, p. 080501, 2005.

[41] R. Renner, N. Gisin, and B. Kraus. "Information-theoretic Security Proof for Quantum-key-Distribution Protocols," *Physical Review A,* vol. 72, p. 012332, 2005.

[42] G. Brassard, N. Lütkenhaus, T. Mor, and B. C. Sanders. "Limitations on Practical Quantum Cryptography," *Physical Review Letters,* vol. 85, p. 1330, 2000.

[43] N. Lütkenhaus and M. Jahma, "Quantum Key distribution with realistic states: Photon-number statistics in the Photon-Number Splitting Attack," *New Journal of Physics,* vol. 4, p. 44, 2002.

[44] W.-Y. Hwang. "Quantum Key Distribution with high Loss: Toward Global Secure Communication," *Physical Review Letters,* vol. 91, p. 057901, 2003.

[45] S. J. Lomonaco. "AQuick gGlance at Quantum Cryptography," *Cryptologia,* vol. 23, pp. 1-41, 1999.

[46] C. Branciard, N. Gisin, B. Kraus, and V. Scarani. "Security of two quantum cryptography protocols using the same four qubit states," *Physical Review A,* vol. 72, p. 032301, 2005.

[47] M. Buchanan. "Small world: Uncovering nature's hidden networks," Diane Pub Co August 30, 2002.

[48] Y. Zhao, C.-H. F. Fung, B. Qi, C. Chen, and H.-K. Lo. "Quantum hacking: Experimental demonstration of time-shift attack against practical quantum-key-distribution systems," *Physical Review A,* vol. 78, p. 042333, 2008.

[49] N. Gisin, S. Fasel, B. Kraus, H. Zbinden, and G. Ribordy. "Trojan-horse attacks on quantum-key-distribution systems." *Physical Review A,* vol. 73, p. 022320, 2006.

[50] V. Scarani and C. Kurtsiefer. "The black paper of quantum cryptography: Real implementation problems," *arXiv preprint arXiv:0906.4547,* 2009.

[51] 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.

[52] T. Honjo, M. Fujiwara, K. Shimizu, K. Tamaki, S. Miki, T. Yamashita, *et al.* "Countermeasure against tailored bright illumination attack for DPS-QKD." *Optics express,* vol. 21, pp. 2667-2673, 2013.

[53] Z. Yuan, J. Dynes, and A. Shields. "Avoiding the blinding attack in QKD." *Nature Photonics,* vol. 4, pp. 800-801, 2010.

[54] L. Lydersen, V. Makarov, and J. Skaar. "Secure gated detection scheme for quantum cryptography," *Physical Review A,* vol. 83, p. 032306, 2011.

[55] B. Schneier. (2008, 10/13/2015). *Quantum Cryptography: As Awesome As It Is Pointless*.Available:http://archive.wired.com/politics/security/commentary/securitymatters/2008/10/securitymatters_1016

[56] B. Schneier, *Schneier on Security*: John Wiley & Sons, 2009.

[57] K. G. Paterson, F. Piper, and R. Schack. "Quantum cryptography: A practical information security perspective," *NATO SECURITY THROUGH SCIENCE SERIES D-INFORMATION AND COMMUNICATION SECURITY,* vol. 11, p. 175, 2007.

[58] S. Ghernaouti-Helie, I. Tashi, T. Laenger, and C. Monyk. "SECOQC business white paper," *arXiv preprint arXiv:0904.4073,* 2009.

[59] S. Cobourne, "Quantum Key Distribution Protocols and Applications," *Surrey TW20 0EX, England,* 2011.

[60] R. Alléaume, F. Roueff, P. Bellot, O. Maurhart, and N. Lutkenhaus. "Topology, architecture and protocols for a Quantum Key Distribution network," in *Workshop on classical and quantum information security (Secoqc),* 2005.

[61] M. Dianati and R. Alléaume. "Architecture of the Secoqc quantum key distribution network," *arXiv preprint quant-ph/0610202,* 2006.

