Quantum Encryption Algorithm Based on Modified BB84 and Authentication DH Algorithm

Rifaat Zaidan Khalaf

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

Doctor of Philosophy
in
Applied Mathematics and Computer Science

Eastern Mediterranean University
August 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 Applied Mathematics and Computer Science.

Prof. Dr. Nazım Mahmudov
Chair, Department of Mathematics

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 Applied Mathematics and Computer Science.

Asst. Prof. Dr. Mustafa Rıza
Supervisor

Examining Committee

1. Prof. Dr. Rashad Aliyev
2. Prof. Dr. Rza Bashirov
3. Prof. Dr. Mehmet Ufuk Çağlayan
4. Prof. Dr. Azmi Gençten
5. Asst. Prof. Dr. Mustafa Rıza

ABSTRACT

This thesis will describe two main contributions to quantum cryptography. First of all the well-known BB84 protocol for quantum key exchange is modified to eliminate the originally high bit error rate completely without compromising on the security. As the classical channel is the only place where eavesdropping could be possible, any attempt to eavesdropping is prevented. Secondly, the Quantum Linear Feedback Shift Register is proposed as a tool to generate the key matrix for the classical Hill-Cipher algorithm. Finally, all proposed methods are combined in an encryption process, proving to be secure, i.e. the resulting quantum encrypted message is less susceptible to attacks as shown in the detailed security.

Keywords : Network security, Quantum cryptography, Quantum computing, BB84 Protocol, Quantum encryption algorithm , polarization filter, Multi-qubit Quantum shift register matrices,.

ÖZ

Bu tezin kuantum şifreleme sistemlerine iki ana katkısı tartışılacaktır. BB84 protokolü kuantum şifre değişiminde literatürde en tanınmış protokolü, güvenliğinden ödün vermeden yüksek bit hata oranını ortadan kaldırmak için değiştirilmiştir. Orijinal BB84 protokolünde tek dinleme olasılığı olan klasik hat modifye edilmiş BB84 protokolünde ortadan kaldırılarak, tüm hatlar kuantum fizik kurallarına tabiidir. Dolayısıyla kuantum klonlanamama (no-cloning theorem) teoremine tabiidir. İkincisi, Kuantum Doğrusal Geri Dönüm Kayan Yazmaç (Quantum Linear Feedback Shift Register) klasik Hill-Şifreleme algoritması için şifre matrisini oluşturmak için bir araç olarak önerilmiştir. Son olarak, tüm önerilen yöntemler bir şifreleme işleminde birleştirilmiştir. Ayrıntılı güvenlik analizi kuantum şifreli mesaj saldırılarına klasik yöntemlere göre daha az duyarlı olduğu, yani güvenli olduğunu kanıtlamaktadır.

Anahtar Kelimeler: Ağ güvenliği, Kuantum kriptografi, Kuantum hesaplama, BB84 Protokolü, Kuantum şifreleme algoritması, polarizasyon filtresi, Multi-qubit Kuantum kayan yazmaç matrisleri.

To my family

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 Associate Prof. 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 behavior 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 EMU. I would also like to say thank from my core of heart to my friend Alharith, as a friendly student, who firstly inspired me pursuing my study once I came to this destination. 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 my friends and fellowship whom have provided me with useful feedback and pushed me forward. Finally, I am greatly indebted to my parents and family especially my wife, 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

DH	Diffie Hellman.
DLP	Discrete Logarithm Problem.
HC	Hill-Cipher.
P	Prime number.
GF	Galois field.
BB84	Charles H. Bennett and Gilles Brassard (1984).
MBB84	Modified BB84.
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.
M	Message.
KM	Key Matrix.
QSR	Quantum Shift Register.
NMR	Nuclear Magnetic Resonance.
OTP	One Time Pad.
EM	Encode Message.
QC	Quantum cipher-text.
DM	Decode Message.
H	Hadmard Gate.
S	SWAP Gate.
X	Pauli-X Gate

Y	Pauli-Y Gate
Z	Pauli-Z Gate
C-Not	C-Not Gate
QLFSR	Quantum Linear Feedback Shift Register

Chapter 1

INTRODUCTION

In cryptography, key based encryption algorithms are classified into two classes i.e., symmetric (secret/private-key) and asymmetric (public-key); If the same key is used for encryption and decryption of a message the algorithm is called a symmetric algorithm (inverse key can be used to decrypt the message), whereas if different keys are used for encryption and decryption, the algorithms are called asymmetric algorithms. In modern cryptography keys are considered as the basis for secure communication, therefore it is a major challenge to ensure a secret key exchange for symmetric encryption. Key exchange protocols provide shared secrets between two or more parties, usually for subsequent use of symmetric keys used for a variety of data security services including encryption, authentication of a message, or authentication of an entity. The key exchange problem is one of the big issues in symmetric algorithms. However, the key exchange is important from the perspective of security with respect to authentication and quality of the key.

Quantum key exchange is based on the principles of quantum mechanics that allows two parties to exchange random keys represented as qubits that can be used as keys for encryption and decryption. The quantum key exchange protocol BB84 proposed by Bennett and Brassard in 1984 [1] has been proven by Shor and Preskill [2] to be unconditionally secure, facilitateting secure communication between parties without any pre-shared secret information. The BB84 protocol was realized experimentally in 1992 by the group lead by Bennett [3]. As we will discuss in Chapter 3 section 3.1, the original BB84 protocol works with a high bit error rate, i.e. the number of successfully agreed bits is ¼ of the number of bits send.

Because of the problem of secure key exchange in symmetric cryptography, public key cryptography became more and more important, e.g. [4]. The securities of public key algorithms strongly rely on the difficulty of prime number factorization. Prime number factorization is still one of the most challenging problems in computer science with a super-polynomial computational complexity. With the introduction of a polynomial time-complexity prime number factorization algorithm, the public key cryptography would disappear immediately. Peter W. Shor introduced in his groundbreaking works [5, 6, 7, 8] a polynomial time-complexity prime number factorization quantum algorithm.

There are many different approaches to design quantum encryption algorithms. E.g Zhou [9] proposed to encrypt a classical bit using three qubits. Another class of quantum encryption algorithms is based on a sequence of unitary operations applied to an encoded plaintext to get the encrypted message [9, 10, 11, 12]. Other encryption algorithms like the Quantum Vernam cipher introduced by Leung [13] are relying on entanglement, where the entangled key is sent over an insecure quantum channel. Boykin et al generalized Leung's algorithm in their work on Optimal encryption of quantum bits [14]. Furthermore, Gui-Hua proposed in [11] an algorithm where a classical binary bit is encrypted using keys in a non-orthogonal quantum state. This work was later extended by Nan-Run and Gui-Hua in [10]. Zhou et al proposed standard a one-time pad encryption algorithm for classical messages without a pre-shared or stored key [15]. Cao and Liu refined this algorithm to a probabilistic algorithm [12]. Several studies on quantum encryption algorithms [16, 12, 17, 18] noticed that the main difference between classical encryption algorithms and quantum encryption algorithms are that the classical algorithms solely depend on mathematical principles, whereas quantum algorithms depend on principles of quantum mechanics. Zhou et al [19] introduced a new quantum image encryption algorithm based on generalized Arnold transform and double random-phase encoding. This algorithm opens up a new field in the domain of quantum encryption.

A quantum circulate cipher by using Yuen 2000 (Y-00) protocol with a suggestions register might be a linear suggestions register (LFSR) or a nonlinear feedback register it's terribly enticing in implementing a secure high-pace optical knowledge gear mechanism for subsequent generation optical networking. Thus far, a LFSR has been utilized in a quantum circulation cipher by means of Y-00 as a jogging key generator, rather of a nonlinear suggestions register. However, it's well known that a suitably designed nonlinear feedback register has larger amount and linear complexness than the corresponding portions of a LFSR driven through a secret key of same size. Though massive linear complexness of a key generator does not now guarantee the safeguard of the important thing generator itself, it forces the listener at least to accumulate extra measure knowledge to hold out the attacks [20, 21].

This leads us to the conclusion that new encryption algorithms resisting attacks of quantum algorithms have to be designed, both pure quantum mechanical and hybrid. One of the main objectives of this thesis is improve the BB84 algorithm.

So, the questions that arise can be stated as following.

1. How can we reduce the bit error rate of the BB84 protocol?

2. Can we get rid of the classical channel to match the basis’s between Alice and Bob?
3. Can we introduce different process to match the basis’s between Alice and Bob?
4. How can we encode and decode the plain text message?
5. Can we propose a new quantum encryption algorithm?

In order to reduce bit error of the transmission in the BB84 protocol the polarized photons concept will be employed to match the basis over a quantum channel. This eliminates the usage of the classical channel for the basis match, which results in an improvement of the bit error rate of the BB84 protocol. After discussing the bit error rate of the original BB84 protocol in chapter 2, we will introduce the modified BB84 protocol in chapter 3, showing also that the improvement of the bit error rate will not affect the unconditional security of the BB84 protocol.

The second contribution of this thesis is, the introduction of the Quantum Linear Feedback Shift Register, used for the generation of the matrix key for the classical Hill-Cipher algorithm, discussed in chapter 4.

In order to show the applicability of these contributions, we propose an encryption process using both approaches in chapter 4. First the key, i.e. the One-Time-Pad, will be exchanged between sender and receiver using the BB84 protocol. Then the key matrices are produced using the Quantum Linear Feedback Shift Register, which will be sent to the receiver employing the Diffie-Hellman concept. The resulting Hill-Cipher cipher-text will be encrypted by XORing the One-Time-Pad with this cipher text, agreed using the modified BB84 protocol at the beginning before being sent over a public channel. This proposed encryption algorithm turns out to be resistant against all possible attack methods, classical as well as quantum.

The (DH) key exchange is one of the known public key algorithms; it aims to distribute keys over insecure channels. The complexity of (DH) is based on discrete logarithm problem (DLP) solved over a finite field, where P is prime which considered a feature from the point of view of security, because of the challenge and difficulties of the solution of the discrete logarithm GF(P).

Chapter 2 presents a brief introduction to the concepts of quantum encryption algorithms and original BB84. Chapter 3 describes the modified BB84. Chapter 4 describes the quantum shift register and Hill-Cipher algorithm. The plaintext message will be encrypted first using the Hill-Cipher algorithm with the key matrix generated by the Quantum Shift register, then the cipher-text will be encrypted again XORing the cipher-text with the One-Time-Pad key agreed using the MBB84 protocol. Finally the results are summarized in chapter 5.

