A NEW QKD PROTOCOL BASED UPON AUTHENTICATION BY EPR ENTANGLEMENT STATE

Abdulbast A. Abushgra

Under the Supervision of Dr. Khaled M. Elleithy

DISSERTATION

SUBMITTED IN PARTIAL FULFILMENT OF THE REQUIREMENTS

FOR THE DEGREE OF DOCTOR OF PHILOSOPHY IN COMPUTER SCIENCE

AND ENGINEERING

THE SCHOOL OF ENGINEERING

UNIVERSITY OF BRIDGEPORT

CONNECTICUT

November 2017

A NEW QKD PROTOCOL BASED UPON AUTHENTICATION BY EPR ENTANGLEMENT STATE

Abdulbast A. Abushgra

Under the Supervision of Dr. Khaled M. Elleithy

Approvals

Committee Members

Name	Signature	Date
Dr. Khaled Elleithy		Nov 29/17
Dr. Miad Faezipour	Miad Faezipour	Nov. 30, 2017
Dr. Xingguo Xiong		Nov. 30, 2017 .
Dr. Navarun Gupta		Nov 30 /17
Dr. Saeid Moslehpour		NOV 17/17

Ph.D. Program Coordinator

Dr. Khaled M. Elleithy		NOV 30, 2017

Chairman, Computer Science and Engineering Department

Dr. Ausif Mahmood	Ausif Mahmood	11-30-2017

Dean, School of Engineering

Dr. Tarek M. Sobh	T. Sobh	11/30/2017

A NEW QKD PROTOCOL BASED UPON AUTHENTICATION BY EPR ENTANGLEMENT STATE

A NEW QKD PROTOCOL BASED UPON AUTHENTICATION BY EPR ENTANGLEMENT STATE

ABSTRACT

Cryptographic world has faced multiple challenges that are included in encoding and decoding transmitting information into a secure communication channel. Quantum cryptography may be another generation of the cryptography world, which is based on the law of physics. After decades of using the classical cryptography, there is an essential need to move a step forward through the most trusted systems, especially enormous amount of data flows through billions of communicating channels (*e.g. The internet*), and keeping this transmitting information away from eavesdropping is obligatory. Moreover, quantum cryptography has proved its standing against many weaknesses in the classical cryptography. One of these weaknesses is the ability to copy any type of information using a passive attack without an interruption, which is impossible in the quantum system.

Theoretically, several quantum observables are utilized to diagnose an action of one particle. These observables are included in measuring mass, movement, speed, etc. The polarization of one photon occurs normally and randomly in the space. Any interruption that happens during sending of a light will cause a deconstruction of the light polarization. Therefore, particles' movement in a three-dimensional space is supported by

Non-Cloning theory that makes eavesdroppers unable to interrupt a communication system. In case an eavesdropper tried to interrupt a photon, the photon will be destroyed after passing the photon into a quantum detector or any measurement device. In the last decades, many Quantum Key Distribution (QKD) protocols have been created to initiate a secret key during encoding and decoding transmitted data operations. Some of these protocols were proven un-secure based on the quantum attacks that were released early. Even though the power of physics is still active and the Non-Cloning theory is unbroken, some QKD protocols failed during the security measurements. The main reason of the failure is based on the inability to provide the authentication between the end users during the quantum and classical channels.

The proposed QKD protocol was designed to utilize some advantages of quantum physics as well as solid functions that are used in the classical cryptography. The authentication is a requirement during different communication channels, where both legitimate parties must confirm their identities before starting to submit data (*plain-text*). Moreover, the protocol uses most needed scenarios to finish the communication without leaking important data. These scenarios have been approved in existing QKD protocols either by classical or quantum systems. The matrix techniques also are used as a part of the preparation of the authentication key, where the end users communicate by an EPR (*related to Einstein, Podolsky, and Rosen theory in 1935*) channel. The EPR channel will be supported by an entanglement of particles. If the EPR communication succeeded, transferring the converted plain-text is required. Finally, both end users will have an authenticated secret key, and the submission will be done without any interruption.

ACKNOWLEDGEMENTS

Primarily, I am thanking God "*Allah*" for guiding me to the right path and helping me to take over all the circumstances that I have faced during my research, and then I will thank my supporters oversees, my mother who has prayed for me whole time. Also, I remember my brother, sisters, and all friends either in US or Libya even by saying a supported word. Moreover, I will not forget my wife, who has taken care of me with different difficulties. My kids are the hope that I struggled to make their life better.

Secondly, I remember the first time when I applied to the UB in 2011, and the communication was with Professor Elleithy to get acceptance into PhD program. I am very honored to be advised by Professor Elleithy during the long time of my search. He supported me with all stresses, and he was as a solution for all hard equations. I think I cannot imagine any words are enough for him.

Lastly, I would thank all faculty members in the Department of Computer Science & Engineering starting from my committee members Dr. Miad Faezipour, Dr. Xingguo Xiong, Dr. Navarun Gupta, and Dr. Saeid Moslehpour. Also, I will not forget Dr. Tarek Sobh and other faculty members at Engineering School for being the support during the student life. Thank you for all.

TABLE OF CONTENTS

LIST OF TABLES

LIST OF FIGURES

CHAPTER 1: INTRODUCTION

Theoretically, cryptography is considered as the art of producing a code, where encoding and decoding a plaintext by a secret key are the main process of security operation. Cryptography has existed for a long time, and encoding and decoding messages were just used by the military communications or as a high secure connection between countries. After spreading out the communication technologies and sharing secure information between legitimate parties, the cryptography became the main goal in many experimental labs and institutions.

Several cryptographic algorithms were released based on the requirements of each generation technology. The classical cryptography depends on different methods that have utilized digits or binary numbers. Moreover, there are many of these methods such as, Symmetric Key Encryption (*Private-Key*), Asymmetric Key Encryption (*Public-Key*), and RSA that are already compromised and have become mostly un-secure. More precisely, these security methods are not fully matched with the existing high technology.

According to several studies, there are many weak points that have been released in the classical cryptography. Most of the used security algorithms have been totally broken because their security functions are not able to stand against professional attacks. Even though there are huge weaknesses in the classical cryptography, there are still many systems running over a secure platform such as RSA, Diffie-Hellman, and Elliptic curve public key cryptosystems. These algorithms are stable to secure some platforms as long as there is no a quantum computer.

Scientists and cryptanalysis are concerned about the first quantum computers that were released recently by governmental and educational foundations. This computer has a powerful system that can exceed any regular computer. Moreover, the quantum computer will be used not only in processing valuable work, but it might be in illegal usages as hacking information systems. To recover the existing classical system before releasing quantum computers publicly, code makers and security scientists have begun to invent another security alternative to stand against any prospective attacks.

Furthermore, the classical cryptography as well as the quantum cryptography will be clearly discussed in this section. It also will demonstrate common features that have been included into the classical and quantum systems. Therefore, this section will describe generally the comparisons between both available security systems and in advance recommend some used advantages.

1.1 Classical Cryptography

Classical cryptography is a technique of repetition processes that is based upon complicated mathematic computing functions. These functions define in percentage, how the operation is hard to solve or guess from the first attempts. Moreover, the efficient definition for the cryptographic methods is well-known by measuring the strength of the shared key. This key is usually kept secure between the legitimate communicating parties, which is used for only one time of communication cycle. Furthermore, the encryption scheme between at least two parties is to enable both participants sending and receiving a message without any gain of the significant information by eavesdroppers.

1.1.1 Symmetric Encryption

Symmetric cryptography (*Private-key*) is a part of the cryptosystem that is based on performing sequential encryption and decryption operations by using the same secret key. The whole symmetric process is carried out by transforming the plaintext into cipher-text, and then using the same algorithm to recover the plaintext [1, 2]. The symmetric encryption phase includes specific parameters such as the plaintext, encryption algorithm, secret key, cipher-text, and decryption algorithm. To ensure the communication is initiated under a secure mode, the encryption algorithm must be robust enough since the opponent cannot release the used mechanism in the encryption algorithm.

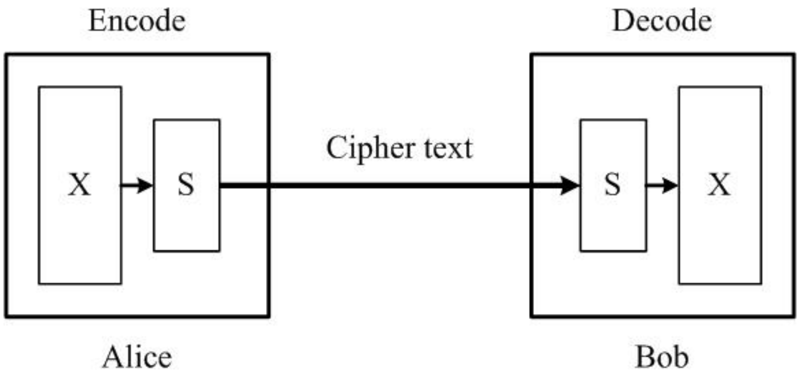


Figure 1. The simple model of the classical cryptography mechanism of submitting a plaintext X into an algorithm S.

Furthermore, the common employed characters in the symmetric cryptography involve the sender (*Alice*) and the receiver (*Bob*) as well as the eavesdropper (*Eve*). Also, the legitimate end users (*Alice and Bob*) should share only one key, whereby the encryption and decryption of the submitted plaintext are confirmed by the created secret key [3]. The main thought of the symmetric cryptography is considered about the ability of making a robust secret key as long as the opponent is unable to figure out the plaintext. Realizing the encryption algorithm or the cipher-text by the opponent does not mean knowing what inside the cipher-text or even the plaintext as long as the secret key is unknown. Functions (1, 2) show the encryption and decryption scheme of submitted plaintext between two parties:

$$Cipher - text \ = \ Encryption\ (Key, Plain - text) \tag{1}$$

$$Plain - text \ = \ Decryption\ (Key, Cipher - text) \tag{2}$$

Therefore, both legitimate parties, Alice and Bob should utilize the same secret key, either into the encryption or decryption process. One of the most famous symmetric algorithms is One-Time-Pad (OTP) algorithm. The OTP encryption technique was invented by Frank Miller in 1882 and then improved during several decades [4]. Generally, the OTP encryption contains the original plaintext, as well as a random generating code. The random code is supposed to have the same length of the original plaintext and should be randomly generated. The XOR operation will be applied between the plaintext and the random code to initiate the cipher-text that will be transferred into communication channels. Both the sender and the receiver should share the secret code to be able to convert the cipher text to the original plaintext.

1.1.2 Asymmetric Encryption

Asymmetric encryption (*Public-key encryption*) is based upon employing a public key during the communication between Alice and Bob. Asymmetric cryptography is essentially encrypting and decrypting a submitted message by two keys, a public key and private key. Transferring a message from Alice to Bob is performed by one of the mentioned keys separately either a public or a private key, and vice versa. One of the most widely used public-key cryptosystem is RSA. The RSA was invented by Ron Rivest, Adi Shamir, and Len Adleman in 1977, where the RSA derives its complicity from factoring a large number [5]. This number will produce large prime numbers that can be easily multiplied, but it cannot be determined the original prime numbers.

Later, several asymmetric encryption algorithms are used in different platforms. Moreover, those algorithms are based upon the complexity of mathematical calculations and two shared keys. Basically, the process of any Public-key encryption algorithm can be explained as follows:

$$D_P\big(E_S(M)\big) = M, \tag{3}$$

$$E_S(D_P(M) = M, \tag{4}$$

where *E* and *D*, are encryption and decryption processes. *M* is the plain text that should be sent by a legitimate sender and received by a legitimate receiver. Also, *S* and *P* represent sequentially private and public keys.

1.2 Quantum Cryptography

Quantum Cryptography (QC) was invented by Stephen Wiesner [6] in the early 1970’s. He started with using the conjugate of state in a linear vector, which is a tool that was used to support the QC. The QC assists the existing systems to improve the key exchange in the cryptography field. Quantum mechanics properties are consumed to offer an unconditional new theoretical system. Quantum Key Distribution (QKD) is the mechanism of creating a secret (*shared*) key between legitimate communicating parties in the quantum system. Moreover, the quantum communication prevents any eavesdropping by a third party (*Eve*), which is guaranteed by the Non-Cloning theory [7, 8].

Based on the emergence of using online transactions, sharing information, shopping online, and bank accounts, there is a high priority service that should be available with those needs. This service should be processed through a secure system without any interruption [9, 10]. Quantum key distribution offers this service, where quantum mechanics features are applied. In the QKD, two parties (*Alice and Bob*) obtain quantum states and then measure these quantum states. They communicate (*all communication from this point onwards is classical*) to determine the measurement results. These results can lead to initiate secret key bits, where some of these bits are discarded in a process so-called the sifting phase because the measurement settings were incompatible.

Furthermore, the communicating parties perform an error correction phase and then estimate security parameters, which describe the amount of information that might have been leaked by an eavesdropper. If the amount of information is above a certain threshold (*a percentage of uncovered qubits*), they will abort the communication as long as they cannot guarantee any secrecy whatsoever. On the other hand, they can apply privacy amplification to squeeze out any remaining information that affected by eavesdropper during exchanging the shared secret key if the unmatched information is below the threshold. Some of these classical communications must be authenticated to avoid the Man-

In-the-Middle attacks. Moreover, some portions of the utilized protocols can fail with negligible probability [11] [12].

1.3 Research Problem and Scope

The common implemented quantum key distribution protocols are mostly employing the classical communication as a second phase of the communicating channels. The reason behind using the classical channel is considered in two main points. First, during the quantum communications, there will be some different noises that would occur by the environment or an eavesdropper. These noises should reflect some errors on the submitted data. Moreover, Alice and Bob are supposed to correct this data into another channel (*classical channel*). Second, the exchanged data (*qubits*) during the classical channel communication is used to improve the qubits that are already sent and received by the end users. Also, using the classical channel in most QKD Protocols provides an authentication for the sender and receiver identities. This improvement varies from a protocol to another based upon the style, the mechanism of reconciliation, and correcting data.

The main issue that faces the existing QKD protocols is surrounded by improving the authentication between the legitimate communicators. Furthermore, most of the QKD protocols utilize heavy communications through the classical channel that will certainly cause a high chance of different attacks. Therefore, the security of each protocol will be failed by two factors. One of these factors is the Runtime-Execution, where the protocol will spend extra time to recover the errors during the quantum channels. Second factor, eavesdroppers can use the classical data to realize at least some of the needed information.

Moreover, the legitimate communicators will be unable to detect any attack because a heavy information traffic will be initiated between the sender and receiver. Thus, the simplicity of the authentication for the communicating parties is the main point in this research as well as the robustness of the proposed scheme.

1.4 Motivation behind the Research

There are several related studies that explain cryptography methods in different mechanism. Our research illustrates a mechanism of cryptography that is based on previous physics and computer science theories as well as providing an authentication. These motivations are explained as follows:

- The new scheme of the proposed algorithm was designed to stand against many weak points that have been seen in the QKD Protocols (*Literature reviews*), and the proposed protocol should treat the used mechanism in the most well-known protocols.
- The proposed QKD protocol utilizes two quantum communication channels, and there is no classical channel into quantum exchanges unlike other well-known QKD protocols.
- The core of the proposed scheme is based on the power of matrix techniques, which the preparation of qubits occurs through a huge matrix (*or matrices*), and the communicating parties use indices of the matrix to build the authentication phase.
- Correcting errors is built in the quantum system, unlike common QKD protocols where the error correction is initiated in a classical channel.

- The proposed protocol resists most popular quantum attacks such as the Man-In-Middle (MIMA) attacks [13], Intercept-Resend (IR) attacks [14, 15], and so on.
- The main advantage of the proposed protocol is approving the authentication between the communicators before exchanging any qubits (*plain-text*), where they begin submitting the content of the secret key into quantum channel.

1.5 Potential Contributions of the Proposed Research

The proposed scheme will assist the researchers to improve the quantum cryptography system, where the scheme will be applied in the classical system with quantum devices. Moreover, the proposed protocol uses a novel technique, which includes fulfilling the authentication between the communicating parties before submitting any valuable information. There is also no wasted time that usually happens when the whole submission fails. On the other hand, the most previous QKD protocols uses a classical channel without any authentication procedure. The novelty of the proposed protocol came from combining the physics theories with solid computer science fundamentals. The EPR Pair Paradox theory is one of the quantum physics facts, where Albert Einstein alongside his colleagues Boris Podolsky and Nathan Rosen were invented in 1935. The main idea of the EPR Pair Paradox is explained as a single photon in two different states. This theory has been experimented in physics labs, and the conclusion shows the EPR (*entangled*) state has fastness of initiation and termination. Furthermore, the proposed protocol considered these advantages to be utilized during the authentication phase.

In addition, the proposed QKD protocol uses a new algorithm that uses different mechanisms compared with the studied QKD protocols. This algorithm executes a huge data to create a secret key. The whole secret key that is created by the proposed scheme will be provided without any errors. The proposed QKD protocol also has approved the possibility of using the EPR theory within authentication processes. Moreover, using the EPR theory; especially during authentication request, will provide a quick connection between the legitimate parties before exchanging any data. Furthermore, the proposed protocol utilizes quantum theories that have been approved as stable theories. For instance, an entangled state creates particles in certain state, where these particles should be read and measured by a two-dimensional space vectors from the EPR source. Using entangled states should be in limited communications, because these states have ability to stay alive in a short time as well as sensitivity of EPR states.

Furthermore, combining between the physics theories and the mathematical functions encourages researchers to improve the existing algorithms and security applications, so that the classical system can use some of the quantum devices. More precisely, improving the classical system to a quantum system requires partially improvement, where the classical system can use some gates or algorithms based on the quantum theories. Meanwhile, using a hybrid system (*classical and quantum*) may help to improve the next generation of technology better than using a classical system or jumping to whole quantum system in one time. Additionally, the proposed QKD protocol is applicable even in the classical system, where some quantum devices and detectors are needed. The quantum system can be restricted in a small portion of the used system, which the user can communicate into a classical system, but the secret key is created by the quantum system.

