Modified Quantum Three Pass Protocol Based on Hybrid Cryptosystem

Alharith Abdulkareem Abdullah

Submitted to the
Institute of Graduate Studies and Research
in partial fulfillment of the requirements for the degree of

Doctor of Philosophy
in
Computer Engineering

Eastern Mediterranean University
October 2015
Gazimağusa, North Cyprus

Approval of the Institute of Graduate Studies and Research

Prof. Dr. Serhan Çiftçioğlu
Acting Director

I certify that this thesis satisfies the requirements as a thesis for the degree of Doctor of Philosophy in Computer Engineering.

Prof. Dr. Işık Aybay
Chair, Department of Computer Engineering

We certify that we have read this thesis and that in our opinion it is fully adequate in scope and quality as a thesis for the degree of Doctor of Philosophy in Computer Engineering.

Asst. Prof. Dr. Mustafa Rıza
Supervisor

Examining Committee

1. Prof. Dr. Mehmet Ufuk Çağlayan
2. Prof. Dr. Azmi Gençten
3. Prof. Dr. Marifi Güler
4. Assoc. Prof. Dr. Alexander Chefranov
5. Asst. Prof. Dr. Mustafa Rıza

ABSTRACT

In this thesis we propose an enhancement to the Quantum Three-Pass Protocol (QTPP) by adding quantum authentication. After detailed analysis of all possible classical as well as quantum attack methods of the original Quantum Three-Pass Protocol, we identified, that the original Quantum Three-Pass Protocol is only vulnerable against the man-in-the-middle attack. By adding authentication and an agent called the Quantum Distribution Centre, the man-in-the-middle attack is eliminated. All communication between the parties is established over quantum channels with non-orthogonal superposition states that are subject to the no-cloning theorem. The security analysis shows that the modified Quantum Three Pass Protocol is unconditionally secure in the sense that the key is random, the protocol is authenticated, and all communication channels are subject to quantum physics. Furthermore, the bit error rate as a function of the noise on the channel is discussed. Using the enhanced QTPP a complete encryption process is designed exploiting also classical algorithms.

Keywords: Quantum Computation, Quantum Cryptography, Quantum Encryption Algorithm, Quantum Three-Pass protocol, Authentication, BB84.

ÖZ

Bu tezde kuantum kimlik doğrulama yöntemini ekli Kuantum Üç Geçişli Protokolü (QTPP) öneriyoruz. Tüm olası klasik ve kuantum saldırı yöntemlerini Kuantum Üç Geçişli Protokolünün analizinde, sadece araya giren adam saldırısına (man-in-the-middle attack) karşı saldırıya maruz kalabileceğini tespit edilmiştir. Kimlik doğrulama yönteimini ve bir Kuantum Dağıtım Merkezin ekleyerek araya giren adam saldırısını elimine edilebileceğini gösterilecektir. Taraflar arasındaki tüm iletişim kanalları süperpozisyon halinde olan bilgiler klonlamama teoremine tabi kuantum kanalları üzerinden kurulur. Güvenlik analizi, kimlik doğrulamalı modifiye Kuantum Üç Geçişli Protokolünün, şifresi rastgele olması, protokolün doğrulanmış olması, ve tüm iletişim kanallarının kuantum fiziğine tabii olması halinde, koşulsuz güvenilirdir. Bunun dışında iletişim kanalının üzerindeki gürültü ile bit hata oranı arasındaki ilişki tartışılmıştır. Gelişmiş QTPP klasik algoritmalarla birlikte kullanarak komple bir şifreleme işlemi tasarlanmıştır.

Anahtar Kelimeler: Kuvantum Hesaplama, Kuantum Kriptografi, Kuantum Şifreleme Algoritması, Kuantum Üç Geçişli protokol, kimlik doğrulama, BB84.

DEDICATION

To my wonderful family,

My Wife Raghad

My son Yamen

My daughter Yem

ACKNOWLEDGMENT

First and foremost I would like to thank Allah, the almighty, for giving me the ability and patience to carry on this work successfully and properly, and as the prophet Muhammad (PBUH) said: “Whoever does not thank people (for their favors) has not thanked Allah (precisely)” I will never forget anyone helps and encourages me during my studies. Then I wish to express my heartfelt gratitude to my supervisor (Assoc. Prof. Dr. Mustafa Riza) for his profitable and valuable time, which he gladly gave me through my whole studies herein by welcome heart. I highly do appreciate his optimistic behaviour that always has been encouraged me to fulfill my difficult task. Indeed, I am truly grateful to him for his endless mentorship, stimulation, supporting, and his friendship during my entirely graduate studies at Eastern Mediterranean University. In addition, he was not only my instructor or supervisor of my thesis but also he was an ideal example for me how to deal patiently and gently with people and students. Next, I want to express special thanks to my PhD instructors and the rest of all my faculty members whose function was to maintain improving my knowledge and widening my perspectives in varied ways. Many thanks to technology, devices and programs that have made my approach easy and fast for collecting beneficial data and leading me to present my thesis in intellectual form. Also I love to say thanks to all my friends and fellowship that have provided me with useful feedback and pushed me forward. Finally, I am greatly indebted to my parents and family especially my wife (Raghad), my son (Yamen) and my daughter (Yem) those who accompany me in all my educational journey, without their moral and financial supports this work has never come to light.

TABLE OF CONTENTS

LIST OF TABLES

LIST OF FIGURES

LIST OF ABBREVIATIONS

QTPP	Quantum Three-Pass Protocol.
BB84	Charles H. Bennett and Gilles Brassard (1984).
QKD	Quantum Key Distribution.
QFT	Quantum Fourier Transform.
RSA	Public-key cryptosystems, initial letters of the surnames of Ron Rivest, Adi Shamir and Leonard Adleman.
TPP	Three-Pass Protocol.
QDC	Quantum Distribution Center.
H	Hadamard Gate.
SF	Switch Function.
S	SWAP Gate.
X	Pauli-X Gate.
Y	Pauli-Y Gate.
Z	Pauli-Z Gate.

Chapter 1

INTRODUCTION

Before we begin to discuss Quantum Encryption, we have to understand the relationship between classical information transferred and processed in the domain of Quantum Computation. As computers cannot store and process information directly, the information has to be coded into bits. In an analogy to classical computation in quantum computation the information is coded in so-called "qubits". The qubits are represented mathematically by the abstract Dirac-Notation. There are two fundamental differences between classical bits and qubits. Let us consider the computational basis $\{|0\rangle, |1\rangle\}$, which is the same for classical as well as for quantum computation. Information in classical computing is then represented as a sequence of bits that are either 0 or 1, which can also be represented in Dirac notation using the pure states $|0\rangle$ or $|1\rangle$. In contrast to classical information, quantum information provides a more probabilistic approach, reflected in the fact that qubits can be represented as superposition of their basis states. If we choose the computational basis $\{|0\rangle, |1\rangle\}$, then a qubit can be represented as $(\alpha|0\rangle + \beta|1\rangle)$, where $\alpha, \beta \in \mathbb{C}$. Because of the probabilistic nature of quantum computation the complex coefficients are interpreted as probability amplitudes, with $|\alpha|^2 + |\beta|^2 = 1$. So, we can encode theoretically (mathematically) infinite information into one qubit. If we look at this infinite set, we can easily identify that every point on this circle is an accumulation point. If, in an open interval around the point *x* of a set, there are infinitely many points, we call this an accumulation point. So every point on the circle, given by

$|\alpha|^2 + |\beta|^2 = 1$, is an accumulation point. Obviously, this is not the case for integers. So, evidently one qubit is sufficient to store a key that is combinatorial inaccessible. The only restriction in this case is that every transmission channel has a certain amount of noise. Therefore, the noise level and the associated error correction are the only limiting characteristics for the information and its transmission. If we neglect this, one qubit is sufficient to store infinite information. The mathematical theory is telling us that the qubit space is infinite, but according to Bekenstein [1], there is an upper limit to the information in the universe contradicting the mathematical claim. So, it is physically not possible to encode infinite information into one qubit. Of course, this property of quantum computing could also be realised using probabilistic computing. The other, perhaps even more important, difference is entanglement. Entanglement is a purely quantum phenomenon that shows that two entangled qubits can no longer be treated independently.

According to computation theory the mother of all computers is the Turing Machine [2]. So, what is more natural than transferring the idea to the domain of quantum computation? Benioff introduced in his work [3] the Quantum Turing Machine. Later, in 1982 Richard P. Feynman shared his ideas on Simulating Physics with computers in [4], where he argues that quantum phenomena can be simulated more efficiently using quantum computers. Actually, the fundamental works of quantum computation and quantum information theory opened up a new field of science. David Deutsch was the first to ask the question implicitly stated by Feynman, whether quantum computation facilitates the solving of problems faster when compared to classical computation [5]. Deutsch and Josza [6] showed in a straightforward example that quantum computation can be superior to classical computation with respect to time complexity. Bernstein, Vazirani and Simon

discussed problems for which the computational complexity is much better on the quantum computer compared to a classical computer [7][8]. Both problems involve finding constant values programmed into a subroutine in which the internal structure is not known. In each case there is a significant speedup when quantum computation is used.

An even better result is achieved with respect to time complexity in the solution to Simon's problem [8]. The complexity of the solution of Simon's problem in classical computation is super-polynomial, whereas the solution using quantum computing reduces to linear complexity. Simon's problem was an inspiration for the Shor's ground breaking factoring algorithm [9]. Prime number factorisation is one of the most challenging problems in classical computation. As is well known, the super-polynomial complexity of prime number factorisation is the basis of the security of public key cryptography. Shor's algorithm shows that prime number factorisation can be performed in polynomial time using quantum computation. Public key encryption became important as the most vulnerable part of the encryption-decryption process is the key sharing process in symmetric encryption. One of the first applications of Quantum Cryptography was the BB84 Quantum Key Distribution QKD protocol created by Charles Bennett and Gilles Brassard [10], proven to be unconditionally secure by Shor and Presskill [11]. This fundamental protocol is described in detail in Appendix A. Most QKD protocols are based on the properties of preparing and measuring quantum states. A different approach was proposed by Ekert [12], in order to distribute a secret key between parties using entangled particles. Ekert's protocol exploits the famous Einstein-Podolsky-Rosen paradox [13][14] and generalized Bell's theorem [15][16] to ensure a safe key agreement between parties. Several quantum key exchange algorithms have been

proposed and realized experimentally like [17][18][19]. Moreover, there have been many quantum commitment protocols proposed like [20][21][22] enabling parties to exchange decisions.

These protocols ensure that after committing a decision by one party it cannot be changed before revealing it to the other party. Furthermore, there are many approaches for the establishment of quantum encryption algorithms based on the idea of quantum cryptography. We would like to refer to the quantum encryption algorithm proposed by Zhou et al [23] in 2006, where a classical plain-text message is encrypted using a quantum computational algorithm employing six quantum keys divided into four groups. Moreover, we would like to refer to the algorithms relying on a set of unitary operations applied to encrypt the plain-text [24][25][26]. Other encryption algorithms like [27] are relying on entanglement, where the entangled key is sent over a secure quantum channel. A generalisation of [27] is given by [28]. Furthermore, in [25] a classical bit is encrypted using keys in a non-orthogonal quantum state, which was extended by [24] to a new quantum encryption algorithm. Zhou proposed a standard one-time pad encryption algorithm for classical messages without a pre-shared or stored key [29]. Cao and Liu improved Zhou et al's quantum encryption algorithm [23] by decreasing the number of used keys [26]. The recent literature on quantum encryption algorithms concentrate more on the enhancement of the classical encryption algorithms using quantum cryptographic principles and image processing [30][31][32][33][34][35].

One of the most interesting classical cryptographic protocols is three-pass protocol, the protocol first proposed by Shamir. Shamir did not publish his work, but it was described fully for the first time in Massey's article [36]. Yang et al [37] and

Kanamori et al [38][39] proposed the Quantum Three-Pass Protocol independently by transferring Shamir's original idea to the quantum domain. Although Kathyaini et al claim in [40], that the Quantum Three-Pass protocol is unconditionally secure, Svozil shows in his paper on *Feasibility of the interlock protocol against man-in-the-middle attacks on quantum cryptography* [41], that the man-in-the-middle attack is always a potential threat to information exchange based on the no-cloning theorem. In chapter 4 we discuss the Quantum Three-Pass protocol and its security against classical and quantum attacks. We showed that the only potential attack method is the man-in-the-middle attack to the QTPP. Therefore, we propose in chapter 5 the enhanced Quantum Three-Pass Protocol, adding authentication over an agent called the Quantum Distribution Centre. The security analysis of the enhanced QTPP shows that additionally to all security features of the original QTPP, with the addition of authentication, the man-in-the-middle attack is eliminated. We also discuss the effect of noise on the quantum bit error rate of the enhanced QTPP. An example illustrates the working principle of the enhanced QTPP.

The thesis is organized as follows: In chapter 2, we give an overview of quantum mechanics and quantum computation theory, which are needed for the understanding of the thesis. In chapter 3, the original Quantum Three-Pass Protocol QTPP proposed Yang et al [37] and Kanamori et al [38][39] is reviewed and discussed in detail. The security analysis of the original QTPP is given in detail. Also, all possible attack methods are discussed individually in detail for the original QTPP algorithm. As a result, only the man-in-the-middle attack turned out to be a threat to the QTPP. In chapter 4, we present the enhanced QTPP based on authentication as discussed above. Chapter 5 closes the thesis with a summary. There are 4 Appendices at the end of this thesis. In Appendix A, the main concepts of quantum cryptography and

the BB84 protocol are reviewed. Appendix B, we review one of our contributions the modified BB84 key exchange protocol [30]. Appendix C, reviews the classical Hill-cipher algorithm. Finally, the glossary is given in Appendix D.

Chapter 2

PRELIMINARIES

The Physics on the atomic shows different characteristics compared to the Physics we experience in our everyday's life, which is described by classical physics. Quantum mechanics is a deeply troubling scientific theory. It challenges some of our most basic notions about physical reality. Examples of some of the basic concepts in Quantum Mechanics are as following:

- Quantum mechanics tells us that both the position and momentum of a particle can not be measured precisely simultaneously. This is known as Heisenberg's uncertainty principle.

- The measurement apparatus becomes part of the system in the quantum domain, therefore the system changes when a measurement is conducted and the state of the system changes significantly.

- In Newtonian mechanics the state of a particle is completely described by the position and momentum at any instant of time. Whereas, in Quantum Mechanics the state of a particle is completely described by the wave function. Thus, in classical mechanics the path the particle takes from *A* to *B* is known, but in Quantum Mechanics the information of the path is not directly accessible.

- Quantum Mechanics is inherently probabilistic. If we prepare two elementary particles in identical states and measure them, the results may be different for each particle.

- Quantum entities may behave like particles or like waves. This is called, the wave-particle dualism.

2.1 The Axioms of Quantum Mechanics

The quantum mechanics is a comprehensive theory developed independently by the two famous physicists, Heisenberg and Schrödinger.

The Heisenberg uncertainty principle states that we can never measure with perfect accuracy the two important physical quantities, describing the motion of a quantum particle, namely its position and momentum. If Δx denotes the accuracy of the measurement of the position and Δp denotes the accuracy of the measurement of the momentum in the one dimensional case, the Heisenberg uncertainty principle can be written as,

$$\Delta x \cdot \Delta p \geq \frac{\hbar}{2}. \tag{2.1}$$

In classical mechanics, studies the motion and behaviour of objects by taking deterministic approach, according that if we know a certain set of quantities as well as all the forces involved we can predict the future position of the object. On the other hand in quantum mechanics completely different approach where Heisenberg uncertainty principle tell us that is impossible to know the exact position and momentum of an particle at any moment in time. Therefore, the quantum mechanics uses a statistical approach. Even through we cannot predict where any particle ends

up, we can determine the probability of finding the particle at a certain position at a certain instant of time.

In classical mechanics, Newton's laws of motion and the conservation of energy are used to describe the motion and behaviour of systems. In quantum mechanics, which incorporates the wave particles duality of matter, the Schrödinger Equation takes the role of describing and predicting the behaviour of systems.

The time independent Schrödinger Equation is given as:

$$\hat{H}\,\Psi(\vec{r}) = E\,\Psi(\vec{r}),\ \text{with}\ \hat{H} = -\frac{\hbar^2}{2m}\cdot\nabla^2 + U(\vec{r}), \tag{2.2}$$

Where $\hat{H}$ denotes the Hamiltonian operator, E is the eigenvalue of $\hat{H}$, $\Psi(\vec{r})$ can be interpreted as probability amplitude and $|\Psi(\vec{r})|^2$ is the probability density to find the particle at the position $\vec{r}$. Since $|\Psi(\vec{r})|^2$is interpreted as probability density, then the probability of finding a particle in the space should be exactly equal to one. So, every wave function describing the motion of a particle has to satisfy the normalization condition

$$\int_{-\infty}^{+\infty} |\Psi(\vec{r})|^2 dr = 1. \tag{2.3}$$

The fundamental principles of quantum mechanics used throughout this thesis can be summarized as following:

- The superposition principle explains that a system can take any of the possible states simultaneously with a certain probability until it is measured.

- The measurement principle tells us how measuring a particle changes its state, and how much information we can access from a particle.

- The unitary evolution axiom governs how the state of the quantum system evolves in time.

- The no-cloning theorem tells us that an unknown quantum state can not be cloned.

In this chapter, we will review the basic axioms of quantum mechanics and quantum computation, forming the basis of this thesis. First, we would like to introduce the Dirac notation, which is a very convenient an abstract description method in quantum mechanics.

2.2 Dirac Notation

P.A.M. Dirac introduced the so-called Bra-Ket notation in his paper [42] to facilitate a coordinate free and abstract description of a quantum state.

Let $v \in \mathbb{C}^m$ be a vector in the *m*-dimensional complex vector space. Then the Ket-vector $|v\rangle$ represents the *m*-dimensional complex column vector v as,

$$|v\rangle = \begin{pmatrix} v_1 \\ v_2 \\ \vdots \\ v_m \end{pmatrix} \tag{2.4}$$

The adjoined (complex conjugate and transpose) vector of the Ket-vector $|v\rangle$ is the so-called Bra-vector $\langle v|$ with,

$$|v\rangle^\dagger = \langle v| = (v_1^*, v_2^*, \dots, v_m^*), \tag{2.5}$$

Representing the vector. The inner product of the vectors u and v can then be easily written in the following form:

$$\langle u|v\rangle = (u_1^*, u_2^*, \dots, u_m^*) \cdot \begin{pmatrix} v_1 \\ v_2 \\ \vdots \\ v_m \end{pmatrix} = u_1^* v_1 + u_2^* v_2 + \cdots + u_m^* v_m \qquad (2.6)$$

Let $|\psi\rangle$ be a quantum state in an N dimensional complex vector space, and let $\{|0\rangle, |1\rangle, \cdots, |N-1\rangle\}$ be an orthonormal basis of this vector space, then the state $|\psi\rangle$ can be described as the superposition of the basis states as following:

Then the inner product of $|\psi\rangle$ with itself is,

$$|\psi\rangle = \sum_{n=0}^{N-1} \alpha_n |n\rangle = \begin{pmatrix} \alpha_0 \\ \alpha_1 \\ \vdots \\ \alpha_{N-1} \end{pmatrix} \qquad (2.7)$$

$$\langle\psi|\psi\rangle = \sum_{m=0}^{N-1} \alpha_m^* \langle m| \sum_{n=0}^{N-1} \alpha_n |n\rangle = \sum_{\substack{n=0 \\ m=0}}^{N-1} a_m^* a_n \langle m|n\rangle = \sum_{n=0}^{N-1} |a_n|^2, \qquad (2.8)$$

With,

$$\langle m|n\rangle = \delta_{mn}. \qquad (2.9)$$

Now we can use the same tools to write the inner product of any two states, $|\psi\rangle$ and $|\phi\rangle$, where

$$|\phi\rangle = \sum_n b_n |n\rangle\,, \qquad (2.10)$$

Their inner product is,

$$\langle\psi|\phi\rangle = \sum_{j,n} a_j^*\, b_n \langle j|n\rangle = \sum_n a_n^* b_n. \qquad (2.11)$$

Notice that there is no reason for the inner product of two states to be real (unless they are the same state), and that

$$\langle\psi|\phi\rangle = \langle\phi|\psi\rangle^* \in \mathbb{C}. \qquad (2.12)$$

In this way, a bra vector may be considered as a "functional." We feed it a ket, and it spits out a complex number.

