Differentiations of QKDPs in Run-Time Execution

Abdulbast Abushgra[#1], Khaled Elleithy[#2]

[#]*Department of Computer Science and Engineering*
University of Bridgeport
221 University Ave. Tech Building, Bridgeport, CT USA
[1#]aabushgr@my.bridgeport.edu [2#]elleithy@bridgeport.edu

Abstract—**Every day, the world opens its eyes on what are very interesting as new theories or devices, but quantum computing is one of the most interesting that will make huge changes in new technology. This paper will focus on this sparkling point and goes specifically with discussion to explain some relations between many aspects and assumes some improvements in a cryptosystem. The main point of this paper will be about generating secure secret key by quantum channel that called Quantum Key Distribution QKD.**

***Keywords*— Quantum Key Distribution, district variable, and continues variable.**

I. Introduction

For many years, scientists and researchers have been trying to create an efficient and secure way to communicate between two entities, which started with conventional cryptosystem described as coding "Cyphering" the plaintext that should be sent from Alice "sender" to Bob "receiver" without eavesdropping by Eve "eavesdropper". To prevent any impersonating or listening both Alice and Bob should send their message after encrypting it by the sender Alice and decrypting it by the receiver Bob. Generally, they use a code "message plus a key" to give cipher text and should be converted by Bob [2]. Cryptosystem has been used for a long time, began with Caesar Cipher, and until these days, several coding systems and algorithms have been used in many ways, but the most interesting invention was created by Bennett and Gilles Brassard, which was Quantum Cryptography (QC).

Quantum Key Distribution (QKD) has been emerged by combining cryptographic technologies with expanding these technologies by commercial enterprises in the United States [1]. QKD is an operation of sharing a key that contains a random string between two entities by encrypting the information in quantum protocol[2]. This system works on physics rules that have been found recently more interesting to play a distinguish role in the cryptography world, which is based on generating a key that will be shared between two users who may communicate on insecure channels. Then QKD has been tested to get two approaches in this system. One of them is a discrete variable (DV) having two parts approach that be coded in the quantum state of single photon, and the binary data should be measured by using single photon detector. The second approach is continuous variable (CV) that has been created recently and generated continuous variables that are encoded on coherent states of weak pulses of light, and continuous data values are measured with homodyne detection methods [1].

Even though the quantum computer might be far away from where we are, today many of the scientists and researchers work on the effects that could happen by this technology; especially breaking cryptosystem that is based on integer factoring such as ECC and RSA; which also provide security service such as confidentiality, data integrity and authentication "digital signature". Consequently, to break a public-key cryptosystem, a large quantum computer (~ 2000 qubits) is supposed to be existed, but the answer was put in the quantum mechanics itself; which is used to transmit a key in quantum protocol[3].

This paper will discuss the mechanism, which has been used in classical cryptosystem with quantum cryptography and the protocols that is still considered these days. It will be focused on BB84 protocol, SARG04, B92, COW, KMB09, EPR, S09, DPS and S13 that are still considered as most important protocols, although many protocols have been seen today in the quantum cryptography world.

II. Literature Review

To clarify what has been done in this field: first we have to mention to the point that changed focusing the scientists and cryptographers from the classical to on the quantum cryptography. When Peter W. Shor invented his algorithm named Shor's algorithm, and this was the starting point, until now. In the wide world, many of the theories are based on these facts. Shor's algorithm is defined as the factoring problem that can be reduced to finding the period of a certain function [book][4]. Today many protocols are concerned just what is needed. As we know, some of the protocols use only one-way quantum communication such as our point in this paper BB84 protocol, and E91. On the other hand, others of quantum key distributions use two-ways communications as Mean King problem[5].

A. Classical Cryptography.

As we know classical cryptography relies on the complexity of mathematics functions, and how to be difficult that even Eve cannot make a copy of the submitted message or tap some of it, but this is not true since classical cryptography is attacked by two kinds of the threat. One of them is active, and the other is passive. The history of classical cryptography had been created since 1900 B.C after finding some messages that had been written in a tomb in ancient Egypt [6].

1# Abdulbast Abushgra is PhD candidate in computer Science & Engineering at University of Bridgeport.
2# Khaled Elleithy is a professor in Department of Computer Science & Engineering at University of Bridgeport.