CHAPTER 2: LITERATURE SURVEY

Quantum Key Distribution (QKD) is a technical mechanism to create a secret key based on the law of physics. In the cryptography, the law of physics explains the measurement modules of the photons, which are controlled naturally by only the environment. Usually a pair of legitimate participants will exist to establish a full communication. Alice and Bob are the common characters, whereby Alice is a sender as well as Bob is a receiver. The illegal interruptions usually are made by Eve, who is an eavesdropper. Sharing a secret key between Alice and Bob is designed to be a long string of bits. These bits are corresponding to the length of the original message (*plain-text*). In addition, the created secret key is utilized in one of the symmetric cryptography algorithms that is called One-Time-Pad (OTP) protocol [4]. The OTP algorithm requires a long secret key that basically should be as long of bits as the original message. Then both the secret key and original message will be XORed to produce the cipher-text [16]. Thus, the security of encoding a message by OTP protocol is very robust as long as the secret key length is unexpected.

Although using quantum key distribution protocols to create a secret key is still not publicly available, the quantum key distribution has proved its stability and secrecy in several studies [17-19] and laboratories [20] [21] [22] [23]. One of the physics fundamentals that supports the QKD protocol usage is the Non-Cloning theory [8, 24, 25]. The Non-Cloning theory provides an alteration to the end users in case any interruption occurs in the quantum system. In other words, the quantum system will be protected by destroying the submitted data if this data (*quantum bits*) was measured. Furthermore, assisting the natural theory (*The Non-Cloning theory*) with algorithmic (*mathematical*) equations will provide a robust system that has the ability to stand against the common security attacks [26]. Essentially, the usability of the created QKD protocol is very important to conclude a stable protocol, which provides a minimum rate of the Runtime-Execution. To explain the methodology and the usability of quantum key distribution protocol, here are some of the well-known QKD protocols that will be exhibited as follows:

2.1 The BB84 Protocol

2.1.1 The history of the BB84 Protocol

In 1984, Charles Bennett and Gilles Brassard were introduced to the BB84 protocol [27]. The BB84 protocol is based on the security approved by the non-cloning theorem. This security comes from supporting unconditional secret keys and efficiency of detecting the eavesdroppers over the quantum channel [28]. The BB84 protocol requires pair of communication channels, the first channel is a quantum channel (*submitting qubits*) and the second is a classical (*submitting bits*) channel. The quantum channel is applied into either a free space (*earth atmosphere or space*) or fiber optic cable while the classical channel should be by any communication system (*e.g. internet*) that unnecessarily needs to be secure [29].

The functionality of the BB84 protocol is based on the photon movement (*polarization*) into different four states in the superposition. The single photon is created by one of the legitimate parties into quantum devices, and then the created photons will pass through one of the two bases detectors. These bases are either rectilinear basis ⊕ where photons are polarized at angle 0° (→) or 90° (↑), or diagonal basis ⊗ where 0 is represented by photons polarized at 45° (↗) and 1 by photons polarized at 135° (↖)[30]. Bennett and Brassard in [31] mentioned that the conventional cryptography is unsecure if the secret key is employed more than once. As a definition, the power of QKD protocol is combined into three aspects: The first aspect relies on the neutrality of the physics law, where the photon will by destroyed in case detecting any interruption. The second aspect is a photon conversion that will be computed mathematically and gives a hard guess to both created functions and algorithms. The third aspect is the previous aspects when will be gathered in computer system, and then is applied in different devices and hardware.

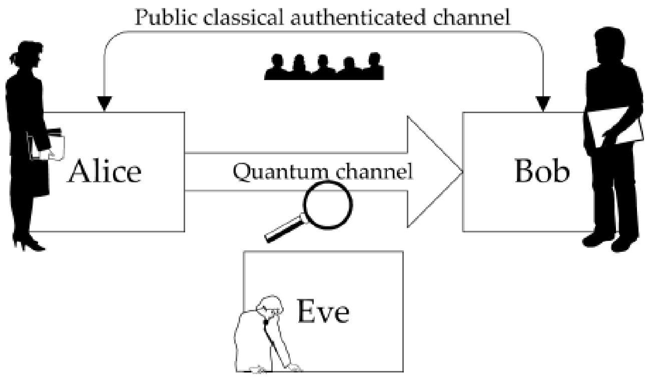


Figure 2. The process of transmitting a message through quantum key distribution protocol between Alice and Bob with possibility to be eavesdropped by Eve.

2.1.2 The functionality of the BB84 protocol

The BB84 protocol is considered the background of QKD protocols, in which most of the invented QKD protocols come from the general methodology of the BB84 method. Practically speaking, the BB84 protocol is based on the polarization of photon states that are unconditionally secure [32]. The process of establishing a secret key between Alice and Bob is explained as follows:

1. Alice creates a random number of bits (n) that mostly corresponds to the length of the plaintext needed to transfer between the legitimate parties. These random bits can be generated in a classical mode.

1 0 0 0 1 1 0 0 1 0

String of Bits that Is Used to Initiate a Random Qubits

2. Alice flips the coin into another operation in order to determine the single bit, in which bases will pass through. Therefore, Alice is unable to determine the bases and the bits in each submission as shown in Table (1).

Table 1. The bases in the BB84 protocol

States/ Basis	$\oplus$	$\otimes$
$\vert 0\rangle$	$\rightarrow$	$\nearrow$
$\vert 1\rangle$	$\uparrow$	$\nwarrow$

3. Alice sends the initiated states to Bob through the quantum channel based on step (2), where the submitted photons polarization should be in one of four states. These states are 0^{o}, 45^{o}, 90^{o}, and 135^{o} angle, where each one angle has a certain reflection [33] as illustrated in Table (2).

Table 2. The procedure of submission for the BB84 protocol

Alice sends n random bits in random bases						
Bit number	0	1	2	3	4	5
Alice’s random bits	0	1	1	0	1	1
Alice’s random bases	+	+	×	+	+	+
Alice sends	→	↑	↖	→	↑	↑

4. Bob measures the upcoming photons by a quantum device detector and then creates a random measurement on the received photons, which these photons will represent pairs of bases as shown in Table (3).

Table 3. The procedure of received photons in the BB84 protocol

Bob receives n random bits in random measurements						
Bit number	0	1	2	3	4	5
Bob’s random bases	×	+	×	×	+	×
Bob observes	↗	↑	↖	↖	↑	↗
Bob’s bits	0	1	1	1	1	0

5. Bob reads the raw secret key that is produced by the measurement in step (4), and Bob then announces the raw key through a classical channel to Alice.

6. Both Alice and Bob start estimating the errors that may be caused by Eve, so that there are many error correction protocols that are used in the BB84. The raw key is the process, where Alice and Bob compare the matched bits and discard the uncorrelated data that is well-known as a shifting procedure. The sifting phase enhances detecting any attempts by Eve, where the legitimate parties can realize if an eavesdropper tried to gain any information or not.

Table 4. The reconciliation phase in the BB84 protocol

Alice and Bob publicly compare bases used						
Bit number	0	1	2	3	4	5
Alice’s random bases	+	+	×	+	+	+
Bob’s random bases	×	+	×	×	+	×
Agreement		✓	✓		✓	
Shared secret key		1	1		1	

2.2 The B92 Protocol

B92 is a QKD protocol that was presented by Charles H. Bennett in 1992. The protocol was designed in non-orthogonal polarization photon or in low-intensity light pulse [34]. The protocol is like the BB84 protocol, except the BB84 protocol uses two bases and four states unlike the B92 protocol that uses two states. The B92 protocol has two channels to communicate between two legitimate parties. The first channel is a quantum channel, where Alice submits photons into different states. The second channel is a classical channel (*e.g. Internet*), which is utilized to confirm the received and submitted qubits by the communicated participants. The classical channel is also employed to correct the errors that occur by the environment or an eavesdropper.

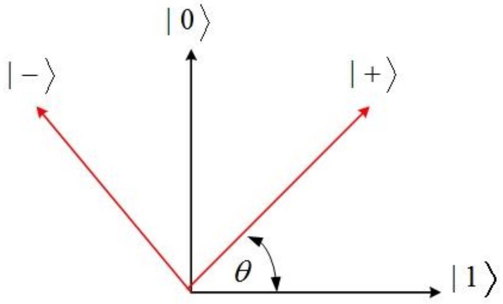


Figure 3. The bases of the B92 protocol polarization

2.2.1 The functionality of B92 protocol

There are several steps to initiate a secret key in the B92 protocol. These steps include the procedures of quantum submissions and classical exchanging. The quantum submissions are based on submitting a vector of qubits through the quantum channel. On the other hand, the classical channel provides an ability to exchange information between the communicated parties for confirming and correcting the quantum communications. The steps are briefly explained in the follows:

- Alice initiates a vector of random bits $\omega \in \{0,1\}^n, where\ n > N$, (*N is the length of the created secret key*) and then sends to Bob in two states $\{|0\rangle, |+\rangle\}$.
- Bob will create a string of random numbers and decides, in which basis will choose; if the random number is (0) he will use ($\otimes$), otherwise he will use ($\oplus$).
- Bob measures the upcoming states $\{|0\rangle, |+\rangle\}$ into random bases $\{\otimes, \oplus\}$ [10].
- Bob is ready to create his string of qubits (*Vector Test T*) $T \in \{0,1\}^n\ n > N.$ by following certain roles: if Bob's measurement equal to $|0\rangle\ or\ |+\rangle$ then the value of *T* = 0, if Bob's measurement is equal to $|1\rangle\ or\ |-\rangle$ then *T* = 1.

The above steps explain the quantum exchanges between two legitimate parties. Later, more critical procedures will be applied in the final phase to provide the secret key. In the classical channel, Alice and Bob should confirm their submissions and ignore any untrusted qubits. The classical communication is established over a public channel to guarantee an error free of exchanged data that occurred during the quantum key distribution process. Furthermore, the reconciliation phase reveals some errors that may have occurred by eavesdropping or an environment during photon submission. The concluded error rate will judge and control the amount of bits that will be distilled [35]. In other words, there is a limit rate that allows both parties to continue the correction phase or not. Therefore, if the error rate has a high number of interrupted qubits, both sides will decide to ignore the whole received qubits (*or vice versa*).

Eve's ability to disrupt the photons is very critical during building a secret key, but as mentioned in [34, 36], there are many considerations that make the B92 or non-orthogonal submission protocol more reliable and robust against Eve's attacks. Moreover, the non-orthogonal states are not necessary to be non-orthogonal pure states $|p_0\rangle\ and\ |p_1\rangle$, but also it is possible to be any non-orthogonal mixed states $|m_0\rangle\ and\ |m_1\rangle$. More precisely, the Man-In-the-Middle (MIM) attack is still a huge challenge for this protocol, because Eve is still able to impersonate one of the communicated parties. The public channel that both (*Alice and Bob*) use to confirm the received photons through quantum channel is still a weak point. Also, there is 50% of losing or leaking these date to an eavesdropper [35]. Meanwhile, the B92 protocol is considered more secure than the BB84 protocol by many scientists and experts.

2.3 The Coherent-One-Way Protocol

Coherent One-Way (COW) protocol was introduced by Damien Stucki, Nicolas Brunner, Nicolas Gisin, Valerio Scarani, and Hugo Zbinden. The COW protocol is well-known by using decoy states through the quantum channels. The decoy states increase the resistance of the control against IRA attack. Moreover, the COW protocol was designed in a unique scheme, where the COW scheme is divided to three sections. The first section is more secure, where Alice can use a mode-locked laser μ to pulse a photon. These pulses emit in fixed time τ with the ability to block some pulses by Alice. Functionally, the logical bits are encoded by a sequential two-pulse as shown in (*equation 5 and 6*)[37]. The second section is data line, which represents transmitting the pulses into optical fibers $\propto = 0.2\, dB/km$. After that, Bob starts distinguishing the upcoming pulses by using interferometer D_B. Bob should obtain one of the non-orthogonal states:

$$|0_A\rangle = |\sqrt{\mu^{e^{i(2k-1)\varphi}}}\Big\rangle |0\rangle_{2k} \tag{5}$$

$$|1_A\rangle = |0\rangle_{2k-1}|\sqrt{\mu^{e^{i(2k)\varphi}}}\Big\rangle \tag{6}$$

Where, $\propto = \sqrt{\mu t t B}$.

Simply, Bob tries to discriminate between $|0_B\rangle$ and $|1_B\rangle$. Later, Bob communicates with Alice to announce the detected photons. The error rate, in this line, is impossible especially if the detector is perfect. There is also no need for a random number generator. The third section represents the monitoring line, where the quantum coherence plays a role. The pulses will be extracted at Bob's beam-splitter, where α_j is the amplitude of pulse j. There are two values of 0 or $\mu t(1 - t_B)$ when the pulse enters the interferometer. If the both α_{j+1} and α_j are *non-zero*, then $\alpha_j = \alpha_{j+1}$. Otherwise, if α_{j+1} and α_j are *zero*, then $|D_{M1}|^2 = |D_{M2}|^2 = \frac{1}{2}\mu t(1 - t_B)$ where,

$$|D_{M1}\rangle = |i\frac{\alpha_j + \alpha_{j+1}}{2}\Big\rangle \tag{7}$$

$$|D_{M2}\rangle = |\frac{-\alpha_j + \alpha_{j+1}}{2}\Big\rangle \tag{8}$$

So, the probability of detecting both photons is $\frac{1}{2}$.

2.3.1 The COW Protocol Scheme

1. Alice initiates a string of binary, which the bits (0) and (1) are assigned with probability $\frac{\mathbf{1-f}}{\mathbf{2}}$, and the decoy bits will be with probability *f*.
2. Bob receives the string of binary and extracts each single bit by time detection. DM detector is used for generating the raw key, and DM_2 detector monitors the security.
3. Alice reveals all the decoy states, and Bob then avoids all Alice's raw key that were detected by sifting phase.
4. Bob measures the detections of compound submitted photons at D_{2M}, and Alice computes the coherence of photons into V_{1-0} and (V_d) as follows:

$$V = \frac{p(M_{D1}) - p(M_{D2})}{p(M_{D1}) + p(M_{D2})} \tag{9}$$

5. Lastly, Alice and Bob apply an error correction phase as well as a privacy amplification to conclude a secret key [38].

The Coherent-One-Way protocol is specialized by using a decoy state during photon submissions, which is well-known for preventing the Photon-Number-Splitting attack.

2.4 The S09 Protocol

S09 protocol was introduced by Eduin Esteban Hernandez Serna in 2009 [39]. The S09 protocol is based on public and private key cryptography, which utilizes two quantum channels of communication. The S09 protocol may not need a reconciliation phase into the process of verifying the participants at each side of communications. The whole phases in this protocol are divided to three phases, which are included preparation, measurement, and verification and key derive. The S09 is a secure protocol because the multiple of exchanges that are created by Alice and Bob during creating the secret keys.

The variation between the S09 and the BB84 protocol is shown into a qubit transmission between Alice and Bob in the quantum channel, where the BB84 protocol uses four different states, unlike S09 protocol that can use any arbitrary states. The S09 protocol is explained in several steps as follows:

2.4.1 Phase one

- Alice initiates a random string of bits a, and she then picks up random bases to generate a string of qubits *s*.
- Alice sends the *s* of qubits to Bob into a quantum channel.
- Bob builds a string of binary g with the same length of *s*.
- Each binary of g_n will be tested as follows:
    - $If\ (g_n\ ==\ 1)$ → Bob applies the *XZ* or *ZX* gate to get G_n.
    - Bob then sends the G_n binary to Alice.
- Alice receives the binary string G_n and measures each qubit by her first initiated bases for generating a string c.
- Alice sums the string $c \otimes$ with the random bits in the previous step to obtain Bob's random binary g.

2.4.2 Phase two

- Bob creates a binary string g_2 with *N* bits long.
- Each bit of g_2 will be under a condition:
    - $If\ (g_n\ ==\ 1)$ → Bob uses one of *XZ* or *ZX* gates to build k_2.
- Bob sends k_2 qubits to Alice.
- Alice measures k_2 in *t* bases and generates a string c_2.
- Alice sums a string $c_2 \otimes$ with the random bits and obtains the string M_2.

2.4.3 Phase three

- Bob creates a string of binary M_3 in *N* bits long.
- Each bit of M_3 in *N* will pass through:
    - If $(M_3\ ==\ 1)$ → Bob applies one of *XZ* or *ZX* gates to generate k_3.
- Bob sends k_3 qubits to Alice.
- Alice measures the k_3 by t bases to provide a string c_3.
- Alice sums a string $c_3 \otimes$ with random bits to build M_3.
- Alice compares all the binary strings *c* and *M*.

The S09 protocol was created to be robust against some common quantum attacks. The Man-In-The-Middle (MIM) attack is one of these attacks, where the S09 protocol have proved to stand against. On the other hand, the S09 protocol is one of the complicated protocols because the qubits are exchanged multiple times during the communication channels between the parties.

2.5 The S13 Protocol

The S13 protocol was introduced by Eduin H. Serna in 2013 [40]. This protocol was designed to share a secret key with the same length of the transmitted qubits. There is a variation between the BB84 and S13, which is included in the classical communication by using a random seed and asymmetric cryptography. The S13 protocol contains two communication channels, and these channels are the quantum and classical channels.