[62] W. H. Zurek. "Decoherence and the transition from quantum to classical--REVISITED," *arXiv preprint quant-ph/0306072,* 2003.

[63] E. Biham, B. Huttner, and T. Mor. "Quantum cryptographic network based on quantum memories," *Physical Review A,* vol. 54, p. 2651, 1996.

[64] W. Dür, H.-J. Briegel, J. Cirac, and P. Zoller. "Quantum repeaters based on entanglement purification," *Physical Review A,* vol. 59, p. 169, 1999.

[65] S. J. Phoenix, S. M. Barnett, P. D. Townsend, and K. Blow. "Multi-user quantum cryptography on optical networks," *Journal of Modern Optics*, vol. 42, pp. 1155-1163, 1995.

[66] C. Elliott. "Building the quantum network," *New Journal of Physics*, vol. 4, p. 46, 2002.

[67] C. Elliott, A. Colvin, D. Pearson, O. Pikalo, J. Schlafer, and H. Yeh. "Current status of the DARPA quantum network," in *Defense and Security*, 2005, pp. 138-149.

[68] A. V. Sergienko. *Quantum Communications and Cryptography*: CRC Press, 2005.

[69] D. Jin, P. K. Verma, and S. V. Kartalopoulos. "Fast convergent key distribution algorithms using a dual quantum channel," *Security and Communication Networks*, vol. 2, pp. 519-530, 2009.

[70] A. Parakh. "A probabilistic quantum key transfer protocol," *Security and Communication Networks*, vol. 6, pp. 1389-1395, 2013.

[71] F. Zamani and P. K. Verma, "A QKD protocol with a two-way quantum channel," in *Advanced Networks and Telecommunication Systems (ANTS), 2011 IEEE 5th International Conference on*, 2011, pp. 1-6.

[72] C.-H. F. Fung, K. Tamaki, and H.-K. Lo. "Performance of two quantum-key-distribution protocols," *Physical Review A*, vol. 73, p. 012337, 2006.

[73] G. A. Barbosa, E. Corndorf, P. Kumar, and H. P. Yuen. "Secure communication using mesoscopic coherent states," *Physical Review Letters*, vol. 90, p. 227901, 2003.

[74] G. A. Barbosa and J. van de Graaf. "Untappable communication channels over optical fibers from quantum-optical noise," *IACR Cryptology ePrint Archive*, vol. 2014, p. 146, 2014.

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

[76] S. Mandal. "Implementation of the Three-stage Protocol Over Free Space Optics," University of Oklahoma, 2012.

[77] M. El Rifai and P. K. Verma. "An Algorithmic Approach to Securing the Three-stage Quantum Cryptography Protocol," in *Trust, Security and Privacy in Computing and Communications (TrustCom), 2013 12th IEEE International Conference on*, 2013, pp. 1803-1807.

[78] 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.

[79] E. Collett. *Polarized Light in Fiber optics*: SPIE Press, 2003.

[80] H.-K. Lo and H. F. Chau. "Unconditional security of quantum key distribution over arbitrarily long distances," *Science,* vol. 283, pp. 2050-2056, 1999.

[81] D. Gottesman, H.-K. Lo, N. Lütkenhaus, and J. Preskill. "Security of quantum key distribution with imperfect devices," in *Information Theory, 2004. ISIT 2004. Proceedings. International Symposium on*, 2004, p. 136.

[82] B. Kraus, C. Branciard, and R. Renner, "Security of quantum-key-distribution protocols using two-way classical communication or weak coherent pulses," *Physical Review A,* vol. 75, p. 012316, 2007.

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

[84] X. Ma, B. Qi, Y. Zhao, and H.-K. Lo. "Practical decoy state for quantum key distribution," *Physical Review A*, vol. 72, p. 012326, 2005.