After that it has been shown many of the attempts that each one that can be made is going to be greatly and considerably complex. Julius Caesar had also a kind of cryptography style that is based on alphabetic cryptosystem. When the plaintext is sent from sender to receiver, it at this moment, can replace each letter with another systematic letter that moved by the sender and the receiver should know that. According to many of the code makers this is very weak because it depends upon exactly small probability "26 letters."

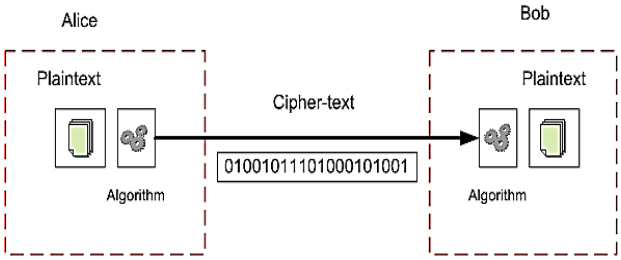

Figure (1) shows the simplified model of Symmetric encryption.

In general, the classical cryptography is insecure since the algorithms and used schemes are based on easy encoding to be broken by code breakers, but the mechanism that has been used in the classic cryptography still work as shown in figure (1). This main thought in cryptography whatever the strength of it is sending the plaintext from the sender "Alice" afterward this plaintext is encrypted by one of the algorithms (e.g. DES, AES,.,.,.), next it is sent as a cipher text through one of the classical communications to be received by Bob, who already tries to encrypt the cipher text by converting the submitted code even he can get the original message.

Furthermore, many of the encryption algorithms have been used in different usages, but each one is better than the others by the encryption key, which specifies the strength or the weakness of using encryption code. Basically, being secure is the first target that Alice and Bob is willing to be, since if Eve captured the key by any of attacking ways the message in turn will be clear.

B. Quantum Cryptography.

In general, for a long time quantum cryptography has been controlling on the scientists' mind because it is the planned solution to many of today's communications. While the main target in cryptosystem is preventing any entities to reach given data except legality communicators, the confidentiality, here is very important to be ensured that means incapability to read the message between sender and receiver.

Quantum cryptography is considered as a symmetric key cryptography (QKD), where is very common to use and gives the confidentiality that we are looking for. Moreover, the key that is used in this mechanism usually be a long string of bits. The interesting point in quantum cryptography is any eavesdropper cannot make a copy of the original qubit and the same time sends it to an intended receiver because if this happened the receiver or the sender for sure will know that. Therefore, dealing with quantum security is a much-needed solution to many communications that are happening these days.

Many requirements have to be done to get a secure connection; one of these requirements is having the quantum channel to transmit data "qubits" to party included information about key distribution. The second one is a classical channel that should be used to know that if the key distribution was seen by eavesdropper or not[7].

Quantum mechanics is one of the spot lights that will convert some of the rules in the cryptography world, where we probably know in the future that public key would no longer work, so quantum key distribution could be the solution in next-generation[8]. Furthermore, the information in quantum mechanics is kept from the eavesdropper by laws of physics, which treats this capability by exchanging the encryption key that is sent on single photon[6].

C. The BB84 protocol.

BB84 was proven in 1984 by Charles Bennett and Gilles Brassard; the goal of this protocol is Alice would send a secret key to Bob into secure channel "Quantum channel," so the operation is described as tossing-coin. In this protocol, it should be two communication channels that will be between quantum and data channels, which the quantum channel is considered as free space or fibre-optic cable. The data channel is any means to transmit the data by, and it is not necessary to be secure. Furthermore, both of the sender and the receiver are indispensable to have random number generators, and four of polarizing filters to pass qubits. This requires the filters to be standardized at ± 15 degrees of the horizontal and vertical plains[9].

To generate a key by this operation, each side of the communicated party (the sender and receiver) should have a generator, which must be in convenient position. The generator can be set in the middle between both. Additionally, when the sender starts sending a single qubit that can be encrypted by QKD process, so the sender and the receiver select and record the filter for each qubit randomly. On the other hand, if the sender and the receiver try to share quantum entanglement, as well as classical communication channels, this gives them permission to submit qubit between each other, but it is not necessary to reduce the number of bits that is supposed to be sent into the classical channel [10].

Using the randomness in an encryption algorithm is a probabilistic encryption, where encoding the same information many times gives various of cipher text [11]. Even though many schemes have been published showing that BB84 is inefficient, and has weak points in its encrypting mechanism, BB84 is still the background that most of researchers and scientists have come up their ideas from this protocol because BB84 links between the simplicity and the durability.