2.5.1 The quantum channel

- The quantum channel reflects exchanges of the encoded photons into four states $|0\rangle$, $|1\rangle$, $|+\rangle$, and $|-\rangle$, of which these states are formatted into two bases B_1 $=\{|+\rangle, |-\rangle\}$, and B_2 $=\{|0\rangle, |1\rangle\}$.
- Alice initiates two random strings S_N and i_N that will be identical to the length of the secret key, and the key should be shared between Alice and Bob.
- Alice starts building the qubits from gathering the two random strings $|\varphi_{S_N i_N}\rangle$ and then sends the built qubits to Bob through the quantum channel.
- Bob creates a random string of binary m_N and measures the upcoming qubits by corresponding bases B_{mN} to obtain the binary string a_N.
- Bob sends a sequence of basis m_N into classical channel.
- Alice matches the received basis m_N and S_N and sends $L_N = S_N \otimes m_N$ to Bob.
- Alice and Bob share a random binary string x_N (*considered as a seed*).

2.5.2 The classical channel

- Alice and Bob will exchange many binary strings with applying to a different function of f as follows:

$$f(z,x,y) \coloneqq f(x) = \begin{cases} x, & z = 0 \\ y, & z = 1 \end{cases} \tag{10}$$

- Alice sums $i_N \oplus j_N$ to obtain y_N and then is submitted to Bob.
- Bob encodes m_N into u_N and v_N as:

$$u_N = n_N \oplus f(m_N, a_N, b_N \oplus y_N), \tag{11}$$

$$v_N = n_N \oplus f(m_N, b_N, a_N \oplus y_N). \tag{12}$$

So, Bob Obtains strings of u_N and v_N that will be sent to Alice.

- Alice sums $t_N \oplus f(s_N, (1 \oplus i_N) \oplus u_N, j_N \oplus v_N)$ and decodes m_N to obtain a private string m_N.
- To process the private reconciliation, Alice compares s_N and m_N to obtain $l_N = s_N \oplus m_N$.
- Bob obtains s_N by summing $m_N \oplus l_N$, and applies:

$$f(l_N, a_N, b_N \oplus y_N) \equiv i_{N,} \tag{13}$$

$$f(l_N, a_N \oplus y_N, b_N) \equiv j_N. \tag{14}$$

In perfect condition of the communication between Alice and Bob, both will share four secure keys $s_N, m_N, i_N, and\ j_N$. This secure key represents the final secret key.

2.6 The SARG04 Protocol

This protocol reflects the originality of the protocol BB84. SARG04 was introduced [41] by Scarain, Acin, Ribordy, and Gisin in 2004. Inventing the SARG04 protocol came after using four states in the BB84, and the authors thought that utilizing the four states could build a new protocol. This protocol would be more robust than BB84; especially when weaken laser pulses are used instead of a single photon source. The authors worked on the SARG04 to be more efficient against the PNS attacks. Furthermore, SARG04 and BB84 are essentially equivalent to each other in the quantum communication phase, but the difference is shown in the encoding and decoding phase of classical information.

The SARG04 protocol is an experiment to solve some situations found in the BB84 protocol such as information that is produced by weak pulses and received by an incomplete detector [42]. Even though the SARG04 came with a new vision, it respects the BB84 in its instructions. For instance, when Alice starts to match the key with equivalent qubits from Bob, the bit error rate could reach to $vs/2$ or more (*precisely, it is a probability until* ½). The difference can be seen occurring when the detection rate is measured in the SARG04. The detection rate will increase in the presence of error, unlike with BB84 [43].

To show the sequential steps between two legitimate parties (*Alice and Bob*), the SARG04 protocol can be summarized in a one-way communication, where a *V*-Photon source (*V* = *1, 2*) as follows:

Step 1: Alice creates an n of signals that starts randomly with each one of the four sets (*states*), and Bob should receive one of the two states.

Step 2: When the signal reaches to Bob, it should be measured randomly in two bases by a quantum detector. If the signal measurement does not match or could not be measured, Bob informs Alice about ignoring this signal.

Step 3: Alice reports each created signal of photon and the state of the photon in the superposition set. Bob then matches the result by two states. If the result was proven as an orthogonal for one of the states in the set, the other state has already been sent. On the other hand, the match will not be an orthogonal to each state in the set. In this case, Bob knows that the result is not incisive, so that he will tell Alice about the result either matched or not.

Step 4: Some bits are chosen randomly to be tested and informed of their positions by Alice, after which Bob will figure out the bit error rate e_y, so if the measurement was very high that leads to the cancelling of the protocol.

Step 5: According to the previous step, Alice and Bob keep the only conclusive untested bits that will be utilized specifically during bit error correction and privacy amplification [44].

2.7 The EPR Protocol

The EPR Pair Paradox protocol was invented by Einstein, Podolsky, and Rosen who presented the thought experiment in 1935 [45-47]. The main thought utilizes three states of polarization with considering $|\theta\rangle$, where the polarization state of photon linearly polarized at angle θ . More precisely, the EPR deeply is pair of particles that can be separated even at great distance, so that both show a paradoxical (*action at a distance*).

To explain the nation of EPR clearly, when one photon is measured in the right side, the outcome can be a vertical linear polarization state $|0\rangle$. On the other hand, the measurement will be a horizontal linear polarization state $|\frac{\pi}{2}\rangle$ at the left side and vice versa. The EPR is one of the four Bell states as follows [48, 49]:

$$|\psi_1\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle) \tag{15}$$

$$|\psi_2\rangle = \frac{1}{\sqrt{2}}(|00\rangle - |11\rangle) \tag{16}$$

$$|\psi_3\rangle = \frac{1}{\sqrt{2}}(|10\rangle + |10\rangle) \tag{17}$$

$$|\psi_4\rangle = \frac{1}{\sqrt{2}}(|10\rangle - |10\rangle). \tag{18}$$

In 1991, Artur K. Ekert proposed the EPR protocol that is completely based on using an entanglement between two remote parties. There also are few modifications that have been occurred since the first publication of EPR became famous. Hwang et al. in [50] explained some of these modifications of EPR protocol. The process of EPR protocol is shown in sequential steps that demonstrate the original protocol as follows [51]:

1. Alice creates a sequence of EPR photons (*Entangled qubits*) *n*, where she keeps one photon in the memory and sends the other photon to Bob.
2. Both communicators choose a random sequence of bases, where these bases are utilized for measuring particles at each side of communication.

Table 5. The measurements in the EPR protocol during an exchanging phase

Alice and Bob measure in each of their random bases						
Bit number	1	2	3	4	5	6
Alice’s random bases	×	×	+	+	×	+
Alice’s observations	↗	↖	→	↑	↗	→
Bob’s random bases	×	+	+	×	×	+
Bob’s observations	↗	→	→	↗	↗	→

3. Alice and Bob match the outcomes of the photon measurement in public and keep just the qubits that were measured in the same basis.

Table 6. The measurements in the EPR protocol during the reconciliation phase

Alice and Bob PUBLICLY compare their bases						
Bit number	1	2	3	4	5	6
Alice’s random bases	×	×	+	+	×	+
Public channel	⇳	⇳	⇳	⇳	⇳	⇳
Bob’s random bases	×	+	+	×	×	+
Agree	✓		✓		✓	✓

The remaining steps of the EPR protocol includes the decision that will be made by the communicating parties. The public channel will be the next choice to ignore errors that may have occurred during exchanging the qubits into the quantum channel.

2.8 The Differential Phase Shift Protocol

Differential Phase Shift (DPS) Protocol [52] was introduced by Kyo Inoue, Edo Waks, and Yoshihisa Yamamoto in 2002. The DPS is based on non-orthogonal four states, which Alice’s photon splits into three pulses and randomly modulated. Furthermore, Bob measures the upcoming photons in a differential phase. As mentioned in [53] the DPS protocol is more convenient for a Fiber-Optics transmission and offering a key creation efficiency higher than the BB84 protocol.

The DPS protocol is technically utilized to create a secret key between two parties. The protocol starts at the sender side when the single photon will be divided to three paths (*a*, *b and c*). The divided photon then will be recombined by a beam splitter (BS) or an optical switcher (SW) as illustrated in Figure (4). Moreover, the time delay between *a*, *b* and *b*, *c* is equal, so that the recombined photon should be converted to ($0 \mid\mid \pi$). In addition, the incoming photons from Alice to Bob are divided into two paths and recombined by a (50:50) beam splitter. The DPS protocol procedure is briefly explained in the following steps:

- Alice sends a single photon from (*a*) to the short path in Bob's side.
- A photon pushes through (*a*) to the long path in Bob, and through (*b*) to the short path in Bob.
- A photon pushes through (*b*) to the long path in Bob, and through (*c*) to the short path in Bob.
- A photon pushes through (*c*) to the long path in Bob.

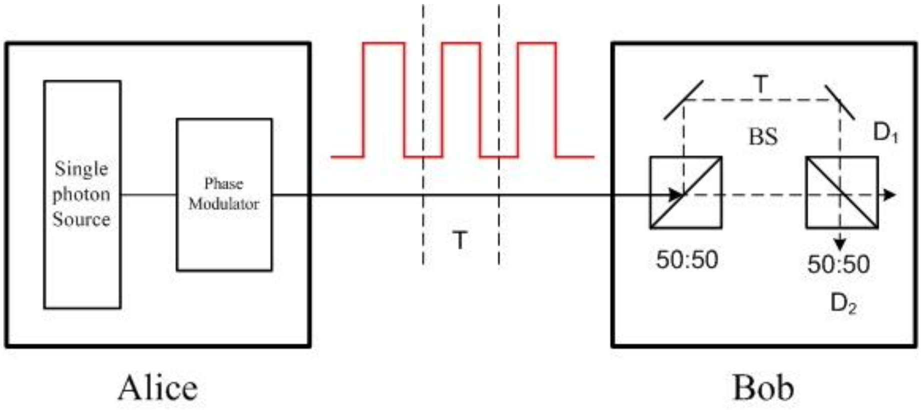


Figure 4. The DPS protocol scheme between two legitimate parties (*Alice and Bob*).

In the first part of processing, two probabilities are interfered in step (2) and (3), where the phase difference (0 or $\pm\pi$) depends on Alice's modulation. Furthermore, each of the detectors clicks on (0) and the other on ($\pm\pi$) are a phase difference. Lastly, when Bob's detectors click, Bob just records the time and the clicked detector. In the classical communication, Alice also knows the clicked detector at Bob.

2.9 The KMB09 Protocol

In 2009, KMB09 protocol was presented in [54] by Khan, Murphy, and Beige, which was designed to be robust against photon number splitting attacks. Khan *et. Al*, described the protocol as being between two parties (*Alice and Bob*) and an eavesdropper (*Eve*). Alice and Bob then must use two states of bases ($e\ and\ f$), where the applied condition should be in different indices i when both use the same basis. Moreover, i index is publicly announced between two legitimate parties, which can be pointed to Alice's prepared indices as i, and Bob's measured indices as j.

In the KMB09 protocol, the authors have tried to create a QKD protocol that is capable to stand against the Intercept-Resend (IRA) attacks. Moreover, the KMB09 was created when the other QKD protocols were employed to a few kilometers, but after that, the system error rate exceeded the eavesdropper's presence [55]. Also, the KMB09 was optimized by testing Quantum Bit Error Rate (QBER) and Index Transmission Error Rate (ITER). Next steps will briefly explain the KMB09 design as follows:

1. Alice generates a random sequence of classical bits and then randomly specifies each bit a certain index ($i = 1, 2 \ldots N$).
2. Alice then sends the prepared bits in single photons into $|e_i\rangle$ or $|f_i\rangle$ to Bob.
3. Each incoming state measured by Bob should be randomly switched between the basis e and f.

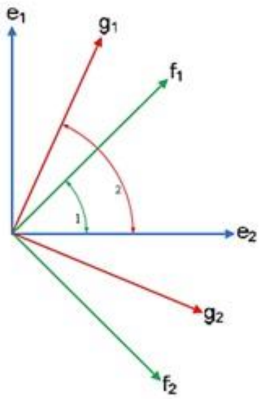


Figure 5. The polarized states that are used by Alice, Bob, and Eve.

4. Alice in public communication announces Bob about the random sequential indices i to create the secret key.
5. Bob translates the measurement outcomes.

6. Bob then communicates with Alice in public for the photon measurements, which were successfully received and have obtained the secret key.
7. Alice and Bob can determine whether Eve was eavesdropping to their communication or not by calculating the equations of the ITER and QBER as follows [56].

$$P_{ITER} = 1 - \frac{1}{2N}\sum_{i=1}^{N}\sum_{k=1}^{N}[|\langle g_k|e_i\rangle^4 + \langle g_k|f_i\rangle^4|], \tag{19}$$

$$P_{QBER} = \frac{2N - \sum_{i=1}^{N}\sum_{k=1}^{N}[|\langle e_i|g_k\rangle^4| + |\langle f_i|g_k\rangle^4|]}{4N - \sum_{i=1}^{N}\sum_{k=1}^{N}[|\langle e_i|g_k\rangle^2| + |\langle f_i|g_k\rangle^2|]^2}. \tag{20}$$

Furthermore, the polarization of one photon is initiated into multi-dimensional states, which is based on orthogonal and non-orthogonal bases.

The KMB09 protocol was designed to be under ideal conditions, where it is impossible for Alice and Bob to have different indices while they use the same basis. This protocol is more robust against any eavesdropper who tries to hide his/her presence. Also, the strong correlation between the QBER and ITER makes the eavesdropper produce a distinct signature that is easy to be detected.

CHAPTER 3: RESEARCH PLAN

According to the previous QKD protocols, there are many weaknesses that give the eavesdroppers a chance to attack any transmitted data (*plain-text*). The tremendous weak point lies on an authentication property that must be approved between the communicating entities before exchanging any information. Moreover, many QKD protocols utilize a public (*classical*) channel to correct errors that might happen during the quantum communications. This public channel is mostly used without any special security protocol, which could be a huge gap to processing a secret key.

3.1 The Designed QKD Protocol

Based on the studied QKD protocols, a new quantum key distribution scheme was developed to stand against the common quantum attacks as well as providing an authentication link before starting any exchanges. Moreover, the protocol is named AK15 protocol and presented at the IEEE LISAT conference in 2015. The proposed protocol was designed to include two quantum channels. One of these channels is an EPR channel that is based on initiating an entangled state [57]. The other channel is a quantum channel, where the sender and the receiver can submit the data to create a secret key.

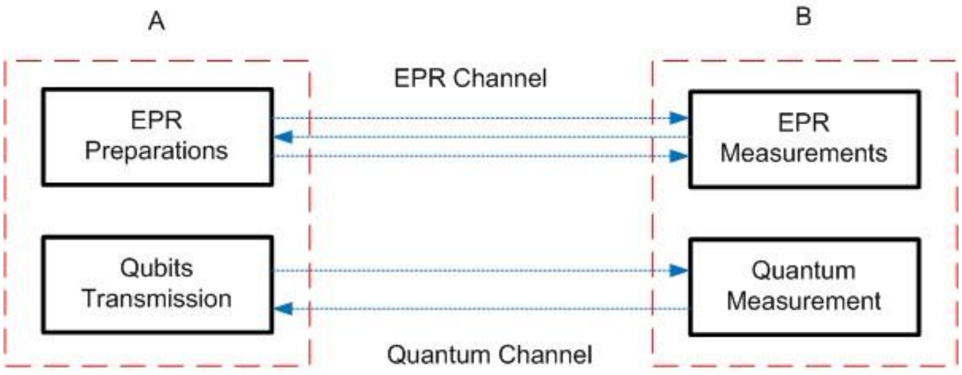


Figure 6. The proposed QKD protocol (*AK15*) scheme between two legitimate parties.

Essentially, the proposed protocol avoids using any public channels except into the EPR channel, which is a small submission of two binaries. These two binary bits are considered as a slight transmission between the sender and the receiver to confirm and release the type of used quantum gates. The protocol begins with preparations by Alice (*the sender*), which sorts the converted plain text into a matrix. This matrix should be filled by data into a lower-triangle matrix, the decoy states into an upper-triangle matrix, and the diagonal line. The diagonal line should be filled after summation to result even rows in the whole matrix.

$$\begin{pmatrix} \omega_{11} & \cdots & \beta_{ij} \\ \vdots & \ddots & \vdots \\ \varphi_{ij} & \cdots & \omega_{ii} \end{pmatrix}$$

Where the matrix may have a 2^n of qubits, ω is the parity states that convert the rows of the matric to even rows, φ the original data that will be initiated as secret key, β is decoy states that will be created randomly by Alice, and $\{i \ and \ j = 1,2,3, \dots \dots . . n\}$.

Based on the previous preparation, Alice can initiate an EPR pair string that contains the following: initiating time t_1, number of used matrices $(if \ any \ i \ = \ 1, 2 \ \dots \ N)$

n, size of matrix (*rows* (a) = *columns* (b)) *m*, string of diagonal parity *p*, number of used states (*dimension of particle*) s, row indices R, and time termination *t*$_2$. Moreover, the EPR string will collapse when one of the communicating parties starts measuring upcoming photons.

$$Open\ key = \{t_1 \quad n \quad m \quad p \quad s \quad R \quad t_2\}$$

During the EPR submission, Alice should communicate with Bob by a public channel. This public channel will be only utilized to send one string of two bits. Each two bits reflects a quantum gate that should be used by Bob. The two bits will be configured as follows:

$$|\Phi +\rangle\ unitary\ operator$$

$$|\Phi -\rangle\ Z\ gate\ (change\ a\ sign)$$

$$|\Psi +\rangle\ X\ gate\ (swap\ order)$$

$$|\Psi -\rangle\ Z\ and\ X\ gate.$$

Therefore, Bob should have the right outcomes after the whole teleportation process. If there are any errors detected by both parties, starting over is the only way to avoid any eavesdroppers.