2.3 The Superposition Principle

Consider a system with n distinguishable (classical) states. For example, the electron in an atom is only allowed to be in one of a discrete set of energy levels, starting with the ground state, the first excited state, the second excited state, and so on. If we assume a suitable upper bound on the total energy, then the electron is restricted to being in one of n different energy levels, the ground state or one of $n - 1$ excited state. As a classical system, we might use the state of this system to store a number between 0 and $n - 1$. The superposition principle says that if a quantum system can be in one of n states then it can also be placed in a linear superposition of these states with complex probability amplitudes.

Let us introduce some notation. We denote the ground state of our n-state system by $|0\rangle$, and the successive excited states by $|1\rangle, \cdots, |n-1\rangle$. These are the n possible distinct states of the electron. The superposition principle tells us that, in general, the quantum state of the electron is $\alpha_0|0\rangle + \alpha_1|1\rangle + \cdots + \alpha_{n-1}|n-1\rangle$, where $\alpha_0, \alpha_1, \cdots, \alpha_{n-1}$ are complex numbers normalized so that $\sum_j |\alpha_j|^2 = 1$. α_j is called the amplitude of the state $|j\rangle$.

The superposition principle is one of the most ambiguous aspects about quantum physics. One way to think about a superposition is that the electron does not make up its mind about whether it is in the ground state or each of the $n - 1$ excited states, and the amplitude α_0 is a measure of its mind towards the ground state. Of course we cannot think of α_0 as the probability that an electron is in the ground state, α_0 can be

negative or imaginary. The measurement principle makes this interpretation of α_0 more precise. Where, when we measure the system, we disturb the state so when we are not looking, the electron is in the superposition of ground and excited. But as soon as we measure it, it quickly makes up its mind and it goes into either ground or excited with certain probabilities. And this is the reason why we wanted the state to be normalized, because these probabilities must add up to 1.

2.4 Hilbert Space

Hilbert space is an infinite dimensional inner product space in which mathematical functions take the place of points, crucial to the place of quantum mechanics and its application. Mathematically, the Hilbert space is a real or complex inner product space, for example the Hilbert space for finite dimension include,

- The real numbers $\mathbb{R}^n$ with $\langle u, v\rangle$ the vector dot product of u and v.
- The complex numbers $\mathbb{C}^n$ with $\langle u, v\rangle$ the vector dot product of u and complex conjugate of v.

An example of an infinite-dimensional Hilbert space is L^2, the set of all functions $f: \mathbb{R}^n \longrightarrow \mathbb{R}^n$ such that the integral of f^2 over the whole real line is finite. In this case, the inner product is, $\langle u, v\rangle = \int_{-\infty}^{+\infty} \mathrm{u}(x)\mathrm{v}(x)\mathrm{dx}$.

2.5 The Measurement Principle (Projective Measurement)

A quantum state is generally given in linear superposition $|\psi\rangle = \sum_{j=0}^{N-1} \alpha_j |j\rangle$. The measurement of the state $|\psi\rangle$ in the basis $\{|0\rangle, |1\rangle, \dots, |N-1\rangle\}$ will return the state $|\psi\rangle$ in one of the basis states $|j\rangle$ with the probability $\left|\alpha_j\right|^2$.

One important aspect of the measurement process is that it alters the state of the quantum system; the effect of the measurement is that the new state is exactly the outcome of the measurement. It means if the outcome of the measurement is $|j\rangle$, then

following the measurement, the qubit is in state $|j\rangle$. This implies that you cannot collect any additional information about the amplitudes α_j by repeating the measurement.

2.6 Single Qubit

Qubits or quantum bits are basic building blocks that involve all fundamental quantum phenomena. They provide a mathematically simple framework in which to introduce the basic concepts of quantum physics. Qubits are two states quantum systems. A qubit can be either in the state $|0\rangle$ or in the state $|1\rangle$ or in a superposition state $\alpha|0\rangle + \beta|1\rangle$. The state of a qubit can be written as a column vector $\binom{\alpha}{\beta} \in \mathbb{C}^2$ or in Dirac notation as,

$$|\psi\rangle = \alpha|0\rangle + \beta|1\rangle \text{ with } \alpha, \beta \in \mathbb{C} \text{ and } |\alpha|^2 + |\beta|^2 = 1, \qquad (2.13)$$

This linear superposition $|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$ is part of the private world of the quantum particle. In order to find out the quantum particles state a measurement has to be carried out. Making a measurement gives us a single classical bit of information 0 or 1. The simplest measurement is in the standard basis, and measuring $|\psi\rangle$ in this $\{|0\rangle, |1\rangle\}$ basis yields 0 with probability $|\alpha|^2$, and 1 with probability $|\beta|^2$.

One important aspect of the measurement process is that it alters the state of the qubit: the effect of the measurement is that the new state is exactly the outcome of the measurement. It means if the outcome of the measurement of $|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$ yields 0, then following the measurement, the qubit is $|0\rangle$. This implies that you cannot collect any additional information about α, β by repeating the measurement.

More generally, we may choose any orthogonal basis $\{|v\rangle, |w\rangle\}$ and measure the qubit in that basis. To do this, we rewrite our state in that basis, $\psi = \alpha' v + \beta' |w$. The outcome of $|v\rangle$ with probability $|\alpha'|^2$, and $|w\rangle$ with probability $|\beta'|^2$. If the outcome of the measurement on $|\psi\rangle$ yields $|v\rangle$, then as before, the qubit is then state $|v\rangle$.

2.7 Two qubits

Now let us examine a system of two qubits of a two state system. In order to describe all possible states of this system, we have to set first the basis. The basis for the description of a 2 qubit system is given as $\{|00\rangle, |01\rangle, |10\rangle, |11\rangle\}$. Analogously to the one qubit system any state in this 2 qubit system can be described by the superposition of the basis vectors, therefore any two qubit system can be written as,

$$|\psi\rangle = \alpha_{00}|00\rangle + \alpha_{01}|01\rangle + \alpha_{10}|10\rangle + \alpha_{11}|11\rangle, \tag{2.14}$$

where $\alpha_{ij} \in \mathbb{C}$, and $\sum_{ij} |\alpha_{ij}|^2 = 1$.

2.7.1 Tensor Product System

Tensor Product is used to describe a system that is made up of multiple independent subsystems. So let's imagine that we have a system of two qubits, and let's say that our first qubit is in this state,

$$|\psi\rangle = \alpha_0|0\rangle + \alpha_1|1\rangle,$$

and the second qubit is in this state,

$$|\phi\rangle = \beta_0|0\rangle + \beta_1|1\rangle,$$

then the state of the composite system is a superposition

$$|\psi\rangle \otimes |\phi\rangle = \alpha_0\beta_0|00\rangle + \alpha_0\beta_1|01\rangle + \alpha_1\beta_0|10\rangle + \alpha_1\beta_1|11\rangle. \tag{2.15}$$

These states are in $\mathbb{C}^2 \otimes \mathbb{C}^2$, which is a subspace of $\mathbb{C}^4$. The physical interpretation of the tensor product state as given in equation (2.15) is that the particles are

independently in the states $|\psi\rangle$ and $|\phi\rangle$, which are single qubit states. This means that any single qubit operation on one of the states does not affect the other state. Therefore, we can identify if the system is a system of two independent qubits, i.e. it can be represented as a tensor product of two qubits or if the system is an entangled system of two qubits described in the following section.

2.7.2 Entanglement

Entanglement it is a fundamental quantum phenomenon occurs in systems of two or more particles, and it's one of the basic features of quantum mechanics that's exploited in quantum computation.

Let us now consider a state $|\mathrm{x}\rangle \in \mathbb{C}^4 \setminus \mathbb{C}^2 \otimes \mathbb{C}^2$, where $|\mathrm{x}\rangle$ is one of the Bell states, $\left\{\frac{1}{\sqrt{2}}(|00\rangle + 11\rangle), \frac{1}{\sqrt{2}}(|00\rangle - 11\rangle), \frac{1}{\sqrt{2}}(|01\rangle + |10\rangle), \frac{1}{\sqrt{2}}(|01\rangle - |10\rangle)\right\}$, which play an important role in quantum computation. Without loss of generality, let

$$|\mathrm{x}\rangle = \frac{1}{\sqrt{2}}(|00\rangle + 11\rangle), \tag{2.16}$$

In order to check if $|\mathrm{x}\rangle \notin \mathbb{C}^2 \otimes \mathbb{C}^2$ we have to try decompose this 2 qubit state into a product of two one qubit states as following:

$$(\alpha_0|0\rangle + \alpha_1|1\rangle) \otimes (\beta_0|0\rangle + \beta_1|1\rangle)$$

So the product state becomes then,

$$\alpha_0\beta_0|00\rangle + \alpha_0\beta_1|01\rangle + \alpha_1\beta_0|10\rangle + \alpha_1\beta_1|11\rangle, \tag{2.17}$$

So now comparing coefficients in the equations (2.16) and (2.17), leads us to four equations with four unknowns that have to be fulfilled simultaneously, namely $\alpha_0\beta_0 = \frac{1}{\sqrt{2}}, \alpha_0\beta_1 = 0, \alpha_1\beta_0 = 0, \alpha_1\beta_1 = \frac{1}{\sqrt{2}}$. The solution of this set of equations is gives an empty set, i.e. there is no solution. Therefore, the state $|x\rangle$ cannot be decomposed it into a tensor product. We say the two qubits are inherently entangled with each other. When the two qubits are entangled, we cannot determine the state of

each qubit individually without affecting the second state. The state of the qubits has as much to do with the relationship of the two qubits as it does with their individual states.

2.8 Operations on Quantum Bits

Qubits are stored in quantum mechanical systems, such as the nuclear spins of atoms, or superconductor, or polarization of photons, etc. Quantum gates can be applied to selected qubits in an n-qubits register and modify the values of the register. The quantum gate can be represented as a matrix operator. As we are dealing with a probabilistic system, the operations preserve the norm of the system, and therefore the determinant of the matrix should be one. E.g. unitary matrices comply with this condition. Furthermore, unitary operators satisfy the relationship $U^{\dagger}U = I$, where I is the identity. All operations on a qubit, represented by the unitary operator, are reversible, because unitary operators have an inverse, with $U^{\dagger} = U^{-1}$.

Let *U* be a general unitary operator in a one qubit system

$$U = a|0\rangle\langle 0| + b|0\rangle\langle 1| + c|1\rangle\langle 0| + d|1\rangle\langle 1| \,, \tag{2.18}$$

be applied to the state $|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$.

The application of a gate *U* to a qubit in the state $|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$ yields to,

$$\begin{aligned} U\,|\psi\rangle &= [a|0\rangle\langle 0| + b|0\rangle\langle 1| + c|1\rangle\langle 0| + d|1\rangle\langle 1|](\alpha|0\rangle + \beta|1\rangle) \\ &= (a\alpha|0\rangle + c\alpha|1\rangle + b\beta|0\rangle + d\beta|1\rangle). \end{aligned} \tag{2.19}$$

The state of the qubit after the application of the operator is now in the state,

$$|\psi\rangle = (a\alpha + b\beta)|0\rangle + (c\alpha + d\beta)|1\rangle. \tag{2.20}$$

In the following we introduce the most important quantum gates from the point of view of this thesis.

2.9 Single Qubit Gates

The single quantum gate will take one qubit as input. So what comes in is a wire, which is carrying a qubit of information. And then, the single quantum gate performs some unitary transformation on this qubit and outputs a transformed qubit, which is in this new state. The most important representatives of single quantum operators are Hadamard –, X–, Y–, Z–, phase shift –, identity –, and measurement operator. These operators (gates) are discussed in the following.

2.9.1 Hadamard Gate

The Hadamard gate acts on a single qubit. It is a very important gate in quantum computation. It maps the computational basis $\{|0\rangle, |1\rangle\}$ to the so-called Hadamard basis $\left\{\frac{|0\rangle+|1\rangle}{\sqrt{2}}, \frac{|0\rangle-|1\rangle}{\sqrt{2}}\right\}$. The Hadmard gate can be represented in Dirac notation as well as in the matrix form as:

$$H = \frac{1}{\sqrt{2}}[|0\rangle\langle 0| + |0\rangle\langle 1| + |1\rangle\langle 0| - |1\rangle\langle 1|], = \frac{1}{\sqrt{2}}\begin{bmatrix}1 & 1\\ 1 & -1\end{bmatrix}. \qquad (2.21)$$

The symbol of Hadamard gate is presented in Figure 1.

Figure 1: Symbol of Hadamard gate.

2.9.2 X Gate

The Pauli-X gate acts on a single qubit. It is equivalent to the NOT gate. It maps $|0\rangle$ to $|1\rangle$ and $|1\rangle$ to $|0\rangle$. The *X*-gate can be represented in Dirac notation as well as in the matrix form as

$$X = [|0\rangle\langle 1| + |1\rangle\langle 0|] = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}. \quad (2.22)$$

Figure 2 shows the graphical symbol of the gate.

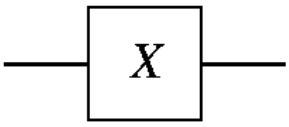

Figure 2. Symbol of X gate

2.9.3 Y Gate

The Pauli-Y gate acts on a single qubit. It maps $|0\rangle$ to i$|1\rangle$ and $|1\rangle$ to −i$|0\rangle$. The *Y*-gate can be represented in Dirac notation as well as in the matrix form as,

$$Y = [i|1\rangle\langle 0| - i|0\rangle\langle 1|] = \begin{bmatrix} 0 & -i \\ i & 0 \end{bmatrix}. \quad (2.23)$$

Figure 3 shows the graphical symbol of the gate.

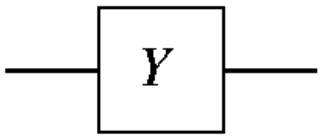

Figure 3: Symbol of Y gate.

2.9.4 Z Gate

The Pauli-Z gate acts on a single qubit. It leaves the state $|0\rangle$ unchanged and it maps $|1\rangle$ to $-|1\rangle$. The Z-gate can be represented in Dirac notation as well as in the matrix form as,

$$Z = [|0\rangle\langle 0| - |1\rangle\langle 1|] = \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}. \quad (2.24)$$

Figure 4 shows the graphical symbol of the gate.

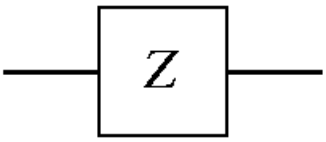

Figure 4: Symbol of Z gate.

2.9.5 Phase Shift Gate

The phase shift gate acts on a single qubit. It leaves the state $|0\rangle$ unchanged and it maps $|1\rangle$ to $e^{i\theta}\ |1\rangle$. The phase shift gate can be represented in Dirac notation as well as in the matrix form as,

$$R(\theta) = \left[|0\rangle\langle 0| + e^{i\theta}|1\rangle\langle 1|\right] = \begin{bmatrix} 1 & 0 \\ 0 & e^{i\theta} \end{bmatrix}. \tag{2.25}$$

Figure 5 shows the graphical symbol of the gate.

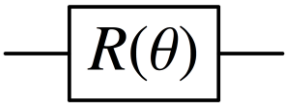

Figure 5: Symbol of the phase shift gate.

2.9.6 Identity Gate

The identity gate acts on a single qubit. It leaves the state $|0\rangle$ and state$|1\rangle$ unchanged. The identity gate can be represented in Dirac notation as well as in the matrix form as,

$$I = [|0\rangle\langle 0| + |1\rangle\langle 1|] = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}, \tag{2.26}$$

Figure 6 shows the graphical symbol of the gate.

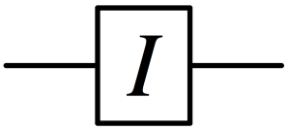

Figure 6: Symbol of the identity gate.

2.9.7 Measurement Gate

A measurement gate performs the measurement of the qubit's state. It leaves the qubit in the state corresponding to the result. Figure 7 presents the measurement gate symbol.

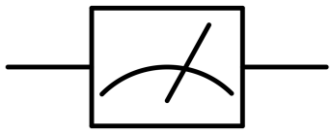

Figure 7: Symbol of the measurement gate.

2.10 Multi Qubits Gates

The multi quantum gate will take two qubits or more as input. And then, the multi quantum gate performs some unitary transformation on these qubits and outputs the same number of qubits, which are now in the new states. The most important representatives of multi quantum gates are the Controlled-NOT gate, the SWAP gate, and Toffoli gate. All these gates and their mathematical representations will be shown in the following.

2.10.1 Controlled-NOT Gate

The Controlled-NOT (C-NOT) gate acts on two qubits. One is the control qubit and the second is the target qubit, depending on the control bit the target bit is changed, where only when the control bit is $|1\rangle$ the target bit will be changed, and otherwise the target qubit will remain unchanged. It maps the basic states as following:

$$|00\rangle \rightarrow |00\rangle$$

$$|01\rangle \rightarrow |01\rangle$$

$$|10\rangle \rightarrow |11\rangle$$

$$|11\rangle \rightarrow |10\rangle$$

Then the C-NOT gate can be represented in Dirac notation as well as in the matrix form as,

$$\text{C-NOT} = [|00\rangle\langle 00| + |01\rangle\langle 01| + |10\rangle\langle 11| + |11\rangle\langle 10|]$$

$$= \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{bmatrix}. \tag{2.27}$$

Figure 8 shows the graphical symbol of the gate.

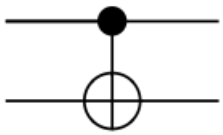

Figure 8: Symbol of the C-NOT gate.

2.10.2 SWAP Gate

The SWAP gate acts on two qubits. It swaps two qubits. The SWAP gate can be represented in Dirac notation as well as in the matrix form as,

$$\text{SWAP} = [|00\rangle\langle 00| + |01\rangle\langle 10| + |10\rangle\langle 01| + |11\rangle\langle 11|]$$

$$= \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix}. \tag{2.28}$$

Figure 9 shows the graphical symbols of the gate.

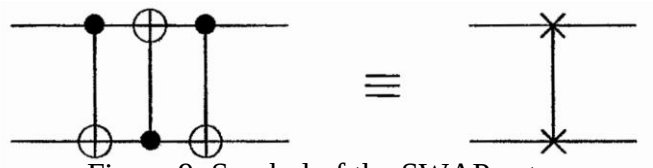

Figure 9: Symbol of the SWAP gate.

The SWAP gate can be also constructed by three C-NOT gates as shown in Figure 9.

2.10.3 Toffoli Gate

The Toffoli gate is a two controlled NOT. It acts on three qubits two controls qubits and one target qubit. Only the state of a target qubit is flipped depending on the states of both control qubits. The gate matrix is:

$$T = \begin{bmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \end{bmatrix}, \tag{2.29}$$

The representation of the gate matrix as Dirac notations is:

$$T = [|000\rangle\langle 000| + |001\rangle\langle 001| + |010\rangle\langle 010| + |011\rangle\langle 011| + |100\rangle\langle 100| + |101\rangle\langle 101| + |110\rangle\langle 111| + |111\rangle\langle 110|], \tag{2.30}$$

In Figure 10 shows the symbol of Toffoli gate. A NOT gate with any number of control.