Chapter 2

QUANTUM ENCRYPTION ALGORITHM

The principle aiming of the complicated encryption algorithm is to transform a plaintext into a cipher-text and prevent the eavesdropper from assessing plaintext from the cipher-text or finding the key. This is only possible, because the strength of modern encryption systems relies on the algorithms in combination with long encryption keys. The classical encryption algorithms are divided into two categories. The first category can be considered as sender and receiver are using the same key for encryption message and decryption message. This process is referred to as the symmetric encryption algorithm. There are many classical symmetric encryption algorithms in the literature. Exemplarily, we would like to mention the most common algorithms of classical symmetric key encryption, like AES [22], Blowfish [23], DES and all its derivatives [24], Serpent [25], Twofish [26]. On the other hand the Vernam algorithm [27] serves as examples for symmetric quantum encryption algorithm. In the second category Alice and Bob use different keys in the encryption and decryption. These algorithms are called asymmetric encryption algorithms or public key cryptography. Well known examples for public key cryptography can be considered as RSA [28].

The security of the widely used RSA encryption algorithm relies on the fact that the keys used for encryption and decryption are products of large prime numbers, and that prime number factorization is known as one of the super-polynomial time complexity problems in literature. Peter Shor showed in his work on Polynomial-time algorithms about a quantum computer in 1997 [8] that can solve the prime number factorization problem in polynomial time. The realization of a quantum computer would immediately make the RSA algorithm as open as any simple substitution cipher used by children.

2.1 Features of Quantum Encryption Algorithm

As the secure information transmission is based on secure key exchange and secure encryption algorithms (i.e. any attack to the cipher-text can only be conducted in super-polynomial time), we consider Quantum Encryption if the key exchange is done using QKD processes. The encryption of the plain text can be then conducted either using quantum algorithms or classical algorithms. The basic ingredients of Quantum Encryption are discussed in the following.

2.1.1 Quantum Key Exchange

As we described above, the security of the transmitted information relies on the secure key exchange and a secure algorithm. The Quantum Key Exchange protocol, namely the BB84 [29], has been demonstrated unconditionally secure by Shor and Preskill [2]. Nevertheless, despite the BB84 protocol being unconditionally secure, the number of agreed bits approximately quarter of the total number of bits to be exchanged, which reduces the key length significantly opening the possibility for attacks related to short keys. This problem will be discussed in section 3.1 in detail and the improvement will be given in section 3.3 by the introduction of the Modified BB84 (MBB84) protocol. The negotiated key by the BB84 or MBB84 should be random and authenticated. The key is subject to the no-cloning theorem [30], discussed explicitly in section 2.3, and evidently to Heisenberg’s uncertainty principle. The eavesdropper Eve cannot determine the original state sent from Alice to Bob by interception due to no-cloning theorem. Based on the negotiated key, that can be either a classical (which is a subset of quantum keys) or quantum key, this key will be used to encrypt the plaintext using either a classical symmetric key or a quantum encryption algorithm. Both types will be discussed explicitly in chapter 4.

2.1.2 Encryption-Decryption and Transmission Process

In the previous section, A secret key is described for sharing Alice and Bob, this key is used either to encrypt the plaintext using a classical symmetric key if the key is a classical key or a quantum block encryption algorithm if the key is a superposition of $|0\rangle$ and $|1\rangle$. In this case the quantum key will be used to encrypt the classical bit message using unitary operations. A set of unitary operations like C-NOT gate, SWAP gate, Hadamard gate, Z gate and etc. is applied to get quantum cipher text.

The table 2.1 shows the differences between the Classical Encryption Algorithm and Quantum Encryption algorithm.

Table 2.1: Difference between Classical Encryption Algorithm and Quantum Encryption Algorithm.

Classical Encryption Algorithm	Quantum Encryption Algorithm
1. The proposed algorithm based on the classical encryption and mathematical principles.	1. The proposed algorithm based on the quantum principles and mathematical principles.
2. Represent information in classical algorithm either 0 or 1 state.	2. Represent information in quantum algorithm be $|\mathbf{0}\rangle$ *or* $|\mathbf{1}\rangle$ state or a linear combination of $|\mathbf{0}\rangle$ and $|\mathbf{1}\rangle$, i.e. $\boldsymbol{\alpha}|\mathbf{0}\rangle+\boldsymbol{\beta}|\mathbf{1}\rangle$
3. Intercept the transmitted data cannot be detected for eavesdropper Eve.	3. Intercept the transmitted data can be detected for eavesdropper Eve.

2.2 Eavesdropping in Quantum Cryptography

The Quantum Key Distribution protocol BB84 has been demonstrated unconditionally secure key exchange method based on quantum mechanical principles. An encryption key in quantum key distribution is using non-orthogonal quantum states for generating between sender and receiver randomly. In contrast to classical physics, in quantum mechanics there is the quantum no-cloning theorem, which states that it is clearly impossible for anyone including an eavesdropper to make an additional copy of an unknown quantum state, increasing the security of the key exchange. In classical cryptography the eavesdropper Eve can store a copy of the complete information sending from sender to receiver giving her chance to run all possible attacks on this information offline.

Quantum No-cloning theorem: This theorem is about an unknown quantum state that cannot be copied.

- Case with no ancilla: This case is given an unknown two qubit state such as $|\beta\rangle|0\rangle$, has shown a quantum copying machine that is mapping $|\beta\rangle|0\rangle \rightarrow |\beta\rangle|\beta\rangle$ does not exist.

- General case: Let $|\beta\rangle$ be an unknown quantum state , a quantum copying machine that can map $|\beta\rangle|0\rangle|0\rangle\rightarrow |\beta\rangle|U_\beta\rangle$ does not exist.

Proof (a): This proof is given information about the contrary. It is important point that is quantum-cloning machines exist. Two orthogonal input states such as $|0\rangle$ and $|1\rangle$ respectively. We have $|0\rangle|0\rangle\rightarrow |0\rangle|0\rangle$ and $|1\rangle|0\rangle \rightarrow|1\rangle|1\rangle$. Consider a general input $|\beta\rangle = a|0\rangle + b|1\rangle$. Since a unitary transformation is linear, by linearity, we have

$|\beta\rangle|0\rangle = (a|0\rangle + b|1\rangle)\,|0\rangle \rightarrow a|0\rangle|0\rangle + b|1\rangle|1\rangle$ (2.1)

In contrast, for quantum cloning, we need:

$|\beta\rangle|0\rangle \rightarrow (a|0\rangle + b|1\rangle)(a|0\rangle+ b|1\rangle) = a^2|0\rangle|0\rangle+ ab|0\rangle|1\rangle+ ab|1\rangle|0\rangle + b^2|1\rangle|1)$ (2.2)

Comparison of equations (2.1) and (2.2) shows that the following equations have to be satisfied simultaneously $a^2 = a, b^2 = b, ab = 0, and\ ba = 0.$ Obviously, the only solution to these equations is $ab = 0$, for this reason quantum cloning (without ancilla) is impossible.

Proof (b): General quantum states are more generally information gain implies disturbance.

Theorem (Information Gain implies disturbance): This theorem is given one state chosen from one of the two distinct non-orthogonal states $|t\rangle$ and $|s\rangle$ (i.e. $\langle t|s\rangle \neq 0$ or 1). For any operation can define about its identity necessarily disturbs the state.

Proof: By means of this proof is given a system initially in state either $|t\rangle$ or $|s\rangle$. Suppose an experimentalist applies some operation on the system. It prepares some ancilla in some standard state $|0\rangle$ and couples it to the system. After applying any operations on the ancilla to retrieve information about the states t and s. Therefore, we have:

$$|t\rangle|0\rangle \rightarrow |t\rangle|\varphi_t\rangle \qquad (2.3)$$

And

$$|s\rangle|0\rangle \rightarrow |s\rangle\,|\varphi_s\rangle \qquad (2.4)$$

for some states $|\varphi_t\rangle$ and $|\varphi_s\rangle$.

At the end, the experimentalist just keeps ancilla. The performance of measurement on the ancilla learns about the initial state of the system. Quantum evolution is unitary and as such it preserves the inner product. By means of this is taking the inner product between Equations such as (2.3) and (2.4). We get the following below:

$$\langle t|\langle 0|0\rangle|s\rangle = \langle t|\langle \varphi_t|\varphi_s\rangle|s\rangle$$

$$\langle t|s\rangle\langle 0|0\rangle = \langle t|s\rangle\langle \varphi_t|\varphi_s\rangle$$

$$\langle t|s\rangle\ 1 = \langle t|s\rangle\langle \varphi_t|\varphi_s\rangle$$

$$\langle t|s\rangle\ (1 - \langle \varphi_t|\varphi_s\rangle) = 0$$

As the states $|t\rangle$ and $|s\rangle$ are non-orthogonal, i.e. $\langle t|s\rangle \neq 0$, therefore the expression in the parenthesis must be zero as

$$1 - \langle \varphi_t|\varphi_s\rangle = 0.$$

From this equation, consequently we get:

$$|\varphi_t\rangle = |\varphi_s\rangle \qquad (2.5)$$

Now, the condition that $|\varphi_t\rangle = |\varphi_s\rangle$ means that the final state of the ancilla is independent of the initial state of the system, which is contradiction to the claim.

Heisenberg Uncertainty Relation:

The measurement of the ancilla will address the experimentalist nothing in regards to the initial state of the procedure, and any try by using the eavesdropper to retrieve any know-how a couple of key in a QKD system will lead to disturbance, which can be detected with the aid of Alice and Bob who can, for illustration, check the bit error fee of a random pattern of the raw transmission data. Alice prepares a sequence of photons, each and every randomly chosen in one of the vital 4 polarizations (vertical, horizontal, 45-degrees and one hundred thirty five-degrees). For, Bob has chosen some of the two polarization bases (rectilinear or diagonal) to participate in a size. Intuitively, the safety comes from the fact that the two polarization bases, rectilinear and diagonal, are conjugate observables. Just like position and momentum are conjugate observables in the common Heisenberg uncertainty principle, no dimension by an eavesdropper Eve can examine the worth of each observable at the same time. As in physics the measured quantities, observables, must be reel numbers, and in quantum physics the measured values correspond to the eigenvalues of operators, we can conclude that an observable is represented by a Hermitian operator. Consequently, the measured values of two conjugate observables are represented by two non-commuting Hermitian operators. According to Heisenberg's uncertainty principle, if A and B are two Hermitian operators, and ΔA denotes the uncertainty, i.e. the root-mean-square deviation of the operator A and ΔB denotes the uncertainty of the operator B, then the general form of Heisenberg's uncertainty relation is

$$\Delta A \cdot \Delta B \geq \frac{1}{2}|\langle[A,B]\rangle|,$$

where $[A,B]$ denotes the commutator of the operators A and Bas

$$[A,B] = A\,B - B\,A.$$

The most known relationship for Heisenberg's uncertainty relation is

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

Mathematically, this means that the operators $A$and B cannot be simultaneously diagonalzed and therefore they cannot be measured simultaneously.