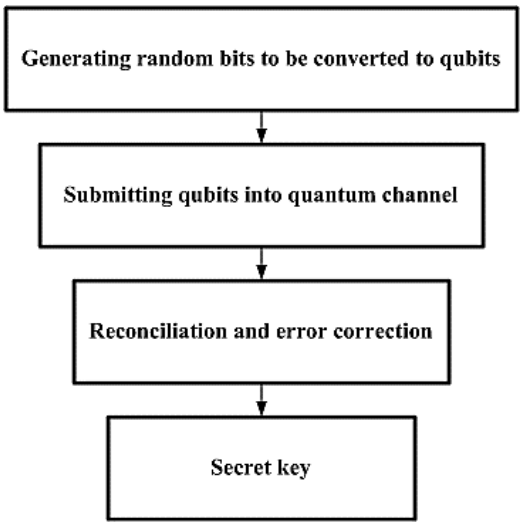

Figure (2) shows the main process in quantum key distribution.

Quantum key distribution is based on none cloning theorem, and Heisenberg uncertainty principle in its security, and also it is guaranteed by none cloning that is derived by superposition principles of quantum mechanism[12]. These features give the protocol more readability in use, but this is not enough because the attackers never stop trying to break any found protocol. So the majority of quantum key distributions these days can be identified under two specializations. The first one is based on non-orthogonal, and the second is based on the quantum-tangle, where both need to go into the same process that shown in figure (2)[13].

- *How quantum key distribution works.*

There are many steps that should be done until each part of the communication can share the secret key;

1. A length (K) should be generated by Alice to be sent to Bob into quantum channel by quantum basis "Qubits", in this case perhaps Eve tries to look at it.

TABLE (1)

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	→	↑	↖	→	↑	↑

2. There are two kinds of attacks if Eve has tried to read the submitted message to Bob. One of these attacks is called intercept/resend attack, and the second one is splitting.
3. When the message reaches to Bob, he tries to read it by measuring the bits that have been sent from Alice, all this happens through quantum channel, and naturally he could not measure all the submitted bits because of some reason like eavesdropping from Eve or dark counts in Bob's detecting device.

TABLE (2)

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

4. After reading Alice's message, Bob announces to Alice by public channel, which is telling her that Bob read the message by his selected own basis.
5. Both Alice and Bob start estimating the errors that could be eavesdropped by Eve, and there are many protocols that are used here but we are focusing on BB84 protocol with mentioning to some of others. The raw secret key is the process when Alice and Bob are comparing the matched bits, which discard the uncorrelated data and is called the shifting procedure. This enhances detecting any attempts by Eve, where legitimate parties can know if Eve tried to gain any information[14].

TABLE (3)

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	

6. Alice and Bob will calculate what both of them have and compare their bits. If the bit error rate was very high, they basically will cancel this communication and start another new one, but if the bit error rate is very low, they can correct it.
7. After that, both Alice and Bob have shared key "raw key," but in fact it is not shared key because Alice and Bob's versions are different. They just remove the m bits from the shared key.
8. Alice and Bob start again correcting the wrong bits in non-compared parts of keys, and they try to reduce the number of bits that are known by Eve.

TABLE (4)

Alice and Bob publicly compare half of the remaining bits						
Bit number	0	1	2	3	4	5
Shared secret keys		1	1		1	
Randomly chosen to compare			✓		✓	
Shared secret key		1	1		1	
Agreements			✓		✓	
Unrevealed secret keys		1				

9. After checking that Alice and Bob share a key that has same string of bits "secret key" [15, 16]. Moreover, Alice can cheat in her position by sending a different

of basis “rectilinear and diagonal photons”, or photons that neither rectilinearly nor diagonally, so that she will not be in position to agree with any of Bob’s table records in step (3) because Bob’s table will record the result of probabilistic behaviour not under her control[17].

Hence, it is very important to see that if Alice tried to cheat in step (1) “for example”, by sending a mixture of rectilinear and diagonal photons, or photons neither rectilinearly and diagonally. Here she will lose the ability to agree with what have been recorded in Bob’s table after step (1). That is because the records are under probabilistic behaviour, not her control[17].