[85] C.-Z. Peng, J. Zhang, D. Yang, W.-B. Gao, H.-X. Ma, H. Yin, *et al.* "Experimental long-distance decoy-state quantum key distribution based on polarization encoding," *Physical review letters,* vol. 98, p. 010505, 2007.

[86] C. W. Helstrom."*Quantum Detection and Estimation Theory"* Academic Press, 1976.

[87] J. A. Bergou. "Discrimination of quantum states," *Journal of Modern Optics,* vol. 57, pp. 160-180, 2010.

[88] C. A. Fuchs. "Distinguishability and accessible information in quantum theory," *arXiv preprint quant-ph/9601020,* 1996.

[89] U. Herzog. "Minimum-error discrimination between a pure and a mixed two-qubit state," *Journal of Optics B: Quantum and Semiclassical Optics,* vol. 6, p. S24, 2004.

[90] (November 3, 2015). *Quantum states of light — Fock states*

Available:http://www.qms.unirostock.de/fileadmin/Physik_Festkoerpertheorie/Lehre_Scheel/Quantenoptik/Quantenoptik-Vorlesung3.pdf

[91] M. El Rifai, K. W. C. Chan, and P. K. Verma. "Multi-stage quantum secure communication using polarization hopping," *Security and Communication Networks,* 2015.

[92] M. El Rifai and P. K. Verma. "Quantum secure communication using a multi-photon tolerant protocol," in *SPIE OPTO*, 2015, pp. 937713-937713-8.

[93] F. Grosshans. (2012, November 4,2015). *How many photons does it take to measure a linear polarization?* Available: http://physics.stackexchange.com/questions/22575/how-many-photons-does-it-take-to-measure-a-linear-polarization

[94] M. Fox. *Quantum Optics: An Introduction: An Introduction* vol. 6: Oxford University Press, 2006.

[95] H. P. Yuen. "Key generation: Foundations and a new quantum approach," *Selected Topics in Quantum Electronics, IEEE Journal of,* vol. 15, pp. 1630-1645, 2009.

[96] Y. Zhao, B. Qi, and H.-K. Lo. "Experimental quantum key distribution with active phase randomization," *Applied Physics Letters,* vol. 90, p. 044106, 2007.

[97] E. Bagan, A. Monras, and R. Munoz-Tapia. "Comprehensive analysis of quantum pure-state estimation for two-level systems," *Physical Review A,* vol. 71, p. 062318, 2005.

[98] A. I. Lvovsky, B. C. Sanders, and W. Tittel. "Optical quantum memory," *Nature photonics,* vol. 3, pp. 706-714, 2009.

[99] N. Sangouard, C. Simon, H. De Riedmatten, and N. Gisin. "Quantum repeaters based on atomic ensembles and linear optics," *Reviews of Modern Physics,* vol. 83, p. 33, 2011.

[100] H. Wu, D. Citrin, L. Jiang, and X. Li. "Polarization-independent slow light in annular photonic crystals," *Applied Physics Letters,* vol. 102, p. 141112, 2013.

[101] H. Haus and J. Mullen. "Quantum noise in linear amplifiers," *Physical Review,* vol. 128, p. 2407, 1962.

[102] T. Ralph and A. Lund. "Nondeterministic noiseless linear amplification of quantum systems," *arXiv preprint arXiv:0809.0326,* 2008.

[103] S. Pandey, Z. Jiang, J. Combes, and C. M. Caves. "Quantum limits on probabilistic amplifiers," *Physical Review A,* vol. 88, p. 033852, 2013.

[104] G.-Y. Xiang, T. Ralph, A. Lund, N. Walk, and G. J. Pryde. "Heralded noiseless linear amplification and distillation of entanglement," *Nature Photonics,* vol. 4, pp. 316-319, 2010.

[105] A. Zavatta, J. Fiurášek, and M. Bellini. "A high-fidelity noiseless amplifier for quantum light states," *Nature Photonics,* vol. 5, pp. 52-60, 2011.