3.2 The proposed Protocol Scheme

The proposed QKD protocol employs two quantum observables. The polarization is one of these observables that can be used in the quantum channel. The second observable is an entanglement state of particles in the EPR channel, where each particle should be one of the Bell states. The proposed protocol includes several sequential steps to create a secret key. These steps are processed in two levels of communications as follows:

3.2.1 Authentication Phase

1. Alice creates a sequence of EPR pair *n* (*Non-Random*) that is based on data filled in the prepared matrix (*or matrices*) in quantum phase and then submits to Bob. This submission will be as a string of qubits, where Alice keeps one photon in the quantum memory and sends the other to Bob.

$$|\varphi\rangle = \alpha|0\rangle + |1\rangle, \qquad unknown\ state \tag{21}$$

$$|\Psi\rangle = \frac{1}{\sqrt{2}}(|01\rangle \pm |10\rangle), Entangled\ state \tag{22}$$

$$|\Phi\rangle = \frac{1}{\sqrt{2}}(|00\rangle \pm |11\rangle).\ Entangled\ state \tag{23}$$

2. Bob receives the EPR string in a certain time, and no matter who measures first, because the particle will collapse on the same state whether Alice or Bob started measuring. These measurements will be in the Bell states as follows:

$$\sigma_x = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, \tag{24}$$

$$\sigma_z = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}, \tag{25}$$

$$\sigma_y = \begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix}. \tag{26}$$

3. After measuring the whole EPR string, Bob will decide if the qubits are still secure or the qubits were compromised by either eavesdropper or the environment. If the outcomes are separated (*Alice's photon with the unknown-photon*), the conclusion will be in entangled states between Alice's states and the unknown states. In this case, the original entanglement will be broken as well as be one of the superposition states.

$$|\varphi\rangle \otimes |\Psi +\rangle \cong \frac{1}{\sqrt{2}}(|\Phi\rangle + |\Psi\rangle + |\Psi\rangle + |\Phi\rangle). \tag{27}$$

This occurred after dropping the photons by Bob.

4. The measurements in the Bell states will physically effect Bob's particles and will separate the photons.

3.2.2 Quantum Phase

1. Alice submits the EPR and data qubits simultaneously to Bob for reducing the Runtime-Execution. The date qubits should be submitted in a two-dimensional photon (*or more*), and this photon will be polarized in two bases $(|\Psi \pm\rangle, |\Phi \pm\rangle)$ and four states $(|0\rangle, |-\rangle, |1\rangle, and\ |+\rangle)$.

$$\{|\uparrow\rangle \quad ... \quad |\rightarrow\rangle \quad ... \quad |\downarrow\rangle\}$$

2. Bob will receive a sequence of qubits and will use well-known measurement based on the EPR communication outcomes in the Bell state.
3. The secret key should be extracted and fully secure, and both parties will know the secret key without need to any public (*classical*) communications.

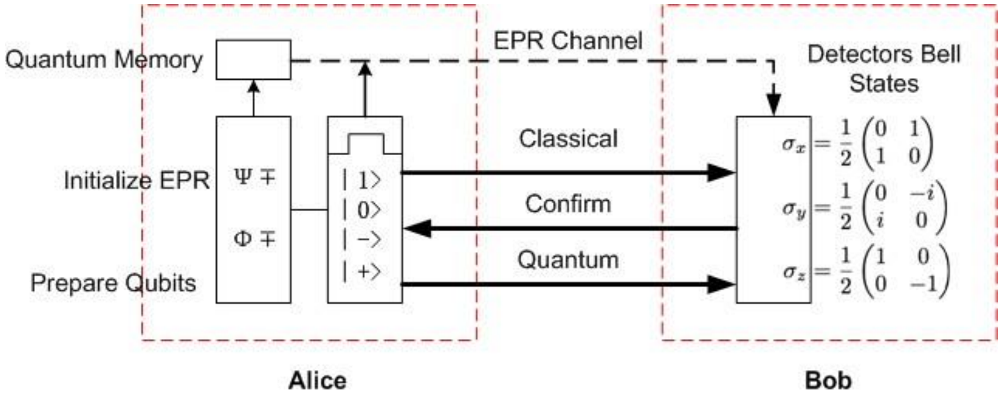

Quantum Memory
Initialize EPR
Prepare Qubits
Ψ ∓
Φ ∓
| 1>
| 0>
| ->
| +>
EPR Channel
Classical
Confirm
Quantum
Detectors Bell States
$\sigma_x = \frac{1}{2}\begin{pmatrix}0 & 1\\ 1 & 0\end{pmatrix}$
$\sigma_y = \frac{1}{2}\begin{pmatrix}0 & -i\\ i & 0\end{pmatrix}$
$\sigma_z = \frac{1}{2}\begin{pmatrix}1 & 0\\ 0 & -1\end{pmatrix}$
Alice
Bob

Figure 7. The mechanism of the multi communications in the proposed protocol.

The previous proposed QKD protocol phases are done simultaneously and both communicating parties can decide either to continue or to start over [58]. Usually, any interruption happened during the quantum channel will not affect the submitted data because the receiver will realize the presence of eavesdropper as well as the position of interrupted photons.

Furthermore, the whole strategy of the proposed protocol is illustrated in Figure (7), where the EPR communication is highlighted on the right side and the qubit communication is highlighted on the left side. In essence, the authentication approval should be confirmed during the EPR communications. Subsequently, transferring the qubits IQUBIT through the quantum channel will be the last step in the exchange of data in order to create a shared secret key (SSK).

As shown in Algorithm (1) [59], the proposed QKD algorithm contains three important loops. These loops represent the main operating functions that are based on EPR preparations, EPR communications IEPR, and qubits submissions IQUBIT. A and B represent the sender and receiver sequentially.

ALGORITHM.1 ***The Proposed QKD Protocol***

```
A prepares $X_n$ qubits into DM                         //Preparing DM
    While ($X_n$ $|\emptyset\rangle \rightarrow \{0,1\}^n$     //Plaintext
              $|\varphi\rangle \rightarrow \{0,1\}^n$          //Decoy states
              $|\omega\rangle \rightarrow \{0,1\}^1$           //Parity states
$X_n \rightarrow DM_A$                                   //Converting X to DM
        $\boldsymbol{then}, DM_B \in DM_A$                   //Preparing $I_{EPR}$
$A \rightarrow \{00,01,10,11\}^n$                         //Quantum gates in classic
$\boldsymbol{if}\ I_{EPR}(A == |0\rangle)$:                //Initiating EPR connection
        $B = |1\rangle$;                                   //Entangled state
$\boldsymbol{esle}$:
        $B = |0\rangle$;                                   //Entangled state
$\boldsymbol{end}$;
$\boldsymbol{while}\ (I_{EPR} \in DM_B)$                    //Setup $I_{EPR}$ into $DM_B$
        $\boldsymbol{then}: DM_B \in DM_A$                  //Adjusting $DM_B$ to be $DM_A$
$\boldsymbol{if}\ (A == B)$:
        $I_{QUBIT} = 1$;                                  //$I_{QUBIT}$ requested
        $I_{QUBIT} \rightarrow SSK$
$\boldsymbol{else}$:
        $error$;                                          //$I_{QUBIT}$ denied
$\boldsymbol{end}$;
$A\ and\ B \approx SSK$                                   //Obtaining SSK.
```

The EPR preparation time also will not be included during the whole Runtime-Execution, where the plaintext X should be prepared by A to extract the needed information for the EPR submission. The prepared information will be sent into entangled states (*EPR channel*). If the EPR communication was applied successfully, A and B will start to exchange qubits through the quantum channel.

CHAPTER 4: IMPLEMENTATIONS

The proposed QKD protocol was implemented by a classical system in MATLAB codes, which are compared with the most common quantum key distribution protocols (*Literature review*). Special quantum libraries (LDPC, QCF, QLib, and QETLAB)[60-62] were used to convert the classical system of particles measurement to the quantum system. For instance, the classical system (*bits*) can read the input and output into just a binary (0 or 1), so that the quantum measurements will not give the right result on the classical system. The exception of having an accurate result depends on customized libraries that will assist the system to read inputs and outputs in the superposition (*qubit*).

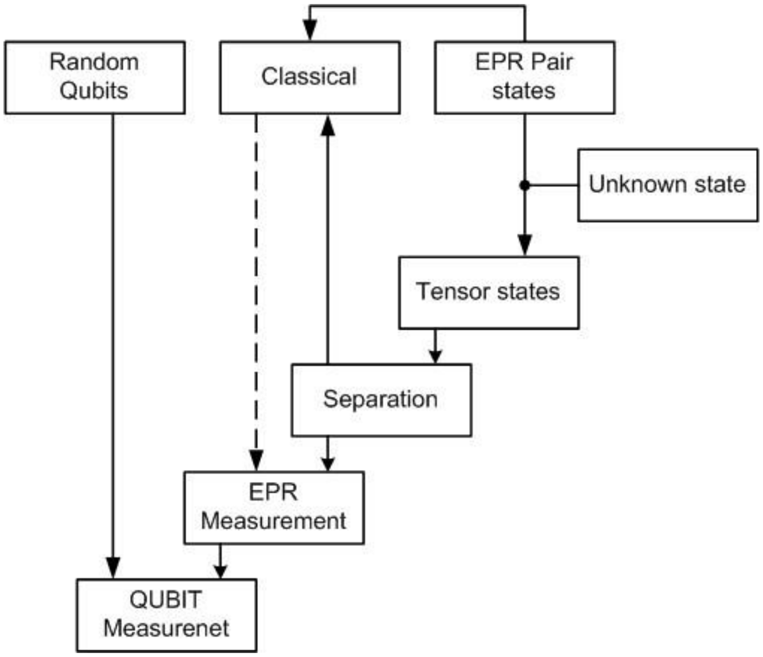


Figure 8. The cycle of creating a secret key into EPR and Quantum channels with approving authentication as well as using minimum rate of classical communication.

The used technique in the proposed protocol is based on two scenarios. First scenario, initiating an entangled state into a communication channel is for transferring only the Bell's states into so called an EPR channel. The EPR channel provides a shared data to the legitimate communicators, who will be authenticated to exchange a secret key. Based on the rate of success during the EPR connection, both party members will be able to finish creating a secret key without any difficulty.

Additionally, many experiments were established to make sure the proposed QKD protocol is efficient. Applying the security equation *J(k)* and the entropy security *S(k)* [63] based on Shannon Entropy as shown in Figure (9) are procedures to test the capability of standing the proposed protocol against the quantum attacks. Moreover, initiating different types of errors is very important to get a high level of result quality.

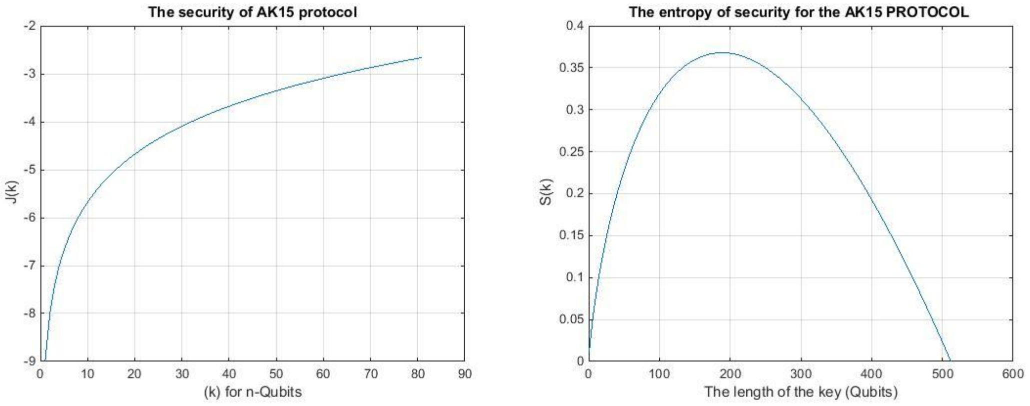


Figure 9. The measurement of the proposed QKD protocol security and the entropy of security.

The result shown above for the proposed QKD protocol provides more secure information than the well-known QKD protocols. The secrecy is approved by many powerful features such as inserting cells of matrix, parity of decoy states, and flipping the submitted rows. Therefore, the security of the proposed protocol has a capability to stand against any attacks either active or passive attacks.

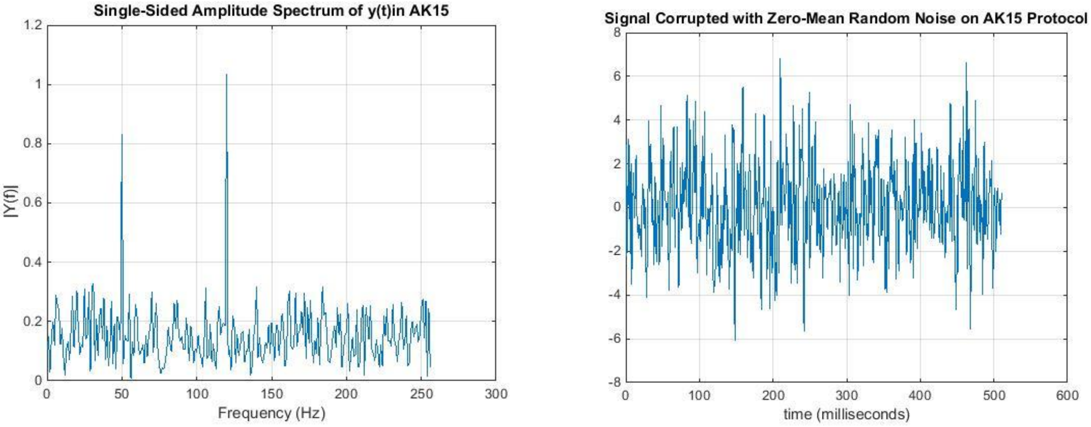


Figure 10. The Single-Sided Amplitude Spectrum and corrupted signal with Zero-Mean Random Noise.

The proposed protocol is considered as a logical scenario to create a secret key, so that some noise resources should be applied to experiment the protocol ability during presenting these noises. As shown in Figures (10) and (11), the White Gaussian Noise was applied with random noise resources.

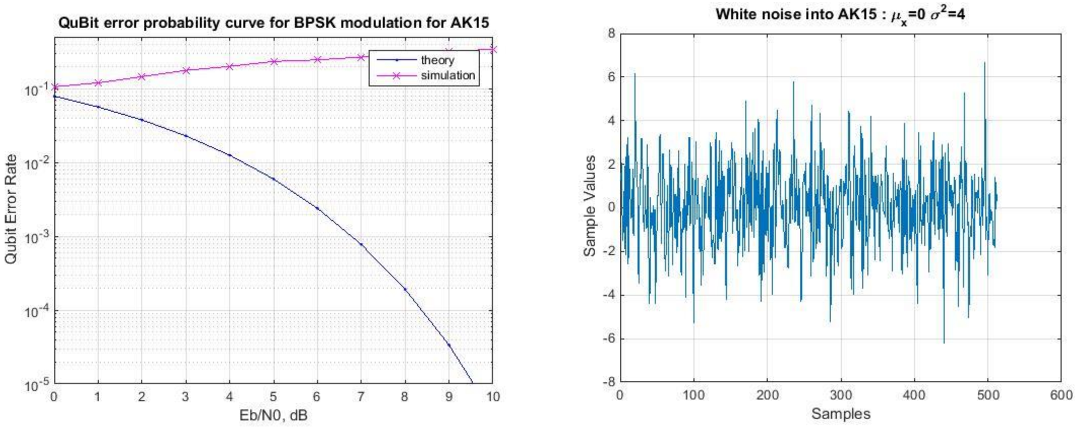


Figure 11. The qubits error probability’s curve for BPSK modulation with White Noise.

As mentioned above, a different type of noise may harm the system and could cause an infinite looping. More precisely, an extra time into the reconciliation phase does mean two vary scenarios. One of these scenarios is the ability to fix gaps that occurred by the corrupted qubits. The second scenario is a chance for listening to the submitted data with an increase of the attacks life.

Although different quantum attacks decrease the efficiency of each QKD protocol, the QKD protocols are protected by the physics theory that is called the non-cloning theory. This theory will guarantee exchanging information by destroying particles. In other words, the non-cloning theory will not guarantee any successes of running the system. Therefore, the physics theory can be a value factor to initiate a secret key, but it should be included with other classical security mechanisms.

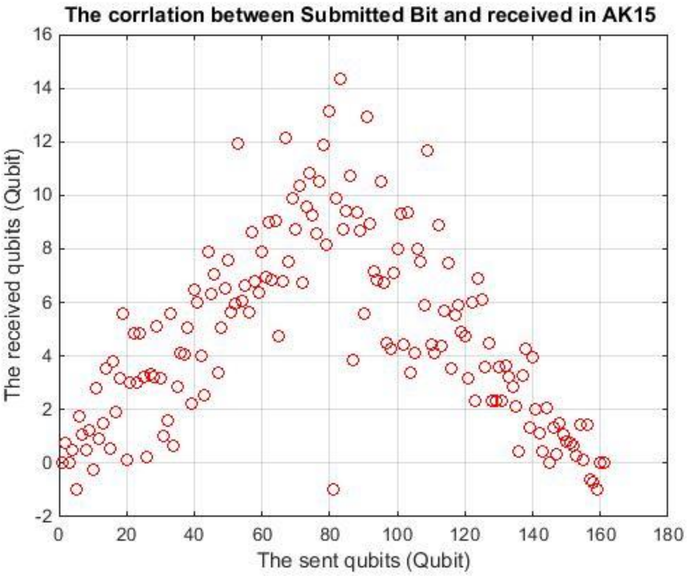


Figure 12. The correlation between the submitted and received qubits.

As illustrated above in Figure (12), the proposed QKD protocol shows no-correlation between the submitted and received qubits. The non-correlation has occurred by using the matrix to sort the submitted qubits. The received qubits also will be inserted into a matrix, and the receiver then will organize the rows depending on the EPR communication. The non-correlation in these measurements prove the difficulty to find out the relation between the submitted and the received qubits. Therefore, an eavesdropper cannot gain any information by attacking this protocol because the submitted data will not match with the original plain text.