2.3 The original BB84 protocol

In the late 1960s Stephen Wiesner proposed some quantum cryptographic ideas without success. Later, Charles H. Bennett and Gilles Brassard found out how to combine conjugate coding with public key encryption [31]. Then, Wiesner reactivated his work on conjugate coding in [32]. So, Wiesner proposed how quantum mechanics can be used to produce bank notes that cannot be forged. Finally, Quantum Key Distribution, based on the ideas of Wiesner, could be realized also experimentally .

In 1984, Bennett et al. published the well-known BB84 QKD protocol [29, 33]. Polarized photons are used in BB84 to allow two communicating parties, conventionally “Sender” and “Receiver”, to establish a secret common key sequence. For this the sender needs two sets of polarization filters. Set one consists of vertical and horizontal filters. This choice is called a rectilinear basis. Second set of filters is the same, except rotated 45˚. This choice is called the diagonal basis.

Shor and Preskill showed in [2], and then the BB84 Quantum Key Distribution Protocol is unconditionally secure. But, because of the algorithm only quarter of the bits sent, are remaining as the agreed key. A precise description of the problem is given in the following.

In the original BB84 protocol in general only about quarter of the key bits can be utilized to form a key, it means distortion many of bits, because the different bases between sender and receiver. As receiver does no longer understand the foundation the photons have been encoded in, all he can do is to choose groundwork at random to measure in, either rectilinear or diagonal. He does this for each photon he receives, recording the time, size basis used and measurement outcomes. After receiver has measured all of the photons, he communicates with Sender over the general public classical channel. Sender publicizes the basis each photon was once sent in, and receiver the basis each and was once measured in. They both discard photon measurements (bits) the place receiver used an additional foundation, which is half on common, leaving 1/2 the bits as a shared key.

2.3.1 Description of original BB84 Protocol

In the original BB84 protocol, Charles Bennett and Gilles Brassard showed [29]. The proportion of matching between the sender and recipient are about 25%, because of the random selection of basis .This protocol has been in use two channels , The first is quantum channel uses to send encoded data in the form of photons and the second is classical channel uses to match the different bits between the sender and the recipient. We are now explaining the main principles of the protocol and then we give an example. The details regarding the visualization of the results of the basis are shown in Table 2.2.

The main principles of BB84 QKD protocol as follows:

- Sender randomly chooses bits
- Sender randomly chooses basis
- Sender encoded the bits
- Sender sends the photons to receiver.
- Receiver randomly chooses basis.
- Receiver receives the bits
- Using classical channel to match the bits.
- Receiver reports bases of received bits.
- Sender determines which bases were correct from receiver.
- Receiver randomly detects some bits key.
- Sender conforms the bits.
- Shared secret key

Table 2.2: The Basis

Basis	0	1
+	↔	↕
x	↗	↖

2.3.2 Example

Both of sender and receiver have the same value where each of sender and receiver crosses between the basis (+, ×) with bits (0, 1), for instance crossing the basis (+) with bit 0 produces a photon ↔ and crossing the basis (×) with bit 1 produces a photon ↖. The details regarding the illustrated of the results of the main principles of BB84 are shown in Table 2.3.

Table 2.3: The main steps of BB84 Protocol

Alice's random bits	0	1	1	0	1	0	0	1
Sending basis randomly from Alice	+	+	x	+	x	x	x	+
Produces photon	↑	→	↘	↑	↘	↗	↗	→
Measuring basis randomly from Bob	+	x	x	x	+	x	+	+
Produce photon Bob measures	↑	↗	↗	↘	→	↗	↑	→
Bits as received by Bob			1					1
Bob basis	+	x	x	x	+	x	+	+
Bob decision on the correct bits	T		T			T		T
Shared bits without Eve	0		1			0		1
Randomly Bob detect some key bits			1			0		
Alice conforms them			T			T		
Shared secret bits	0							1

Chapter 3

MODIFIED BB84 QUANTUM KEY DISTRBUTION PROTOCOL

3.1 The problems of BB84

In the original BB84 protocol in general only about 25% of the key bits can be utilized to form a key, because of the different bases between sender and receiver. According to Shor and Preskill [2] the original BB84 protocol it is unconditionally secure. However, the generated key is not efficient because the qubits transmitted in the quantum channel cannot be completely employed. The process in the protocol is a probabilistic as a classical channel is involved in the negotiation process of the key, so it requires compute the quantum bit error rate (QBER) for the continued operation of the protocol. Relying on it can be re-work protocol more than once depending on the (QBER).

Because of the presence of classical channel, the attacks, such as individual attack, collective attack, and joint attack to the protocol by the eavesdropper Eve to recover information on the key and hence find plaintext of the cipher-text, become possible.

3.2 Possible Attacks to BB84

At the beginning, let us first to focus on eavesdropping attacks. Note that there is a large number of methods of eavesdropping attacks that can be lead against the BB84 protocol, such as the individual attack, collective attack, and joint attack. In the following we will discuss these attack methods explicitly to underline the necessity of the modification of the original BB84 protocol.

3.2.1 Individual attack

The simplest type of possible attack is the intercept-resend attack, area Eve measures the breakthrough states (photons) beatific by the Sender and again sends backup states to the Receiver, able in the accompaniment she measures. In the BB84 protocol, this produces errors in the key Sender and Receiver share. As Eve has no ability of the base an accompaniment beatific by Sender is encoded in, she can alone assumption which base to measurement in, in the aforementioned way as the Receiver. If she chooses the base correctly, she measures the actual photon animosity accompaniment as beatific by the Sender, and resends the actual accompaniment to Receiver. However, if she chooses the base incorrectly, the accompaniment she measures is random, and the accompaniment beatific to the Receiver cannot be the aforementioned as the accompaniment beatific by the Sender. If the Receiver again measures this accompaniment in the aforementioned base the Sender sent, he gets a accidental result—as Eve has beatific him an accompaniment in an altered basis—with a 50% adventitious of incorrect aftereffect (instead of the actual aftereffect he would get after the attendance of Eve). In the table (3.1) below shows an example of this type of attack.

The anticipation Eve chooses the incorrect base is 50% (assuming Sender chooses randomly), and if the Receiver measures this intercepted photon in the base Sender beatific he gets a accidental result, i.e., an incorrect aftereffect with anticipation of 50%. The probability an intercepted photon generates an error in the key string is then 50% × 50% = 25%. If now Sender and Receiver publicly compare n of their key bits (thus discarding them as key bits, as they are no longer secret) the probability they find disagreement and identify the presence of Eve is,

$$P_d = 1 - \left(\frac{3}{4}\right)^n$$

So to detect an eavesdropper with probability $P_d = 0.999999999$ Sender and Receiver need to compare $n = 72$ key bits.

Table 3.1: individual attack on BB84

Sender 's random bit	0	1	1	0	1	0	0	1
Sender random sending basis	+	+	x	+	x	x	x	+
Photon polarization Sender sends	↑	→	↘	↑	↘	↗	↗	→
Eve's random measuring basis	+	x	+	+	x	+	x	+
Polarization Eve measures and sends	↑	↗	→	↑	↘	→	↗	→
Receiver random measuring basis	+	x	x	x	+	x	+	+
Photon polarization Receiver measures	↑	↗	↗	↘	→	↗	↑	→
PUBLIC DISCUSSION OF BASIS								
Shared secret key	0		0			0		1
Errors in key	✓		✘			✓		✓

3.2.2 Collective attack

Eve couples each photon to an ancilla, the result of photon/ancilla will be sent to Receiver. Eve keeps all ancilla bits, in contrary to the individual attack. Eve postpones the measurement to the time after she retrieves the conversation between Sender and Receiver. Then Eve decides on the measurement of the ancilla to get information about key. The type of attack is presented in Table 3.2.

3.2.3 Joint attack

Eve acts for all of photons as a single quantum system and then couples with ancilla. And then she listens to the general discussion between Sender and Receiver before the measurement. The Table 3.3 shows an example of this type of attack.

Table 3.2: Collective attack on BB84

Sender random bits	1	0	0	1	1
Sender random basis	+	+	x	x	+
Photons polarization Sender sends	↔	↨	↗	↖	↔
Eve couples photon with ancilla	↔,0	↕,0	↗,0	↖,0	↔,0
Receiver received photons from Alice	↔	↨	↗	↖	↔
Receiver random measurement basis	+	x	+	x	x
Receiver bits	1	1	0	0	1
Receiver random measurement basis					
Receiver bits	1	1	0	0	1
Public discussion of basis					
Sender receives bits from Receiver	1	1	0	0	1
Correct bits from Sender and sends photons	↔	↔	↗	↗	↔
Eve measures	↔↔	↕↔	↗↗	↖↗	↔↔
Eve bits	1	-	0	-	1

Table 3.3: Joint attack on BB84

Sender bits	1	0	0	1	1
Sender random basis	+	+	x	x	+
Photons polarization Sender sends	↔	↨	↗	↖	↔
Eve address all photons as a single and then couples with ancilla	|↔	↨	↗	↖	↔>
Receiver received photons from Sender	↔	↨	↗	↖	↔
Receiver random measurement basis	+	x	+	x	x
Receiver received photons from Sender	1	1	0	0	1
Receiver random measurement basis					
Receiver bits	1	1	0	0	1
Public discussion of basis					
Sender receives bits from Receiver	1	1	0	0	1
Correct bits from Sender and sends photons	↔	↔	↗	↗	↔
Eve measures	↔↔	↕↔	↗↗	↖↗	↔↔
Eve bits	1	-	0	-	1

3.3 Modified BB84 protocol

This work 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 her 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. In order to prevent the attack methods, discussed in the previous section the MBB84 protocol will be proposed in the following.