[106] S. Van Enk. "Unambiguous state discrimination of coherent states with linear optics: Application to quantum cryptography," *Physical Review A,* vol. 66, p. 042313, 2002.

[107] F. Becerra, J. Fan, and A. Migdall. "Implementation of generalized quantum measurements for unambiguous discrimination of multiple non-orthogonal coherent states," *Nature Communications,* vol. 4, 2013.

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

[109] H.-K. Lo. "Getting something out of nothing," *arXiv preprint quant-ph/0503004,* 2005.

[110] C.-H. F. Fung, B. Qi, K. Tamaki, and H.-K. Lo. "Phase-remapping attack in practical quantum-key-distribution systems," *Physical Review A,* vol. 75, p. 032314, 2007.

[111] N. Lütkenhaus. "Security against individual attacks for realistic quantum key distribution," *Physical Review A*, vol. 61, p. 052304, 2000.

[112] K. W. C. Chan, M. El Rifai, P. Verma, S. Kak, and Y. Chen. "Multi-Photon Quantum Key Distribution Based on Double-Lock Encryption," in *CLEO: QELS_Fundamental Science*, 2015, p. FF1A. 3.

[113] I. C. Society. "802.1X," in *IEEE Standard for Local and Metropolitan Area Networks Port-Based Network Access Control*, ed. NY,USA: IEEE.

[114] C. He and J. C. Mitchell "Analysis of the 802.11 i 4-Way Handshake," in *Proceedings of the 3rd ACM Workshop on Wireless Security*, 2004, pp. 43-50.

[115] C. He and J. C. Mitchell. "Message attack on the 4-Way Handshake," *Submissions to IEEE*, 2004.

[116] F. De Rango, D. C. Lentini, and S. Marano. "Static and dynamic 4-way handshake solutions to avoid denial of service attack in Wi-Fi protected access and IEEE 802.11 i," *EURASIP Journal on Wireless Communications and Networking*, vol. 2006, pp. 73-73, 2006.

[117] C. H. J. C. Mitchell. "Security analysis and improvements for IEEE 802.11 i," in *The 12th Annual Network and Distributed System Security Symposium (NDSS'05)*, 2005, pp. 90-110.

[118] Z. Bai and Y. Bai. "4-way handshake solutions to avoid denial of service attack in ultra wideband networks," in *Intelligent Information Technology Application, 2009. IITA 2009. Third International Symposium on*, 2009, pp. 232-235.

[119] S. Wijesekera. "Quantum Cryptography for Secure Communication in IEEE 802.11 Wireless Networks," University of Canberra, 2011.

[120] T. M. T. Nguyen, M. A. Sfaxi, and S. Ghernaouti-Hélie. "Integration of quantum cryptography in 802.11 networks," in *Availability, Reliability and Security, 2006. ARES 2006. The First International Conference on*, 2006, p. 8 pp.

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

[122] G. Ganeshkumar, P. Edwards, W. Cheung, L. Barbopoulos, H. Pham, and J. Hazel. "The University of Canberra quantum key distribution testbed," 1999.

[123] P. Edwards and P. Lynam. "The University of Canberra–Telstra Tower Free-Space Quantum Key Distribution Testbed," *ITEE Society Monitor (March 2002)*, 2002.

[124] P. J. Edwards. "The University of Canberra–Telstra Tower Quantum Crypto-Key Telecommunications Link, Advanced Telecommunications and Electronics Research Centre," ed.

[125] S. Wijesekera, X. Huang, and D. Sharma. "Multi-Agent Based Approach for Quantum Key Distribution in WiFi Networks," in *Agent and Multi-Agent Systems: Technologies and Applications*, ed: Springer, 2009, pp. 293-303.

[126] G. Weiss. *Multiagent Systems: A Modern Approach to Distributed Artificial Intelligence*: MIT Press, 1999.

[127] R. Nomula, M. E. Rifai, and P. Verma."Multi-photon tolerant protocols for quantum secure communication in wireless standards," International Journal of Security and Networks, vol. 11, 2015.