- *Functionality of BB84.*

As we know, BB84 is secure as mentioned in [18], but it is more complex, and this complexity depends on the physicality that causes during generating the key. Generally, BB84 protocol’s goal is as One-Time-Pad protocol whence Alice wishes to send a key to Bob into the Quantum channel. Here, some details that describe the protocol more precisely:

In superposition, Alice sends a basis that should be either in (×) basis or (+) basis (as mentioned above), where in this case, Bob has to work on one of these. Furthermore, if Alice sent the × basis to submit a $|1\rangle$, she will send a $|\nwarrow\rangle$. As the same, if she wants to send a $|\uparrow\rangle$ and Bob measured as $|\uparrow\rangle$ in the + basis, he will record a $|1\rangle$. Furthermore, if Alice sends photons as $|\nearrow\rangle$ or $|\nwarrow\rangle$ and Bob just measures the photons in the basis (+), that means the measurement in a superposition of states as following:

$$|\nearrow\rangle = \frac{1}{\sqrt{2}}|\uparrow\rangle + \frac{1}{\sqrt{2}}|\rightarrow\rangle \quad \ldots\ldots\ldots\ldots \quad (1)$$

Or

$$|\nwarrow\rangle = \frac{1}{\sqrt{2}}|\uparrow\rangle + \frac{1}{\sqrt{2}}|\rightarrow\rangle \quad \ldots\ldots\ldots\ldots\ldots \quad (2)$$

Then, we can say that there is a 50% chance of recording $|0\rangle$ or $|1\rangle$ by Bob. Therefore, there are four possibilities[4] :

$$|\nwarrow\rangle \text{ with } (+) = \frac{1}{\sqrt{2}}|\uparrow\rangle - \frac{1}{\sqrt{2}}|\rightarrow\rangle \quad \ldots\ldots\ldots\ldots \quad (3)$$

$$|\nearrow\rangle \text{ with } (+) = \frac{1}{\sqrt{2}}|\uparrow\rangle + \frac{1}{\sqrt{2}}|\rightarrow\rangle \quad \ldots\ldots\ldots\ldots\ldots \quad (4)$$

$$|\uparrow\rangle \text{ with } (\times) = \frac{1}{\sqrt{2}}|\nearrow\rangle + \frac{1}{\sqrt{2}}|\nwarrow\rangle \quad \ldots\ldots\ldots\ldots \quad (5)$$

$$|\rightarrow\rangle \text{ with } (\times) = \frac{1}{\sqrt{2}}|\nearrow\rangle - \frac{1}{\sqrt{2}}|\nwarrow\rangle \quad \ldots\ldots\ldots\ldots \quad (6)$$

These possibilities have been reflected on the Bloch sphere to show that measuring polarizations of each state can be in 3D space as (*x*, *y*, and *z*).

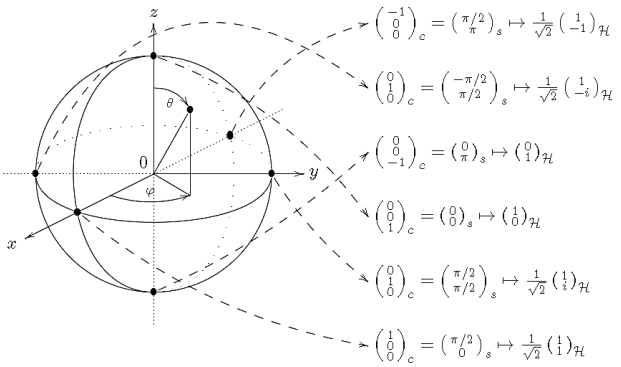

Figure (3) shows Bloch sphere.

III. THE SECURITY OF QUANTUM

There are three categories that cryptosystem designers try to achieve: First, it is designing a cryptographic algorithm, where the submitted data should be mixed up heavily to be more complex; creating encryption keys that work as unlock and lock the algorithm; and distributing the secure keys between communicated entities[9]. Furthermore, several attempts still work to break QKD or to show the weak point in this protocol, but unfortunately, until now none of them can prove that, even when someone “Eve” tries to read or intercept the submitted message “Qubits” and generate new qubits instead of them. She wishes to read and generate just 25% of the original message, and the rest of it stays as null[9].

One of the well-known attacks against QKD is intercepted/resend strategy that is actually the most popular use, which is based upon when Alice sends her qubits to Bob. Eve in the same time replaces some of qubits by applying random bases’ measurements and leaves the rest of these qubits without changes that will reach to Bob as the same as be sent. Next, when both of Alice and Bob start to compare the matching qubits, Eve constructs her one by leaving bits to be incompatibility measurements[19].