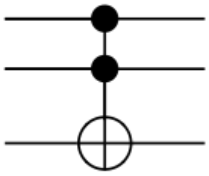

Figure 10: The symbol of Toffoli gate.

2.11 No-Cloning Theorem

The no-cloning theorem is one of the most important theorems in quantum computation showing that it is impossible to create identical copies of an arbitrary unknown state. It was presented by Wootters and Zurek [43] and Dieks [44] in 1982, and has deep implications for quantum computation and quantum cryptography. It also plays a central role in our proposed algorithm. According to Asher Peres and David Kaiser [45][46], the publication of the no-cloning theorem was prompted by a

proposal from Nick Herbert [47] for a device using quantum entanglement. A review of quantum cloning is given in [48].

In this thesis, the no-cloning theorem plays an important role as it shows that known classical and quantum attack methods that are discussed in the following chapter can be prevented. The no-cloning theorem usually implies two quantum states either identical or orthogonal if we allow a cloning to be on two quantum states by using unitary operator U that represents the time evolution operator and the copier. So assume we have a quantum system A, and it has quantum state $|\varphi\rangle_A$ and we want copy this state, therefore we assume another quantum system B with the same state space and initial state $|e\rangle_B$. Then the copier should act as following:

$$|\varphi\rangle_A \otimes |e\rangle_B \xrightarrow{U} |\varphi\rangle_A \otimes |\varphi\rangle_B. \tag{2.31}$$

Now, we select two an arbitrary states $|\varphi\rangle_A$ and $|\psi\rangle_A$ drawn from the Hilbert space. Let us consider the inner product of them because *U* is unitary and it preserves the inner product.

$$\langle e|_B\langle\varphi|_A|\psi\rangle_A|e\rangle_B = \langle e|_B\langle\varphi|_A U^\dagger U|\psi\rangle_A|e\rangle_B = \langle\varphi|_B\langle\varphi|_A|\psi\rangle_A|\psi\rangle_B. \tag{2.32}$$

Thus,

$$\langle\varphi|\psi\rangle_A = \langle\varphi|\psi\rangle_A\langle\varphi|\psi\rangle_B. \tag{2.33}$$

By omitting subscripts A and B, we have,

$$\langle\varphi|\psi\rangle = (\langle\varphi|\psi\rangle)^2 \tag{2.34}$$

This implies that either $\langle\varphi|\psi\rangle = 1 \; or \; \langle\varphi|\psi\rangle = 0$, so we obtain either $|\varphi\rangle$ is identical to $|\psi\rangle$ or $|\varphi\rangle$ is orthogonal to $|\psi\rangle$. However, this cannot be the case for two arbitrary states. Therefore the opponent or the universal copier U cannot clone a

general quantum state. Since the opponent does not know the sender state, it is not possible to clone the sender quantum state.

Looking at it in this way we can conclude that the no-cloning theorem intuitively follows the uncertainty principle because the opponent who wants to clone any arbitrary unknown state would have to be able to measure the state, and hence disturb the state based on the uncertainty theorem. This means that the opponent will not know anything about the initial state of the system and any attempt by an opponent to grab information will lead to a disturbance, which can be discovered later by the sender and receiver. The no-cloning theorem represents the main idea of the security of the quantum encryption algorithm. This will be abundantly clear when classical and quantum attacks are discussed later.

2.12 Summary

In this Chapter we presented information about the quantum mechanics and quantum computations essential to understand the thesis. We presented a very simple and a new, direct method of learning quantum mechanics. And this is going to be in terms of the building blocks of quantum computation, qubits and quantum gates. So this new way of looking at quantum mechanics also emphasizes the most paradoxical features of quantum mechanics, and it is some of these paradoxical features that are used most prominently in quantum computing. At the end of the Chapter we presented a non-cloning theorem.

Chapter 3

QUANTUM THREE-PASS PROTOCOL (QTPP)

This chapter describes a new quantum protocol, which is a quantum three-pass protocol $QTPP$. In section 4.1 we introduce the fundamental parts of the classical protocol as put forward by Shamir [36]. In section 4.2 we review the details of the Quantum-Three-Pass-Protocol according to Yang et al [37]. Section 4.3 illuminates the differences between the classical three-pass protocol and the quantum three-pass protocol. In Section 4.4 we discuss the security of the well known classical and quantum three pass protocols. Finally, we summarize the chapter in 4.5.

3.1 Classical Three-Pass Protocol (TPP)

One of the most interesting classical cryptographic protocols is three-pass protocol, the protocol proposed by Shamir, Shamir did not publish his work, but it was described fully for the first time in Massey's article [36]. The protocol is used in many applications [49][50][51][52][53]. The protocol declares that privacy can be obtained with no advance distribution of secret keys or public keys. In this protocol the sender and receiver use the same encryption algorithm E_K, where E denotes the encryption algorithm and K denotes the key. This encryption algorithm is commutative with respect to the order of the usage of keys. Mathematically this can be expressed as

$$E_{K_S}(E_{K_R}(P)) = E_{K_R}(E_{K_S}(P)), \tag{3.1}$$

where K_S denotes the key of the sender and K_R denotes the key of the receiver. This means that the result of a dual encryption is the same whether the receiver is first encrypted K_S or K_R or vice versa.

The classical Three-Pass Protocol is illustrated step by step in the following:

- The sender and receiver randomly select their own private secret keys, K_S and K_R, respectively.
- The sender sends a secret plain-text P to the receiver, the sender encrypts P with the senders key K_S, and then sends the resulting cipher-text C_1 to the receiver.

$$C_1 = E_{k_S}(P). \tag{3.2}$$

- Then the receiver receives C_1 and encrypts C_1 with the receivers key $\mathrm{K_R}$. The receiver sends the resulting cipher-text C_2 back to the sender.

$$C_2 = E_{K_R}(C_1) = E_{K_R}(E_{K_S}(P)). \tag{3.3}$$

- When the sender receives C_2, he decrypts C_2 with the senders key K_S. Because of the commutative property in equation (3.1), this removes the previous encryption by K_S and the result is,

$$C_3 = E_{K_S}^{-1}(E_{k_R}(E_{k_S}(P))) = E_{K_S}^{-1}(E_{k_S}(E_{k_R}(P))) = E_{k_R}(P). \tag{3.4}$$

  Then, the sender sends C_3 back to the receiver.

- When the receiver receives C_3, he decrypts C_3 with the receiver key K_R to obtain the plain-text P that the sender has successfully sent.

In summary, the plain-text is delivered in a two-box securely to a receiver, the receiver using two keys to open the two-box without sharing keys to open the two-box, all the procedure for the classical three pass protocol are shown in following Figure 11.

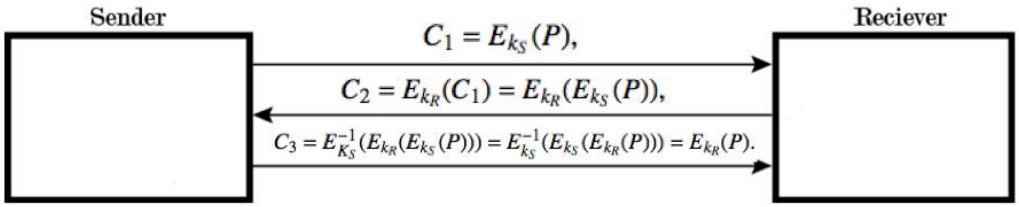

Figure 11: Classical Three-Pass Protocol.

3.2 Quantum Three-Pass Protocol (QTPP)

In recent years, the three-pass protocol TPP has been widely used in many applications in cryptography. The quantum three-pass protocol is a new addition to the protocols of the quantum cryptography protocol and depends mainly on Shamir's three-pass protocol in classical cryptography [36]. Later, similar versions of the QTPP were presented in various articles [37][38][39]. A feature of this protocol is that it uses only the quantum channel unlike the other quantum protocols that use the quantum channel and the classical channel. Part of the procedure of this protocol is using the photon as a qubit; therefore each classical bit is encrypted to the quantum bit. After the classical bit is encoded to the photon, the polarization for the photon is rotated by an angle θ, which is selected arbitrarily for each of the qubits. The rotation operation is represented as:

$$R(\theta) = \begin{pmatrix} \cos\theta & \sin\theta \\ -\sin\theta & \cos\theta \end{pmatrix} \tag{3.5}$$

$$= \cos(\theta)\,|0\rangle\langle 0| + \sin(\theta)\,|0\rangle\langle 1| - \sin(\theta)\,|1\rangle\langle 0| + \cos(\theta)\,|1\rangle\langle 1|$$

This operation can be considered as encryption and the angle θ represents the encryption key, while the rotation operation by the angle −θ can be considered as decryption. In the quantum three pass protocol there is no shared key between the sender and receiver, the sender generates its own secret $K_{\theta S}$ where ($K_{\theta S} = \theta_S \,|0 \leq \theta_S < \pi$) for each session. And the receiver generates her/his own secret key $K_{\theta R}$ where ($K_{\theta R} = \theta_R \,|0 \leq \theta_R < \pi$) for each session. It is impossible for the opponent to discover these keys. For *n*-qubits, the key for the sender and the receiver changed with each qubit, this key and its inverse are used for encryption and decryption. Therefore the new key will block any data related to the key and the information from being infiltrated. Now, if it we assume that the plain-text P is a single photon encrypted to the qubit as $P = |1\rangle$, the sender and receiver generate their own keys, the key of the sender is $K_{\theta S}$ and key of the receiver is $K_{\theta R}$. The sender encrypts the plain-text P with its generation key as in the following:

$$E_{K_{\theta_S}}[P]: R(\theta_S)\,|1\rangle \;=\; sin\,\theta_S\;|0\rangle \;+\; cos\,\theta_S\;|1\rangle \;=\; |\varphi_1\rangle, \qquad (3.6)$$

where $E_{K_{\theta_S}}$ denotes the encryption of the plain-text P with $K_{\theta S}$, resulting is the superposition state $|\varphi_1\rangle$.

The receiver receives the photon in $|\varphi_1\rangle$ and encrypts it with its own key as in the following:

$$E_{K_{\theta_R}}\left[E_{K_{\theta_S}}[P]\right]: R(\theta_R)\,|\varphi_1\rangle \qquad (3.7)$$

$$= sin\,(\theta_R + \theta_S)|0\rangle \;+\; cos\,(\theta_R + \theta_S)\;|1\rangle \;=\; |\varphi_2\rangle.$$

Where $|\varphi_2\rangle$ is a superposition state. The receiver sends $|\varphi_2\rangle$ back to the sender. The sender receives $|\varphi_2\rangle$ and decrypts it by using the angle θ_S by applying the rotation operation with the angle $-\theta_S$ resulting in the state $|\varphi_3\rangle$ as

$$D_{K_{\theta_S}}\left[E_{K_{\theta_R}}\left[E_{K_{\theta_S}}[P]\right]\right] = E_{K_{\theta_R}}[P]: R(-\theta_S)\,|\varphi_2\rangle \tag{3.8}$$

$$= sin\,(\theta_R)|0\rangle + cos\,(\theta_R)\,|1\rangle = |\varphi_3\rangle.$$

Where $D_{K_{\theta_S}}$ is the decryption operation with the angle $-\theta_S$. Then, the sender sends the resulting message $|\varphi_3\rangle$ back to the receiver. The receiver gets $|\varphi_3\rangle$ and decrypts it by using the angle $-\theta_R$ to retrieve the original plain-text P= $|1\rangle$ that the sender has sent.

$$D_{K_{\theta R}}\,[E_{K_{\theta R}}[P]]: R(-\theta_R)\,|\varphi_3\rangle\; =\; |1\rangle \tag{3.9}$$

Finally, the receiver has the plain-text $|1\rangle$. The whole procedure of the protocol is shown in Figure 12.

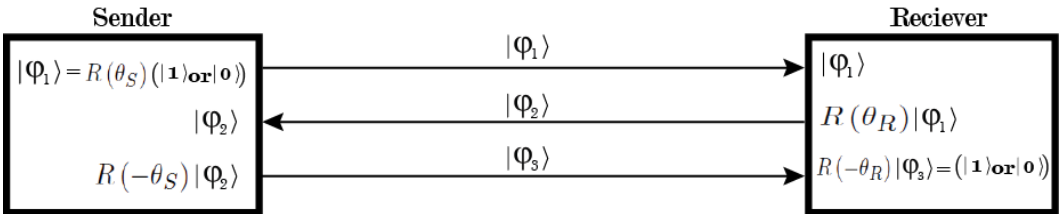

Figure 12: Quantum Three-Pass Protocol Procedure.

3.3 Security Analysis of QTPP

3.3.1 Cipher-Text-Only Attack

A cipher-text only attack can only be conducted if the cipher-text is in an orthogonal state, otherwise any measurement will collapse the cipher-text state into one of the basis states. As the plain text massage $|P\rangle \in \{|0\rangle, |1\rangle\}$, the rotation K_{θ_S}, also rotates the computational basis and the cipher-text $|\varphi_1\rangle = K_{\theta_S}\,|P\rangle$, will be orthogonal in the rotated computational basis. Therefore, if the opponent tries to intercept the cipher-text, he can only be successful if the rotation angle θ_S is known, otherwise the cipher-text, also subject to the no-cloning theorem can not be copied. Analogously, this fact applies to the further steps of the protocol, i.e. the

cipher-text $|\varphi_2\rangle = K_{\theta_S} K_{\theta_R} |P\rangle$, can only be intercepted if the angles θ_S and θ_R are known, etc. The probability of a successful retrieval of the cipher-text is based on the size of the angle space. So if the angle space has the size *n*, then the probability in case of equally distributed angles of retrieving the cipher-text is $\frac{1}{n}$. Keeping in mind that the opponent has only one chance for the measurement, it will be sufficient to make the key space sufficiently big, that this kind of attack will be statistically irrelevant. Obviously, this attack method has to be considered in the context with the man in the middle attack, because retrieving the information is equivalent to measurement. Therefore, all problems discussed in the man-in-the middle attack appear here as well.

3.3.2 Known-Plain-Text and Chosen-Plain-Text Attack

These strategies are not reasonable as the cipher-text can only be retrieved without any loss, if the angles are known. So, the argumentation for retrieving the cipher-text is the same as in the previous section. An analysis of the plain text, known fully or partially, is then in this case obsolete, as the angles have to be known already in advance to retrieve the cipher-text.

3.3.3 Individual Particle Attack

The opponent tries to intercept each sender state independently by joining the intercepted state with its own state (either tensor product state of the sender state and a known state or entangled state by both states). This type of attack is known as an individual particle attack [55]. It is regarded as a significant type of attack because the opponent applies a unitary operation on this joint state without changing the original state sent by the sender. Therefore, neither the sender nor the receiver will be aware of it. For example in our QTPP we have three transmitted states (i.e., Sender → Receiver, Receiver → Sender, Sender → Receiver). E.g. if the opponent applies

C-Not gate between the sender and receiver, where the control bit is the transmitted state; for instance, $|0\rangle$ and the target is the opponent state; for instance, $|1\rangle$ then the state for the opponent will not change and he will conclude the sender state is $|0\rangle$ and vice versa. But in our case this is not possible because all the three sender state $|\varphi 1\rangle$, $|\varphi 2\rangle$ and $|\varphi 3\rangle$ are superposition so even with an attack of this kind, the opponent cannot get the plain-text because the opponent needs to measure this state in a chosen basis which will leave the state in the one of the basis states with a certain probability, i.e. the opponent will get a random state and the key angle is unknown.

3.3.4 Intercept-Resend Attack

Let us assume that an opponent intercepts the transmitted photon from the sender. After a measurement of the photon, opponent resends it to receiver. This attack cannot break the protocol because the opponent cannot obtain the original state without knowing the key angle.

For example, let us assume the sender transmits a quantum state $|1\rangle$ with rotation by $\theta = 45^{\circ}$ (i.e., represented as $|\psi\rangle = (\sin(45^{\circ})|0\rangle + \cos(45^{\circ})\,|1\rangle))$. If the opponent intercepts the state $|\psi\rangle$, unknown to opponent, and measures it in a horizontal-vertical polarization base, the opponent will get zero or one with a probability of 50%. In our protocol, the angles θ_i for each bit are chosen randomly. Therefore, the opponent will get zero or one randomly on the average when he measures the sequence of polarized photons. Since half of opponent's measured data may be correct because $|\psi\rangle$ is $|0\rangle$ or $|1\rangle$ anyway, if the opponent resends the measured results to Bob, the transmission error rate (incorrect data/all data) will rise to 50 %. Thus, we can easily detect the existence of an opponent.

3.3.5 Trojan-Horse Attack

According to the usage of different keys in the QTPP which are the angles used for encryption, we have different quantum cipher-texts. Therefore, the Trojan- horse attack is not efficient even if the opponent can sneak into the encryption system because of the non-orthogonally of different quantum cipher-text states with the original computational basis.

3.3.6 Man-in-the-middle attack

The man-in-the middle attack can affect the quantum channel. In Quantum Three-Pass Protocol the opponent can pretend to be the receiver to sender or vice-versa. The opponent receives the states from the sender but resends similar but fake states back to the receiver. He continues with this tactical procedure until he disables the QTPP (i.e. Sender→ opponent → Receiver, Receiver → opponent → Sender, Sender → opponent → Receiver) as following in the Figure 13.

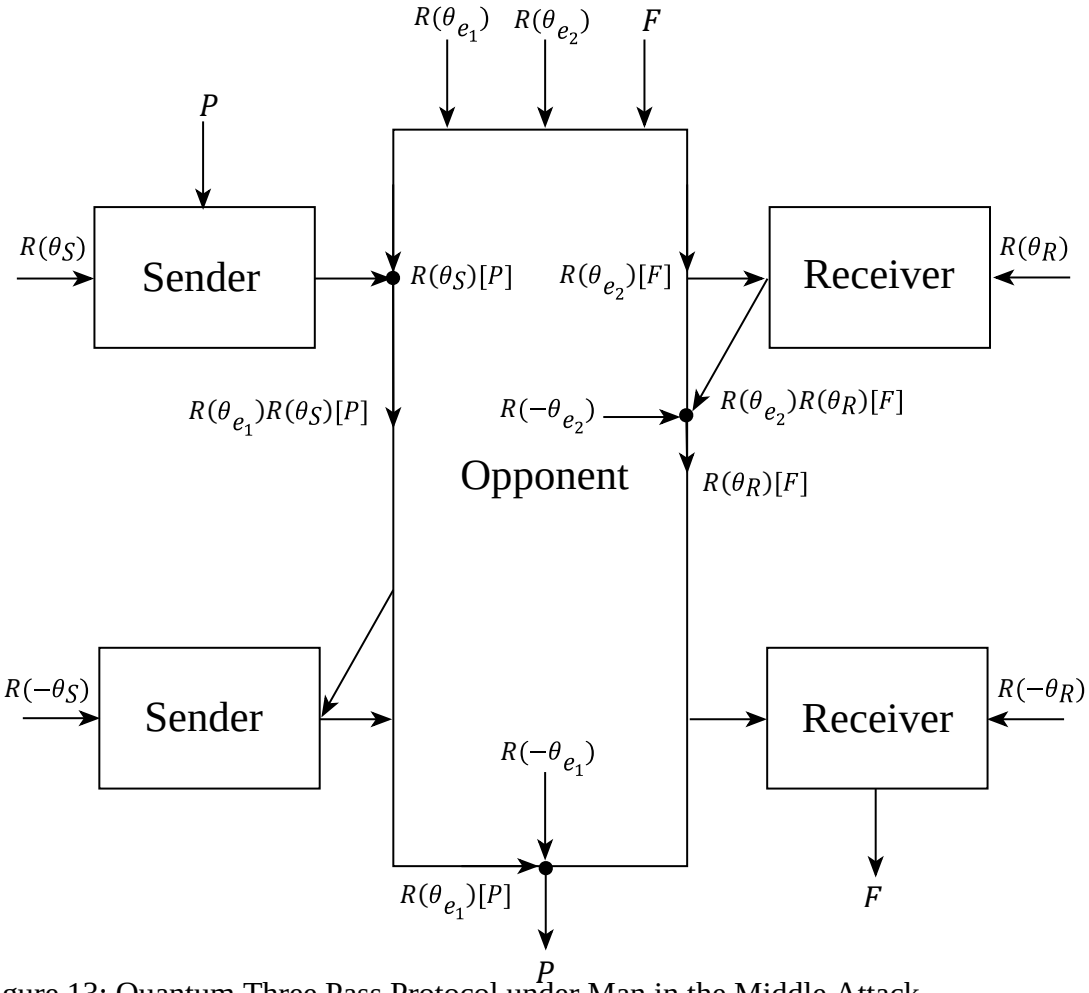

Figure 13: Quantum Three Pass Protocol under Man in the Middle Attack

Instead of $R(\theta_R)$ the opponent selects $R(\theta_{e_1})$ (which is also commutative) and fakes a response which looks similar to what receiver would have done. The opponent pretends as sender to receiver with the transformation (θ_{e_2}) , which is commutative to $R(\theta_R)$ and instead of plain-text message *P* sends a gibberish *F*. So, from interaction with sender he acquires value *P* and sends a junk *F* to receiver and hence disables the protocol.