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, $1 \leq i \leq n$

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

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

$$|\psi_1, +\rangle = \leftrightarrow = |0\rangle = \frac{1}{\sqrt{2}}(|+\rangle + |-\rangle)$$

$$|\psi_1, -\rangle = \updownarrow = |1\rangle = \frac{1}{\sqrt{2}}(|+\rangle - |-\rangle)$$

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 $1 \le i \le n$. 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.

3.4 Example of Modified BB84 protocol

The Sender informs the Receiver by sending a plaintext message indicating her choices like 1 as rectilinear and 0 as diagonal as it is shown in the table 3.4.

Table 3.4: The Basis

Bit	+	Bit	×
1	↔ , ↕	0	↖ , ↗

According to the following table, sending a one-time pad of 01010 with these bases, Sender’s photon pattern is shown in the following table 3.5.

Table 3.5: Preparation of photons by Sender

Sender One Time Pad	0	1	0	1	0
Basis	×	+	×	+	×
Photon Polarization	↖	↔	↗	↨	↖

Each bit is determined. The polarization is using these bits for given the one time pad and the sequence of base. If the Receiver selects the correct basis, we will get correct bits as in table 3.6, while if the Receiver selects the wrong basis, we will get random bits.

Table 3. 6: Measurement of photons by Receiver

Receiver basis	×	+	×	+	×
Photon Polarization	↔	↖	↕	↗	↔
Shared Secret Key	0	1	0	1	0

3.5 Estimate Quantum Bit Error Rate in Modified BB84 Protocol

A parameter called Quantum Bit Error Rate (QBER) must be calculated, to estimate the error produced in the quantum key distribution (QKD) system. This parameter is calculated when the sifted key is obtained. The sifted key represents the remaining shared secret bits between Sender and Receiver. In principle it is defined as the ratio of error bits to the total number of bits received, it can be expressed as a function of rates as.

$$QBER = \frac{N_{error}}{N_{correct} + N_{error}}$$

$$= \frac{Number\ o\ f\ bit\ s\ error}{Number\ of\ correct\ bits + Number\ of\ bits\ \ error} \tag{3.1}$$

The computed QBER is used to detect a possible eavesdropper. After that the revealed bits will be discarded from the sifted key, causing a reduction in the length of the final key. Finally the computed QBER will be compared with a threshold error or Max Error level and if the QBER > error max they stop the communication and repeat the processes on a different channel.

BB84 QKD implemented with ideal devices would give (QBER = 0) if there are no eavesdropping attacks. If eavesdropping attacks exist in the quantum channel, the QBER at the Sender’s and Receiver’s sifted keys will increase. Non-zero QBER can also be attributed to imperfect devices. Since QBER resulted from eavesdropping attacks and QBER based on imperfect devices are indistinguishable, Sender and Receiver must always assume that errors in their sifted key are due to eavesdropping attacks to the quantum channel. All the attackers to MBB84 (individual, collective, and joint) have no effect on the key it means (QBER = 0). Because of that, all the attack methods (individual, collective, and joint) are targeted to obtain information on the key through the communication between the Sender and Receiver through the public channel; in MBB84 these attack methods are totally prevented by the elimination of the public channel, resulting that the attackers can not get any information about the key.

3.6 Comparison Between BB84 and Modified BB84 protocol

An overview of the different between proposed scheme and BB-84 protocol will be presented in table 3.7.

Table 3.7: Comparison between BB84 and MBB84protocol

BB84 Protocol	MBB84 Protocol
1. Unconditionally secure	1. Unconditionally secure.
2 The key generated from BB84 is not efficient.	2. The key generated from MBB84 is efficient.
3. The protocol needs quantum and classic channel.	3. The protocol needs only quantum channel.
4. The protocol needs to compute QBER .	4. The protocol does not need to compute QBER.
5. Eve can get information about the key by classical channels.	5. Eve cannot get any information about the key.

3.7Advantage of Modified BB84 Protocol

Modified BB84 protocol has many advantages. The following advantages are given below:

(1) Both parties influence the outcome of the protocol; no one can determine the shared key alone. The modified BB84 Protocol does not need a classical channel to check the different bits. So, by cancelling the classical channel Eve cannot get any information about the key without being detected. For instance, for each photon, Eve chooses one of the two polarization bases (rectilinear or diagonal) to perform a measurement. The security comes from the fact that the two polarizations bases, rectilinear and diagonal, are conjugate observables in the standard Heisenberg uncertainty principle, no measurement by an eavesdropper Eve can determine the value of both observables simultaneously. The Sender sends the bit 0 with polarization diagonal and bit 1 with polarization rectilinear. The probability to detect the polarization as diagonal by Eve is $\frac{1}{2}$ and also the probability to detect the polarization as rectilinear is $\frac{1}{2}$. In other words, even if Eve was not detected, for each transmitted bit Eve can find the correct bit with a probability of $\frac{1}{4}$. If the message consists of n bits the likelihood will be $\frac{1}{4^{n}}$.

(2) The MBB84 has 100 % qubit efficiency.

The receiver uses the same polarization as the sender (bit 0 with polarization diagonal and bit 1 with polarization rectilinear). If the recipient receives a photon with ↔ or ↨, the recipient can easily identify the bit as 1 because of the polarization. If the recipient receives ↖ or↗, the recipient can easily identify the bit as 0. But if the recipient receives ↨ with the diagonal basis easy to know that photon ↨ and therefore it can detect that Eve tried to intercept it, then the recipient corrects the basis and find the correct bit, so correct all the bits that have been intercepted by Eve without a classical channel to match the different bits, and therefore, it will be used all the bits generated between the sender and the recipient.

(3) It provides about the unconditional security.

Diffie and Hellman define the term unconditionally secure in their work on New Directions in Cryptography [34] as a system that can resist any cryptanalytic attack, even with unlimited computational resources. So, we illuminate how this applies to the MBB84 protocol. For a secure key exchange algorithm unconditionally secure means that we have show that the key is random and authenticated, i.e. we have to make sure that both parties have the same key. Shor and Preskill used the average entropy of the key to prove the unconditional security of BB84 [2]. The key agreed by the MBB84 protocol is secure as it is random and authenticated, therefore MBB84 is also unconditionally secure.

Let us first examine the case that the key is random. If the key is random the average entropy of the key is maximal. The entropy of the key agreed using the MBB84 protocol can be calculated as:

$$H(X) = -\sum_{i=0}^{n} p(X_i)\log_2(p(X_i))\,,\text{where } X_i \in \{D, R\}$$

with D denoting the diagonal polarization, and R denoting the rectilinear polarization. So, with the probabilities:

$$p(D) = P = \frac{1}{2} \text{ and } p(R) = 1 - P = \frac{1}{2}$$

then we get for the entropy

$$H(X) = -P\log_2 P - (1-P)\log_2(1-P) = 1.$$

The entropy is so proven to be maximal, and therefore the key to be random.

Secondly we have to show that the key is authenticated.

- Suppose that there is no noise on the communication channel

  As the classical channel is removed, possible attacks on the classical channel are also removed in the MBB84 protocol. Therefore, all qubits sent from sender to receiver do not change, i.e. the quantum bit error rate vanishes (QBER=0). As we can be sure that all bits are transmitted without error, we can say that the key transmitted using the MBB84 protocol is authenticated. Finally, we can conclude that the MBB84 protocol is unconditionally secure as the key is random and authenticated, because even unlimited computational resources will not break the protocol.

- Suppose that there is noise on the communication channel

  Sender sends the state $|S\rangle$ to receiver over a noisy communication channel. Let μ be the noise, then the receiver will get the state $|S + \mu\rangle$. If the noise is small a measurement will give the state $|S\rangle$. If the noise is large, the receiver will measure the complement basis. If sender encodes the bit 0 with diagonal basis, then sender sends a photon $|\nearrow\rangle$ or $|\nwarrow\rangle$. The receiver receives the photon $|\nearrow +\mu\rangle$ or $|\nwarrow +\mu\rangle$. If the value of μ is high, the receiver interprets the state as $|\underline{\updownarrow}\rangle$ or $|\leftrightarrow\rangle$. Then, the receiver selects the complement basis, measuring the state now in $|\nearrow\rangle$ or $|\nwarrow\rangle$. Therefore, we can say that the MBB84 protocol corrects all error bits and random phase errors.

(4) The protocol uses one operation (deterministic) to match the generating key between sender and receiver. The algorithm uses the concept of bases: rectilinear and diagonal for the Sender and the Receiver respectively. This is a deterministic algorithm in which the two communicating parties use the same orthogonal bases to measure each qubit of the transmitted message.

Chapter 4

QUNTUM ENCRYPTION ALGORITHM USING MODIFIED BB84 FOR KEY EXCHANGE

4.1 Introduction

In this thesis, we investigate the function of the quantum shift register (QSR) made of swap gates. The quantum shift register means a quantum circuit which can shift every data qubit to the nearest qubit in a specific direction. We further study its applications to arithmetic calculation and bit-wise operations on two quantum registers. As it well known, the swap gate consists of three CNOT gates [35] and can be realized by NMR [36], which is useful for reordering of qubits such as in the quantum Fourier transform [37].

The Hill cipher (HC) is without doubt one of the notoriously symmetric cryptosystem. The major operation of HC is matrix manipulations; it multiplies a plaintext vector through a key matrix to get the ciphertext. It is extremely attractive as a result of its simplicity and excessive throughput [38] The elemental suggestion of the HC is to position the letters of the plaintext into blocks of length m, assuming an m x m key matrix, and then each block of plaintext letters is then converted into a vector of integers consistent with the alphabet chosen after which increased by using the m x m key matrix. The results are then converted back to letters and the ciphertext message is produced. The key for HC system encompass an m x m square invertible matrix, the place the larger the scale the more relaxed the encryption will be. To ensure the key matrix k is invertible, the det(k) have got to be rather top to the modulus N, to satisfy this we require

gcd(det(K) mod N,N)=1. (4.1)

4.2 General Approach of Modified BB84 with Classical Encryption Algorithm

In cryptography, key based encryption algorithms are classified into two classes i.e., symmetric (secret/private-key) and asymmetric (public-key); If the same key is used for encryption and decryption of a message the algorithm are called symmetric algorithm (inverse key can be used to decode the encryption). Some of the most popular examples of modern symmetric key cryptosystems include AES [22] (Advanced Encryption Standard), DES (Data Encryption Standard) [24] RC5 [23], Hill Cipher , and many others. On the other hand, if different keys are used for encryption and decryption, the algorithms are called asymmetric algorithms. In modern cryptography keys are considered as the basis for secure communication, therefore it is a major challenge to ensure a secret key exchange for symmetric encryption. For example, the cryptosystem RSA [28] relies on difficulty of factoring large integers, while El-Gamal [39] cryptosystem relies on discrete logarithm problem DLP.