More precisely, if the eavesdropper “Eve” tries to tap on what is moving between Alice and Bob, and she and Bob used the identical bases sent by Alice. Bob will get the alike basis and also the eavesdropper, where nobody can detect Eve. In other word, if Eve used different measurements to intercept the bases sent by Alice, she will be on the face of uncertainty change the polarisation[20].

IV. SARG04 PROTOCOL

A. Functionality of SARG04.

This protocol came from the original protocol BB84. SARG04 was written by Scarain-Acin-Ribordy-Gisin in 2004. Inventing SARG04 protocol came after four states used BB84, and they thought it could build a protocol that would be more robust than BB84; specially when weaken laser pulses are used instead of single photon source. They worked on

SARG04 to be more efficient against the PNS attack. Furthermore, SARG04 and BB84 basically equivalent to each other in the quantum communication phase, but the difference is shown in the encoding and decoding of classical information.

SARG04, in fact, was as looking further to solve some situations such as the information that is produced by weak pulses and received by an incomplete detector[21].

Even though SARG04 came with a new vision, it still respects the BB84 in its instructions; for example, when Alice starts to match the key with equivalent qubits from Bob, the bit error rate could reach to $v_s/2$ or more precisely, it has probability until ½. Then it can be seen that the difference occurs when measuring the detection rate in SARG04. It will increase in the presence of error, unlike with BB84 is satisfied by sifting in:

$$\varepsilon_n = \frac{\tilde{\varepsilon}_n}{\frac{1}{2} + \tilde{\varepsilon}_n}$$

To show the sequential steps between two legitimate parties Alice and Bob, we can summarize it as SARG04 in one-way communication where a v-photon source (v = 1, 2) as following:

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

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

Step 3: Alice reports for each signal from where the states were chosen of the sets. Then Bob matches the result by two states. If the result was proven as orthogonal to one of the states in the set that means the other state has been sent. On the other hand, the match was not orthogonal to each state in the set. In this case, Bob knows it is not incisive result, so he asks Alice about what he got if it is the right result or not.

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

Step 5: According to what is in previous step, both Alice and Bob keep the only conclusive untested bits that will be used in specifying bit error correction and privacy amplification[22].

V. B92 Protocol

A. Functionality of B92.

B92 was proposed in 1992 by Bennett as a protocol in QKD, and it has been involved in this protocol just two state rather than two in BB84. The two states should be non-orthogonal as shown the figure (4). The process in this protocol is involved in the quantum phase:

1. Alice sends to Bob a set of qubit strings randomly, where $A \in \{0,1\}^n$, n >N (which N is the length of final key), so if Alice sent the state $|0\rangle$, that means $A_i = 0$, and $A_i = 1$ if she sent state if $|+\rangle$, for all $i \in \{0,1,\ldots..n\}$.
2. On the other side, Bob creates a vector of bits where $B \in \{0, 1\}^n$, $n > N$ which if $B_i = 0$ then Bob chose the basis $\oplus$ and if $B_i = 1$, he chose the basis $\otimes$ for all $i \in \{0,1,\ldots\ldots n\}$.
3. When Alice's qubits reach to Bob, he measures them by the selected bases ($\oplus$ or $\otimes$).
4. After measuring the vector of states, he starts complying the following rules. If the measurement of Bob produces $|0\rangle$ or $|+\rangle$ then, $T_i = 0$ and if it produces $|1\rangle$ or $|-\rangle$, $T_i = 1$ for all $i \in \{0, 1\ldots n\}$.

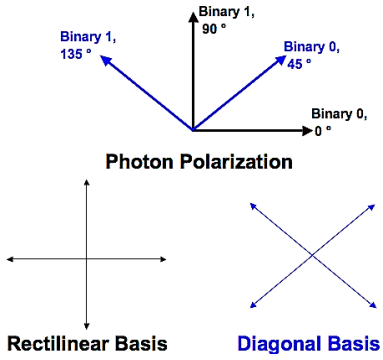

Figure (4) shows the polarized states in B92

VI. Coherent One-way protocol

It is a simple protocol, which it depends upon decoding the information in time. Alice (emitter) sends coherent pulses either in logic states as {0, 1} or decoy state. Each logical bit is encoded to μ - 0 for logical "0" or 0 - μ for logical "1" by sequences of two pulses.