Let us first consider the interaction of sender and opponent. The sender wants to send plain-text letter *P* to the receiver.

$$|\varphi_1\rangle = R(\theta_S)|\mathrm{P}\rangle. \tag{3.10}$$

The opponent receives $|\varphi_1\rangle$ and generates its fake own angle θ_{e_1}, by using equation (4.5) he compute fake $|\varphi_2\rangle$:

$$|\varphi_2\rangle = R(\theta_{e_1})|\varphi_1\rangle. \tag{3.11}$$

The resulting state fake $|\varphi_2\rangle$ is sent back to the sender. The sender receives and decrypts it by rotating it with the angle $-\theta_S$.

The sender computes $|\varphi_3\rangle$ by using equation (4.5) and sends it back again as follows:

$$|\varphi_3\rangle = R(-\theta_S)|\varphi_2\rangle. \tag{3.12}$$

The opponent gets $|\varphi_3\rangle$ and decrypts it by rotating with the angle $-\theta_{e_1}$, by using equation (4.5). Then the opponent has the sender state as follows:

$$|P\rangle = R(-\theta_{e_1})|\varphi_3\rangle. \tag{3.13}$$

For example, if the sender wants send letter *P* to the receiver and the opponent sends instead of *P* the fake letter *B*, where the first qubit state is $|0\rangle$. After that the sender encrypts it by using a self-generated angle. For instance, if the sender uses $\theta_S = 30^\circ$, we can calculate the state $|\varphi_1\rangle$ using (4.5) as:

$$\big|\varphi_1\rangle = R(30^\circ)\big|0\rangle = \cos(30^\circ)|0\rangle - \sin(30^\circ)|1\rangle$$

The opponent receives $|\varphi_1\rangle$ and generates its fake own angle. The opponent use $\theta_{e_1} = 22^\circ$, and by using equation (4.5) he compute $|\varphi_2\rangle$:

$$|\varphi_2\rangle = R(22^\circ)|\varphi_1\rangle = R(22^\circ)(\cos(30^\circ)|0\rangle - \sin(30^\circ)|1\rangle)$$

$$= \cos(52^\circ)|0\rangle - \sin(52^\circ)|1\rangle$$

The resulting state $|\varphi_2\rangle$ is sent back to the sender. The sender receives and decrypts it by rotating it back with the angle $\theta_S = -30^\circ$.

The sender computes $|\varphi_3\rangle$ by using $R\ (\theta_S)$ as in equation (4.5) and sends it back again as follows:

$$|\varphi_3\rangle = R(-30^\circ)|\varphi_2\rangle = R(-30^\circ)(\cos(52^\circ)|0\rangle - \sin(52^\circ)|1\rangle)$$

$$= \cos(22^\circ)|0\rangle - \sin(22^\circ)|1\rangle$$

The opponent gets $|\varphi_3\rangle$ and decrypts it by rotating it back with the angle $\theta_{e_1} = -22^{\circ}$ using equation (4.5). Then the opponent has the first sender state as follows:

$$R(-22^{\circ})(\cos(22^{\circ})|0\rangle - \sin(22^{\circ})|1\rangle) = |0\rangle$$

The sender sends the rest of the quantum bits as shown in the following table 1.

Table 1: The opponent communicates with the sender and break letter "P".

Sender State	$\boldsymbol{\theta_S}$	$\boldsymbol{\lvert\varphi 1\rangle}$	$\boldsymbol{\theta_{e_1}}$	**Fake ($\lvert\varphi 2\rangle$)**	$\boldsymbol{\lvert\varphi 3\rangle}$	**Receiver state**
$\lvert 0\rangle$	30°	$\cos(30^{\circ})\lvert 0\rangle - \sin(30^{\circ})\lvert 1\rangle$	22°	$\cos(52^{\circ})\lvert 0\rangle - \sin(52^{\circ})\lvert 1\rangle$	$\cos(22^{\circ})\lvert 0\rangle - \sin(22^{\circ})\lvert 1\rangle$	$\lvert 0\rangle$
$\lvert 1\rangle$	113°	$\sin(113^{\circ})\lvert 0\rangle + \cos(113^{\circ})\lvert 1\rangle$	14°	$\sin(127^{\circ})\lvert 0\rangle + \cos(127^{\circ})\lvert 1\rangle$	$\sin(14^{\circ})\lvert 0\rangle + \cos(14^{\circ})\lvert 1\rangle$	$\lvert 1\rangle$
$\lvert 1\rangle$	20°	$\sin(20)\lvert 0\rangle + \cos(20^{\circ})\lvert 1\rangle$	76°	$\sin(96^{\circ})\lvert 0\rangle + \cos(96^{\circ})\lvert 1\rangle$	$\sin(76^{\circ})\lvert 0\rangle + \cos(76^{\circ})\lvert 1\rangle$	$\lvert 1\rangle$
$\lvert 1\rangle$	145°	$\sin(145^{\circ})\lvert 0\rangle + \cos(145^{\circ})\lvert 1\rangle$	16°	$\sin(161^{\circ})\lvert 0\rangle + \cos(161^{\circ})\lvert 1\rangle$	$\sin(16^{\circ})\lvert 0\rangle + \cos(16^{\circ})\lvert 1\rangle$	$\lvert 1\rangle$
$\lvert 1\rangle$	4°	$\sin(4^{\circ})\lvert 0\rangle + \cos(4^{\circ})\lvert 1\rangle$	135°	$\sin(139^{\circ})\lvert 0\rangle + \cos(139^{\circ})\lvert 1\rangle$	$\sin(135^{\circ})\lvert 0\rangle + \cos(135^{\circ})\lvert 1\rangle$	$\lvert 1\rangle$

At the same time, the opponent communicates with the receiver and sends the fake state, where fake state is $|F\rangle$. After that the opponent encrypts it by using a fake self-generated angle θ_{e_2}, the fake state $|\varphi_1\rangle$ received by the receiver, becomes:

$$|\varphi_1\rangle = R(\theta_{e_2})|F\rangle. \tag{3.14}$$

The receiver receives the fake $|\varphi_1\rangle$ and generates its own angle θ_R. Then the state sent by the receiver yields to $|\varphi_2\rangle$:

$$|\varphi_2\rangle = R(\theta_R)|\varphi_1\rangle. \tag{3.15}$$

The resulting state $|\varphi_2\rangle$ is sent back to the opponent. The opponent receives and decrypts it by rotating it back with the angle $-\theta_{e_2}$.

The opponent computes fake $|\varphi_3\rangle$ by using $R\ (-\theta_{e_2})$ as in equation (4.5) and sends it back again to the receiver as follows:

$$|\varphi_3\rangle = R(-\theta_{e_2})|\varphi_2\rangle. \tag{3.16}$$

The receiver gets fake $|\varphi_3\rangle$ and decrypts it by rotating it back with the angle $-\theta_R$ using equation (4.5). Then the receiver has the fake state $|F\rangle$ as follows:

$$|F\rangle = R(-\theta_R)|\varphi_3\rangle. \tag{3.17}$$

Let us now give a concrete numerical example. Let the opponent send the fake letter "B" to the receiver, where the first qubit state is $|0\rangle$. After that the opponent encrypts it by using a fake self-generated angle $\theta_{e_2} = 126°$, the state $|\varphi_1\rangle$ received by the receiver, becomes:

$$|\varphi_1\rangle = R(126^\circ)|0\rangle = \cos(126^\circ)|0\rangle - \sin(126^\circ)|1\rangle$$

The receiver receives $|\varphi_1\rangle$ and generates its own angle $\theta_R = 7°$. Then the state sent by the receiver yields to $|\varphi_2\rangle$:

$$|\varphi_2\rangle = R(7^\circ)|\varphi_1\rangle = R(7^\circ)(\cos(126)|0\rangle - \sin(126^\circ)|1\rangle)$$

$$= \cos(133^\circ)|0\rangle - \sin(133^\circ)|1\rangle$$

The resulting state $|\varphi_2\rangle$ is sent back to the opponent. The opponent receives and decrypts it by rotating it back with the angle $\theta_{e_2} = -126^{\circ}$.

The opponent computes $|\varphi_3\rangle$ by using $R(\theta_{e_2})$ (4.5) and sends it back again to the receiver as follows:

$$|\varphi_3\rangle = R(-126^{\circ})|\varphi_2\rangle = R(-126^{\circ})(\cos(133^{\circ})|0\rangle - \sin(133)|1\rangle)$$

$$= \cos(7^{\circ})|0\rangle - \sin(7^{\circ})|1\rangle$$

The receiver gets $|\varphi_3\rangle$ and decrypts it by rotating it back with the angle $\theta_R = -7^{\circ}$ using (4.5). Then the receiver has the first fake state as follows:

$$R(-7^{\circ})(\cos(7^{\circ})|0\rangle - \sin(7^{\circ})|1\rangle) = |0\rangle$$

The opponent sends the rest of the fake quantum bits as shown in the following table 2.

Table 2: The opponent communicates with the receiver and sends fake letter "B".

Fake state	θ_{e_2}	**Fake ($\|\varphi 1\rangle$)**	θ_R	$\|\varphi 2\rangle$	**Fake ($\|\varphi 3\rangle$)**	**Receiver fake state**
$\|0\rangle$	126°	$\cos(30^\circ)\|0\rangle - \sin(30^\circ)\|1\rangle$	7°	$\cos(133^\circ)\|0\rangle - \sin(133^\circ)\|1\rangle$	$\cos(7^\circ)\|0\rangle - \sin(7^\circ)\|1\rangle$	$\|0\rangle$
$\|0\rangle$	46°	$\cos(46^\circ)\|0\rangle - \sin(46^\circ)\|1\rangle$	83°	$\cos(129^\circ)\|0\rangle - \sin(129^\circ)\|1\rangle$	$\cos(83^\circ)\|0\rangle - \sin(83^\circ)\|1\rangle$	$\|0\rangle$
$\|0\rangle$	57°	$\cos(57^\circ)\|0\rangle - \sin(57^\circ)\|1\rangle$	101°	$\cos(158^\circ)\|0\rangle - \sin(158^\circ)\|1\rangle$	$\cos(101^\circ)\|0\rangle - \sin(101^\circ)\|1\rangle$	$\|0\rangle$
$\|0\rangle$	128°	$\cos(128^\circ)\|0\rangle - \sin(128^\circ)\|1\rangle$	23°	$\cos(151^\circ)\|0\rangle - \sin(151^\circ)\|1\rangle$	$\cos(23^\circ)\|0\rangle - \sin(23^\circ)\|1\rangle$	$\|0\rangle$
$\|1\rangle$	12°	$\sin(12)\|0\rangle + \cos(12^\circ)\|1\rangle$	149°	$\sin(161^\circ)\|0\rangle + \cos(161^\circ)\|1\rangle$	$\sin(149^\circ)\|0\rangle + \cos(149^\circ)\|1\rangle$	$\|1\rangle$

3.4 Difference between Classical Three-Pass protocol (TPP) and Quantum Three-Pass Protocol (QTPP)

The difference between Classical Three-Pass protocol and Quantum Three-Pass Protocol are listed in table 3.

Table 3: Difference between classical three-Pass protocol and quantum three-pass protocol.

Classical Three-Pass Protocol	**Quantum Three-Pass Protocol**
1.Based on the mathematical computation.	1. Based on the concepts of mathematical computation and quantum mechanics.
2. The protocol realized by utilizing discrete algorithm problem and by X-OR operation.	2. The protocol realized by using a photon as a qubit.
3. All the information is either 0 or 1 state.	3. The information is either $\|0\rangle$ or $\|1\rangle$ or superposition state $(\alpha\|0\rangle + \beta\|1\rangle)$.
4. The transmission is via classical channel where a classical channel is a connection channel, which can carry only classical information.	4. The transmission is via quantum channel where a quantum channel is a channel, which can carry quantum information, as well as classical information.
5. The security of transmissions classical data is infeasible since opponent can easily save the transmitted data and analyze them.	5. The security of transmissions is feasible and higher since opponent cannot clone the transmitted state and then analyze them because all the information is based on quantum physics.

3.5 Main Properties of QTPP

The quantum three-pass protocol is distinguished from other quantum protocols by some features. These are as follows:

- One of its most important characteristics that the protocol uses only a quantum channel unlike the other quantum protocols, which use a classical channel and a quantum channel. For instance, BB84 uses both a classical and a quantum channel for the transmission.

- The QTPP does not need a shared key between the sender and receiver. Both of them generate their own secret keys for each session.

- The quantum state that QTPP shares between the sender and receiver is always a superposition and it is unfeasible to break this state without corrupted based on the no-cloning theorem [43].

- The QTPP guarantees the security and the confidentiality of communication [55].

- The opponent can be discovered more easily in the QTPP protocol compared to other quantum protocols like BB84, because attacks against the QTPP increases the bit error rate up to 50% [56].

3.6 Summary

This chapter presents the quantum three-pass protocol QTPP. This protocol depends on an extension of the classical three-pass protocol TPP to the quantum domain and the concepts of quantum physics as well. The QTPP protocol is different from the other quantum protocols in that it uses all transmitted data, for deterministic quantum key distribution and for secure data transmission. The main properties of the protocol are discussed and it is clear that this protocol distinguishes itself from the rest of the quantum protocols in many of its characteristics and features.

The security analysis of this protocol is discussed in details and we conclude that the protocol is secure against all the classical and quantum attack except the man-in-the middle attack. In the next chapter we introduce a modified QTPP that is resistant to the man-in-the-middle attack, as well to all other mentioned attack methods.

Chapter 4

ENHANCEMENT OF THE QTPP BASED ON THE HYBRID CRYPTOSYSTEM

In this chapter we present in section 5.1 how the man-in-the-middle attack can be prevented by extending QTPP by adding a two security layers algorithms, forming a quantum-classical hybrid protocol. First layer represented as a classical algorithm to encrypted and decrypted plain-text message using one of the classical cryptography algorithms [54]. After encrypting the plain-text message using classical algorithms, the encrypted plain-text message will be transferred into qubits. Let us assume that qubits are physically realized by photons. Then, the polarization of each photon is rotated by an angle θ, which is selected arbitrarily for each qubit. Second layer represented as a quantum authentication algorithm where the sender and receiver communicate with the quantum distribution centre QDC to authenticate the transmission of the quantum three-pass protocol QTPP. Section 5.2 shows how the algorithm works illustrating the process using a simple example. The security of this algorithm is analysed in detail in section 5.3, the noise of the modified protocol discussed in section 5.4. Finally, we summarize this chapter in section 5.5.

4.1 Description of The Proposed Hybrid Cryptosystem Scheme to Enhance The QTPP

In our proposed protocol, we modified the quantum three-pass protocol by proposing a hybrid cryptosystem authentication to enhance the security of the QTPP. The idea of the hybrid cryptosystem against the main-in-the middle attacks is summarized in Figure 14.

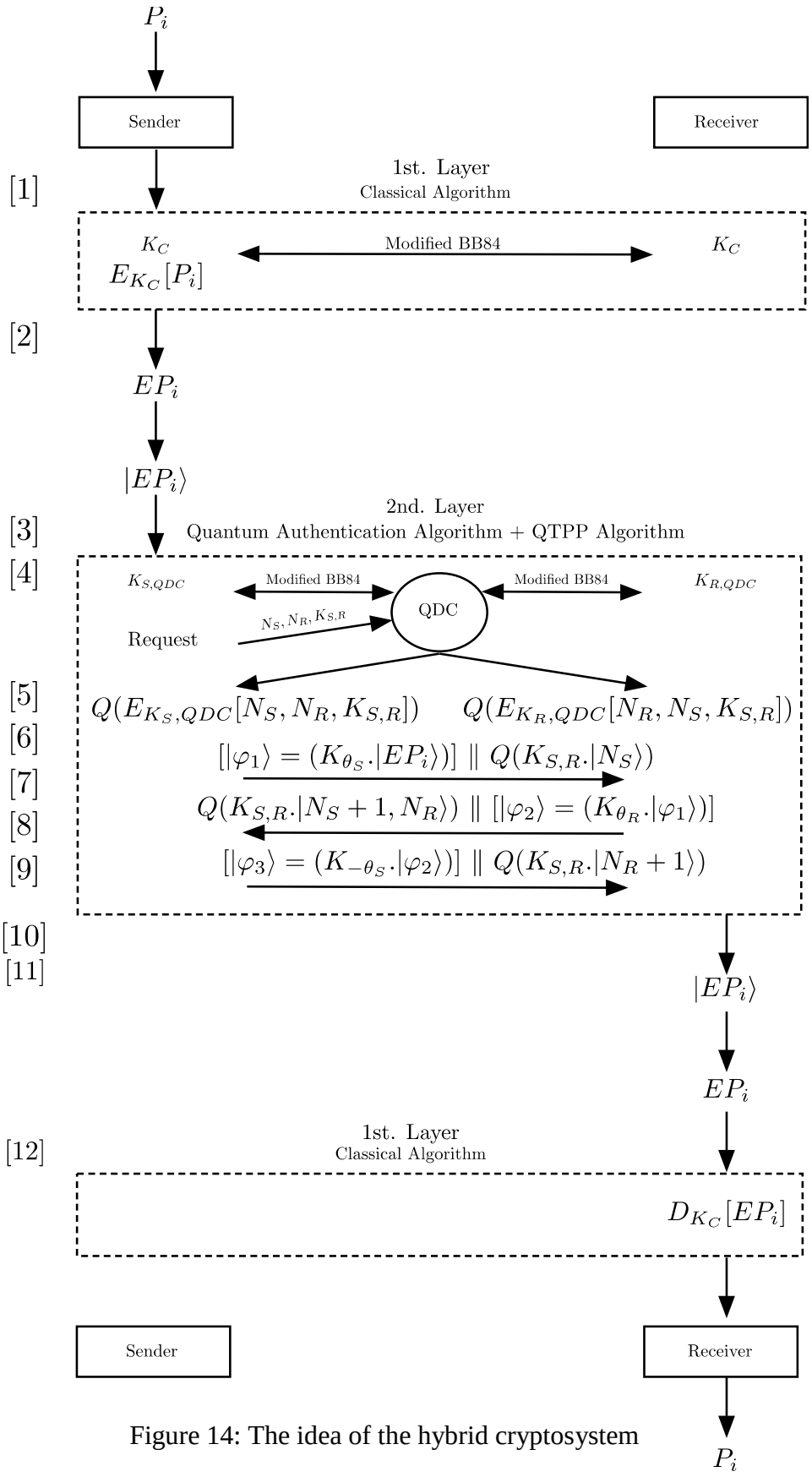

Figure 14: The idea of the hybrid cryptosystem

The hybrid cryptosystem consists of two security layers, first security layer is a classical algorithm to encrypt the plain-text message before transmitting by the QTPP, Indeed this work is part form our proposed algorithm that we proposed in [54].