CHAPTER 5: RESULTS

5.1 The Runtime-Execution

The Runtime-Execution is one of the measurements that is primary considered in this case-study. All the studied QKD protocols and the proposed protocol were converted to programing codes on MATLAB with supporting by quantum libraries [64-66]. The studied protocols were tested during the Runtime-Execution time into many sequential sizes of qubits. The results show variations based on each protocol algorithm. For instance, the B92 protocol is one of the few QKD protocols that runs in short time. Moreover, the B92 protocol uses a simple qubits initiation in two non-orthogonal states. The following figures will show the Runtime-Executions for all the QKD protocols with 500 qubits.

Furthermore, the differentiations of the Runtime-Executions are based on the mechanism of each QKD protocol algorithm. Executing multi-steps of the QKD protocol during exchanging data between the communicated parties might be either an advantage or disadvantage. If the designed complicity in the algorithm of the QKD protocol provides an impossibility to reach the exchanged data or to interrupt any submitted information, so that the complicity will be an advantage. On the other hand, measuring and computing data during the communication will be a disadvantage, if the difficulty causes long procedures with a breakable system.

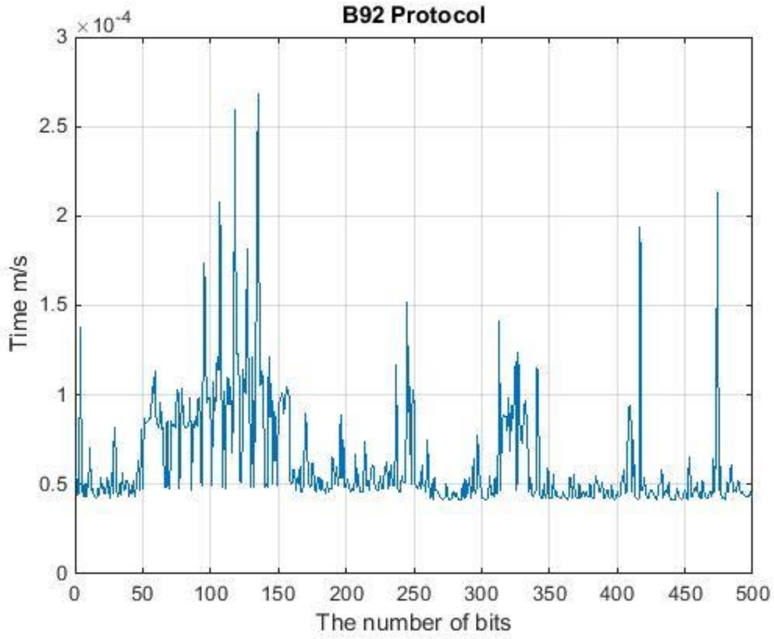


Figure 13. The Runtime-Execution during exchanging data between two legitimate parties in the B92 protocol, which reflects a 500 photons (*Qubits*) string with applying a noise.

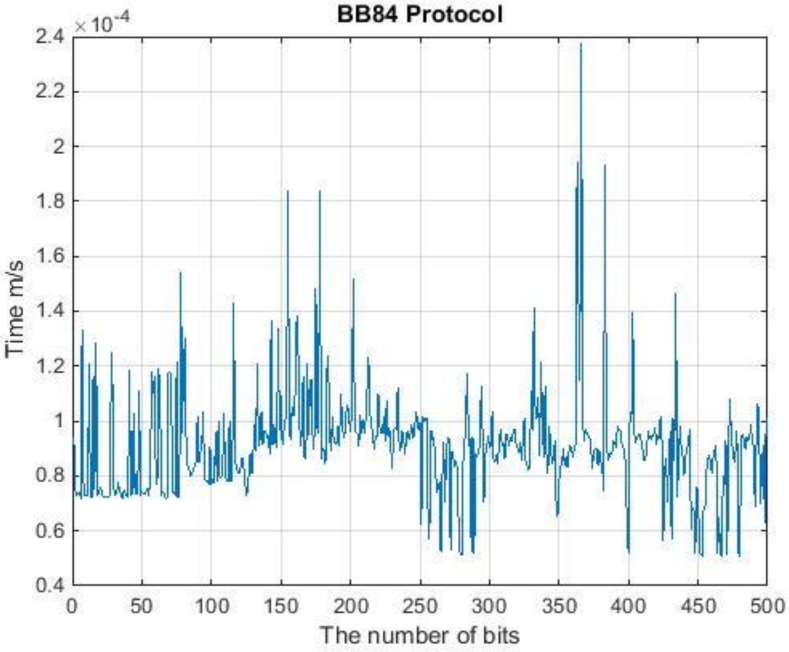


Figure 14. The Runtime-Execution during exchanging data between two legitimate parties in the BB84 protocol, which reflects a 500 photons (*Qubits*) string with applying a noise.

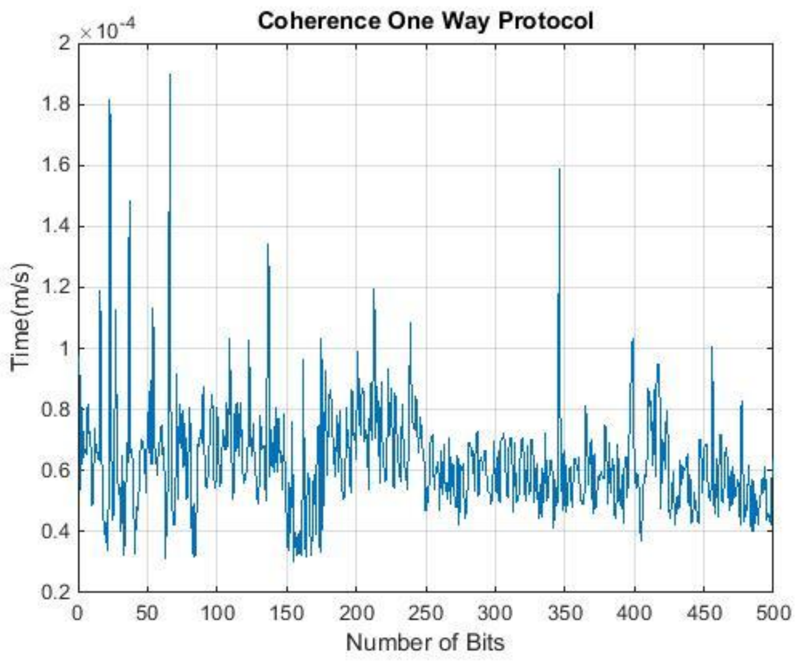


Figure 15. The Runtime-Execution during exchanging data between two parties in the Coherent-One-Way protocol, which reflects a 500 photons (*Qubits*) string as well as applying decoy states with a noise.

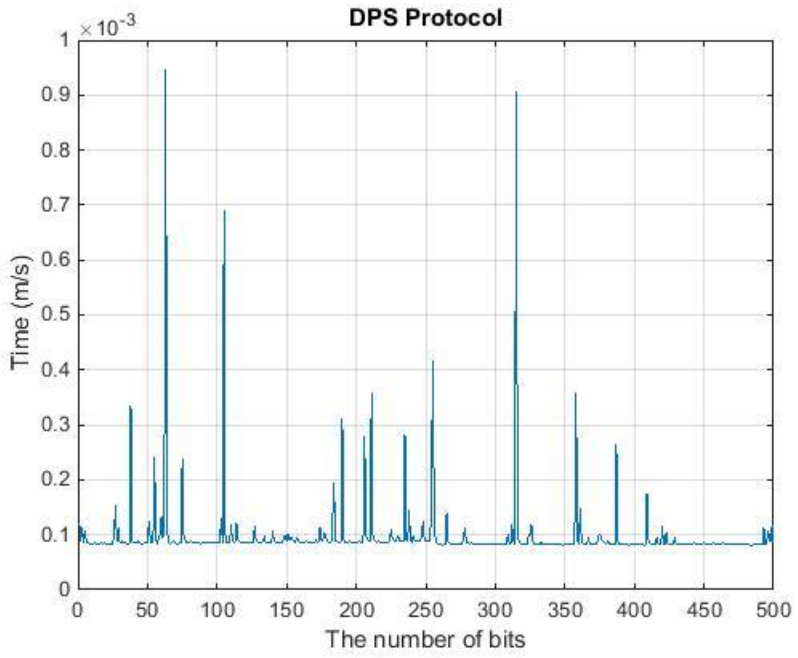


Figure 16. The Runtime-Execution during exchanging data between two legitimate parties in the Deferential-Phase-Shifting (DPS) protocol, which reflects measuring a qubits string in slot time.

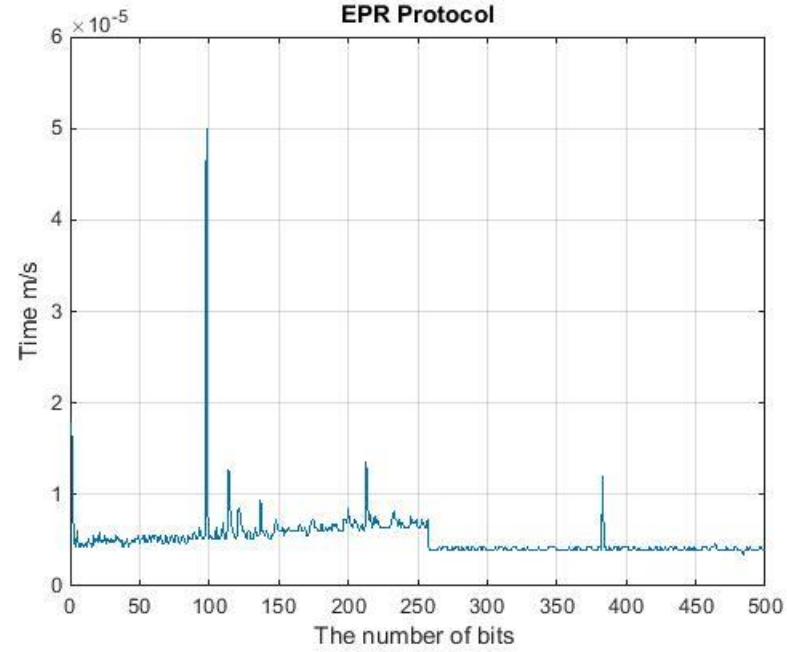


Figure 17. The Runtime-Execution during exchanging data between two legitimate parties in the EPR protocol, which reflects a 500 photons (*Qubits*) string with applying a noise.

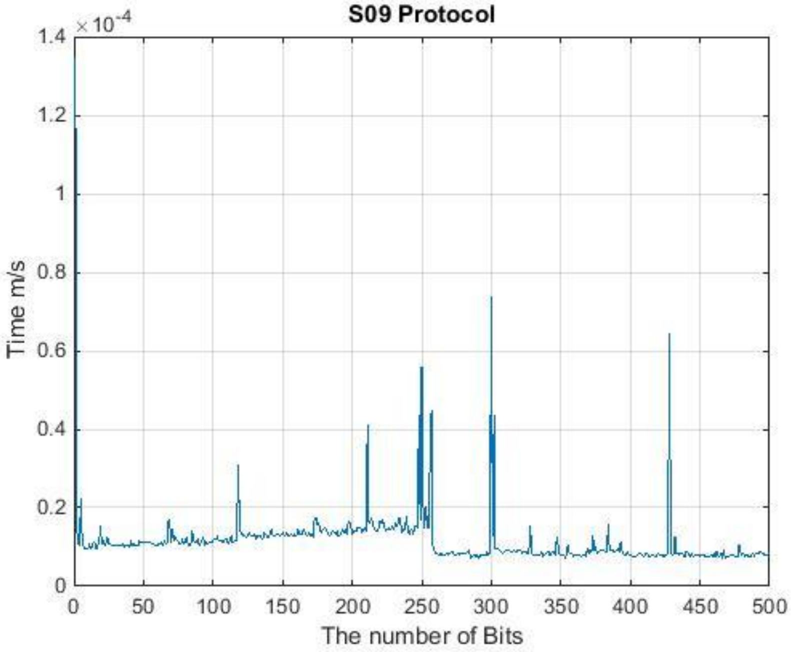


Figure 18. The Runtime-Execution during exchanging data between two legitimate parties in the S09 protocol, which reflects a 500 photons (*qubits*) string with applying a white noise.

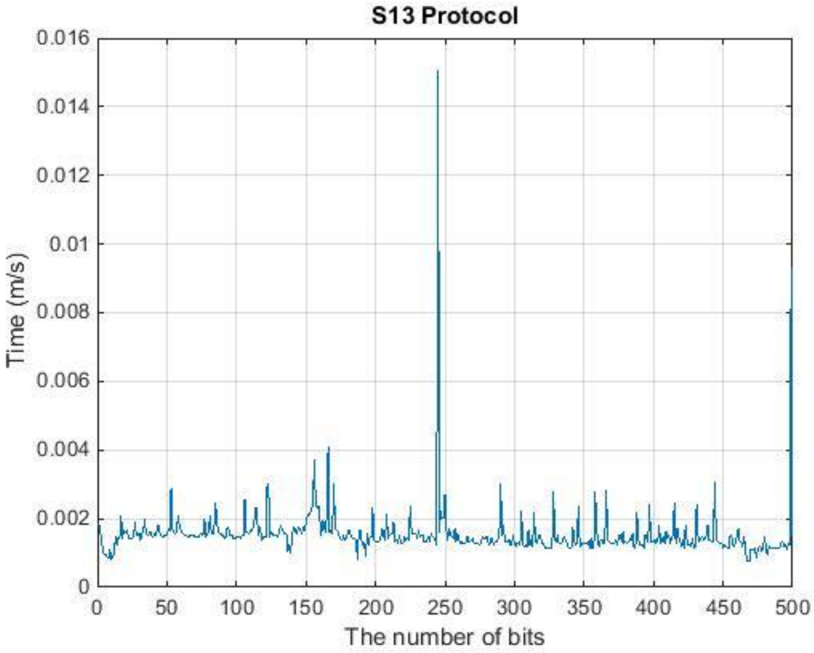


Figure 19. The Runtime-Execution during exchanging data between two legitimate parties in the S13 protocol, which reflects a 500 photons (*Qubits*) string with a white noise.

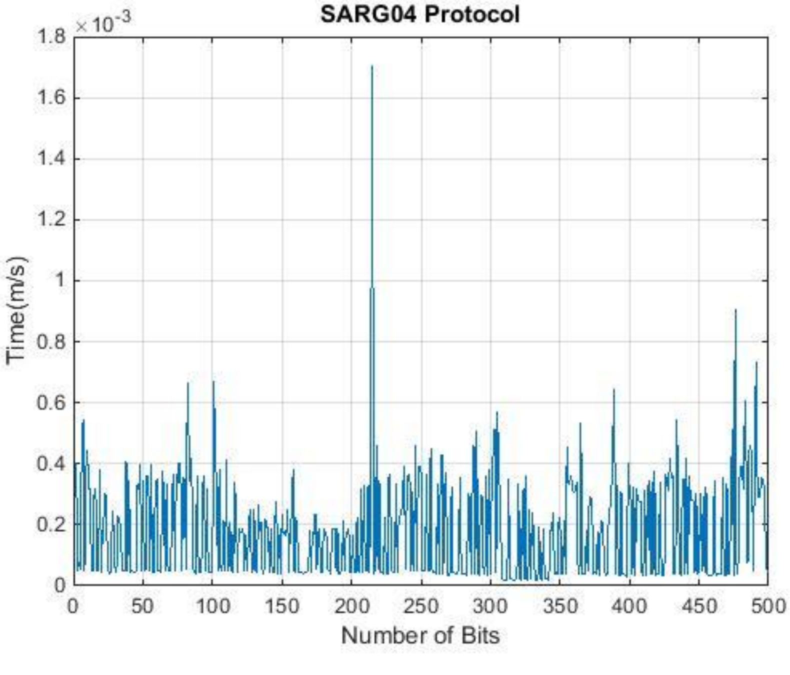


Figure 20. The Runtime-Execution during exchanging data between two legitimate parties in the SARG04 protocol, which has similarity to the BB84 protocol except in the classical connection.

Table 7. The Runtime-Execution for the QKD protocols (*ms*).

QKD Protocols	32	64	128	256	512	1024	2048	Average
BB84	0.000440	0.000670	0.000794	0.000857	0.000674	0.000756	0.001200	0.0007701
B92	0.000165	0.000177	0.000204	0.000263	0.000271	0.000286	0.000288	0.0002361
SARG04	0.000600	0.000850	0.000908	0.000990	0.001000	0.001220	0.001300	0.0009811
EPR	0.000100	0.000164	0.000165	0.000172	0.000178	0.000180	0.000183	0.0001631
KMB09	0.002500	0.005100	0.005800	0.009100	0.010600	0.013200	0.018100	0.0092000
DPS	0.030900	0.039400	0.039500	0.039800	0.058400	0.078300	0.092430	0.0541043
COW	0.000450	0.000620	0.000983	0.001100	0.001240	0.001900	0.001954	0.0011782
S09	0.020700	0.024200	0.024400	0.025000	0.025700	0.026000	0.035600	0.0259429
S13	0.000217	0.000297	0.000305	0.000558	0.000558	0.000612	0.000672	0.0004599
AK15	0.004000	0.004300	0.005400	0.006200	0.007100	0.007600	0.008100	0.0061000

The previous Table (7) shows the Runtime-Execution measurement in different qubits lengths. The DPS protocol shows the highest running time because the DPS protocol depends on the solt time during the measurement. On the other hand, the DPS is not considered as the worse Runtime-Execution, if the protocol runs low number of qubits (*256 and below*). Next, the S09 protocol takes a long time of processing, because the S09 was designed to be a complicated exchanging protocol. The S09 does not have a classical channel to reconcilate errors during the quantum communication, which is based on communications through only quantum channels. The multiple exchanges during the quantum channels consume a long time of processing from initaition steps to creation of the secret key. Otherwise, the S09 protocol is stable as long as the length of qubit string is below 1024 qubits.