Furthermore, to improve the security of this protocol, Alice adds decoy sequences μ - μ during sending the logical states. So, if the submitted pulses in Bob side on the interferometer is well aligned, that basically considers all detections on D_{M1} (interferometer) and no detection on D_{M2} (detector). When loss of coherence is seen on the detector, it describes a presence of eavesdropper [23].

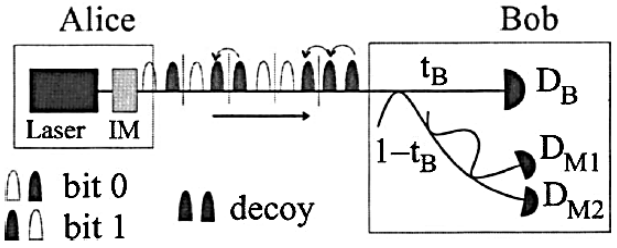

Figure (5) shows Coherent One Way Scheme.

In this protocol, the transmission and reception of data depend on the time of arrival of the signal and do not depend on the polarization of the optical signals.

The protocol briefly works as following:

Step 1: It starts with Alice sending a sequence of binary bits using time slots to be transmitted to Bob, as known generating both logical state |1> or |0> has same probability unless adding decoy state, so while getting |1> or |0> by probability ½ to each of them, and adding the decoy state is calculated by ((1-f)/2) (where, f is the probability of decoy state generation).

Step 2: Bob exploits the time detection to generate the raw key that all of these processes will be done by different detectors for having security.

Step 3: Bob declares the number of bits by simultaneously procedures between data detector and time detection in his side.

Step 4: On the monitoring detectors, Alice ensures that the sequence of decoy states and bit sequences are still existed, if not that explains Eve tapped to communication; then in this case Alice will break the coherence to each two pulses to be able to detect it.

Step 5: Alice informs Bob about the bits that she has removed from the raw key since they belongs to the decoy state sequence.

Step 6: The secret key is extracted after dropping the decoy sequences from the raw key by using classical process and with an error correction and privacy amplification can be obtained the shared key[24]

This protocol as mentioned in [25] is designed as more robust quantum protocol against reduced interference visibility and photon number-splitting (PNS) attacks.

VII. KMB09 PROTOCOL

This protocol basically was created in 2009 by (Khan, Murphy, Beige), which designed to be robust against photon number splitting attack. *Khan et. al*, described the protocol that being between two parties (Alice and Bob) and an eavesdropper (Evan), and then both must use two bases states *e* and *f*, where the condition should both of them have different indices *i* when both use the same basis[26]. Moreover, *i* index is publically announced between two legitimate parties, which can be pointed to Alice's prepared indices as *i*, and Bob's measured indices as *j*.

In KMB09, the authors have tried to create a protocol able to be against *intercept-resend attack*. KMB09 was created when the other protocols have been employed to few kilometres, but after that the system error rate could exceed the eavesdropper's presence. Also, they optimized this work by testing Quantum Bit Error Rate (QBER) and Index Transmission Error Rate (ITER). To briefly explain how KMB09 is designed, it will be as in the following steps:

1. Alice generates randomly a sequential classical bits, and then randomly specifies to each bit an index *i = 1, 2,....., N*.
2. Alice sends the prepared bits in single photons into $|e_i\rangle$ or $|f_i\rangle$ to Bob.
3. Each incoming state is measured by Bob to be randomly switched between the basis *e* and *f*.
4. Alice announces in public communication with Bob the random sequential indices *i* to get the secret key.
5. Bob translates the measurement outcomes.
6. Bob communicates with Alice publically to tell her the photon measurements were successfully received and obtained the secret key.
7. Alice and Bob can determine whether Eve was eavesdropping to their communication or not[27].

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

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

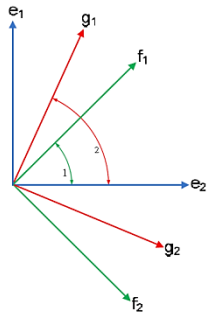

Figure (6) Shows 2 Basis vectors used by Alice, Bob and Evan in the N = 2 protocol.