Second security layer is a quantum authentication algorithm to authenticate the QTPP before transmitting the encrypted message and to eliminate the man-in-the middle attack. The procedure of the modified QTPP is as follows.

[1] First of all, the sender encrypts the plain-text message by using one of the classical cryptography e.g. (Hill-cipher algorithm, DES, 3DES, AES and etc.) where the plain-text message label as $P_i = (P_1, P_2, \cdots, P_m)$, the sender and receiver agree on the classical key K_C using modified BB84 protocol which is our proposed in [30] (see Appendix B), and then the sender implements the algorithm and encrypts the plain-text message as follows.

$$\mathrm{E}_{\mathrm{K}_C}[P_i], \tag{4.1}$$

where E denotes the encryption algorithm.

[2] Each letter in the encrypted plain-text message *EP* is converted to the binary code. After the conversion of the letters to the binary code, all the information will be transferred into quantum bits, resulting in the state $|EP_i\rangle$ as in [54].

[3] The sender and the receiver communicate with a third party, which is represented by the Quantum Distribution Centre QDC, which works as the central authority for authentication. The sender and the receiver communicate with the QDC via quantum channels and therefore the exchange of information between sender and QDC and receiver and QDC is done by using qubits and we denote as $Q(.)$ to express the conversion of classical bits to quantum bits. After

the QDC receives the information, it converts the quantum bits to classical bits, processes it, and transforms it again into qubits before transmission.

[4] The sender and the receiver negotiate first the encryption keys $K_{S,QDC}$ and $K_{R,QDC}$ respectively with the QDC using the modified BB84 protocol [30] (see Appendix B). These keys ensure the secure communication between sender-QDC and receiver-QDC. The sender requests from the QDC the nonce of the sender N_S, the nonce of the receiver N_R, and the session key between sender and receiver $K_{S,R}$.

[5] The QDC distributes a message to the sender and receiver with the sender's nonce, receiver's nonce and the session key $K_{S,R}$ between the sender and the receiver. The message to the sender is encrypted as follows,

$$Q\left(\mathrm{E}_{\mathrm{K_{S,QDC}}}[\mathrm{N_S}, N_R, K_{S,R}\,]\right). \tag{4.2}$$

The message to the receiver is encrypted using the algorithm and the same information but with the key $\mathrm{K_{S,QDC}}$.

$$Q\left(\mathrm{E}_{\mathrm{K_{R,QDC}}}[\mathrm{N_R}, N_S, K_{S,R}\,]\right). \tag{4.3}$$

[6] Now, the QTPP will be applied to transfer the secret information securely where the sender and the receiver start authenticate the communication channel against a man in the middle attack following with the quantum encrypted plain-text message $|EP_i\rangle$.

[7] For the first pass of the Quantum Three Pass Protocol the sender generates his session key $\mathrm{K_{\theta_S}}$, represented as an rotation angle, and encrypts the information to be transmitted securely alongside with the sender nonce $\mathrm{N_S}$ after encrypted with the session key $\mathrm{K_{S,R}}$. Then, the transmitted message to the receiver is,

$$[|\varphi_1\rangle = (K_{\theta_S} \cdot |EP_i\rangle)] \Vert \mathrm{Q}\big(\mathrm{K_{S,R}}.|N_S\rangle\big). \quad (4.4)$$

[8] The receiver receives $[|\varphi_1\rangle = (K_{\theta_S} \cdot |EP_i\rangle)] \Vert \mathrm{Q}\big(\mathrm{K_{S,R}}.|N_S\rangle\big)$, decrypts the message $[\mathrm{N_S}]$ to assure that the message came from the sender. Then the receiver encrypts $|\varphi_1\rangle$ with his key $\mathrm{K_{\theta_R}}$ and sends it back to the receiver alongside with an encrypted message comprising $\mathrm{N_S} + 1$ and his own nonce $\mathrm{N_R}$ by using the session key $\mathrm{K_{S,R}}$ to assure that the message came from the receiver to authenticate the channel,

$$\mathrm{Q}\big(\mathrm{K_{S,R}}.|N_S + 1, N_R\rangle\big) \Vert [|\varphi_2\rangle = (K_{\theta_R} \cdot |\varphi_1\rangle)]. \quad (4.5)$$

[9] The sender receives $\mathrm{Q}\big(\mathrm{K_{S,R}}.|N_S + 1, N_R\rangle\big) \Vert [|\varphi_2\rangle = (K_{\theta_R} \cdot |\varphi_1\rangle)]$, decrypts the message $[\mathrm{N_S} + 1, \mathrm{N_R}]$ using the session key to get $\mathrm{N_S}$ +1 and $\mathrm{N_R}$. Then he decrypts $|\varphi_2\rangle$ by rotating it back with the angle $\mathrm{K_{-\theta_S}}$ and sends the resulting to the receiver again alongside with an encrypted message comprising $\mathrm{N_R} + 1$ by using the session key $\mathrm{K_{S,R}}$ to assure that the message came from the sender to authenticate the channel.

$$[|\varphi_3\rangle = \big(K_{-\theta_S} \cdot |\varphi_2\rangle\big)] \Vert \mathrm{Q}\big(\mathrm{K_{S,R}}.|N_R + 1\rangle\big). \quad (4.6)$$

[10] The receiver receives $[|\varphi_3\rangle = \big(K_{-\theta_S} \cdot |\varphi_2\rangle\big)] \Vert \mathrm{Q}\big(\mathrm{K_{S,R}}.|N_R + 1\rangle\big)$, decrypts the message $[\mathrm{N_R} + 1]$ using the session key to get $\mathrm{N_R} + 1$ and to assure the channel is authenticate. Then decrypts $|\varphi_3\rangle$ by rotating it back with the angle $\mathrm{K_{-\theta_R}}$.

$$|EP_i\rangle = K_{-\theta_R} \cdot |\varphi_3\rangle. \quad (4.7)$$

[11] The receiver gets all the encoded plain-text qubits $|EP_i\rangle$, then transferred to the binary code.

[12] After that all the binary code is converted to letters and then decrypted to the plain-text P by using the inverse key of the classical cryptography algorithm as in [54].

$$\mathrm{D}_{K_C}[EP_i]. \tag{4.8}$$

Now the receiver has the original plain-text P_i. The whole procedure is shown in Figure 15.

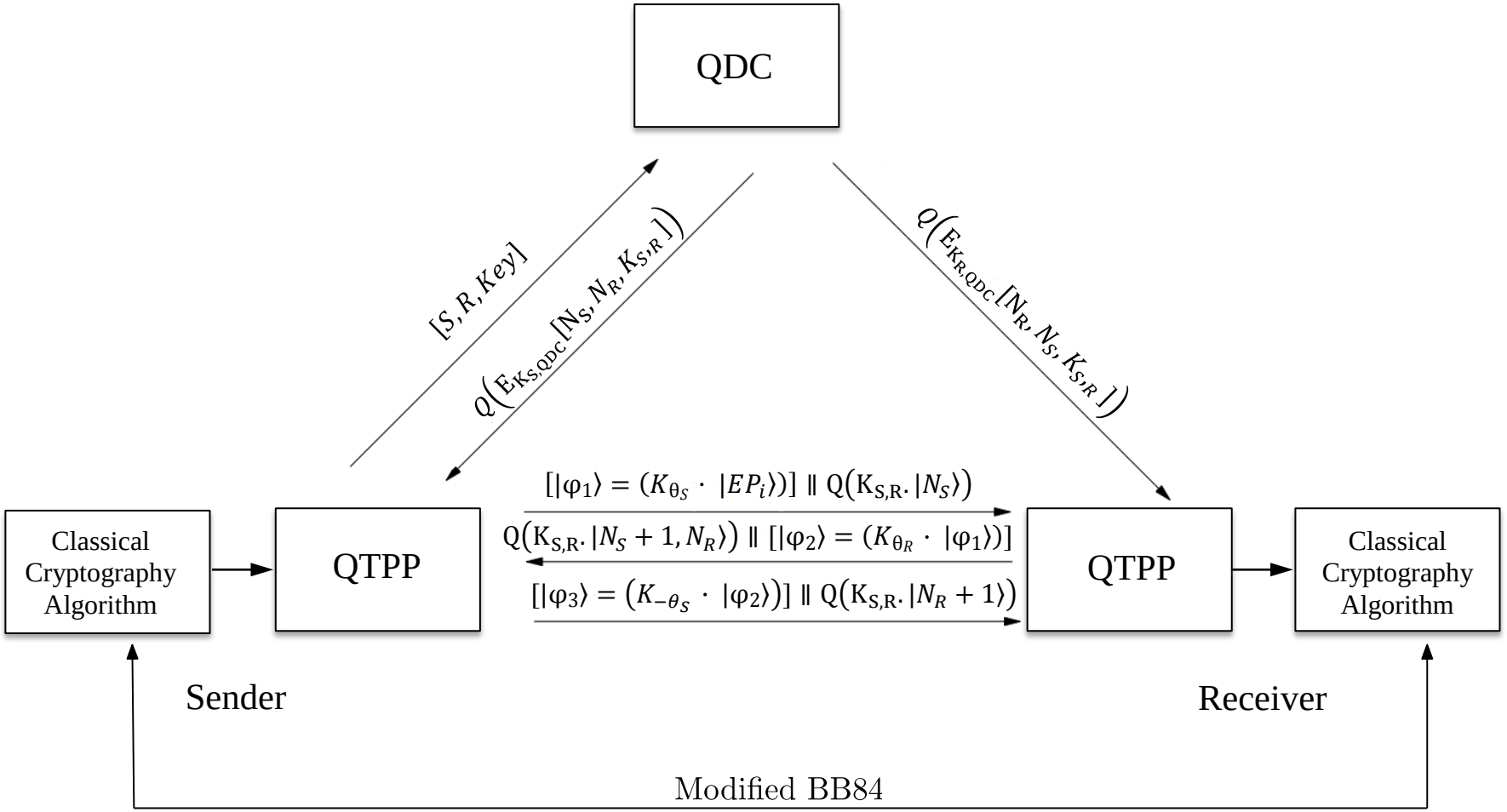

Figure 15: Quantum Three-Pass Protocol Authentication Based on Hybrid Cryptosystem.

4.2 Example

Here we give a simple example to show how the proposed algorithm works and to demonstrate how robust the proposed quantum encryption system is.

The plain-text message is the word "HELP", and we want to send it via a secure route. According to the algorithm we have first to encrypt the plain-text message by a classical algorithm. In order to give an educational example we choose here the Hill-cipher algorithm with the encryption key matrix (2 × 2), where the sender and receiver agree on the classical key using modified BB84.

So "HELP", is encrypted for this example. The first step includes the choice of an invertible modulo 26 (n × n) matrix for a Hill 2-cipher (2 × 2) key matrix. Let K be the 2×2 key matrix as

$$K = \begin{bmatrix} 1 & 2 \\ 0 & 3 \end{bmatrix}.$$

Next the plain-text is divided into pairs and replaced with the corresponding numerical value from table 4.

Table 4: Correspondence table for Encoding

A	B	C	D	E	F	G	H	I	J	K	L	M
0	1	2	3	4	5	6	7	8	9	10	11	12
N	O	P	Q	R	S	T	U	V	W	X	Y	Z
13	14	15	16	17	18	19	20	21	22	23	24	25

Now the corresponding numerical values are,

$$\begin{bmatrix} H \\ E \end{bmatrix} = \begin{bmatrix} 7 \\ 4 \end{bmatrix} \text{ and } \begin{bmatrix} L \\ P \end{bmatrix} = \begin{bmatrix} 11 \\ 15 \end{bmatrix}$$

And by using the equation ($EP = K_C \cdot P \bmod N$) we get,

$$\begin{bmatrix}1 & 2\\0 & 3\end{bmatrix}.\begin{bmatrix}7 & 11\\4 & 15\end{bmatrix}=\begin{bmatrix}15 & 41\\12 & 45\end{bmatrix} \bmod 26$$

$$EP=\begin{bmatrix}15 & 15\\12 & 19\end{bmatrix},$$

so the encrypted plain-text *EP* is:

$$EP_1=\begin{bmatrix}15\\12\end{bmatrix}=\begin{bmatrix}P\\M\end{bmatrix}, EP_2=\begin{bmatrix}15\\19\end{bmatrix}=\begin{bmatrix}P\\T\end{bmatrix},$$

Now the encrypted plain-text is "PMPT" and each letter in encrypted plain-text is converted to the binary code as in the following table 5.

Table 5: Correspondence table for the binary code

P	M	P	T
01111	01100	01111	10011

Now, we have the classically encrypted plain-text message to be transmitted to the receiver. The next step before the application of the QTPP is the authentication of the direct communication channel. Therefore, the sender and the receiver negotiate first the encryption keys $K_{S,QDC}$ and $K_{R,QDC}$ respectively with the QDC using the modified BB84 protocol. The sender requests the nonce of the sender, the nonce of the receiver, and the session key to be used for the authentication of the communication channel between sender and receiver. After the successful distribution of the nonce's and the session key to both parties, the authentication of the communication channel starts. Let the nonce of the sender be $N_S = 12 = 01100$, the nonce of the receiver be $N_R = 18 = 10010$, and the session key be $K_{S,R} = 32 = 00100000$.

The message $M_{S,QDC} = [N_S, N_R, K_{S,R}]$ is encrypted by classical algorithm one-time-pad and with the key that the sender shares with the QDC $(K_{S,QDC}) =$ 000111100100001100.

$$E_{S,QDC} = K_{S,QDC} \oplus M_{S,QDC}$$

$$E_{S,QDC} = 000111100100001100 \oplus 011001001000100000$$

$$E_{S,QDC} = 011110101100101100$$

The QDC also sends a message $M_{R,QDC} = [N_R, N_S, K_{S,R}]$ to the receiver that has the receiver's identity $N_R = 18 = 10010$, sender's identity $N_S = 12 = 01100$ and the key session between the sender and the receiver $K_{S,R} = 32 = 00100000$ in it.

The message is encrypted with the key that the receiver shares with the QDC $(K_{R,KDC}) = 111111111000000000$.

$$E_{R,QDC} = K_{R,QDC} \oplus M_{R,QDC}$$

$$E_{S,QDC} = 111111111000000000 \oplus 100100110000100000$$

$$E_{S,QDC} = 011011001000100000$$

Now, the sender and the receiver apply the quantum three-pass protocol QTPP. The sender starts with the N_S to authenticate the protocol, where all the classical bit sequence transform into quantum bits and rotated by using the key session which is $K_{S,R} = 32°$ following with the first encrypted letter which is "P" from left to right, where the first qubit state is $|0\rangle$. After that the sender encrypts it by using a self-generated angle. So the sequence of the sender state in the first channel will be as following in the table 6.

Table 6: Sequence sender state of the first stage of the protocol.

State	**The Key Angle ($\boldsymbol{\theta}$)**	**Sequence Sender State**
$\|0\rangle$	$K_{S,R} = 32^{\circ}$	$\cos(32^{\circ})\|0\rangle - \sin(32^{\circ})\|1\rangle$
$\|1\rangle$	$K_{S,R} = 32^{\circ}$	$\sin(32^{\circ})\|0\rangle + \cos(32^{\circ})\|1\rangle$
$\|1\rangle$	$K_{S,R} = 32^{\circ}$	$\sin(32^{\circ})\|0\rangle + \cos(32^{\circ})\|1\rangle$
$\|0\rangle$	$K_{S,R} = 32^{\circ}$	$\cos(32^{\circ})\|0\rangle - \sin(32^{\circ})\|1\rangle$
$\|0\rangle$	$K_{S,R} = 32^{\circ}$	$\cos(32^{\circ})\|0\rangle - \sin(32^{\circ})\|1\rangle$
$\|0\rangle$	$\theta_S = 30^{\circ}$	$\cos(30^{\circ})\|0\rangle - \sin(30^{\circ})\|1\rangle$
$\|1\rangle$	$\theta_S = 113^{\circ}$	$\sin(113^{\circ})\|0\rangle + \cos(113^{\circ})\|1\rangle$
$\|1\rangle$	$\theta_S = 20^{\circ}$	$\sin(20^{\circ})\|0\rangle + \cos(20^{\circ})\|1\rangle$
$\|1\rangle$	$\theta_S = 145^{\circ}$	$\sin(145^{\circ})\|0\rangle + \cos(145^{\circ})\|1\rangle$
$\|1\rangle$	$\theta_S = 4^{\circ}$	$\sin(4^{\circ})\|0\rangle + \cos(4^{\circ})\|1\rangle$
$\|0\rangle$	$\theta_S = 121^{\circ}$	$\cos(121^{\circ})\|0\rangle - \sin(121^{\circ})\|1\rangle$
$\|1\rangle$	$\theta_S = 7^{\circ}$	$\sin(7^{\circ})\|0\rangle + \cos(7^{\circ})\|1\rangle$
$\|1\rangle$	$\theta_S = 30^{\circ}$	$\sin(30^{\circ})\|0\rangle + \cos(30^{\circ})\|1\rangle$
$\|0\rangle$	$\theta_S = 63^{\circ}$	$\cos(63^{\circ})\|0\rangle - \sin(63^{\circ})\|1\rangle$
$\|0\rangle$	$\theta_S = 140^{\circ}$	$\cos(140^{\circ})\|0\rangle - \sin(104^{\circ})\|1\rangle$
$\|0\rangle$	$\theta_S = 31^{\circ}$	$\cos(31^{\circ})\ \|0\rangle - \sin(31^{\circ})\|1\rangle$
$\|1\rangle$	$\theta_S = 60^{\circ}$	$\sin(60^{\circ})\|0\rangle + \cos(60^{\circ})\|1\rangle$
$\|1\rangle$	$\theta_S = 40^{\circ}$	$\sin(40^{\circ})\|0\rangle + \cos(40^{\circ})\|1\rangle$
$\|1\rangle$	$\theta_S = 80^{\circ}$	$\sin(80^{\circ})\|0\rangle + \cos(80^{\circ})\|1\rangle$
$\|1\rangle$	$\theta_S = 45^{\circ}$	$\sin(45^{\circ})\|0\rangle + \cos(45^{\circ})\|1\rangle$
$\|1\rangle$	$\theta_S = 110^{\circ}$	$\sin(110^{\circ})\|0\rangle + \cos(110^{\circ})\|1\rangle$
$\|0\rangle$	$\theta_S = 4^{\circ}$	$\cos(4^{\circ})\|0\rangle - \sin(4^{\circ})\|1\rangle$
$\|0\rangle$	$\theta_S = 3^{\circ}$	$\cos(3^{\circ})\|0\rangle - \sin(3^{\circ})\|1\rangle$
$\|1\rangle$	$\theta_S = 65^{\circ}$	$\sin(65^{\circ})\|0\rangle + \cos(65^{\circ})\|1\rangle$
$\|1\rangle$	$\theta_S = 39^{\circ}$	$\sin(39^{\circ})\|0\rangle + \cos(39^{\circ})\|1\rangle$

The receiver receives the states and check if the state is authenticated or not where he knows the string of qubits and how many qubits are used for the authentication, after that the receiver sends $N_S + 1$ and N_R to authenticate the channel following with the resulting state $|\varphi_2\rangle$ and sends back to the sender as following table 7.