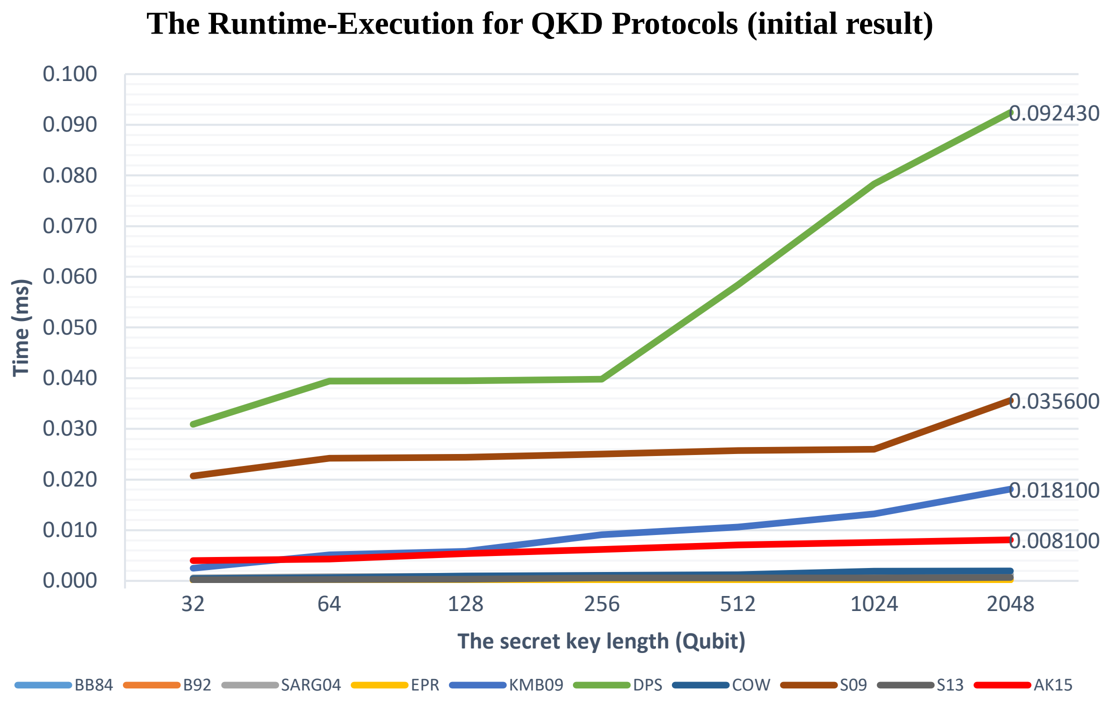


Figure 21. The Runtime-Execution for QKD Protocols (*ms*).

The Runtime-Execution provides a wide evaluation about the mechanism of running each protocol. As above-mentioned results in Table (7), the proposed QKD protocol could not fulfill the best result of running time, but it is not the worst. The delay of the proposed protocol and the DPS protocol depend on the design of each protocol. Moreover, the proposed protocol includes a preparation phase, where this preparation should deal with inserting qubits in each cell of well-known size matrix. This operation takes an extra time more than the regular encryption operations. On the other hand, the DPS protocol is based on submitting a sequence of photons into different beam-splitters, and these photons will be measured by passing through detectors. As a result of these experiments, the Runtime-Execution is very critical measurement, especially, when any delay could cause a loss for data. Therefore, the quantum cryptography has tried to solve this issue physically by carrying a lot of data in one photon [67].

5.2 The efficiency

The efficiency measurements in the quantum cryptography are determined by the Qubit Error Rate (QBER), so that any QKD protocol can be diagnosed to be secure or insecure against the quantum attacks. The proposed QKD protocol fulfilled a low QBER that makes the protocol more efficient than the most common QKD protocols. This measurement shows a few qubits that are advanced as correct qubits as well as error qubits. To calculate the QBER, the whole submitted and received qubits will be calculated and then applied as follows:

$$QBER = \sum \frac{s_i}{n} \times 100 \tag{28}$$

where, *S* is the number of qubits after sifting phase, and *n* is the total qubits that are initiated by the sender.

According to the previous collected results, the QBER recorded a different level of security. The highest percentage of the measured qubits in each protocol denotes more efficient procedure. Although the listed QKD protocols are the most common and well-known protocols, the proposed protocol records the highest reading of efficiency measurement. The measurement of each protocol started at a string of 32 qubits (2^n) and then added to 64 qubits (*until 2048 qubits*). The capacity of each string should be duly noted and considered very important. A single qubit in the quantum system will take more space than the regular bit in the classical system. More precisely, measuring one qubit will take a huge space of the regular classical memory. Therefore, the ability of measuring an enormous number of qubit requires a quantum memory.

To explain the outcomes of the QBER for each protocol, some fundamentals should be defined. when the string of qubits contains a huge number of data, the complicity will be a linear. Hence, the ability of each QKD protocol to include a huge number of data is approved, unlike the classical system. For instance, the QKD protocol is sharply affected when the data increases or decreases, so that the protocol has a limited capacity. Therefore, the QKD protocol will not be an efficient protocol in all needed scenarios, if the protocol is unable to progress a big number of data. Here, this research determined the main differentiations between each QKD protocol based on analyzing algorithms.

Table 8. The QBER measurements for the QKD protocol (the rate of QBER %).

QKD Protocols	32	64	128	256	512	1024	2048	Average
BB84	0.5394	0.5404	0.5547	0.5032	0.5002	0.4992	0.4943	0.5188
B92	0.5938	0.6875	0.6969	0.7232	0.7237	0.7325	0.7411	0.6998
SARG04	0.5291	0.5304	0.5547	0.5819	0.5904	0.6083	0.5992	0.5706
EPR	0.4983	0.4991	0.5022	0.5192	0.5093	0.5095	0.4985	0.5052
KMB09	0.6792	0.6804	0.6852	0.6876	0.6906	0.7095	0.7134	0.6923
DPS	0.5933	0.6032	0.6542	0.6602	0.6538	0.6522	0.6519	0.6384
COW	0.6402	0.6375	0.6349	0.6306	0.629	0.6286	0.6284	0.6327
S09	0.6108	0.6149	0.6192	0.6248	0.629	0.6202	0.6187	0.6197
S13	0.6904	0.6915	0.7019	0.7036	0.7103	0.7084	0.7093	0.7022
AK15	0.7813	0.7825	0.7928	0.7937	0.7981	0.7985	0.8102	0.7939

The Table (8) shows collected results of running codes for the studied QKD protocols. These QKD protocols have been tested by MATLAB, where some of special libraries were applied. The main purpose of measuring the efficiency is to compare the QKD protocols and determine the usability. Furthermore, each QKD protocol has a specific number of the submitted data after the reconciliation phase. For instance, the BB84 protocol provides a low efficiency as well as the EPR protocol. The failure is reflected by using a simplicity of qubit process in the both protocols. On the other hand, the proposed QKD and the B92 protocols have assorted as the best outcomes of the efficiency as shown in Figure (18).

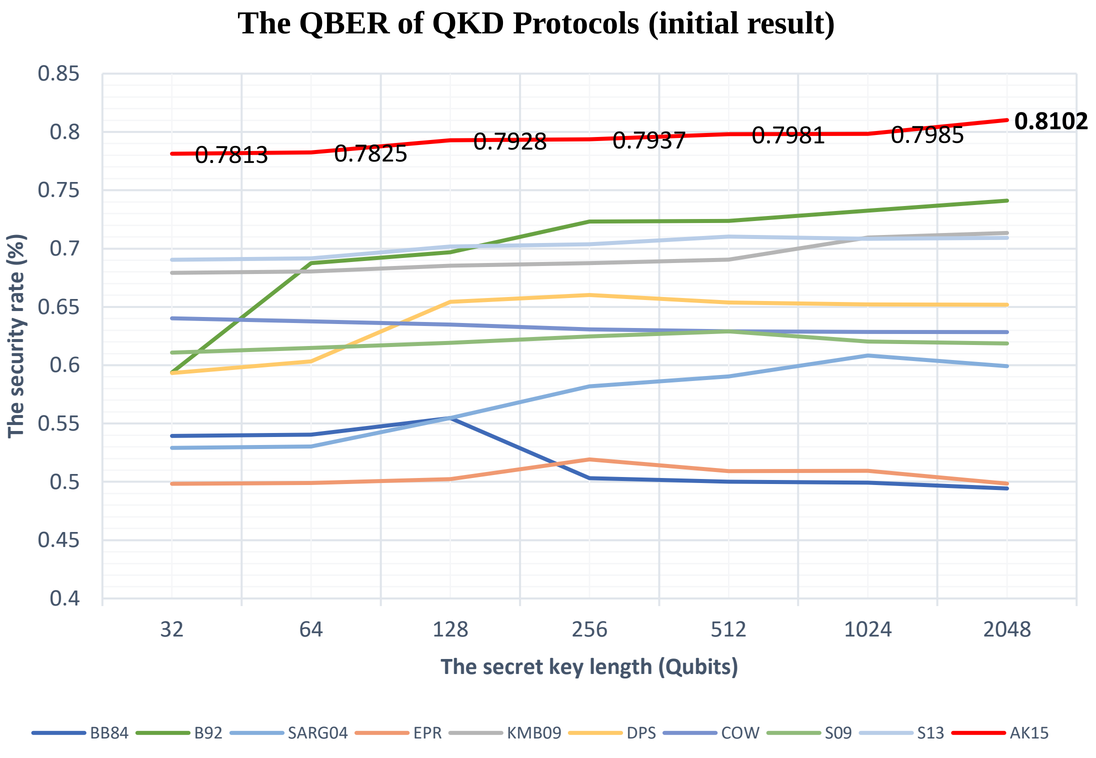


Figure 22. The QBER Measurements for QKD Protocols before Sifting Phase.

Based on the result of QBER during variations of qubits length, the proposed QKD protocol fulfills a high percentage of the matched plaintext after applying the sifting phase as shown in Figure (18). Although the QBER rises with increasing the length of the submitted qubits, the B92 and KMB09 protocols occupied the second better rate, unlike the KMB09 protocol that shows increasing in the QBER. The KMB09 utilizes indices of a matrix to correct the errors that may happen during exchanging data.

5.3 The security

Many experiments on the QKD Protocols were applied, because several concerns about security are still active. Some experiments have changed the considerations of the classical system. According to many public announcements about the quantum cryptography, scientists agreed on that the next generation of cryptography will be the quantum cryptography. Moreover, using the law of physics during the exchange of data will extend the confidence between the legitimate communicators. In this research, the security represents matching between the submitted and received data after the conciliation phase. In addition, the security measurement could be applied by several methods, but this research utilizes the Shannon Entropy [68, 69] to measure the level of security.

$$H = -\sum_i P_i \log_b P_i, \tag{29}$$

where Pi is the probability of the shown character (*certain qubits*) in i numbers.

Table 9. The security measurements for the QKD protocols (*sifting qubits* %).

QKD Protocols	**32**	**64**	**128**	**256**	**512**	**1024**	**2048**	**Average**
BB84	0.6502	0.6632	0.6918	0.7062	0.6911	0.6834	0.625	0.6730
B92	0.6373	0.703	0.7618	0.7294	0.7624	0.7452	0.7366	0.7251
SARG04	0.6467	0.6659	0.7023	0.7059	0.7192	0.7052	0.6948	0.6914
EPR	0.4939	0.5093	0.5486	0.5302	0.5294	0.51	0.5048	0.5180
KMB09	0.7129	0.7157	0.7292	0.7198	0.7065	0.7033	0.7003	0.7125
DPS	0.6039	0.6087	0.6106	0.6043	0.6021	0.5982	0.5977	0.6036
COW	0.5592	0.5834	0.5903	0.5974	0.6672	0.6803	0.6501	0.6183
S09	0.6903	0.6911	0.6905	0.6877	0.6735	0.6704	0.6593	0.6804
S13	0.5899	0.6043	0.6307	0.6461	0.6503	0.6511	0.6499	0.6318
AK15	0.7008	0.7023	0.7173	0.7392	0.7603	0.7566	0.7511	0.7325

The result in Table (9) was collected after running each QKD protocol into the whole process of algorithm to initiate a secret key. Furthermore, each protocol runs a different number of qubits string with applying a noise. Therefore, the result included different stages of qubit length, which contain 32, 64, 128, 256, 512, 1024, and 2048 qubits.

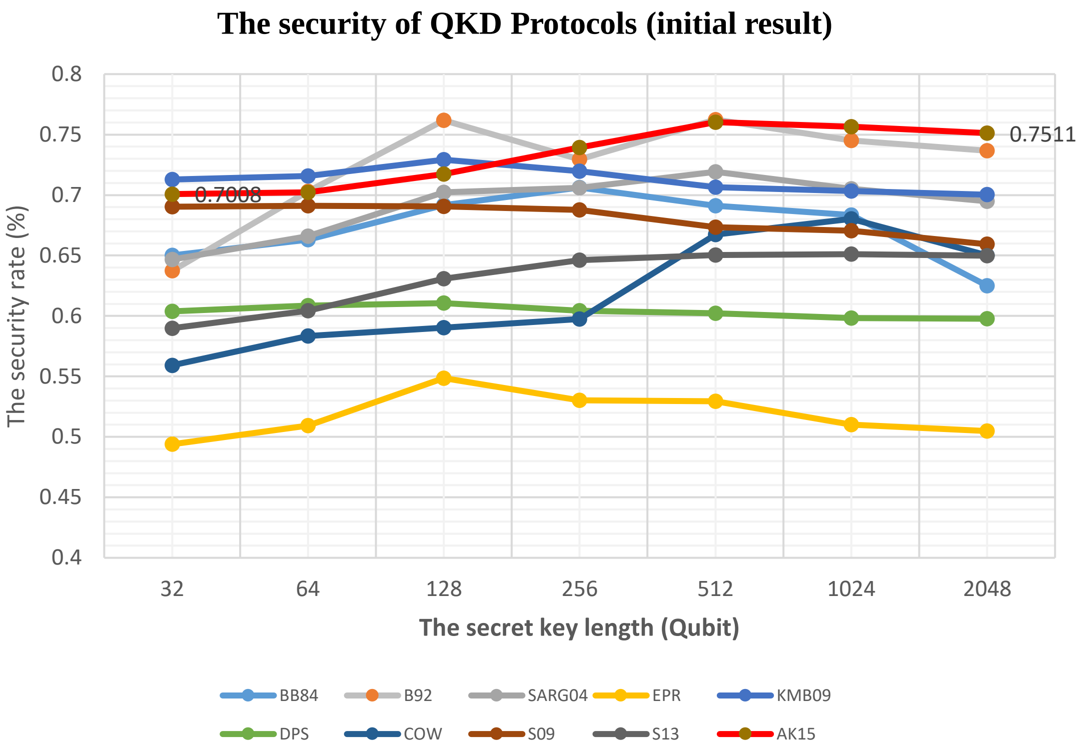


Figure 23. The security measurement for QKD Protocols in different Qubits String length. (*from 32, 64, 128, 256, 512, 1024, and 2048*).

Sequentially, the security of each QKD protocol is calculated based on two factors. The first factor of the security is the number of qubits in the plaintext *n*. The second factor is the number of uncovered qubits after passing through the sifting phase, where several filtrations are applied. According to the previous outcomes, the proposed QKD protocol could not provide a good result at 32 qubits, but the security rises up as long as the length of qubits goes up. This advantage will be observed only in the proposed protocol. For instance, the KMB09 protocol gains the best security rate at 32 qubits, but the security curve will go down after 128 qubits as shown in Figure (19).

5.4 The comparison between the QKD protocols

To figure out the efficiency of our research, data about all the most well-known QKD protocols can be necessary collected. It is also important to dig deeply into each protocol although some of those QKD protocols have limited official publications. For instance, the S09 was presented to be a protocol closer to the computer science than the physics field, but the protocol cannot be used at least in a present day. Later, the S13 was presented by the same author of the S09 after 4 years. The S13 came as a modification to the last protocol, and the protocol can be now more efficient for using on the existing devices.

In addition, the differentiation of each QKD algorithm creates a great chance to build an ideal protocol. Moreover, many QKD protocols have approved a part of cryptography, but there are still other uncompleted cryptographic requirements. The collected data will exhibit different features that have been used into these QKD protocols. The Table (10) will release classical and quantum cryptography techniques and will determine the utilized algorithms based on the original protocol.

Table 10. The comparison between the studied QKD protocols in physics and cryptographic phases.