Key exchange protocols provide shared secrets between two or more parties, usually for subsequent use of symmetric keys used for a variety of data security services including encryption, authentication of a message, or authentication of an entity. The key exchange problem is one of the big issues in symmetric algorithms. However, the key exchange is important from the perspective of security with respect to authentication and quality of the key.

An encryption algorithm is unconditionally secure if the cipher-text does not give enough information to check uniquely the corresponding plaintext, regardless of the cipher-text, which can be accessed. That is, no matter how much time Eve has, it is impossible for her to decrypt the cipher-text. Except the scheme called the one-time pad, there is no encryption algorithm that is secure and easy to use. Accordingly, an algorithm that meets one or both of the following standards can be considered as secure.

1. The cost of solving the cipher-text should be more than the value of the encrypted information.
2. The time required for compromising the encrypted information should be reasonably big. So that he information is not valuable any more when it is decrypted.

The complexity of an encryption algorithm must be small to meet both standards. Shor's algorithm [8] is a quantum algorithm for factoring a number N in $O((\log N)^3)$ time and $O(\log N)$ space complexity. So, the invention of a quantum computer will make breaking public key algorithms based on the difficulty of prime number factorization possible by reducing prime number factorization from super-polynomial complexity to polynomial complexity as proposed by Shor’s algorithm.

Like most of the quantum computer algorithms, Shor's algorithm is probabilistic: Repetitive application of the algorithm reduces the likelihood of failure.

Present symmetric cryptography and hashes are believed to be suitable to some extent against quantum computing. And because of longer symmetric keys require exponentially more work to run a brute force attack, a sufficiently long symmetric key makes this type of attack useless. So, up to our current knowledge, even a quantum computer cannot reduce the complexity of a brute force attack to classical symmetric key algorithms from super-polynomial to polynomial.

If the size of the key is *n* bits, there are 2^n viable keys. When *n* is increasing, then the number of viable keys grows exponentially. In classical computing if the key is *n* bits, then the key space has the size 2^n, and therefore at least 2^{n-1} applications of the key have to be run to breach the algorithm. On a quantum computer, the number of operations can be reduced up to $2^{n/2}$using Grover's search algorithm [40]. But the time complexity for breaching the information is still super-polynomial. This means e.g. if we are using DES with 128-bit key, Grover's search algorithm would reduce this to a key length of 64 bit. As AES is standard dealing with 256 bit keys, so breaking the AES algorithm by brute force would require 2^{128}applications of the algorithm, which still will require significantly more time than a humans life time.

Bennett, Bernstein, Brassard, and Vazirani proved in 1996 [41] that a brute-force key search on a quantum laptop can't be faster than about $2^{n/2}$ when compared with about 2^n in the classical case. Hence, the existence of a large quantum computer reduces the security of n-bit to n/2 bit. For $n > 160$ a brute force attack using a quantum computer is as useless as using a classical computer.

According to the latest information in the literature, attacks to classical symmetric key algorithms are still conducted in super polynomial even with quantum computers.

In this thesis, we introduced the Modified BB84 scheme that uses single photons in batches. The states of these single photons themselves can be considered as one-time pads. Evaluating the protocol with using EPR pairs, this scheme is functional and already in use in modern technology. The unconditional security of the MBB84 protocol can be used for the adoption to many applications.

4.3 Hill-Cipher and Quantum Shift Register

In this chapter, we will introduce and explain the generation process of the secret key by Quantum Shift Register. This secret key is represented the matrix key of Hill-Cipher which are used to encode the plaintext message .And now we will clarification in detail.

4.3.1 Circuit of The Quantum Shift Register

It can be said that the QSR circuit represented by set of input qubits and memory qubits and set of output qubits and updated memory qubits. It feeds the memory back into the application for the next cycle and this concept is similar to the operation of a classical shift register [42]. The QSR circuit consists of swap gates, which can be quantum computationally represented using three CNOT gates as in figure 3.2. The properties of CNOT are discussed in [35]. One possible physical realization of the Quantum CNOT gate was presented by Linden et al [36] . The QSR circuit can shift every data qubits to the nearest qubit in a specific direction and apply the applications for instance arithmetic calculation and bit-wise operations on two quantum registers where these operations are very useful for quantum computers and quantum computation. The circuit of the QSR is presented and considered in [43] in which shift and rotation operations on qubits are performed by swap gates and controlled swap gates.

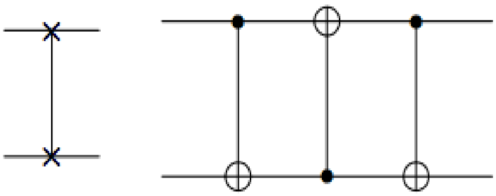

Figure 4.1: SWAP gate using CNOT gates

4.3.2 Description of Quantum Shift Register

In figure 3.1 if we denote the ancilla qubits as $|a_i\rangle$= $|a_1\, a_2\, ...\, a_k \ \rangle$, where i=1 to k. And the data qubits as $|b_j\rangle$ = $|b_1\, b_2\, ...\, b_n \ \rangle$, where j=1 to n. Then the initial state of the shift register (omitting the control qubit) is:

$$|a_i\rangle \otimes \ |b_j\rangle \ \equiv \ |a_1\, a_2\, ...\, a_k\, ; b_1\, b_2\, ...\, b_n \ \rangle. \qquad (4.2)$$

In this quantum circuit, the types of the operation activated is governed by the control qubit. We have two cases for control C, if C is set to $|0\rangle$then the shift operation active, if C is set to $|1\rangle$ then the rotation operation active.

First, the ancilla qubits can be initially set to $|0\rangle$ for convenience. In this case, each swap operation transforms the state of the register as:

$$|a_1\, a_2\, ...\, a_k\, ; b_1\, b_2\, ...\, b_n \ \rangle \rightarrow |a_2\, a_1\, ...\, a_k\, ; b_1\, b_2\, ...\, b_n \ \rangle \rightarrow$$

$$|a_2 ...\, a_k \ b_n\, ; b_1 b_2 \ldots a_1 b_{n-1}\rangle \rightarrow |a_2\, ...\, a_k \ b_n\, ; a_1\, b_1 b_2 \ldots b_{n-1}\rangle \qquad (4.3)$$

Since the control qubit C is set to |0⟩, the last swap between a_k and b_1 is inhibited. After one shift (i.e., after $n + k - 1$ swaps), the ancilla qubits becomes

$|a_{2\ldots}\, a_k\ b_n\rangle$. Note that, during the swaps and the shift, the ancilla qubits remain disentangled from the data qubits.

Second, let us consider the rotation left operation. In this case, the control bit is set to $|1\rangle$ to allow the swap between the last ancilla qubit and the first data qubit after the shift-left operation on the data qubits. Then we obtain:

$$|a_1\, a_2 \ldots a_k\ ;\ b_1 b_2 \ldots b_n\rangle \rightarrow \ldots |a_2 \ldots a_k\ b_n\, ;\ a_1\, b_1 b_2 \ldots b_{n-1}\rangle \rightarrow$$

$$|a_2 \ldots a_k\ a_1\, ;\ b_n\, b_1 b_2 \ldots b_{n-1}\rangle \qquad (4.4)$$

Which is equal to output obtained by operating left rotation both on n-data qubits and on k-ancilla qubits. It is straightforward to generalize the shift register to a shift-right and a rotation-right register by simply reversing the order of the swap,

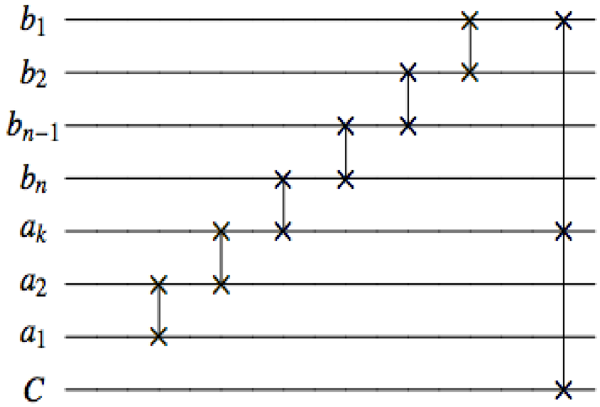

Figure 4.2: the ancilla qubit $|a_1\, a_2 \ldots a_k\rangle$and data qubit $|\, b_1 b_2 \ldots b_n\rangle$

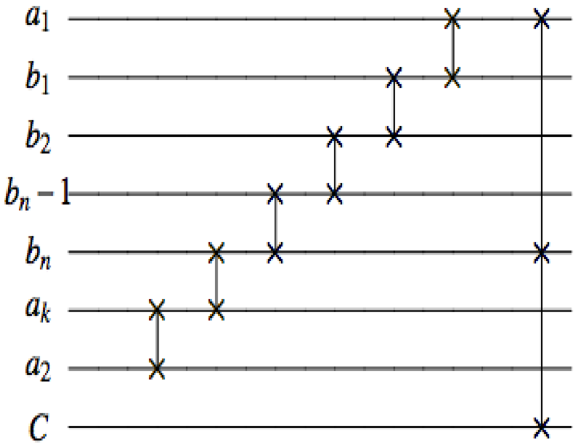

Figure 4.3: after one shift the ancilla qubits and data qubit become $|a_2\, a_1 \ldots a_k\ ;\ b_1 b_2 \ldots b_{n-1}\, b_n\ \rangle$

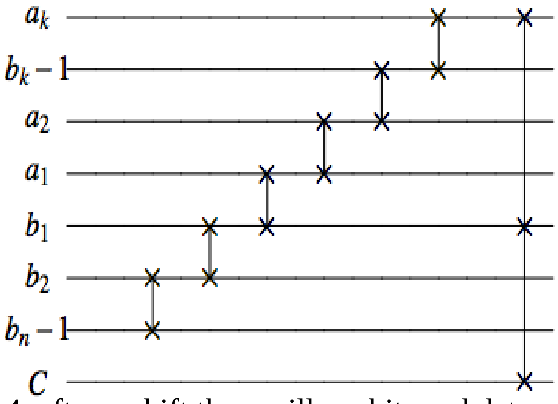

Figure 4.4: after n-shift the ancilla qubits and data qubit become $|b_n\, b_{n-1} \ldots b_1\, ; a_k \ldots a_1\ \rangle$.