Table 7: Sequence sender state of the second stage of the protocol.

State	**The Key Angle ($\boldsymbol{\theta}$)**	**Sequence Sender State**
$\|0\rangle$	$K_{S,R} = 32^{\circ}$	$\cos(32^{\circ})\|0\rangle - \sin(32^{\circ})\|1\rangle$
$\|1\rangle$	$K_{S,R} = 32^{\circ}$	$\sin(32^{\circ})\|0\rangle + \cos(32^{\circ})\|1\rangle$
$\|1\rangle$	$K_{S,R} = 32^{\circ}$	$\sin(32^{\circ})\|0\rangle + \cos(32^{\circ})\|1\rangle$
$\|0\rangle$	$K_{S,R} = 32^{\circ}$	$\cos(32^{\circ})\|0\rangle - \sin(32^{\circ})\|1\rangle$
$\|1\rangle$	$K_{S,R} = 32^{\circ}$	$\sin(32^{\circ})\|0\rangle + \cos(32^{\circ})\|1\rangle$
$\|1\rangle$	$K_{S,R} = 32^{\circ}$	$\sin(32^{\circ})\|0\rangle + \cos(32^{\circ})\|1\rangle$
$\|0\rangle$	$K_{S,R} = 32^{\circ}$	$\cos(32^{\circ})\|0\rangle - \sin(32^{\circ})\|1\rangle$
$\|0\rangle$	$K_{S,R} = 32^{\circ}$	$\cos(32^{\circ})\|0\rangle - \sin(32^{\circ})\|1\rangle$
$\|1\rangle$	$K_{S,R} = 32^{\circ}$	$\sin(32^{\circ})\|0\rangle + \cos(32^{\circ})\|1\rangle$
$\|0\rangle$	$K_{S,R} = 32^{\circ}$	$\cos(32^{\circ})\|0\rangle - \sin(32^{\circ})\|1\rangle$
$\|0\rangle$	$\theta_S + \theta_R = 75^{\circ}$	$\cos(75^{\circ})\|0\rangle - \sin(75^{\circ})\|1\rangle$
$\|1\rangle$	$\theta_S + \theta_R = 130^{\circ}$	$\sin(130^{\circ})\|0\rangle + \cos(130^{\circ})\|1\rangle$
$\|1\rangle$	$\theta_S + \theta_R = 32^{\circ}$	$\sin(32^{\circ})\|0\rangle + \cos(32^{\circ})\|1\rangle$
$\|1\rangle$	$\theta_S + \theta_R = 176^{\circ}$	$\sin(176^{\circ})\|0\rangle + \cos(176^{\circ})\|1\rangle$
$\|1\rangle$	$\theta_S + \theta_R = 174^{\circ}$	$\sin(174^{\circ})\|0\rangle + \cos(174^{\circ})\|1\rangle$
$\|0\rangle$	$\theta_S + \theta_R = 251^{\circ}$	$\cos(251^{\circ})\|0\rangle - \sin(251^{\circ})\ \|1\rangle$
$\|1\rangle$	$\theta_S + \theta_R = 151^{\circ}$	$\sin(151^{\circ})\|0\rangle + \cos(151^{\circ})\|1\rangle$
$\|1\rangle$	$\theta_S + \theta_R = 60^{\circ}$	$\sin(60^{\circ})\|0\rangle + \cos(60^{\circ})\|1\rangle$
$\|0\rangle$	$\theta_S + \theta_R = 168^{\circ}$	$\cos(168^{\circ})\|0\rangle - \sin(168^{\circ})\|1\rangle$
$\|0\rangle$	$\theta_S + \theta_R = 172^{\circ}$	$\cos(172^{\circ})\|0\rangle - \sin(172^{\circ})\|1\rangle$
$\|0\rangle$	$\theta_S + \theta_R = 62^{\circ}$	$\cos(62^{\circ})\|0\rangle - \sin(62^{\circ})\|1\rangle$
$\|1\rangle$	$\theta_S + \theta_R = 195^{\circ}$	$\sin(195^{\circ})\|0\rangle + \cos(195^{\circ})\|1\rangle$
$\|1\rangle$	$\theta_S + \theta_R = 47^{\circ}$	$\sin(47^{\circ})\|0\rangle + \cos(47^{\circ})\|1\rangle$
$\|1\rangle$	$\theta_S + \theta_R = 245^{\circ}$	$\sin(245^{\circ})\|0\rangle + \cos(245^{\circ})\|1\rangle$
$\|1\rangle$	$\theta_S + \theta_R = 135^{\circ}$	$\sin(135^{\circ})\|0\rangle + \cos(135^{\circ})\|1\rangle$
$\|1\rangle$	$\theta_S + \theta_R = 197^{\circ}$	$\sin(197^{\circ})\|0\rangle + \cos(197^{\circ})\|1\rangle$
$\|0\rangle$	$\theta_S + \theta_R = 129^{\circ}$	$\cos(129^{\circ})\|0\rangle - \sin(129^{\circ})\|1\rangle$
$\|0\rangle$	$\theta_S + \theta_R = 100^{\circ}$	$\cos(100^{\circ})\|0\rangle - \sin(100^{\circ})\|1\rangle$
$\|1\rangle$	$\theta_S + \theta_R = 240^{\circ}$	$\sin(240^{\circ})\|0\rangle + \cos(240^{\circ})\|1\rangle$
$\|1\rangle$	$\theta_S + \theta_R = 144^{\circ}$	$\sin(144^{\circ})\|0\rangle + \cos(144^{\circ})\|1\rangle$

The sender receives $N_S + 1$ and N_R and check if the channel is authenticated or not, the sender computes $|\varphi_3\rangle$ and sends it back again to the receiver with the $N_R + 1$ as follows in the following table 8.

Table 8: Sequence sender state of the third stage of the protocol.

State	**The Key Angle (θ)**	**Sequence Sender State**
$\|1\rangle$	$K_{S,R} = 32^{\circ}$	$\sin(32^{\circ})\|0\rangle + \cos(32^{\circ})\|1\rangle$
$\|0\rangle$	$K_{S,R} = 32^{\circ}$	$\cos(32^{\circ})\|0\rangle - \sin(32^{\circ})\|1\rangle$
$\|0\rangle$	$K_{S,R} = 32^{\circ}$	$\cos(32^{\circ})\|0\rangle - \sin(32^{\circ})\|1\rangle$
$\|1\rangle$	$K_{S,R} = 32^{\circ}$	$\sin(32^{\circ})\|0\rangle + \cos(32^{\circ})\|1\rangle$
$\|1\rangle$	$K_{S,R} = 32^{\circ}$	$\sin(32^{\circ})\|0\rangle + \cos(32^{\circ})\|1\rangle$
$\|0\rangle$	$\theta_R = 45^{\circ}$	$\cos(45^{\circ})\|0\rangle - \sin(45^{\circ})\|1\rangle$
$\|1\rangle$	$\theta_R = 17^{\circ}$	$\sin(17^{\circ})\|0\rangle + \cos(17^{\circ})\|1\rangle$
$\|1\rangle$	$\theta_R = 12^{\circ}$	$\sin(12^{\circ})\|0\rangle + \cos(12^{\circ})\|1\rangle$
$\|1\rangle$	$\theta_R = 31^{\circ}$	$\sin(31^{\circ})\|0\rangle + \cos(31^{\circ})\|1\rangle$
$\|1\rangle$	$\theta_R = 170^{\circ}$	$\sin(170^{\circ})\|0\rangle + \cos(170^{\circ})\|1\rangle$
$\|0\rangle$	$\theta_R = 130^{\circ}$	$\cos(130^{\circ})\|0\rangle - \sin(130^{\circ})\|1\rangle$
$\|1\rangle$	$\theta_R = 144^{\circ}$	$\sin(144^{\circ})\|0\rangle + \cos(144^{\circ})\|1\rangle$
$\|1\rangle$	$\theta_R = 30^{\circ}$	$\sin(30^{\circ})\|0\rangle + \cos(30^{\circ})\|1\rangle$
$\|0\rangle$	$\theta_R = 105^{\circ}$	$\cos(168^{\circ})\|0\rangle - \sin(105^{\circ})\|1\rangle$
$\|0\rangle$	$\theta_R = 32^{\circ}$	$\cos(32^{\circ})\|0\rangle - \sin(32^{\circ})\|1\rangle$
$\|0\rangle$	$\theta_R = 31^{\circ}$	$\cos(31^{\circ})\|0\rangle - \sin(31^{\circ})\|1\rangle$
$\|1\rangle$	$\theta_R = 135^{\circ}$	$\sin(195^{\circ})\|0\rangle + \cos(135^{\circ})\|1\rangle$
$\|1\rangle$	$\theta_R = 7^{\circ}$	$\sin(47^{\circ})\|0\rangle + \cos(7^{\circ})\|1\rangle$
$\|1\rangle$	$\theta_R = 165^{\circ}$	$\sin(165^{\circ})\|0\rangle + \cos(165^{\circ})\|1\rangle$
$\|1\rangle$	$\theta_R = 90^{\circ}$	$\sin(90^{\circ})\|0\rangle + \cos(90^{\circ})\|1\rangle$
$\|1\rangle$	$\theta_R = 87^{\circ}$	$\sin(87^{\circ})\|0\rangle + \cos(87^{\circ})\|1\rangle$
$\|0\rangle$	$\theta_R = 125^{\circ}$	$\cos(125^{\circ})\|0\rangle - \sin(125^{\circ})\|1\rangle$
$\|0\rangle$	$\theta_R = 97^{\circ}$	$\cos(97^{\circ})\|0\rangle - \sin(97^{\circ})\|1\rangle$
$\|1\rangle$	$\theta_R = 175^{\circ}$	$\sin(175^{\circ})\|0\rangle + \cos(175^{\circ})\|1\rangle$
$\|1\rangle$	$\theta_R = 105^{\circ}$	$\sin(105^{\circ})\|0\rangle + \cos(105)\|1\rangle$

The receiver gets $N_R + 1$ and checks if the channel is authenticated or not, after that $|\varphi_3\rangle$ is decrypted. Then the receiver has all the encoded plain-text qubits after that transfer it to the binary code. Finally, the receiver converts the whole received binary code into corresponding letters and then decrypts the letters to get the plain-text

message by using the inverse of the Hill-cipher algorithm. Eventually, the plain-text is obtained by using the equation ($P = K^{-1} \cdot E \bmod N$). Where,

$$\begin{bmatrix} 1 & 8 \\ 0 & 9 \end{bmatrix} \cdot \begin{bmatrix} 15 & 15 \\ 12 & 19 \end{bmatrix} = \begin{bmatrix} 111 & 167 \\ 108 & 171 \end{bmatrix} \bmod 26 \Rightarrow P = \begin{bmatrix} 7 & 11 \\ 4 & 15 \end{bmatrix}.$$

Which is “HELP”.

4.3 Security of The Proposed Hybrid Cryptosystem Scheme to Enhance The QTPP

In order to design a secure protocol utilizing the quantum encryption, three critical conditions must be always satisfied: First, Keys must be random. Second, The protocol must be authenticated. Third, The protocol is subject to the principles of quantum physics [57].

As we will discuss later, the proposed protocol satisfies all three conditions. Since the keys in this protocol are randomly chosen where we use two keys; the first one is the encryption key is represented by angles θ_S for the sender and θ_R for the receiver, the second one is decryption key is represented by angles and its inverse represented by angles $-\theta_S$ for the sender and $-\theta_R$ for the receiver. Since the proposed algorithm uses a quantum three-pass protocol and one of the important properties for this protocol is that there is no shared key between the sender and receiver, the sender therefore generates his own secret key K_{θ_S} where ($K_{\theta_S} = \theta_S \,|0 \leq \theta_S < \pi$) for each qubit transmitted to the receiver, and the receiver generates his own secret key K_{θ_R} where ($K_{\theta_R} = \theta_R \,|0 \leq \theta_R < \pi$) for each qubit sent back to the sender. These keys are changed for each qubit shared between sender and receiver. Hence, the angles are changed continuously for each qubit. This process is repeated for all *n*-qubits of the message. Therefore, it is impossible for the opponent to discover these keys.

Through addition our proposed hybrid cryptosystem to the QTPP we authenticate all the communication channels of the QTPP protocol and hence prevent the only possible attack the man-in-the-middle attack, therefore by adding the authentication to the communication channels the second condition is satisfied.

The proposed enhanced protocol also satisfies the third condition. Through the security of this encryption relying on the no-cloning theorem, a quantum physics property guarantees that no one can make a copy of any unknown non-orthogonal state. Hence, by transmitting data as non-orthogonal quantum states, no one can make a copy of the transmitted data without errors.

There are many fundamental advantages to the proposed modified QTPP protocol comparing with the original QTPP. Where In [40] claim that the qubit efficiency of the QTPP is 100% comparing with the other quantum key distribution protocol an in Figure 16. But we approved mathematically in the security analysis of QTPP (Section 4.5.6) that the man-in-the-middle attack is always a potential threat to information exchange based on the no-cloning theorem therefor the man-in-the middle attack can break the protocol and decrees the efficiency. By proposed our modified QTPP protocol to the original QTPP the man-in-the middle attack is eliminate through add two security layers one classical algorithm [54] and the other is quantum authentication protocol theses two layers represents the hybrid cryptosystem and we approved that mathematically in (Section 5.2) therefore the efficiency will amplified through eliminate the man-in-the middle attack.

In the original QTPP algorithm the security of the system would be of the order of $2^n \times 2^n \times 2^n$ if the number of bits in the key is 'n'. This stated security can is the best security that can be achieved by the QTPP protocol, but the opponent gets the entire qubits through the man-in-the middle attack. We have overcome this attack by add hybrid cryptosystem to eliminate the-man-in the middle attack, the order of security provided by the hybrid cryptosystem is high enough to resist a brute force

attack, through the security of the first security layer which is 2^n and second security layer which is also $2^n \times 2^n$.

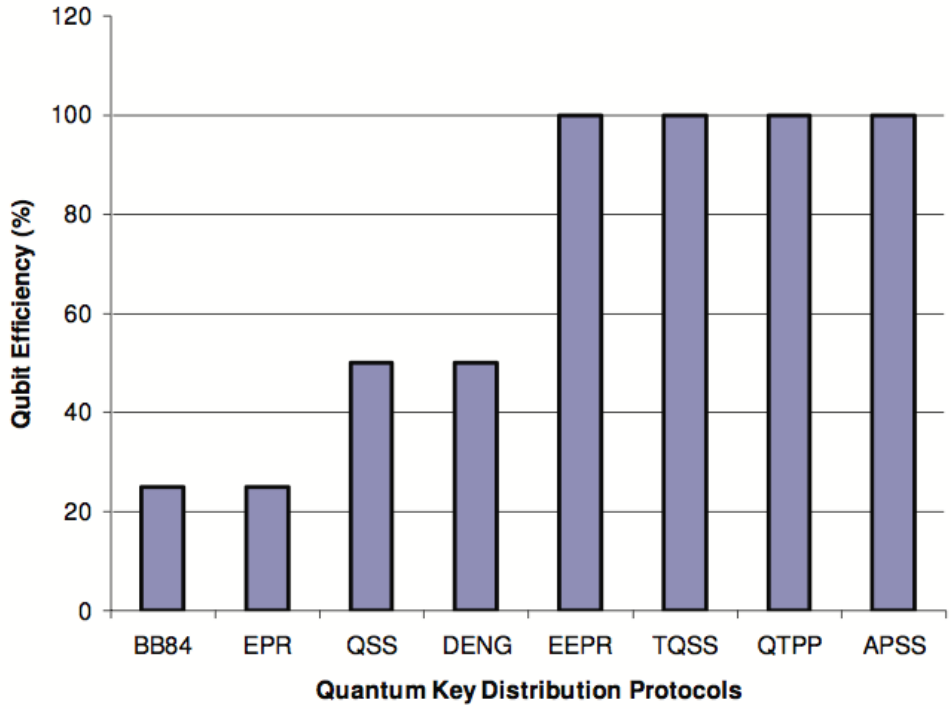

Figure 16: Qubit efficiency of quantum key distribution protocol [40].

Through The modified QTPP protocol employs polarized photons in superposition states for authentication, which provides high security against the attacks, where all transmissions use non-orthogonal qubits, and therefore the message is all subject to the no-cloning theorem. Finally, the hybrid cryptosystem provides new directions in cryptography through combination classical cryptography and quantum cryptography.

4.4 Noise analysis

There are two contributions to noise, i.e. one by the environment and one by any type of attacks of the communication and we discussed that in section (4.5). Now, we will discuss the environmental noise. The environmental noise is generally fluctuating,

but the fluctuations of the environmental noise do not vary significantly over time and space, therefore the approximation of taking the noise as constant is well justified. In our following considerations, the environmental noise will be taken as constant. The collective rotation noise, as described in [58], states that statistically, noise affects every particle transmitted over a communication channel the same way, e.g. it causes the state of each particle to be deflected clockwise by an angle θ. In general, the noise ε can be mapped to an angle using the following mapping,

$$f: \varepsilon \mapsto \theta, \text{with } \varepsilon \in [0,1]. \tag{4.9}$$

The range of this function is $[0, \theta_{max}]$. θ_{max} is determined by the relationship $\sigma(\varepsilon = 0) = 0$ and $\sigma(\varepsilon = 1) = 1$, where $\sigma(\varepsilon)$ is a strictly increasing function on the interval [0,1]. Here in our proposed system, for a qubit state |x⟩, clockwise deflection is denoted as $|x - \theta\rangle$. For instance, the state |x⟩, |0⟩ and |1⟩ are as shown in Figure 16.

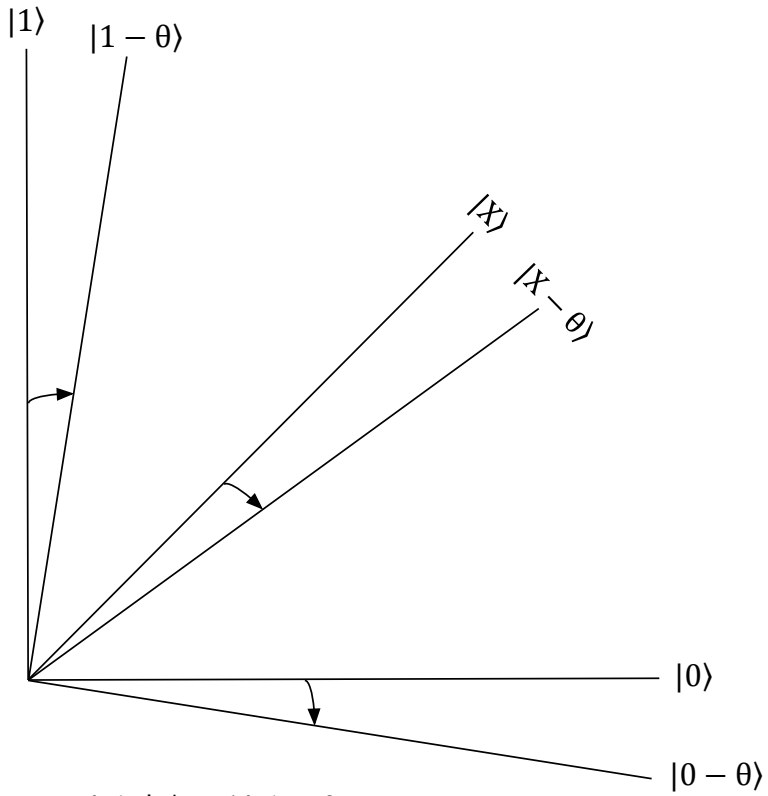

Figure 17: The state |X⟩, |0⟩ and |1⟩ deflection to the clockwise direction.

$$|0\rangle \rightarrow |0-\theta\rangle = \cos\theta|0\rangle - \sin\theta|1\rangle$$
$$|1\rangle \rightarrow |1-\theta\rangle = \sin\theta|0\rangle + \cos\theta|1\rangle. \quad (4.10)$$

The parameter θ depends on the noise of the quantum channel. Because the noise has been assumed to be constant, the parameter θ is also constant.