Cases	Quantum Key Distribution Protocols									
	BB84	**B92**	**SARG04**	**COW**	**KMB09**	**EPR**	**S09**	**S13**	**DPS**	**AK15**
Properties	Heisenberg	Heisenberg	Heisenberg	Arbitrary	Heisenberg	Entanglement	Public private key	Heisenberg	Arbitrary	Heisenberg
Number of States	4 states	2 States	4 States	Time slots	2 states	Entangled 2 of photons	Arbitrary states	4 states	4 States	n-states
Detection of presence	QBER	QBER	QBER	Break of coherence	ITER	Bell’s inequality	appending parity bits	Random Seed	Time-Slot	QBER, Parity Cell
Polarization	Orthogonal	Non-orthogonal	Orthogonal	Arbitrary	Arbitrary	Orthogonal	Bit-Flip Phase-Flip	2 orthogonal	DPS	Arbitrary
State Probability	Various	50%	50%	Calculated	50%	Equal	Various	Various	Equal	Various
Qubit String	Discrete	Discrete	Discrete	Discrete	Discrete	Discrete	No	Discrete	Discrete	Discrete
Classical channels	Yes	Yes	Yes	Yes	Yes	Yes	No	Yes	Yes	No
Decoy States	No	No	No	Yes	No	No	Yes	No	No	Yes
Sifting phase	Revealing Bases	Alice = 1 - Bob	Revealing non-orth. state	Revealing times 2k+1	Revealing Indices	Bell's Inequality	No	Revealing Bases	Time-Slot	embedded
Bell's inequality	No	No	No	No	No	Yes	No	No	No	Yes
PNS attack	Vulnerable	Vulnerable	It's better than BB84	Robust	Robust	N/A	N/A	N/A	Robust	Robust
IRUD attack	Vulnerable	Vulnerable	Vulnerable	Under Test	Under Test	Vulnerable	N/A	N/A	N/A	N/A
BS attack	Vulnerable	Vulnerable	Robust	Robust	Robust	Vulnerable	N/A	N/A	Robust	Robust
DoS attack	Vulnerable	Vulnerable	Vulnerable	Vulnerable	Vulnerable	Vulnerable	N/A	N/A	Robust	N/A
MAM attack	Vulnerable	Robust	Robust	Robust	Robust	Robust	Robust	N/A	Robust	Robust
IRA attack	Vulnerable	Vulnerable	Robust	Robust	Robust	Bell's inequality	Robust	N/A	Robust	Robust
Authentication	No	No	No	No	No	No	No	classic	No	Quantum

The above mentioned comparison of QKD protocols elucidate different mechanisms that have been used for creating a secret key [70]. These cryptographic mechanisms were extracted from several studied resources. These resources are specific data and details based on the original published schemes. Therefore, this research ignored any updated algorithms for these QKD protocols after the first modifications.

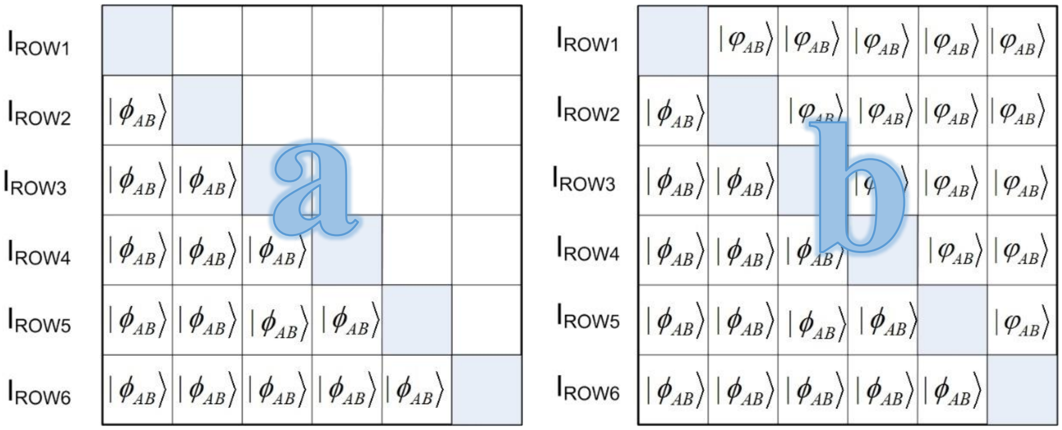
5.5 The proposed Protocol Modifications

According to the proposed scheme that already was explained above, there are some modifications to improve the Runtime-Execution as well as the security of this protocol against well-known quantum attacks. These adjustments are illustrated in two phases as follows:

5.5.1 The Decoy States

Using decoy states during the proposed QKD protocol gives more stability and trustworthy to the legitimate end users of this protocol. On the other hand, the decoy states waste much time based upon the rate of used decoy qubits. To solve this conflict here, the upper-triangle of the matrix (*or matrices*) will be filled in by the plaintext X, but the mechanism of filling this triangle will be different.

Moreover, this scheme utilizes the same previous proposed scheme, but it differs in the initiated decoy states in the upper-triangle. The upper-triangle should be filled sequentially from up to down by the plaintext with ignoring the diagonal line as explained above. Hence, the new modification ignores the decoy states (random states) that should be filled in the upper-triangle of the prepared matrix.

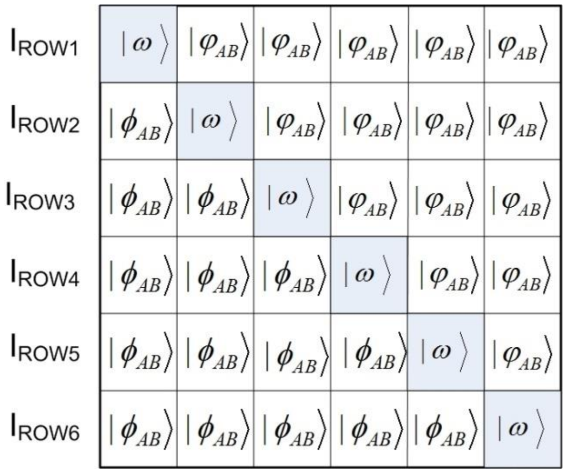


I_{ROW1}						
I_{ROW2}	$\vert\phi_{AB}\rangle$					
I_{ROW3}	$\vert\phi_{AB}\rangle$	$\vert\phi_{AB}\rangle$				
I_{ROW4}	$\vert\phi_{AB}\rangle$	$\vert\phi_{AB}\rangle$	$\vert\phi_{AB}\rangle$			
I_{ROW5}	$\vert\phi_{AB}\rangle$	$\vert\phi_{AB}\rangle$	$\vert\phi_{AB}\rangle$	$\vert\phi_{AB}\rangle$		
I_{ROW6}	$\vert\phi_{AB}\rangle$	$\vert\phi_{AB}\rangle$	$\vert\phi_{AB}\rangle$	$\vert\phi_{AB}\rangle$	$\vert\phi_{AB}\rangle$	

I_{ROW1}		$\vert\varphi_{AB}\rangle$	$\vert\varphi_{AB}\rangle$	$\vert\varphi_{AB}\rangle$	$\vert\varphi_{AB}\rangle$	$\vert\varphi_{AB}\rangle$
I_{ROW2}	$\vert\phi_{AB}\rangle$		$\vert\varphi_{AB}\rangle$	$\vert\varphi_{AB}\rangle$	$\vert\varphi_{AB}\rangle$	$\vert\varphi_{AB}\rangle$
I_{ROW3}	$\vert\phi_{AB}\rangle$	$\vert\phi_{AB}\rangle$		$\vert\varphi_{AB}\rangle$	$\vert\varphi_{AB}\rangle$	$\vert\varphi_{AB}\rangle$
I_{ROW4}	$\vert\phi_{AB}\rangle$	$\vert\phi_{AB}\rangle$	$\vert\phi_{AB}\rangle$		$\vert\varphi_{AB}\rangle$	$\vert\varphi_{AB}\rangle$
I_{ROW5}	$\vert\phi_{AB}\rangle$	$\vert\phi_{AB}\rangle$	$\vert\phi_{AB}\rangle$	$\vert\phi_{AB}\rangle$		$\vert\varphi_{AB}\rangle$
I_{ROW6}	$\vert\phi_{AB}\rangle$	$\vert\phi_{AB}\rangle$	$\vert\phi_{AB}\rangle$	$\vert\phi_{AB}\rangle$	$\vert\phi_{AB}\rangle$	

Figure 24. Inserting quantum states after converting the plaintext X to qubits, and the insertion is located at the lower-triangle, upper-triangle, and then diagonal line.

More precisely, the sender starts filling the lower-triangle from up to down as shown in Figure (24). After inserting the qubits in the previous lower-triangle, Alice starts filling the upper-triangle, but here should be from down to up. In this case scenario, the whole matrix should be filled by the plaintext X except the diagonal line that will be utilized as parity cells as shown in Figure (25).



I_{ROW1}	$\vert\omega\rangle$	$\vert\varphi_{AB}\rangle$	$\vert\varphi_{AB}\rangle$	$\vert\varphi_{AB}\rangle$	$\vert\varphi_{AB}\rangle$	$\vert\varphi_{AB}\rangle$
I_{ROW2}	$\vert\phi_{AB}\rangle$	$\vert\omega\rangle$	$\vert\varphi_{AB}\rangle$	$\vert\varphi_{AB}\rangle$	$\vert\varphi_{AB}\rangle$	$\vert\varphi_{AB}\rangle$
I_{ROW3}	$\vert\phi_{AB}\rangle$	$\vert\phi_{AB}\rangle$	$\vert\omega\rangle$	$\vert\varphi_{AB}\rangle$	$\vert\varphi_{AB}\rangle$	$\vert\varphi_{AB}\rangle$
I_{ROW4}	$\vert\phi_{AB}\rangle$	$\vert\phi_{AB}\rangle$	$\vert\phi_{AB}\rangle$	$\vert\omega\rangle$	$\vert\varphi_{AB}\rangle$	$\vert\varphi_{AB}\rangle$
I_{ROW5}	$\vert\phi_{AB}\rangle$	$\vert\phi_{AB}\rangle$	$\vert\phi_{AB}\rangle$	$\vert\phi_{AB}\rangle$	$\vert\omega\rangle$	$\vert\varphi_{AB}\rangle$
I_{ROW6}	$\vert\phi_{AB}\rangle$	$\vert\phi_{AB}\rangle$	$\vert\phi_{AB}\rangle$	$\vert\phi_{AB}\rangle$	$\vert\phi_{AB}\rangle$	$\vert\omega\rangle$

Figure 25. The prepared matrix after filling the upper-triangle, upper-triangle, and the diagonal line sequentially by the sender, where each raw should be a total even number after summation.

The updated results after the previous modifications for the proposed scheme were changed, which the Runtime-Execution is improved as well as the efficiency of the qubit submission. The improvements factor occurred by decreasing the required qubits that should be prepared by Alice and measured by Bob as shown in the Figure (26). The Runtime-Execution also is improved critically, where the proposed protocol was in the worst-case scenario during the Runtime-Execution in the previous design as shown in Figure (21).

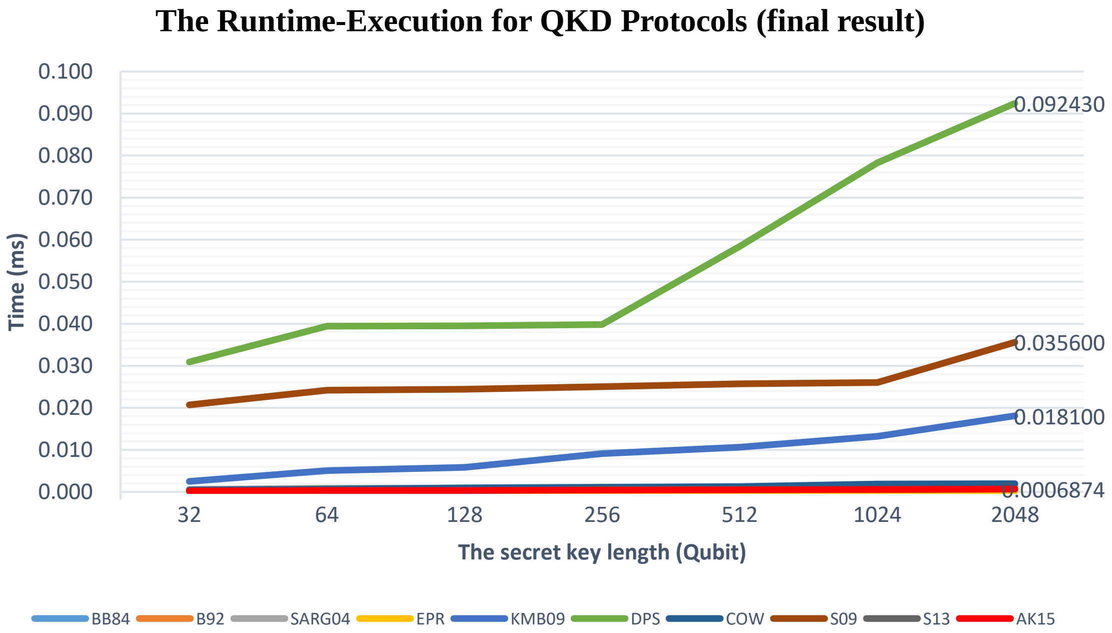


Figure 26. The Runtime-Execution of the proposed QKD protocol after utilizing the last modification.

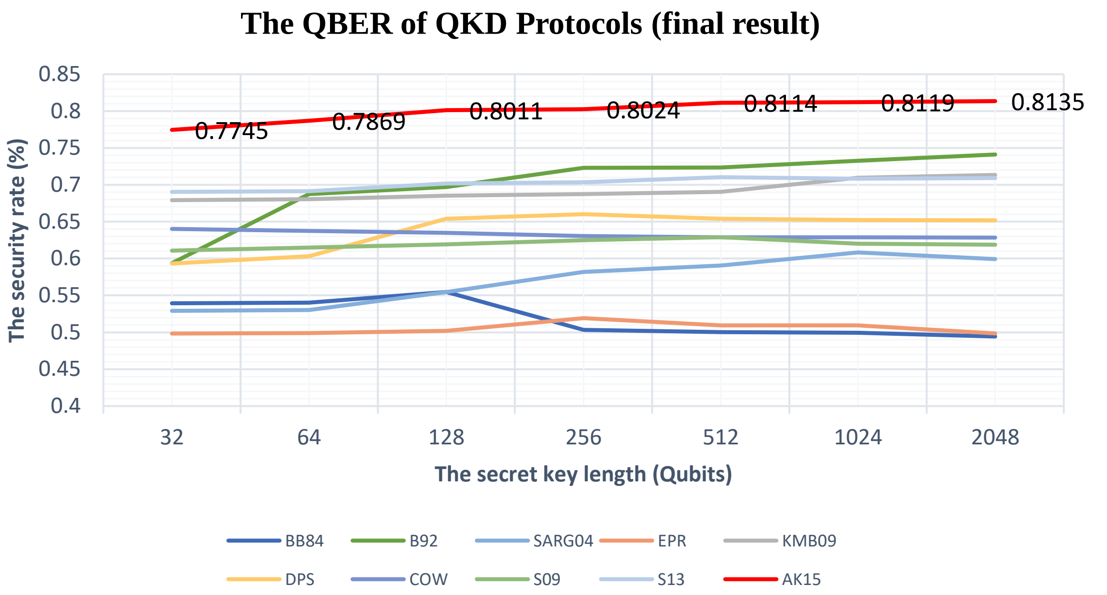


Figure 27. The QBER measurement of the proposed QKD protocol after editing the decoy states filled into the prepared matrix.

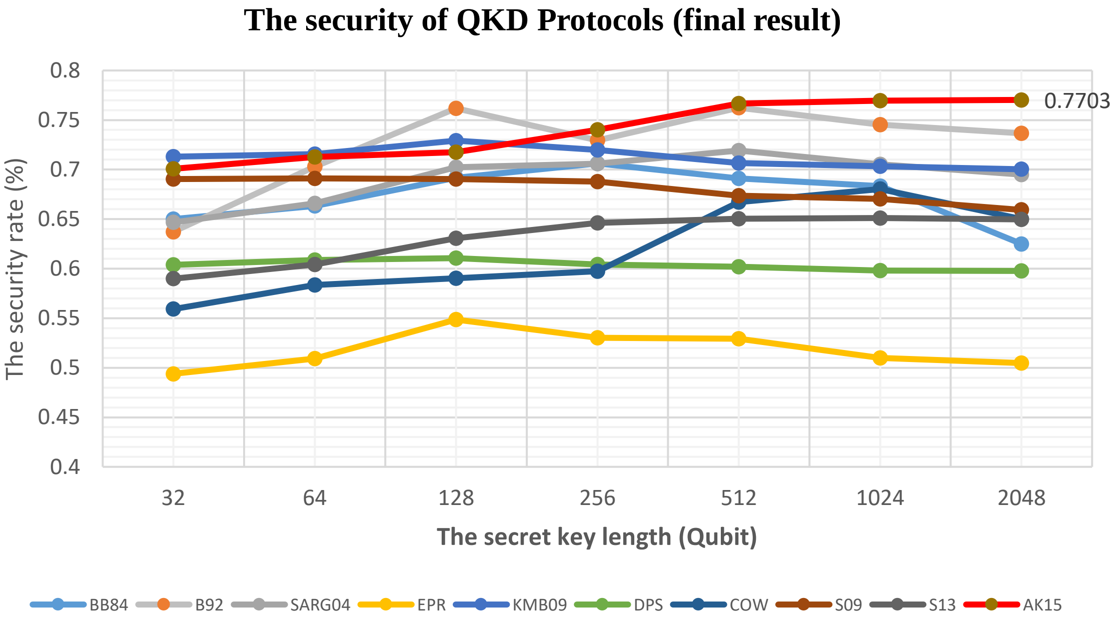


Figure 28. The security measurement of the proposed QKD protocol after modifying the prepared matrix by Alice.

Furthermore, there are two other measurements that were improved based on the last update. The efficiency is now better than the previous design, where the rate of uncovered 2048 qubits during the quantum communication is around 0.8135 as in Figure (27) rather than 0.8102 as in Figure (22). Moreover, the security measurement was changed slightly based on the both measurements, where the previous security rate was 0.7511 as shown in Figure (23), but the rate of security after the update is 0.7703 as shown in Figure (28). This update improves the simplicity of the proposed QKD protocol, where the sender and the receiver will not utilize extra qubits accept the parity qubits (*diagonal line in the matrix*).