4.3.3 Comparison between Classical Shift Register and QSR

The quantum shift register consists of swap gate, while the classical shift register consist of flip-flops. The exchange of qubits is equivalent to the shift operation. Since a unitary evolution is reversible, the information contained in the quantum shift register does not disappear contrary to the case of the classical shift register . Hence, to preserve the information, we need at least k extra qubits to operate k shifts.

4.3.4 Matrix of Quantum Shift Register

Quantum Shift Register (QSR) matrices are a class of square matrices which will be used in the proposed algorithm: The QSR has a number of positions. Each of these positions contains one qubit. In quantum register all qubit can be shifted one or more positions to the left or to the right. The length of QSR is determined by the number of qubits (states), the contents of each Q-bit are shift to the next qubit in each pulse, the outputs of final qubit shows a quantum feedback function and the resulting sequence from the QSR is the content of the first qubit.

In the figures 4.5 and 4.6 the quantum linear feedback shift register (QLFSR) based stream cipher using

- Quantum shift register,
- Quantum C-NOT gate, and
- Quantum feedback shift register

Are presented for two and *n* qubits.

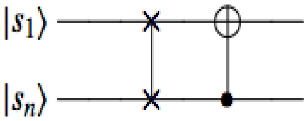

Figure 4.5: Quantum Linear Feedback Shift Register consist of SWAP and C-Not gate on 2-qubit.

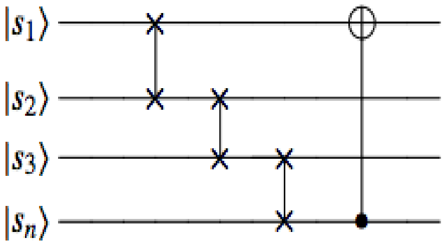

Figure 4.6: Quantum Linear Feedback Shift Register consist of SWAP and C-Not gate on n-qubit

In the Quantum shift register the shift operation depends on the swap gate. The shift is done between data and the process continues until the qubits repeat themselves.

The quantum C-NOT gate acts on the connection states in quantum register, we choose the connection state such that we can achieve the maximum period. The quantum C-NOT gate action is as follows: The second qubit is the result of a C-NOT operation between the first and second qubit, while the first qubit is conserved. If the two qubit state is initially in the state $|10\rangle$, then the application of the C-NOT gate gives C-NOT $|10\rangle = |11\rangle$. The quantum feedback shift register represents the outputs of quantum C- NOT function and is positioned in the final state qubit of quantum Register. In order to illustrate the way, how to utilize the QLFSR, we would like to discuss the following example with 2 qubits. The two qubits are initially in the states $|s_1\rangle = a_1|0\rangle + b_1|1\rangle$ and $|s_2\rangle = a_2|0\rangle + b_2|1\rangle$. So, the two qubit product state becomes:

$$|\psi\rangle = \ |s_1\rangle \otimes |s_2\rangle = a_1a_2|00\rangle + a_1b_2|01\rangle + b_1a_2|10\rangle + b_1b_2|11\rangle$$

The QLFSR was applied on the first state $|\psi\rangle$and the computation compute as follows:

$$|Shift_1\rangle = |\psi_1\rangle = C - NOT(1,2)SWAP(1,2)|\psi\rangle$$
$$= a_1a_2|00\rangle + a_1b_2|11\rangle + b_1a_2|01\rangle + b_1b_2|10\rangle$$

taking the output of first shift as input to the second shift

$$|Shift_2\rangle = |\psi_2\rangle = C - NOT(1,2)SWAP(1,2)|\psi_1\rangle$$
$$= a_1a_2|00\rangle + a_1b_2|10\rangle + b_1a_2|11\rangle + b_1b_2|01\rangle$$

taking the output of second shift as input to the second shift

$$|Shift_3\rangle = |\psi_3\rangle = C - NOT(1,2)SWAP(1,2)|\psi_2\rangle$$
$$= a_1a_2|00\rangle + a_1b_2|01\rangle + b_1a_2|10\rangle + b_1b_2|11\rangle$$

Based on the resulting states of the shift register we can generate the so-called shift register matrix A by associating the first column with the state belonging to a_1a_2, the second column with the state belonging to a_1b_2, the third column belonging to b_1a_2, and finally the forth column belonging to b_1b_2. For example let us consider $|Shift_2\rangle$, and generate the shift register matrix using this method. Therefore, we have to use the equivalency of the two basis's in the Dirac notation and in the column vector notation, i.e.

$$\{|00\rangle, |01\rangle, |10\rangle, |11\rangle\} \equiv \left\{\begin{pmatrix}1\\0\\0\\0\end{pmatrix}, \begin{pmatrix}0\\1\\0\\0\end{pmatrix}, \begin{pmatrix}0\\0\\1\\0\end{pmatrix}, \begin{pmatrix}0\\0\\0\\1\end{pmatrix}\right\}.$$

So, we get for the matrix for $|Shift_2\rangle$:

$$A = \begin{bmatrix}1 & 0 & 0 & 0\\0 & 0 & 0 & 1\\0 & 1 & 0 & 0\\0 & 0 & 1 & 0\end{bmatrix}$$

Now from the above matrix A of order 4 we can generate matrix generate the codes by considering the column vectors of the transpose of the matrix A :

$$|g_0\rangle = |00\rangle$$

$$|g_1\rangle = |11\rangle$$

$$|g_2\rangle = |01\rangle$$

$$|g_3\rangle = |10\rangle$$

$$|g_0\rangle + |g_1\rangle = |00\rangle + |11\rangle$$

$$|g_0\rangle + |g_1\rangle + |g_2\rangle = |00\rangle + |11\rangle + |01\rangle$$

$$\vdots$$

And so on. Matrix are arranged in increasing order and then bring the required number in the matrix, to generate matrix codes as shown below and we work X-OR among rows matrix, in similar way we can generate QSR matrix of any desired order and generate any number of codes from it.

$$|g_1\rangle = |11\rangle$$

$$|g_3\rangle = |10\rangle$$

$$|g_1\rangle + |g_3\rangle = |11\rangle + |10\rangle$$

$$|g_2\rangle = |01\rangle$$

$$|g_1\rangle + |g_2\rangle = |11\rangle + |01\rangle$$

$$|g_2\rangle + |g_3\rangle = |01\rangle + |10\rangle$$

$$|g_1\rangle + |g_2\rangle + |g_3\rangle = |11\rangle + |01\rangle + |10\rangle$$

$$|g_0\rangle = |00\rangle$$

$$|g_0\rangle + |g_1\rangle = |00\rangle + |11\rangle$$

$$|g_0\rangle + |g_3\rangle = |00\rangle + |10\rangle$$

$$|g_0\rangle + |g_1\rangle + |g_3\rangle = |00\rangle + |11\rangle + |10\rangle$$

$$|g_0\rangle + |g_2\rangle = |00\rangle + |01\rangle$$

$$|g_0\rangle + |g_1\rangle + |g_2\rangle = |00\rangle + |11\rangle + |01\rangle$$

$$|g_0\rangle + |g_2\rangle + |g_3\rangle = |00\rangle + |01\rangle + |10\rangle$$

$$|g_0\rangle + |g_1\rangle + |g_2\rangle + |g_3\rangle = |00\rangle + |11\rangle + |01\rangle + |10\rangle$$

4.3.5 Hill-Cipher Algorithm

The main idea in HC algorithm based on separating the plaintext into blocks of m letters. The corresponding key matrix should be a $m \times m$ matrix that is used to convert every block of the plaintext into a vector of integers based on the position of the corresponding letter in the alphabet. The results are then converted back to letters and the cipher-text message is produced. The key for HC process includes a $m \times m$ square invertible matrix K. The larger the size of the key matrix, the more secure is the algorithm. The key matrix K has to be invertible, therefore the key matrix has to satisfy the condition $\det(K) \neq 0$. In order to reduce the repetitions in the key matrix we have to satisfy additionally the condition:

$$\gcd(\det(K) \bmod N, N) = 1 \tag{4.5}$$

where m denotes the block size and N denotes the number of letters in the alphabet. Both m and N are selected positive integers (e.g., N=26 for standard alphabet). det(K) denotes the determinant of the key matrix K and gcd(a,b) denotes the greatest common divisor function, determining the greatest common divisor of the integers a and b. Suppose the sender and receiver want to exchange a secret key using HC; they share securely a non-singular invertible key matrix K. If sender wants to encrypt a plaintext vector, P, she gets the cipher-text vector, C, as follows:

$$C=K.P \bmod N \tag{4.6}$$

The receiver decrypts the cipher-text vector C by

$$P=K^{-1}.C \bmod N \tag{4.7}$$

Where K^{-1} is the inverse of the key matrix K and N is the alphabet cardinality. For existence of K^{-1}, we require K to satisfy (4.5).

4.4 Diffie-Hellman Algorithm

The implementation of Diffie-Hellman, the two parties sender and receiver, when talking by a channel they must to be secure, sender and receiver agree on positive whole numbers p and q, such that p is prime and q is a generator of p. The generator q is a number that, when raised to a positive integer power will be less than the prime number p. Any two entire numbers do not produce the same outcomes. The value of p must be large be while the value of q is normally small.

Once sender and receiver have agreed on p and q in secret, they select their individual keys x and y, both less than the prime number p. Neither sender nor receiver shares their individual key with anybody; ideally they memorize these numbers and do not write them down. Subsequent, sender and receiver compute public keys x* and y* on their individual keys in step with the formulas;

$x^* = q^x \bmod p$

and

$y^* = q^y \bmod p$

The two users can share their public keys x* and y* over a communications channel assumed to be insecure. From these public keys, a number *z* will also be generated for both sender and receiver based on their own private keys. Alice computes *z* utilizing this method.