In a noisy quantum channel, each qubit that is sent, the final qubit error rate σ is constant and equal to $\sin^2\theta$, which is can be used to measure the noise level. The larger the noise, the closer the deflection angle will approach θ_{max}, and vice versa.

In our proposed protocol, a qubit is transmitted through the quantum channel three times between sender and receiver, each of which is subject to the rotation noise. The effect of the bit error rate due to rotation noise in the channel on the QTPP is described in the following in detail.

Based on the protocol, a rotation operator is applied to the qubit in each round to map the qubit to a non-orthogonal state. Therefore, the rotation noise changes the non-orthogonal quantum state by θ. Since the sender and the receiver will reverse their rotation operations eventually, the actual value of the rotation operator does not affect the results of the analysis. In order to make the derivation concise, the rotation operators are not shown in the derivation.

After the first stage, the deflection angle can be θ_S, the possible qubit states can be written as,

$$\begin{aligned} |0\rangle &\rightarrow |0-(\theta_S+\theta)\rangle = \cos(\theta_S+\theta)|0\rangle - \sin(\theta_S+\theta)|1\rangle \\ |1\rangle &\rightarrow |1-(\theta_S+\theta)\rangle = \sin(\theta_S+\theta)|0\rangle + \cos(\theta_S+\theta)|1\rangle \end{aligned} \tag{4.11}$$

In the second pass we have to encrypt the incoming message with the receiver's key θ_R, then the resulting states incorporating the noise as well become,

$$\begin{aligned} |0\rangle &\rightarrow |0-(\theta_S+\theta_R+2\theta)\rangle \\ &\qquad = \cos(\theta_S+\theta_R+2\theta)|0\rangle - \sin(\theta_S+\theta_R+2\theta)|1\rangle \\ |1\rangle &\rightarrow |1-\theta(\theta_S+\theta_R+2\theta)\rangle \\ &\qquad = \sin(\theta_S+\theta_R+2\theta)|0\rangle + \cos(\theta_S+\theta_R+2\theta)|1\rangle \end{aligned} \tag{4.12}$$

In the third pass, the sender decrypts the message using the inverse key $-\theta_S$, resulting in the states received by the receiver as,

$$\begin{aligned} |0\rangle &\rightarrow |0-(\theta_S+\theta_R-\theta_S+3\theta)\rangle = \cos(\theta_R+3\theta)|0\rangle - \sin(\theta_R+3\theta)|1\rangle \\ |1\rangle &\rightarrow |1-(\theta_S+\theta_R-\theta_S+3\theta)\rangle = \sin(\theta_R+3\theta)|0\rangle + \cos(\theta_R+3\theta)|1\rangle \end{aligned} \tag{4.13}$$

The probability that qubit $|0\rangle$ is recognized as 0 is $\cos^2(3\theta)$ and the probability that qubit $|0\rangle$ is recognized as 1 is $\sin^2(3\theta)$. The error rate is given by $\sin^2(3\theta)$.

In all the stages of the proposed protocol the qubit error rate σ can be easily obtained,

$$\sigma = \frac{1}{2}\sin^2(3\theta) + \frac{1}{2}\sin^2(3\theta) = \sin^2(3\theta) \quad (4.14)$$

An initial qubit error rate σ_i can be set according to the channel noise. When the qubit error rate σ of a quantum communication channel is larger than σ_i, it can be determined that the quantum channel is insecure and that there exists eavesdropping, regardless of the reason.

Generally speaking, σ_i should be set to be slightly larger than $\sigma = \sin^2(3\theta)$ in practice, which is the quantum bit error rate in only noise environments without eavesdropping. So, $\sigma = \sigma_i = \sin^2(3\theta)$ can be set as the criterion used to determine whether or not there is eavesdropping.

for example, the easiest relationship between the bit error rate and the noise is a linear relationship as $\sigma(\varepsilon) = \varepsilon$. Then if the noise level ε is equal to 6% the corresponding value of σ_i is also equal to 6%, which is the criterion of judging. So if the qubit error rate σ is larger than σ_i = 6%, it is determined that the quantum channel is insecure and there is eavesdropping.

4.5 Summary

The quantum cryptography is an emerging technology and is constantly developing. One day the quantum computer will be the driving force in this field and a combination of classical and quantum cryptography will be used in the future. Based on this concept we proposed in this chapter an enhancement of the quantum three-pass protocol based on hybrid cryptosystem.

Although QTPP protocol is secure against all the classical and quantum attacks that we presented in section 3.3 it can be successfully subjected to man-in-the-middle

attack. Therefore, we proposed quantum authentication protocol with a third party, the Quantum Distribution Centre QDC. The QDC is responsible for distributing the nonces, and the session key between sender and receiver. All communication channels are channels used in the protocol and are subject to the domain of quantum mechanics, where before applying the QTPP the sender and receiver authenticates all channels through session key know only to sender and receiver. The main vulnerability of the original QTPP was the man-in-the-middle attack as identified in chapter 4. So, by adding the authentication to the QTPP, the modified QTPP becomes resistant to all attack strategies discussed in the previous chapter. The security analysis shows clearly that the modified QTPP is unconditionally secure with respect to the randomness of the key, the authentication of the protocol, and the usage of non-orthogonal superposition states, originated from quantum physics.

Furthermore, the analysis provides an understanding of the effect of the noise level on the channels of the QTPP protocol where the changes of the qubit error rate increase the security of the protocol.

Chapter 5

CONCLUSION

As the recent literature reveals, a combination of classical and quantum cryptography will be used in the future to encrypt classical information. In this sense, this work presents a new classical and quantum mixed encryption algorithm to enhance the security of the quantum three-pass protocol and the transferred information.

Algorithms like Shor's prime number factorisation algorithm are considered a threat to classical public key encryption once a quantum computer is realised. Therefore, as we are dealing with classical information, hybrid cryptosystems will become more and more important. In this work, the enhancement to the Quantum Three-Pass Protocol QTTP is presented as two security layers represented the hybrid cryptosystem to authenticate the protocol, where we proposed in first security layer classical algorithm to encrypt the plaintext message [54] and in second security layer we proposed new quantum authentication protocol based on third party called the quantum distribution centre QDC, which securely distributes the nonces and the session key between sender and receiver by modified BB84 [30]. The analysis of the modification of the original QTPP also shows that the only possible strategic attack left to the QTPP, i.e. the man-in-the-middle attack, is prevented. Additionally all communication channels are quantum communication channels, hence, subject to the no-cloning theorem. Therefore, this authentication protocol is unconditionally secure with respect to the randomness of the key, the authentication of the protocol, and the usage of non-

orthogonal superposition states, originated from quantum physics. The security analysis for all possible attack strategies shows explicitly that this algorithm is unconditionally secure against the analysed potential classical and quantum attacks.

REFERENCES

[1] Bekenstein, J. D. (1981). Universal upper bound on the entropy-to-energy ratio for bounded systems. *Phys. Rev. D*, 23, 287–298.

[2] Turing, A. M. (1936). On computable numbers, with an application to the Entscheidungsproblem. *J. of Math*, 58(345-363), 5.

[3] Benioff, P. (1980). The computer as a physical system: A microscopic quantum mechanical Hamiltonian model of computers as represented by Turing machines. *Journal of Statistical Physics*, 22, 563–591.

[4] Feynman, R. (1982). Simulating physics with computers. *International Journal of Theoretical Physics*, 21, 467–488.

[5] Deutsch, D. (1985). Quantum theory, the church-turing principle and the universal quantum computer. *Proceedings of the Royal Society of London A: Mathematical, Physical and Engineering Sciences*, 400, 97–117.

[6] Deutsch, D., & Jozsa, R. (1992). Rapid solution of problems by quantum computation. *Proceedings of the Royal Society of London A: Mathematical, Physical and Engineering Sciences*, 439, 553–558.

[7] Bernstein, E, & Vazirani, U. (1993). Quantum complexity theory. *In Proc. 25th Annual ACM Symposium on Theory of Computing, ACM*, pp. 11–20.

[8] Simon, D. (1994). On the power of quantum computation. *Foundations of Computer Science, 1994 Proceedings., 35th Annual Symposium on, Nov*, pp. 116–123.

[9] Shor, P. W. (1994). Polynomial time algorithms for discrete logarithms and factoring on a quantum computer. *Algorithmic Number Theory*, pp. 289–289, Springer.

[10] Bennett, C. H., & Brassard, G. (1984). Quantum cryptography: Public key distribution and coin tossing. *Proceedings of IEEE International Conference on Computers, Systems and Signal Processing*, vol. 175, pp. 175–179, New York.

[11] Shor, P. W., & Preskill, J. (2000). Simple proof of security of the BB84 quantum key distribution protocol. *Physical review letters*, 85(2), 441.

[12] Ekert, A. K. (1991). Quantum cryptography based on bell's theorem. *Phys. Rev. Lett.*, 67, 661–663.

[13] Einstein, A., Podolsky, B., & Rosen, N. (1935). Can quantum-mechanical description of physical reality be considered complete? *Phys. Rev.*, 47, 777–780.

[14] Bohm, D. (2012). *Quantum theory*. Courier Corporation.

[15] Bell, J. S. et al. (1964). On the einstein-podolsky-rosen paradox. *Physics, 1*, 195-200.

[16] Clauser, J. F., Horne, M. A., Shimony, A., & Holt, R. A. (1969). Proposed experiment to test local hidden-variable theories. *Phys. Rev. Lett.,* 23, 880–884.

[17] Yuan, Z. L., Dixon, A. R., Dynes, J. F., Sharpe, A. W., & Shields, A. J. (2009). Practical gigahertz quantum key distribution based on avalanche photodiodes. *New Journal of Physics,* 11, 045019.

[18] Takesue, H., Nam, S. W., Zhang, Q., Hadfield, R. H., Honjo, T., Tamaki, K., & Yamamoto, Y. (2007). Quantum key distribution over a 40-db channel loss using superconducting single-photon detectors. *Nat Photon,* 1, 343–348.

[19] Dixon, A. R., Yuan, Z. L., Dynes, J. F., Sharpe, A. W., & Shields, A. J. (2008). Gigahertz decoy quantum key distribution with 1 mbit/s secure key rate. *Opt. Express*, 16, 18790–18979.

[20] Lo, H.-K., & Chau, H. F. (1998). Why quantum bit commitment and ideal quantum coin tossing are impossible. *Physica D: Nonlinear Phenomena*, 120, 177-187.

[21] Mayers, D. (1996). The trouble with quantum bit commitment. arXiv preprint quant-ph/9603015.

[22] Mayers, D. (1997). Unconditionally secure quantum bit commitment is impossible. *Phys. Rev. Lett.,* 78, 3414–3417.

[23] Zhou, N., Zeng, G., Nie, Y., Xiong, J., & Zhu, F. (2006). A novel quantum block encryption algorithm based on quantum computation. *Physica A: Statistical Mechanics and its Applications*, 362, 305–313.

[24] Nan-Run, Z., & Gui-Hua, Z. (2005). A realizable quantum encryption algorithm for qubits. *Chinese Physics*, 14, 2164.

[25] Guihua, Z. (2004). Encrypting binary bits via quantum cryptography. *Chinese Journal of Electronics*, 13, 651–653.

[26] Cao, Z., & Liu, L. (2012). Improvement of one quantum encryption scheme. Intelligent Computing and Intelligent Systems (ICIS), *2010 IEEE International Conference on*, vol. 1, pp. 335–339, IEEE.

[27] Leung, D. (2002). Quantum vernam cipher. *Quantum Information and Computation*, 2, 14–34, cited By (since 1996)40.

[28] Boykin, P. O., & Roychowdhury, V. (2003). Optimal encryption of quantum bits. *Physical review A*, 67, 042317.

[29] Zhou, N., Liu, Y., Zeng, G., Xiong, J., & Zhu, F. (2007). Novel qubit block encryption algorithm with hybrid keys. *Physica A: Statistical Mechanics and its Applications*, 375, 693–698.

[30] Khalaf, R. Z., & Abdullah, A. A. (2014). Novel quantum encryption algorithm based on multi-qubit quantum shift register and hill cipher. *Advances in High Energy Physics*, Volume 2014 (2014), 5.

[31] Le, P. Q., Iliyasu, A. M., Dong, F., & Hirota, K. (2010).Fast geometric transformations on quantum images. *IAENG International Journal of Applied Mathematics*, 40, 113–123.

[32] Zhou, R.-G., Wu, Q., Zhang, M.-Q., & Shen, C.-Y. (2013). Quantum image encryption and decryption algorithms based on quantum image geometric transformations. *International Journal of Theoretical Physics*, 52, 1802–1817.

[33] Yang, Y.-G., Xia, J., Jia, X., & Zhang, H. (2013). Novel image encryption/decryption based on quantum fourier transform and double phase encoding. *Quantum Information Processing*, 12, 3477–3493.

[34] Song, X.-H., Wang, S., Abd El-Latif, A., & Niu, X.-M. (2014). Quantum image encryption based on restricted geometric and color transformations. *Quantum Information Processing*, 13, 1765–1787.

[35] Zhou, N. R., Hua, T. X., Gong, L. H., Pei, D. J., & Liao, Q. H. (2015) Quantum image encryption based on generalized arnold transform and double random- phase encoding. *Quantum Information Processing*, 14, 1193–1213.

[36] Massey, J. (1988). An introduction to contemporary cryptology. *Proceedings of the IEEE*, 76, 533–549.

[37] Yang, L., Wu, L.-A., & Liu, S. (2002). Quantum three-pass cryptography protocol. Photonics Asia 2002, pp. 106-11, *International Society for Optics and Photonics.*

[38] Kanamori, Y., & moo Yoo, S. (2009). Quantum three-pass protocol: Key distribution using quantum superposition states. *International Journal of Network Security & Its Applications*, 1.2 (2009) 64-70.

[39] Kanamori, Y., Yoo, S.-M., & Al-Shurman, M. (2005). A quantum no-key protocol for secure data communication. *Proceedings of the 43rd Annual Southeast Regional Conference* - Volume 2, New York, NY, USA, pp. 92–93, ACM-SE 43, ACM.

[40] Kathyaini, N. A., & Ananthakumaran, S. (2012, April). Unconditional security based privacy protected user communication in Wireless Mesh Networks. *In Recent Advances in Computing and Software Systems (RACSS),* 2012 *International Conference on* (pp. 201-206). IEEE.

[41] Svozil, K. (2005). Feasibility of the interlock protocol against man-in-the-middle attacks on quantum cryptography. *International Journal of Quantum Information*, 3, 649–654.

[42] P. A. M. Dirac (1939). A new notation for quantum mechanics. Mathematical *Proceedings of the Cambridge Philosophical Society*, 35, pp 416-418. doi:10.1017/S0305004100021162.

[43] Wootters, W. K., & Zurek, W. H. (1982). A single quantum cannot be cloned. *Nature*, 299, 802–803.

[44] Dieks, D. (1982). Communication by epr devices. *Physics Letters A*, 92, 271-272.

[45] Peres, A. (2003). How the No-Cloning Theorem Got its Name. *Fortschritte der Physik* 51 (45): 458–461.

[46] Kaiser, D. (2011). How the Hippies Saved Physics: Science, Counterculture, and the Quantum Revival. *W. W. Norton*. ISBN 978-0-393-07636-3.

[47] Herbert, N. (1982). FLASH—a superluminal communicator based upon a new kind of quantum measurement. *Foundations of Physics*, 12(12), 1171-1179.

[48] Scarani, V., Iblisdir, S., Gisin, N., and Acin, A. (2005). Quantum cloning. *Reviews of Modern Physics*, 77, 1225.

[49] Yi, X. I. N., Ran, T. A. O., & Yue, W. A. N. G. (2008). Application of MFRFT to the Shamir's Three-pass Protocol. *Acta Armamentarii*, 29, 667–672.

[50] Lim, M.-H., Yeoh, C.-M., Lee, S., Lim, H., & Lee, H. (2008). A secure and efficient three-pass authenticated key agreement protocol based on elliptic curves. *NETWORKING 2008 Ad Hoc and Sensor Networks, Wireless Networks, Next Generation Internet*, pp. 170–182, Springer.

[51] Anselme, T. (2012). Zwei anwendungen des paillier-kryptosystems: Blinde signature und three-pass-protocol. arXiv preprint arXiv:1206.1078.

[52] Lee, S.-M., & Kim, T.-Y. (1999). Three-pass hybrid key establishment protocol based on esign signature. *Computer Safety, Reliability and Security*, pp. 459–467, Springer.

[53] Uchoa, A., Pellenz, M., Santin, A., & Maziero, C. A. (2007). A three-pass protocol for cryptography based on padding for wireless networks. *Consumer Communications and Networking Conference, 2007. CCNC 2007. 4th IEEE*, Jan, pp. 287–291.

[54] Alharith A. Abdullah, Rifaat K., & Riza, M. (2015). A realizable quantum three-pass protocol authentication based on hill-cipher algorithm. *Mathematical Problems in Engineering*, 2015 (2015), 6.

[55] Bouwmeester, D., Ekert, A. K., & Zeilinger, A. (2000). *The physics of quantum information*, vol. 38. Springer Berlin.

[56] Rieffel, E. (2000). An introduction to quantum computing for non-physicists. *Los Alamos Physics Preprint Archive*.

[57] Harper, C., Grimaila, M. R., & Baumgartner, G. (2013). Security Standards and Best Practices for Quantum Key Distribution. *In Proceedings of the International Conference on Security and Management (SAM) (p.1).* The

Steering Committee of The World Congress in Computer Science, Computer Engineering and Applied Computing (WorldComp).

[58] Ball, L. J., & Banaszek, K. (2004). Potential for Quantum Cryptography over Collective Noise Channels. *In Proceedings of AIP Conference Proceedings, Glasgow, UK*, 25–29 July 2004; pp. 295–298.

[59] Bennett, C. H., & Brassard, G. (1985). An update on quantum cryptography. *Advances in cryptology*, pp. 475–480, Springer.

[60] Scarani, V., Acin, A., Ribordy, G., & Gisin, N. (2004). Quantum cryptography protocols robust against photon number splitting attacks for weak laser pulse implementations. *Physical Review Letters*, 92, 057901.

[61] Hill, L., & of Pennsylvania, C. C. U. (1929). Cryptography in an Algebraic Alphabet. *Mathematical Association of America*.

[62] Hill, L. S. (1931). Concerning certain linear transformation apparatus of cryptography. *The American Mathematical Monthly*, 38, pp. 135–154.

[63] Overbey, J., Traves, W., & Wojdylo, J. (2005). On the Keyspace of the Hill Cipher. *Cryptologia*, 29, 59–72.