VIII. EPR PAIR PROTOCOL

EPR is back to Einstein, Podolsky ,and Rosen, who presented in a famous paper in 1935, that has been led to argument around quantum mechanics is not complete physical theory. The main thought utilizes three states of polarization with considering $|\theta>$, 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, for example, in the right side; the outcome can be vertical linear polarization state |0>. On the other hand, at the left side the measurement will be the opposite, horizontal linear polarization state $|\pi/2>$ and vice versa. The EPR is one of the four bell states:

$$|\psi_1\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$$
$$|\psi_2\rangle = \frac{1}{\sqrt{2}}(|00\rangle - |11\rangle)$$
$$|\psi_3\rangle = \frac{1}{\sqrt{2}}(|10\rangle + |01\rangle)$$
$$|\psi_4\rangle = \frac{1}{\sqrt{2}}(|10\rangle - |01\rangle).$$

IX. S09 PROTOCOL

S09 protocol was created by Eduin Esteban in 2012, where this protocol has different technique according to the previous protocols. S09 is based on the public-private key cryptography, and the main idea of this protocol is that Alice and Bob are exchanging a qubit multiple times to build a secret key. Moreover, it transfers the qubit in any arbitrary states that will be between Alice and Bob just through quantum channel.

The sequences of the protocols steps are explained briefly as fallowing:

Step 1: It starts with generating a bit ***i*** by Alice that would be in element of a secret base $\mathbf{B_k}$ to create the qubit $|\Psi, k\rangle$, which in turn is sent to Bob into quantum channel.

Step 2: Bob in the other side, applies $\mathbf{U_j}$ to the qubit $|\Psi, k\rangle$ that should be known just by Bob, and then sends the outcome of qubit to Alice.

Step 3: When Alice receives the qubit, she measures it in the base B_k including the bit j, where the qubit must be in a pure state by the operator density [26]:

$$\rho = |\Psi, k\rangle\langle\Psi, k|$$

Where this qubit interaction with the environment produces.

$$\acute{\rho} = \sum_j E_j \rho E_j^{\dagger} \qquad \ldots\ldots\ldots\ldots\ldots\ldots \quad (7)$$

Where, $\mathbf{E_j}$ operator acting in the space of a qubit. After that, these operators will convey the state of qubit $|\Psi, k\rangle$ in the overlap.

$$|\Psi, k\rangle \rightarrow E_j |\Psi, k\rangle \qquad \ldots\ldots\ldots\ldots\ldots\ldots \quad (8)$$

Step 4: After a complex operation in (3), parity bits are appended by or/and.

Step 5: The previous step will be attached to be a distribution and sending addresses or the hashed values.

In this approach of this protocol, Eve can get nothing of her eavesdropping since $\mathbf{B_k}$ and $\mathbf{U_j}$ transformations can be changed as frequently as needed.

X. S13 PROTOCOL

S13 is a quantum key distribution protocol was created by Eduin H. Serna in 2013. This protocol comes with corresponding to BB84 in the quantum procedures, but it differs in the classical channel. S13 has been created to be implemented in existing devices with no need to any modifications [28].

Generally, S13 has the same quantum part of BB84 that will be escaped in this paper and get to the second part where the differences between both are:

1. Quantum Part

- *Raw key exchange*: (as shown in BB84).
- *Random seed*: one of the communicators creates a random binary string $x_1\ x_2\ \ldots\ldots\ x_N$.
- *Missing key exchange*:
  - Alice makes a summation of the random binary string with the binary basis in the first part, which obtains binary basis $t_1\ t_2\ \ldots\ldots\ t_N$. Then she generates another string of binary randomly $j_1\ j_2\ \ldots\ldots\ j_N$, where this will be as an exchanged key with Bob.
  - Bob sums each of the sequences sent by him to Alice with the created binary string as $(1 \oplus m_k) \oplus x_k$, where $k = 1,2,\ldots\ldots N$. Then it will come up the binary string basis $n_1\ n_2\ \ldots\ldots\ n_N$. After that he measures the received state $|\Psi_{t_k\ j_k}\rangle$ with the corresponding of the base $\mathbf{B_{nk}}$ to generate $b_1\ b_2\ \ldots\ldots\ b_N$.

2. Classical Part

Alice and Bob apply in different binary to the function f to exchange a set of binary string:

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

a. Asymmetric cryptography.

- Alice sums the binary string created by her in quantum part *i* with the random string of binary values that created in missing key exchange *j*.

$$i_k \oplus j_k\ ,\ k = 1, 2, \ldots\ldots\ldots\ N.$$

To obtain $y_1\ y_2\ \ldots\ y_N$, that will be sent to Bob.