4.4.1 Example

After the secret key has been generated by Quantum Shift Register between sender and receiver, we apply the DH algorithm to match the key between sender and receiver and eliminate the man in the middle attack by using the public values $|P\rangle$ and $|g\rangle$ and secret values of $|x\rangle$ and $|y\rangle$. The example below shows the process of matching.

• Alice and Bob agree to use a prime basis $|P\rangle$= $|10111\rangle$, (the basis p are selected from matrix of QSR). Transform the binary bits of $|P\rangle$to decimal value, Then $|P\rangle$= $|23\rangle$.

• Alice and Bob agree to use a base $|g\rangle$= $|10111\rangle$ (the basis g are selected from matrix of QSR). Then the binary bits of g are transformed into decimal, giving $|g\rangle$= $|5\rangle$ (which is a primitive root modulo $|23\rangle$).

• A secret basis chooses by sender $|x\rangle$= $|10111\rangle$, (where the basis *x* are selected from matrix of QSR), transform the binary bits of $|x\rangle$ to decimal value, then $|x\rangle$= $|3\rangle$. Alice compute $|A\rangle = |g^x \text{mod}\, p\ \rangle = |5^3 \text{mod}\ 23\rangle = |10\rangle$ and sends it to Bob.

• Bob chooses a secret basis $|y\rangle$= $|00010\rangle$, (where the basis *y* is selected from matrix of QSR), transform the binary bits of $|y\rangle$ to decimal value, then $|y\rangle$ = $|2\rangle$. Bob computes $|B\rangle = |g^y \text{mod}\, p\ \rangle = |5^2 \text{mod}\ 23\rangle = |2\rangle$ and sends this to Alice.

• Alice computes $|K_A\rangle = |B^a\ \text{mod}\, p\rangle = |2^3 \text{mod}\ 23\rangle = |8\rangle$, where $|K_A\rangle$ the key of Alice.

• Bob computes $|K_B\rangle = |A^y \text{mod}\, p\rangle = |10^2 \text{mod}\ 23\rangle = |8\rangle$ (where $|K_B\rangle$ the key of Bob).

• Alice and Bob now share a secret $|K_A\rangle$= $|K_B\rangle$= $|8\rangle$.

• The secret exchange key between Alice and Bob is $|8\rangle$. The key $|8\rangle$ corresponds to $|g_1\rangle \oplus\ |g_6\rangle \oplus\ |g_0\rangle \oplus\ |g_2\rangle \oplus\ |g_7\rangle \oplus\ |g_3\rangle \oplus |g_8\rangle$ while non existing values are ignored in the matrix.

• The g's represent Row numbers and the corresponding bits 0, 1 will be selected by the related parties to produce a key.

4.5 Quantum Encryption Algorithm

The algorithm is divided into three parts namely: encryption, transmission and decryption.

4.5.1 Encryption Part

Encryption process as it is shown in the figure 4.7 includes the following steps,

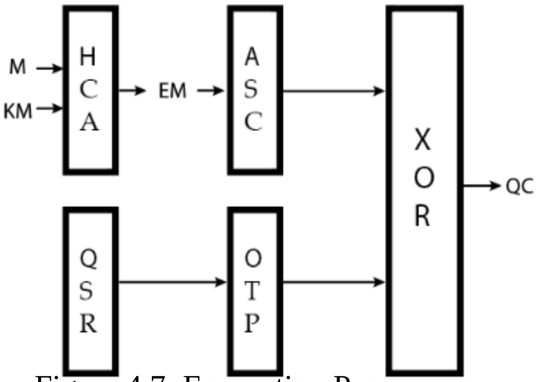

Figure 4.7: Encryption Process

- The size of the QSR matrix depends on the length of the message.
- Construct encoded QSR matrix by the operation X − OR between the rows (basis).
- Generate the secret key between Alice and Bob using authentication DH key exchange. Alice and Bob match the values of two values P and G, where G is a generator of P and P is a prime number. Then, we apply the DH algorithm to match the key between Alice and Bob.
- The secret key should be read from left to right, segment the secret key to five bits based on standard alphabets (26 letters) such that the first segment is represents a_{11} and second segment represent a_{12} and so on. Put the values a_{11}, a_{12}, . . . in to a matrix. This matrix represent matrix key of HC (K).

$$\begin{bmatrix} a_{11} & a_{12} & \cdots & a_{1\mathrm{m}} \\ \vdots & & \ddots & \vdots \\ a_{m1} & a_{m2} & \cdots & a_{mm} \end{bmatrix}$$

• Encoded the message by using matrix key of HC (K) by the relation

$$|E\ M\rangle = |(M \times K)\ mod\ 26\rangle.$$

- Generate the quantum one time pad (OTP) key between Alice and Bob.

- To construct quantum ciphertext, using the formula

$$|QC\rangle = |E\ M\rangle \oplus |OTP\rangle. \tag{4.8}$$

4.5.2 Transmission Part

The communication process as it is shown in the figure 4.8 between Alice and Bob includes two main parts:

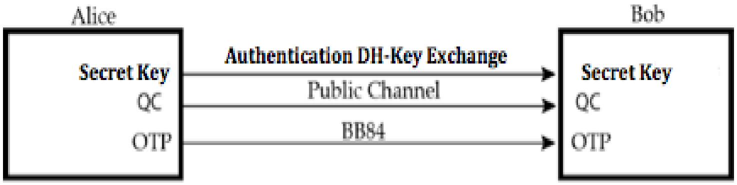

Figure 4.8: Transmission Process

4.5.2.1 Generate Quantum OTP Key

The first step in BB84 is quantum transmission. Alice generates a random bits (0 or 1) and then selects one of her two basis's (rectilinear or diagonal in this case) to transmit it in. She then prepares a photon polarization state depending both on the bit value and basis, as shown in section 3.8.

4.5.2.2 HC Matrix Key

Alice and Bob generate the same rows from encoded QSR matrix Subsequently they have the same bits (0,1) based on DH algorithm as shown in section 4.5.

4.5.3 Decryption Part

Decryption process as it is shown in the figure 4.9 includes the following steps:

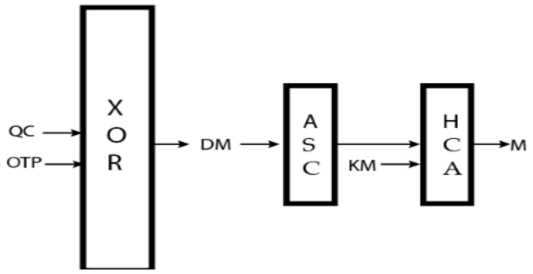

Figure 4.9: Decryption Process

- Bob decrypts the encoded message after receiving the OTP key using

$$|DM\rangle = |QC\rangle \oplus |OTP\rangle. \qquad (4.9)$$

- After Bob receives the HC-matrix key as a sequence of bits, he segments these bits to five bits five bits to generate the matrix. With the inverse of matrix we get the original plaintext by a

$$|M\rangle \ = \ |(DM \ \times K^{-1})\, mod\ 26\rangle. \qquad (4.10)$$

4.6 Example

In this example, we will provide how to generate the secret and quantum keys, encoded the message and construct the quantum cipher-text.

Step 1: Generate the secret key using the authentication of DH key exchange as shown in section 4.5. Suppose that Alice and Bob match the key K_A = K_B = $|105644\rangle$.

Step 2: Encoded the message

The key that has been agreed between Alice and Bob, Alice converts it into binary and then divides the bits into portions of five bits (standard alphabet=26). The key of Alice becomes K_A = $|00011001110010101100\rangle$. Then we convert each string of five bits length to corresponding decimal value.

$$|00011\rangle \rightarrow \ |3\rangle = a_{11}$$

$$|00111\rangle \rightarrow |7\rangle = a_{12}$$

$$|00101\rangle \rightarrow |5\rangle = a_{21}$$

$$|01100\rangle \rightarrow |12\rangle = a_{22}$$

Then we convert it to a matrix as follows:

$$\begin{bmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{bmatrix} = \begin{bmatrix} 3 & 7 \\ 5 & 12 \end{bmatrix}$$

If we have plaintext, P=he, then encoding message |E M) = K_A ×P.

$$\begin{bmatrix} 3 & 7 \\ 5 & 12 \end{bmatrix} \times \begin{bmatrix} 8 \\ 5 \end{bmatrix} = \begin{bmatrix} 59\ mod\ 26 \\ 100\ mod\ 26 \end{bmatrix} = \begin{bmatrix} 7 \\ 22 \end{bmatrix} = \begin{bmatrix} g \\ v \end{bmatrix}$$

$$|E\ M\rangle = |gv\rangle = |0011110110\rangle.$$

After that we match the quantum key between Alice and Bob as shown in the example in section 3.8:

Following table 4.1 and 4.2 clarify matching quantum key between Alice and Bob.

Table 4.1: Preparation of photons by Alice

Random bits	0	1	1	0	1	0	0	1	1	1
Basis	×	+	+	×	+	×	×	+	+	+
Photon Polarization	↖	→	↨	↗	↖	↗	↖	↨	→	→

Table 4.2: Measurement of photons by Bob

Measuring basis	×	+	+	×	+	×	×	+	+	+
Photon Polarization	↗	↨	↨	↖	↔	↖	↗	→	↨	→
Shared Secret Key	0	1	1	0	1	0	0	1	1	1

Alice and Bob matching the OTP quantum key (shared secret key).

$$OTP = |0110100111\rangle$$

Alice will to construct the quantum cipher-text using the one time pad as:

$$|QC\rangle = |E\ M\rangle \oplus |OTP\rangle = |0011110110\rangle \oplus |0110100111\rangle = |0101010001\rangle$$

Then the cipher-text is sent to Bob, where Bob first decrypts the cipher-text using the one time pad key as:

$$|DQC\rangle = |QC\rangle \oplus |OT\ P\rangle = |0101010001\rangle \oplus |0110100111\rangle = |0011110110\rangle$$

Then the binary message is splitter into a sequence of five bits and converts each 5 bit chunk to the corresponding letter getting:

$$|DQC\rangle = |gv\rangle.$$

After that the matching quantum key (OTP) between Alice and Bob. Then we can represent $|DQC\rangle$ as

$$|gv\rangle = \begin{bmatrix} 7 \\ 22 \end{bmatrix}$$

With

$$K_B = \begin{bmatrix} 3 & 7 \\ 5 & 12 \end{bmatrix},$$

Bob find the inverse key,

$$K_B^{-1} = \begin{bmatrix} 12 & 19 \\ 21 & 12 \end{bmatrix}$$

Decoding message

$$|DM\rangle = K_B^{-1}\ |gv\rangle$$

$$|DM\rangle = \begin{bmatrix} 12 & 19 \\ 21 & 12 \end{bmatrix} \begin{bmatrix} 7 \\ 22 \end{bmatrix} = \begin{bmatrix} 8 \\ 5 \end{bmatrix}$$

which corresponds to $\begin{bmatrix} H \\ E \end{bmatrix}$.