[64] Saeednia, S. (2000). How to make the hill cipher secure. *Cryptologia*, 24, 353-360.

[65] Overbey, J., Traves, W., & Wojdylo, J. (2005). On the Keyspace of the Hill Cipher. *Cryptologia,* 29, 59–72.

APPENDICES

Appendix A: Quantum Cryptography

A.1. Basic Ideas of Quantum Cryptography

In this section we will present the main concepts of quantum cryptography and what is the differences with the classical cryptography.

Quantum cryptography is a new science using the principles of quantum mechanics, which helps the sender and receiver to deals with quantum key using to encrypt and decrypt plain-text message.

The most important goal in the quantum cryptography is the discovery of an opponent if he tried to break the key and because the key is quantum bits so it cannot be cloned, if sender sends the key to receiver and an opponent tries to break the key, then It has to corrupt the qubits based on quantum mechanics concept which is a quantum system can not be measured without annoying the system.

One of the important theories that make the quantum key distribution is effective is no-cloning theorem, where the opponent cannot recognize between two non-orthogonal state without collapsing the quantum state of at least one of them.

We clarify that by considering $|A\rangle$ and $|B\rangle$ to be the non-orthogonal quantum states opponent is trying to know that. If theses quantum states interact with a standard state $|u\rangle$,

$$|A\rangle|u\rangle \rightarrow |A\rangle|v\rangle \qquad \text{(A.1)}$$

$$|B\rangle|u\rangle \rightarrow |B\rangle|v'\rangle \quad \text{(A.2)}$$

Opponent trying $|v\rangle$ and $|v'\rangle$ to be different, to know the identity of the quantum state. However the inner product are kept depand on thewe unitary transformations.

$$\langle v|v'\rangle\langle A|B\rangle = \langle u|u\rangle\langle A|B\rangle \text{ or } \langle v|v'\rangle = \langle u|u\rangle = 1 \quad \text{(A.3)}$$

Therefor, $|v\rangle$ and $|v'\rangle$ must be identical and opponent in order to gain any information must be interrupt one of the two quantum states.

A.2 The Differences between Classical Cryptography and Quantum Cryptography

During the last decades classical cryptography systems was the real guarantee for reliable communications and protect the information from eavesdropper. Although most classical encryption systems still in use so far but it proved theoretically that it is possible to penetrate these systems.

Most of the classical cryptography systems are secured based on the complexity of mathematical computational processes, which is limited by abilities of current technology. With the rapid development in technology it has become possible to tapped and stored plain-text messages, therefore the powerful of decryption of these plain-text message is possible now.

In quantum cryptography, the systems are based on properties of quantum mechanics therefore the decryption of plain-text message is not possible even with the current technology. Where we cannot measure the quantum state without collapsing it and hence degrading the key. In quantum cryptography, because qubits cannot be copied and stored so the transmission of the qubits is continuous and this is another

difference with the classical cryptography where the encrypted message is stored and transmitted. Indeed there are quantum repeaters to store the quantum state theoretically but practically still not applied and it is not sure to increase the reliability.

A.3. Quantum Key Distribution

In quantum cryptography we do not send a secret information directly, but instead of that we distribute and send a secret key randomly as in figure A.1. When the transmission of key is done, it can be used in a classical symmetric encryption or to encrypt and decrypt information. Now we explain how the quantum key distribution protocol work.

Quantum key distribution protocol was proposed in 1984 by Charles H. Bennet and Gilles Brassard which called later BB84 [59]. It Utilized the uncertainty concept and no-cloning theorem to guarantee that the transmission of the key have not been eaves- dropped or altered.

The Stages of a secure key in BB84 protocol can be divided into three parts summarized in figure A.2.

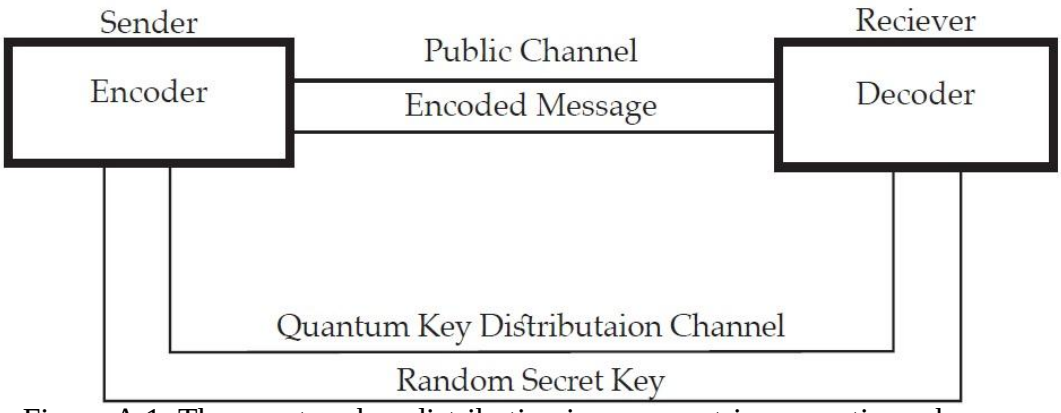

Figure A.1: The quantum key distribution in a symmetric encryption scheme.

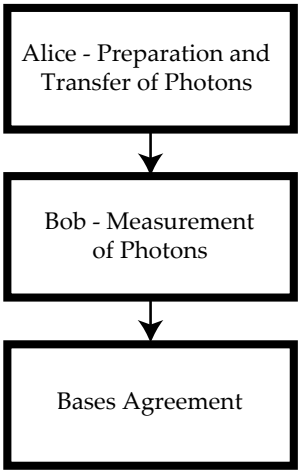

Figure A.2: the key agreement procedure in BB84 protocol.

For example, Alice chooses random values (0 or 1) and random bases (rectilinear or diagonal) where rectilinear bases represent ($\rightarrow = 0^{\circ} = 0bit,\ \uparrow = 90^{\circ} = 1bit$) and diagonal bases represent ($\nearrow = 45^{\circ} = 0bit,\ \searrow = 135^{\circ} = 1bit$). Then she prepares photons with spin orientation according to randomly chosen values and bases as in table A.1.

Table A.1: Prepares photons with random values (0, 1) in random bases (rectilinear, diagonal).

Alice's Bit	1	0	1	1	1	0	0	0
Alice's Basis	⊕	⊕	⊗	⊕	⊗	⊗	⊗	⊕
Alice's Polarization	↑	→	↘	↑	↘	↗	↗	→

Next, Alice sends polarized photons to Bob over quantum channel. At the end Bob receives a photon, he randomly chooses the measurement basis. He measures the photon in the basis of his choice and stores the result along with the base used for measurement as in table A.2.

Table A.2: Measurement of photons in BB84 protocol.

Bob's Basis	⊕	⊗	⊗	⊗	⊕	⊗	⊕	⊕
Bob's Measurement	1	0	1	0	0	0	0	0

After sufficient number of values have been transfered, the phase of bases agreement begins where Alice and Bob exchange information about their bases for each photon and discard values for which bases did not comply. After such procedure Alice and Bob have the same value of the key, that is 1100 as in table A.3.

Table A.3: Bases discussion procedure in BB84 protocol.

Discussion Basis	⊕	⊗	⊗	⊗	⊕	⊗	⊕	⊕
Agreed Key	1		1			0		0

Since photons were sent over an insecure channel they may have been eavesdropped or manipulated. To check for eavesdropping Bob choose random subset of key bits (usually one third of them is enough) and reveals them to Alice. Alice confirms whether she has the same values. If any of the bits vary the transmission may have been eavesdropped or altered, therefore it needs to be repeated. If all the test bits are confirmed, the remaining bits can be used as the key.

Despite the fact that all communication takes place over channels prone to eavesdropping, the protocol is still secure. Due to the no-cloning theorem photons cannot be copied in order to measure the copy and leave the original photon intact. If eavesdropper Eve wants to reveal useful information from the photon she has to measure it in the basis of her choice. If she happens to choose the correct base there is no way Alice and Bob will notice. But if she chooses an incorrect basis (which

happens in half the cases) Alice and Bob will not agree upon bit value, knowing the transmission was eavesdropped. This feature of quantum key distribution ensures communicating parties that the secret key was not compromised. The public discussion of the measurement basis also does not compromise the key because knowledge of the basis after all the photons were measured is not useful to Eve. Nevertheless, technological imperfection can compromise the protocol. In currently available physical realizations usually a weak laser pulse is used as a photon source. As such a source does not deterministically emit one photon per pulse, the protocol is prone to photon number splitting attacks [60]. Under certain conditions, Eve is able to block single photon pulses and save one photon from multi photon pulses in her quantum memory. Since all photons from one pulse are polarized in the same basis, Eve can wait until basis agreement between Bob and Alice and then measure her memorized photons in correct basis, revealing the key.

Appendix B: Modified BB84 Protocol

B.1. Basic Ideas of Modified BB84 protocol

This idea employs the polarization technique to BB84 protocol, so that both parties can negotiate a shared secret key without any loss of information. The modified BB84 protocol (MBB84 protocol) allows a Sender to encode his contribution into photons to send them to a Receiver via a quantum channel. After that, the Receiver will use the same polarization to generate the key. Finally, both parties negotiate a shared key accordingly.

The steps of the protocol are listed below:

- Sender randomly choses n-bits string K_A^i ={ K_A^1, K_A^2, K_A^3, … K_A^n } and P^i ={P^1, P^2, P^3 , . . . P^n } this represents the polarization of bits. Where K_A^i and P^i denote the polarizations of the i-th bits.

- Sender generates the corresponding photons into one of the following four photon states $|\psi_{A^i}, P^i\rangle$ according to the bit information of K_A^i and polarize P^i, $1 \leq i \leq n$

$$|\psi_0, +\rangle = \nearrow = |+\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle) \quad \text{(B.1)}$$

$$|\psi_0, -\rangle = \nwarrow = |-\rangle = \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle) \quad \text{(B.2)}$$

$$|\psi_1, +\rangle = \leftrightarrow = |0\rangle = \frac{1}{\sqrt{2}}(|+\rangle + |-\rangle) \quad \text{(B.3)}$$

$$|\psi_1, -\rangle = \updownarrow = |1\rangle = \frac{1}{\sqrt{2}}(|+\rangle - |-\rangle) \quad \text{(B.4)}$$

In the above encoding process, if $K_A^i = 0$, P^i is encoded by the diagonal basis, and if $K_A^i = 1$, P^i is encoded by the rectilinear basis. After that, Sender sends the photons to Receiver in sequence through a quantum channel.

- Upon receiving the photons, Receiver polarization are P^i={P^1, P^2, P^3 , . . . P^n } for 1 ≤ i ≤ n. if $P^i = |+\rangle$ or $|-\rangle$ then $K_B^i = 0$, if $P^i = |0\rangle$ or $|1\rangle$ then $K_B^i = 1$.

Then the n-bit string for Bob is K_B^i ={ K_B^1 , K_B^2 , K_B^3 ,… K_B^n }. The n-bit string obtained by receiver represents the encryption key (quantum key). Sender and receiver are using the same quantum key for encryption message and decryption message.

Appendix C: Classical Hill-Cipher

C.1. Hill-Cipher Algorithm

The classical Hill cipher HC is an example of a block cipher. Hill cipher was invented in 1929 by Lester Hill [61][62]. It is very common algorithm because of its simplicity and high productivity [63][64][65].

The main concept of the HC is in order to encrypt a message using the Hill cipher, the sender and receiver must first agree upon a key matrix A of size (n × n). A must be invertible (mod 26). The plain-text will then be enciphered in blocks of size n. Although this cipher can be deployed as a digraphic or trigraphic (or n-graphic for that matter) we will handle this topic in the context of digraphs which is mean (n × n) matrix.

To begin, choose a (2 × 2) of elements of Z26 to serve as the:

$$Key = \begin{bmatrix} a & b \\ c & d \end{bmatrix},$$

Suppose that the positions of the first two characters in the plain-text message are P_1 and P_2 respectively. Then the positions of the first two cipher-text characters, C_1 and C_2 are computed by means of the matrix multiplication:

$$\begin{bmatrix} C_1 \\ C_2 \end{bmatrix} = \begin{bmatrix} a & b \\ c & d \end{bmatrix} \begin{bmatrix} P_1 \\ P_2 \end{bmatrix} \ mod\ 26,$$

in general, for an odd integer k,

$$\begin{bmatrix} C_k \\ C_{k+1} \end{bmatrix} = \begin{bmatrix} a & b \\ c & d \end{bmatrix} \begin{bmatrix} P_k \\ P_{k+1} \end{bmatrix} \ mod\ 26, \qquad \text{(C.1)}$$

Now, to decipher the plain-text message, we calculate the inverse of the key A as follows:

$$A^{-1} = \det(A)^{-1} = \begin{bmatrix} d & -b \\ -c & a \end{bmatrix} mod\ 26,$$

Then multiply the inverse of the key by each pair of cipher-text C_1 and C_2 to recover the plain-text message P1 and P2 as following:

$$\begin{bmatrix} P_1 \\ P_2 \end{bmatrix} = \det(A)^{-1} = \begin{bmatrix} d & -b \\ -c & a \end{bmatrix} \begin{bmatrix} C_1 \\ C_2 \end{bmatrix} mod\ 26,$$

in general, for odd integer k,

$$\begin{bmatrix} P_k \\ P_{k+1} \end{bmatrix} = \det(A)^{-1} = \begin{bmatrix} d & -b \\ -c & a \end{bmatrix} \begin{bmatrix} C_k \\ C_{k+1} \end{bmatrix} mod\ 26, \qquad (C.2)$$

The following example show how Hill cipher works, and for the purposes of examining the Hill cipher we will consider only (2 × 2) matrix encryption key:

Hill Cipher Encryption

• Sender and receiver agree that the matrix key is:

$$Key = \begin{bmatrix} 3 & 3 \\ 2 & 5 \end{bmatrix},$$

• Sender want to send the message "HATS" to the receiver.

• Sender splits the message into blocks of two characters "HA" and "TS", the numerical representation for "HA" is 7 and 0, and for "TS" is 19 and 18.

• To encrypt "HA" and "TS" sender multiplies the matrix key by the numerical representation.

$$\begin{bmatrix}3 & 3\\2 & 5\end{bmatrix}\begin{bmatrix}7\\0\end{bmatrix} = \begin{bmatrix}(7\times 3)+(0\times 3)\\(7\times 2)+(0\times 5)\end{bmatrix} mod\ 26 = \begin{bmatrix}21\\14\end{bmatrix}$$

$$\begin{bmatrix}3 & 3\\2 & 5\end{bmatrix}\begin{bmatrix}19\\18\end{bmatrix} = \begin{bmatrix}(19\times 3)+(18\times 3)\\(19\times 2)+(18\times 5)\end{bmatrix} mod\ 26 = \begin{bmatrix}7\\24\end{bmatrix}$$

• The encrypted message is 21, 14, 7 and 24, this is represents "VOHY".

Hill Cipher Decryption

• Decryption requires using the inverse of the matrix K. The inverse K^{-1} of a matrix K is defined by ($K.K^{-1} = K^{-1}.K = I$), where I is the identity matrix (1 − s on the diagonal, other elements – zeroes). The inverse of the matrix does not always exist, but when it does, it satisfies the preceding equation. In this case, the inverse of matrix key is,

$$Key^{-1} = \begin{bmatrix}15 & 17\\20 & 9\end{bmatrix},$$

• Now, receiver has the decryption key and the cipher-text "VOHY".

• Receiver splits the cipher-text into blocks of two characters "VO" and "HY", the numerical representation for "VO" is 21 and 14, and for "HY" is 7 and 24.

• To decrypt "VO" and "HY" receiver multiplies the decryption key by the numerical representation.

$$\begin{bmatrix}15 & 17\\20 & 9\end{bmatrix}\begin{bmatrix}21\\14\end{bmatrix} = \begin{bmatrix}(21\times 15)+(14\times 17)\\(21\times 20)+(14\times 9)\end{bmatrix} mod\ 26 = \begin{bmatrix}7\\0\end{bmatrix}$$

$$\begin{bmatrix}15 & 17\\20 & 9\end{bmatrix}\begin{bmatrix}7\\24\end{bmatrix} = \begin{bmatrix}(7\times 15)+(24\times 17)\\(7\times 20)+(24\times 9)\end{bmatrix} mod\ 26 = \begin{bmatrix}19\\18\end{bmatrix}$$

• The decrypted message is 7, 0, 19 and 18, this is represents "HATS".

Appendix D: GLOSSARY

D.1 List of Glossary

- **Quantum circuit:** “It just sequence of logical qubits carried along wires and quantum gates that acts on the qubits”.

- **Ancilla:** “ It is an extra bit which is used in quantum circuit”.

- **Spin:** “It is a purely quantum mechanics property which means it act like tiny bar magnets. This can be used in quantum computing applications”.

- **Polarization:** “It is a property of waves that can oscillate with more than one orientation”.

- **Trojan horse attack:** “This type of attack works both in classical cryptography and in quantum cryptography. The Trojan horse attack is formed from the drawback of structure of the system (e.g. algorithm, protocol and program or device). The main idea of the Trojan horse attack is that the opponent can infiltrate any system without fear of discovery, get useful information from the system and then break the system”.

- **Man-in-the-middle attack:** “This type of attack is one of the most dangerous types of attacks on classical cryptography and quantum cryptography. It also works against classical and quantum cryptography as well. The opponent simply enters between the sender and the receiver and is now unknown third party in the

flow of data between sender and receiver. This allows him to embed contents of the data as well as the possibility to modify it and send it again".

- **Individual particle attack:** "This type of attack is based on unitary operations and as we know the unitary operation is reversible, so the state will not change. Here the opponent acts as a unitary operator between the sender and receiver for each state separately allowing for eavesdropping without the knowledge of either the sender of the receiver".

- **Plain-text:** "This is what you want to encrypt".

- **Cipher-text:** "The encrypted output".

- **Enciphering or Encryption:** "The process by which plain-text is converted into cipher-text.

- **Encryption Algorithm:** "The sequence of data processing steps that go into transforming plain-text into cipher-text. Various parameters used by an encryption algorithm are derived from a secret key. In cryptography for commercial and other civilian applications, the encryption and decryption algorithms are made public".

- **Secret Key:** "A secret key is used to set some or all of the various parameters used by the encryption algorithm. The important thing to note is that, in classical cryptography, the same secret key is used for encryption and decryption. It is for this reason that classical cryptography is also referred to as symmetric key

cryptography. On the other hand, in the more modern cryptographic algorithms, the encryption and decryption keys are not only different, but also one of them is placed in the public domain. Such algorithms are commonly referred to as asymmetric key cryptography, public key cryptography, etc.".

- **Deciphering or Decryption:** "Recovering plain-text from cipher-text".

- **Decryption Algorithm:** "The sequence of data processing steps that go into transforming cipher-text back into plain-text. In classical cryptography, the various parameters used by a decryption algorithm are derived from the same secret key that was used in the encryption algorithm".

- **Ciphertext-only attack:** "In this type of attack, an opponent listens to the communication between sender and receiver, intercepting the cipher-text. Then based on the cipher-text, the opponent can analyse offline the cipher-text in order to reconstruct the corresponding key and plain-text message".

- **Known-plaintext attack:** "In this type of attack, an opponent has both the plain-text message and the corresponding cipher-text, and tries to reconstruct the key used for encryption of the plain-text".

- **Chosen-plaintext attack:** "In this type of attack, an opponent gets to choose what a plain-text message is encrypted, and this gives the opponent much powerful because if the opponent can figure out the specific part how the encryption text place is this give him cross to the key".