5.5.2 The Third Party of Submitting Entangled States

One of the advantages that may help any communication systems is using a trusted third party. This third party will initiate a critical communication information instead of the communicating parties. Moreover, the third party will give more confidence to the communicating parties as long as both end users need to share information. In this study, the third party should be trusted and well-known security provider. The third party also should have needed mechanisms to establish any type of communications (*availability*). Hence, the sender will initiate a connection with the well-known third party by providing information about the plaintext (*prepared matrix*). The third party then prepares the plaintext MD into a matrix (*or matrices if any*) and sends a string of the EPR I_{EPR} to both parties (*Alice and Bob*) at the same time as shown in Figure (29) [71].

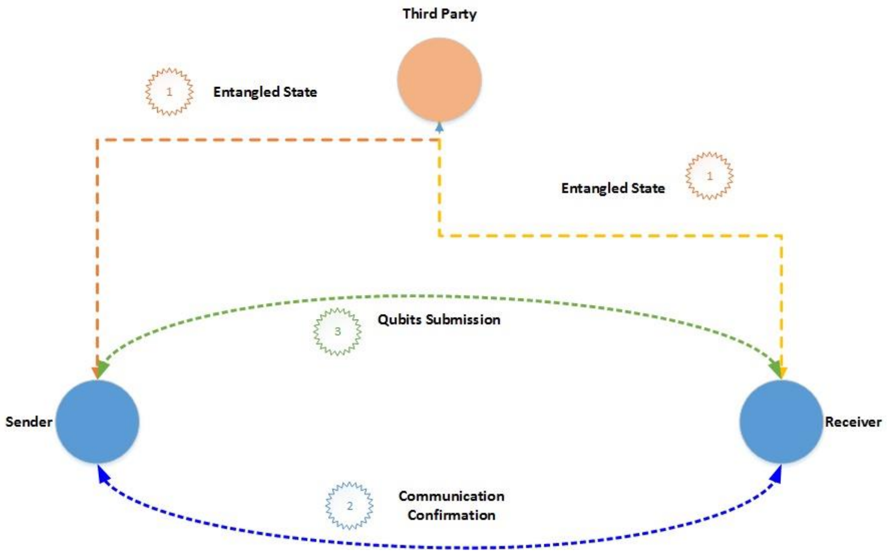


Figure 29. The Entangled States submitted by third party.

Based on several simulations, the production of the EPR string will not be affected either by trusted third party or Alice (*the sender*). On the other hand, including a third party during any communication would increase the Runtime-Execution, which needs an extra time to initiate a secret key. In addition, the long-time of any connection spent between the legitimate parties causes a high chance to attack the communication many times by eavesdroppers. Therefore, the communication with a third party is ignored in this research, where the proposed QKD protocol should be initiated between only two participants.

CHAPTER 6: CONCLUSIONS

The proposed QKD scheme is one of the reliable QKD protocols as well as the most secure algorithm. The obtained results in this research show that the proposed QKD protocol can stand against most of the well-known quantum attacks. Moreover, the utilized mechanism during processing the proposed QKD protocol also has been approved successfully in two aspects. The two aspects include two communication channels, where each channel carries a specific type of information. Particularly, the first type of communication channel in the proposed QKD protocol uses entangled states to configure the authentication phase, which has a limited accessibility from any eavesdropper. The authentication phase (*EPR channel*) was framed to transfer limited qubits, and there is no exception even if the connection fails. The second aspect is related to transferring qubits (*plain-text*) from the sender to the receiver, whereby this transfer gives a full confidence. There is also no interruption that may happen to the submitted data without warning. The qubits will be emitted into a quantum channel in a string of sequential qubits. Furthermore, the proposed QKD protocol was designed to be convenient for exchanging a huge data, where inserting data into a matrix (*or matrices*) is required by both legitimate parties.

The legitimate communicators should sort the inputs and outputs of data during the EPR channel through a logical movement of information. The logical movement should be a process that is used by either the sender or receiver. In addition, both the sender and receiver should collect data in certain polarization methods with specific measuring tools.

In other words, the designed mechanism of the proposed QKD protocol focuses on fulfilling the authentication between the end users, where the EPR communication must be simulated and approved before exchanging any valuable data. Providing an authentication at the beginning of any communication gives a high percentage of trust to both legitimate parties. Furthermore, the data of the plain-text should be transferred to whom is well-known as a sender or receiver without any doubt. As a result, the proposed QKD protocol has been evaluated in different security modes with some security methods of the well-known QKD protocols. The outcomes also have brought the proposed QKD protocol to the top of security strategies if not the first one with some QKD protocols. The novelty of this QKD protocol is included when approving an authenticated system before exchanging any data between the end users. The encryption and decryption codes will be extracted by using a secure channel (*entangled states*) in short time of processing. At the end, the QKD protocol provides an authentication between any end users, and the quantum mechanics roles will be utilized during transferring a data.

REFERENCES

[1] S. William and W. Stallings, *Cryptography and Network Security, 4/E*: Pearson Education India, 2006.

[2] W. C. Barker and E. B. Barker, "SP 800-67 Rev. 1. Recommendation for the Triple Data Encryption Algorithm (TDEA) Block Cipher," 2012.

[3] M. Bellare, A. Desai, E. Jokipii, and P. Rogaway, "A concrete security treatment of symmetric encryption," in *Foundations of Computer Science, 1997. Proceedings., 38th Annual Symposium on*, 1997, pp. 394-403.

[4] Steven M Bellovin, "Frank Miller: Inventor of the One-Time Pad," *Cryptologia,*, vol. 35, pp. 203-222, 2011.

[5] Ronald Rivest, Adi Shamir, and Leonard Adleman, "A Method for Obtaining Digital Signatures and Public-Key Cryptosystems," *Communications of the ACM*, vol. 21, pp. 120-126, 1978.

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

[7] A. K. Ekert, "Quantum cryptography based on Bell’s theorem," *Physical Review Letters*, vol. 67, p. 661, 1991.

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

[9] D. Kartheek, G. Amarnath, and P. Reddy., "Security in Quantum Computing Using Quantum Key Distribution Protocols," presented at the 2013 International Multi-Conference on Automation Computing Communication Control and Compressed Sensing (iMac4s),, Kerala, India, 2013.

[10] M. Elboukhari, M. Azizi, and A. Azizi, "Quantum key distribution protocols: A survey," *International Journal of Universal Computer Sciences,* vol. 1, pp. 59-67, 2010.

[11] A. Acín, L. Masanes, and N. Gisin, "Equivalence between two-qubit entanglement and secure key distribution," *Physical Review Letters*, vol. 91, p. 167901, 2003.

[12] X. Tan and J. Sen, "Introduction to quantum cryptography," *Theory and Practice of Cryptography and Network Security Protocols and Technologies, ISBN*, pp. 978-953, 2013.

[13] W. Yong, W. Huadeng, L. Zhaohong, and H. Jinxiang, "Man-in-the-Middle Attack on BB84 Protocol and its Defence," presented at the 2nd IEEE International Conference on Computer Science and Information Technology (ICCSIT) 2009.

[14] Jason Lin, Hsin-Yi Tseng, and T. Hwang., "Intercept–Resend Attacks on Chen et al.'s Quantum Private Comparison Protocol and the Improvements," *Optics Communications,,* vol. 284, pp. 2412-2414, 2011.

[15] M. Curty and N. Lütkenhaus, "Intercept-resend attacks in the Bennett-Brassard 1984 quantum-key-distribution protocol with weak coherent pulses," *Physical Review A,* vol. 71, p. 062301, 2005.

[16] Peter Shor and John Preskill, "Simple Proof of Security of the BB84 Quantum Key Distribution Protocol," *Physical Review Letters,* vol. 85, p. 441, July 10 2000.

[17] Z. Sheng-Mei, L. Fei, and Z. Bao-yu, "A proof of security of quantum key distribution in probabilistic clone scheme," presented at the International Conference on Communication Technology Proceedings (ICCT 2003), Beijing, China, 2003.

[18] Nicolas Cerf, Mohamed Bourennane, Anders Karlsson, and N. Gisin., "Security of Quantum Key Distribution Using d-Level Systems," *The American Physical Society,* vol. 88, p. 4, March 25 2000.

[19] H. Zheng-Fu and L. Hong-Wei, "Security of practical quantum key distribution system," in *Intelligent Signal Processing and Communications Systems (ISPACS), 2011 International Symposium on*, 2011, pp. 1-3.

[20] R. Djellab and M. Benmohammed., "Securing Encryption Key Distribution in WLAN via QKD," presented at the International Conference on Cyber-Enabled Distributed Computing and Knowledge Discovery (CyberC), 2012.

[21] N Benletaief, H Rezig, and A. Bouallegue., "Reconciliation for Practical Quantum Key Distribution with BB84 Protocol," presented at the 11th Mediterranean Microwave Symposium (MMS), 2011.

[22] L Moli-Sanchez, A Rodriguez-Alonso, and Gonzalo Seco-Granados, "Performance Analysis of Quantum Cryptography Protocols in Optical Earth-Satellite and Intersatellite Links," *IEEE Journal on Selected Areas in Communications,,* vol. 27, pp. 1582-1590, 2009.

[23] D. Gottesman, L. Hoi-Kwong, Lu, x, N. tkenhaus, and J. Preskill, "Security of quantum key distribution with imperfect devices," presented at the International Symposium on Information Theory. ISIT 2004. Proceedings., Chicago, IL, USA, 2004.

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

[25] C.-H. F. Fung, K. Tamaki, and H.-K. Lo, "Performance of Two Quantum-Key-Distribution Protocols," *Physical Review A,* vol. 73, p. 012337, 2006.

[26] Fei Gao, Su-Juan Qin, Fen-Zhuo Guo, and Q.-Y. Wen., "Dense-Coding Attack on Three-Party Quantum Key Distribution Protocols," *IEEE Journal of Quantum Electronics,,* vol. 47, pp. 630-635, 2011.

[27] C. H. B. G. Brassard, "Quantum Cryptography: Public Key Distribution and Coin Tossing " *International Conference on Computers, Systems & Signal Processing,* p. 5, December 10 - 12, 1984 1984.

[28] S.-M. Zhao, F. Li, and B.-Y. Zheng, "A proof of security of quantum key distribution in probabilistic clone scheme," in *Communication Technology Proceedings, 2003. ICCT 2003. International Conference on*, 2003, pp. 1507-1509.

[29] J. Russell, "Application of quantum key distribution," in *Military Communications Conference, 2008. MILCOM 2008. IEEE*, 2008, pp. 1-6.

[30] N. Benletaief, H. Rezig, and A. Bouallegue, "Reconciliation for practical quantum key distribution with BB84 protocol," in *Mediterranean Microwave Symposium (MMS), 2011 11th*, 2011, pp. 219-222.

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

[32] A. Sharma, V. Ojha, and S. Lenka, "Security of entanglement based version of BB84 protocol for Quantum Cryptography," presented at the 3rd IEEE International Conference on Computer Science and Information Technology (ICCSIT), 2010.

[33] N. S. Yanofsky, M. A. Mannucci, and M. A. Mannucci, *Quantum computing for computer scientists* vol. 20: Cambridge University Press Cambridge, 2008.

[34] Charles H Bennett, "Quantum Cryptography Using any Two Nonorthogonal States," *Physical Review Letters,*, vol. 68, p. 3121, 1992.

[35] G. Álvarez Marañón, F. Montoya Vitini, and A. B. Orúe, "On the security of the Quantum Key Distribution protocols," 2001.

[36] A. Abushgra and K. Elleithy, "Initiated decoy states in quantum key distribution protocol by 3 ways channel," presented at the Systems, Applications and Technology Conference (LISAT), IEEE Long Island, New York, 2015.

[37] N. Gisin, G. Ribordy, H. Zbinden, D. Stucki, N. Brunner, and V. Scarani, "Towards practical and fast quantum cryptography," *arXiv preprint quant-ph/0411022,* 2004.

[38] D. Stucki, N. Brunner, N. Gisin, V. Scarani, and H. Zbinden, "Fast and simple one-way quantum key distribution," *Applied Physics Letters,* vol. 87, p. 194108, 2005.

[39] E. E. a. H. Serna, "Quantum Key Distribution Protocol with Private-Public Key," *Quantum Physics,* p. 3, May 12 2009.

[40] E. H. Serna, "Quantum Key Distribution from a random seed," *arXiv preprint arXiv:1311.1582,* p. 3, Nov. 12 2013.

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

[42] M. Stipčević, "How secure is quantum cryptography?," presented at the MIPRO, IEEE Proceedings of the 35th International Convention, Opatija, Croatia, 2012.

[43] A. Abushgra and K. Elleithy, "Security of Quantum Key Distribution," presented at the Northeast Section American Society for Engineering Education 2015 Conference ASEE, Northeastern University, 2015.

[44] Stefan Rass, Peter Schartner, and Michaela Greiler, "Quantum Coin-Fipping-based Authentication," presented at the IEEE International Conference on Communications (ICC'09) Dresden, Germany, 2009.

[45] H. Ma and S. Wang, "High performance quantum cryptography architectures in IEEE 802.11 WLAN," presented at the 2nd International Conference on Advanced Computer Control (ICACC), 2010.

[46] N. Bohr., "Can Quantum-Mechanical Description of Physical Reality be Considered Complete?," *Physical Rev.*, vol. 48, p. 696, 1935.

[47] A. Einstein, B. Podolsky, and N. Rosen, "Can quantum-mechanical description of physical reality be considered complete?," *Physical review,* vol. 47, p. 777, 1935.

[48] Xiaoyu Li and Liju Chen, "Quantum Authentication Protocol Using Bell State," presented at the The First International Symposium on Data, Privacy, and E-Commerce, ISDPE, 2007.

[49] John S Bell, "On the Einstein Podolsky Rosen Paradox," *Physics,,* vol. 1, pp. 195-200, 1964.

[50] T. Hwang and K.-C. Lee, "EPR quantum key distribution protocols with potential 100% qubit efficiency," *Information Security, IET*, vol. 1, pp. 43-45, 2007.

[51] N. S. Yanofsky and M. A. Mannucci, *Quantum computing for computer scientists* vol. 20: Cambridge University Press Cambridge, 2008.

[52] Kyo Inoue, Edo Waks, and Y. Yamamoto., "Differential Phase-Shift Quantum Key Distribution," presented at the Photonics Asia, 2002.

[53] K Inoue, E Waks, and Y Yamamoto, "Differential-Phase-Shift Quantum Key Distribution Using Coherent Light," *Physical Review,*, vol. 68, p. 022317, August 27 2003.

[54] Muhammad Khan, Michael Murphy, and A. Beige., "High Error-Rate Quantum Key Distribution for Long-Distance Communication," *New Journal of Physics,*, vol. 11, p. 063043, 2009.

[55] a. K. E. Abdulbast Abushgra, "Indexing Qubits Based on Matrix Processing By QKDP's," *Journal Of Theoretical Physics & Cryptography*, vol. 12, pp. 1-5, 2016.

[56] Muhammad Mubashir Khan, Jie Xu, and A. Beige., "Improved Eavesdropping Detection in Quantum Key Distribution," *arXiv preprint arXiv:1112.1110,*, p. 9, December 5 2011.

[57] H.-Y. Tseng, J. Lin, and T. Hwang, "New quantum private comparison protocol using EPR pairs," *Quantum Information Processing*, vol. 11, pp. 373-384, 2012.

[58] Abdulbast Abushgra and K. Elleithy., "Simultaneous Initiating EPR and Quantum Channel by Quantum Key Distribution Protocol," *Global Journal of Computer Science and Technology: E Network, Web & Security,* vol. 16, pp. 1-5, 2016.

[59] Abdulbast Abushgra and Khaled Elleithy, "A Shared Secret Key Initiated By EPR Authentication and Qubit Transmission Channels," *IEEE Access,* vol. 5, pp. 17753-17763, 2017.

[60] Shai Machnes, "QLib-A Matlab Package for Quantum Information Theory Calculations with Applications," *arXiv preprint arXiv:0708.0478,*, 2007.

[61] Fox Charles. (2003, Quantum Computing Functions (QCF) for Matlab. 1-10.

[62] Nathaniel Johnston. (2016, January 12, 2016). QETLAB: A MATLAB Toolbox for Quantum Entanglement. [Application]. Available: http://www.qetlab.com

[63] Marcin Niemiec and A. Pach., "The Measure of Security in Quantum Cryptography," presented at the IEEE Global Communications Conference (GLOBECOM), 2012.

[64] Peter Rohde, "Quack!-A Quantum Computer Siulator For MATLAB," *Centre for Quantum Computer Technology, Department of Physics,* p. 4, November 8, 2005.

[65] G. Tóth, "QUBIT4MATLAB V3. 0: A program package for quantum information science and quantum optics for MATLAB," *Computer Physics Communications,* vol. 179, pp. 430-437, 2008.

[66] S. M. Tan, "A quantum optics toolbox for Matlab 5," *J. Opt. B: Quantum Semiclass. Opt*, vol. 1, p. 161, 1999.

[67] T. Tentrup, T. Hummel, T. Wolterink, R. Uppu, A. Mosk, and P. Pinkse, "Transmitting more than 10 bit with a single photon," *arXiv preprint arXiv:1609.04200,* 2016.

[68] MacKay and D. JC., *Information Theory, Inference and Learning Algorithms*: Cambridge University Press, 2003.

[69] Yichen Huang, "Computing Quantum Discord is NP-Complete," *New Journal of Physics,* vol. 16, p. 033027, 2014.

[70] A. Abushgra and K. Elleithy, "QKDP's Comparison Based upon Quantum Cryptography Rules," presented at the 2016 IEEE Long Island Systems, Applications and Technology Conference (LISAT), 2016.

[71] Abdulbast Abushgra and K. Elleithy., "QKD Protocol Based on Entangled States by Trusted Third Party," presented at the 2017 IEEE Long Island Systems, Applications and Technology Conference (LISAT), 2017.