4.7 Security Analysis of Proposed Algorithm

The proposed quantum encryption algorithm is unconditionally secure against all the attackers classical and quantum. This algorithm relies on security of quantum key generated from Modified BB84 protocol and classical key generated by authentication DH algorithm. This algorithm is unconditionally secure, as we will show this in the following:

- The MBB84 has been shown to be unconditionally secure in the previous section.
- If Eve gets a quantum cipher-text created with the One Time Pad, where the One Time Pad is the only known classical cipher that is known to be unconditionally secure, then there is no way in which they can find the corresponding plaintext or key. Since the key is random and has the same length as the plaintext, there is no information in the cipher-text (such as the frequency of letters) that the Eve can use to determine the plaintext/key. Also, even if a brute force attack could be applied, where Eve decrypts the cipher-text will all possible keys, Eve has no chance to retrieve the plain text from the cipher text. This is because a brute force attack will produce many potential plaintexts that make sense to the Eve.

- Eve does not have enough information to determine the plaintext from the cipher-text. Because of there is no relation between plaintext and cipher-text.

- The process of finding the plaintext from the cipher-text includes solving a mathematical problem that is just too difficult for Eve.

- The known-plaintext and chosen- plaintext attack are unfeasible because Eve has no chance to know the correspondence of cipher-text and plaintext. This property results from the uncertainty principle in quantum mechanics.

- The Trojan horse attack cannot gain any useful information. The Trojan horse attack may be created from the drawback of structure of the system. For instance, algorithm, protocol, program or device. The idea of a Trojan horse attack is that the Eve can sneak in any system easily and can get useful information from the system and then break this system. This kind of attack is not only in classical cryptography but also exist in quantum cryptography as well. The concept of non-orthogonality in the quantum cipher-text makes the attack of the Trojan horse senseless and will not get any useful information even if it sneaked in the encryption system. For instance, the Trojan horse will return available information 0 and 1 when the cipher-text is in state $|0\rangle$ or $|1\rangle$. However, when the cipher-text is in states $|+\rangle$ or $|-\rangle$, there is no determined return information.

Chapter 5

CONCLUSION

In this thesis, we have identified that the original BB84 protocol proposed by Bennet an Bassard is inefficient with respect to the number of sent and finally agreed bits. Statistically, only one out of four bits can be negotiated successfully. By elimination of the classical channel in the original BB84 protocol, we proposed the modified BB84 protocol. As the original BB84 protocol has been proven to be unconditionally secure to any types of attacks, the modified BB84 protocol conserves this property. Based on the MBB84 protocol one can design a huge number of hybrid cryptosystems, combining classical symmetric key cryptography with the Quantum Key Exchange using MBB84. Furthermore, it was shown how to generate the key matrix using the Quantum Linear Feedback Shift Register, discussed in chapter 4. As one example of a hybrid cryptosystem, we used the MBB84 to negotiate the One-Time-Pad key, then we exchanged the key matrix generated out of the Quantum Linear Feedback Shift Register for the Hill Cipher algorithm using Diffie-Hellman authentication. Finally, the encoded message is XOR’ed with the One-Time-Pad key already negotiated using the modified BB84 protocol. The cipher-text is transmitted over a public channel. The decryption and decoding is conducted using the inverse operation of encryption and encoding. The security analysis of the overall encryption process is presented in chapter 4.7. It shows that none of the possible attack methods, neither classical, nor quantum mechanical lead to success, and that this proposed encryption algorithm is unconditionally secure.

REFERENCES

[1] Bennett, C. H., & Brassard, G. (1985, January). An update on quantum cryptography. *In Advances in cryptology* (pp. 475-480). Springer Berlin Heidelberg.

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

[3] Bennett, C. H., Bessette, F., Brassard, G., Salvail, L., & Smolin, J. (1992). Experimental quantum cryptography. *Journal of cryptology*, 5(1), 3-28.

[4] Rivest, R. L., Shamir, A., & Adleman, L. (1978). A method for obtaining digital signatures and public-key cryptosystems. *Communications of the ACM*, 21(2), 120-126.

[5] Shor, P. W. (1994) Algorithms for quantum computation: discrete logarithms and factoring. *Foundations of Computer Science, 1994 Proceedings., 35th Annual Symposium on*, pp. 124–134, IEEE.

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

[7] Shor, P. W. (1995). Scheme for reducing decoherence in quantum computer memory. *Phys. Rev. A*, **52**, R2493–R2496.

[8] Shor, P. W. (1997). Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer. *SIAM journal on computing*, **26**, 1484–1509.

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

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

[11] Gui-Hua, Z. (2004). Encrypting binary bits via quantum cryptography. *Chinese Journal of Electronics*, **13**, 651–653.

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

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

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

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

[16] Sandip Dutta, N., Anand Kumar (2011). Network security based on quantum cryptography and multi-qubit hadamard matrices. *Global Journal of Computer Science* & *Technology*.

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

[18] Hua, T., Chen, J., Pei, D., Zhang, W., & Zhou, N. (2014). Quantum image encryption algorithm based on image correlation decomposition. *International Journal of Theoretical Physic*s, 54(2), 526-537.

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

[20] Hirota, O., Sohma, M., Fuse, M., & Kato, K. (2005). Quantum stream cipher by the Yuen 2000 protocol: Design and experiment by an intensity-modulation scheme. *Physical Review A*, 72(2), 022335.

[21] Kato, K., & Hirota, O. (2008). A Quantum stream Cipher by Yuen 2000 protocol with Nonlinear Random Number Generator. *In Proceedings of SPIE,*

the International Society for Optical Engineering (pp. 70920H-1). Society of Photo-Optical Instrumentation Engineers.

[22] Daemen, J., & Rijmen, V. (2013). The design of Rijndael: AES-the advanced encryption standard. *Springer Science & Business Media*.

[23] Rivest, R. (1995). The RC5 encryption algorithm. *Proc of the 2nd Workshop on Fast Software Encryption*, Springer, pp. 86-96.

[24] Data Encryption Standard. (1997). *Federal Information Processing Standards Publication* (FIPS PUB) 46, National Bureau of Standards, Washington, DC. (http://csrc.nist.gov/publications/fips/fips46-3/fips46-3.pdf), [Last access date is 23-09-2009].

[25] Ross J. Anderson (2006-10-23). "Serpent: A Candidate Block Cipher for the Advanced Encryption Standard". *University of Cambridge Computer Laboratory*. Retrieved 2013-01-14.

[26] Kelsey, J., Schneier, B., & Wagner, D. (1997). Related-key cryptanalysis of 3-way, biham-des, cast, des-x, newdes, rc2, and tea. *Information and Communications Security*, 233-246.

[27] Schneier, B. (2007). Applied cryptography: protocols, algorithms, and source code in C. *john wiley & sons.*

[28] Rivest, R. Shami. A. & Adleman, L. (1978). A Method for Obtaining Digital Signatures and Public-Key Cryptosystems. *Communications of the ACM*, 21(2): pp. 120–126.

[29] Bennett, G., Charles H & Brassard (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.

[30] Wootters, W. K., & Zurek, W. H. (1982). A single quantum cannot be cloned.Nature, 299(5886), 802-803.

[31] Bennett, C. H., Brassard, G., Breidbart, S., & Wiesner, S. (1983, January). Quantum cryptography, or unforgeable subway tokens. *In Advances in Cryptology* (pp. 267-275). Springer US.

[32] Wiesner, S. (1983) Conjugate coding. *SIGACT News*, 15, 78–88.

[33] Bennett, C. H., & Brassard, G. (2014). Quantum cryptography: Public key distribution and coin tossing. *Theoretical Computer Science*, 560, 7-11.

[34] Diffie, W., & Hellman, M. E. (1976). New directions in cryptography. *Information Theory, IEEE Transactions on*, 22(6), 644-654.

[35] Barenco, A., Deutsch, D., Ekert, A., & Jozsa, R. (1995). Conditional quantum dynamics and logic gates. *Physical Review Letters,* 74(20), 4083.

[36] Linden, N., Kupče, Ē., & Freeman, R. (1999). NMR quantum logic gates for homonuclear spin systems. *Chemical physics letters*, 311(3), 321-327.

[37] Coppersmith, D. (2002). An approximate Fourier transform useful in quantum factoring. arXiv preprint quant-ph/0201067.

[38] Overbey, J., Traves, W., & Wojdylo, J. (2005). On the keyspace of the Hill cipher. *Cryptologia*, 29(1), 59-72.

[39] Elgamal, T. (1985). A public Key Cryptosystem and A Signature Scheme Based on Discrete Logarithms, *IEEE Trans. on Information Theory*, 31(4): pp. 469-473.

[40] Grover, L. K. (1996, July). A fast quantum mechanical algorithm for database search. *In Proceedings of the twenty-eighth annual ACM symposium on Theory of computing* (pp. 212-219). ACM.

[41] Bennett, C. H., Bernstein, E., Brassard, G., & Vazirani, U. (1997). Strengths and weaknesses of quantum computing. *SIAM journal on Computing,* 26(5), 1510-1523.

[42] Khalaf, R. Z., & Abdullah, A. A. (2015).Generate Quantum Key by Using Quantum Shift Register. *International Journal of Computer Networks and Communications Security*, VOL. 3, NO. 6, JUNE 2015, 248–252.

[43] Khalaf, R. Z., & Abdullah, A. A. (2014). Novel Quantum Encryption Algorithm Based on Multiqubit Quantum Shift Register and Hill Cipher. *Advances in High Energy Physics*, 2014.