- To obtain the public key, Bob encrypts:

$$u_k = n_k \oplus f(m_k, a_k, b_k \oplus y_k),$$

$$v_k = n_k \oplus f(m_k, b_k, a_k \oplus y_k).$$

- Alice makes summation to have the private string of m_k, which is:

$$t_k \oplus f(s_k, (1 \oplus i_k) \oplus u_k, j_k \oplus v_k),$$

And then decrypts the string $m_1\ m_2\ \ldots\ m_N$.

b. Private Reconciliation

- Bob receives the binary sequence $l_1\ l_2\ \ldots\ldots\ l_N$ after finishing the comparison between $s_1\ s_2\ \ldots s_N$ and $m_1\ m_2\ \ldots\ m_N$ by Alice.
- Bob sums the sequence of basis m_k with l_k , where $(m_k \oplus l_k)$, $k = 1, 2, \ldots\ldots\ldots\ldots\ N$.

This is to obtain the private string s_k.

$$f(l_k, a_k, b_k \oplus y_k) \equiv i_k$$

$$f(l_k, a_k \oplus y_k, b_k) \equiv j_k \qquad k = 1, 2, \ldots\ldots\ N.$$

Then, Bob gets the private string from Alice $i_1\ i_2\ \ldots\ldots\ldots\ i_N$.

XI. DIFFERENTIAL-PHASE-SHIFT (DPS)

This protocol was created in 2002 by Kyo Inoue, Edo Waks and Yoshihisa Yamamoto. DPS is based upon non-orthogonal four states, which Alice's photon splits to three pulses, and it is randomly modulated. On the other side, Bob measures the coming photons by measuring the differential phase. As mentioned in [3] DPS protocol is more convenience for fiber optics transmission and offering a key creation efficiency higher than BB84.

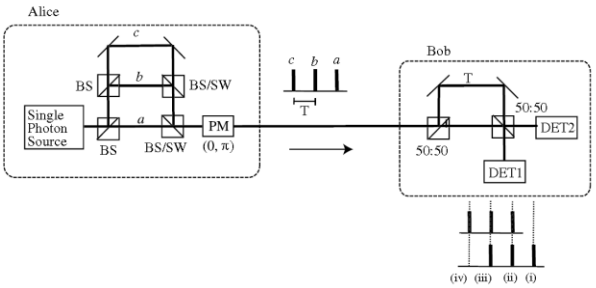

Figure (7) shows the DPS scheme.

Technically, DPS is utilized to create a secret key between two parties, and it starts at Alice's side when the single photon is divided to three paths (a, b and c) and then recombined them by beam splitter (BS) or optical switcher (SW) as it is seen the figure (1). Moreover, the time delay between a, b and b, c are equal, so that the recombined photon is converted to each of (0 or π). The incoming photons from Alice to Bob are divided to two paths and recombined them by 50:50 beam splitter. The whole process of DPS are done in the following steps and based on the figure (1):

1. At Alice's side, a photon is sent from (a) to the short path in Bob's side.
2. A photon pushes through (a) to the long path in Bob, and through (b) to the short path in Bob.
3. A photon pushes through (b) to the long path in Bob, and through (c) to the short path in Bob.
4. A photon pushes through (c) to the long path in Bob.

In the first part of processing, two probabilities are interfered in step (2) and (3), where the phase difference is 0 or $\pm\pi$ depending on Alice's modulation. Furthermore, each of the detectors clicks on 0 and the other on $\pm\pi$ phase difference. At the end, when Bob's detectors click, Bob just records the time and which detector clicks. After that, with classical communication between Bob and Alice, she knows which one clicked at Bob's detector [25].

Table (5) shows the comparisons between quantum key distributions

Cases	Quantum Key Distribution Protocols								
	BB84	**B92**	**SARG04**	**COW**	**KMB09**	**EPR**	**S09**	**S13**	**DPS**
Properties	Heisenberg	Heisenberg	Heisenberg	Entanglement	Heisenberg	Entanglement	Public private key	Heisenberg	Entanglement
Number of States	4 states	2 States	4 States	Time slots	2 states	Entangled 2 of photons	arbitrary states	4 states	4 States
Detection of presence	QBER	QBER	QBER	Break of coherence	ITER	complemente d state	appending parity bits	Ran. Seed Asymmetric	Time-instance
Polarization Situation	2 orthogonal	1 non-orthogonal	coded bits	No, using DPS	No	No	Bit-Flip Phase-Flip	2 orthogonal	4 non-orthogonal
Probability of each state	Various	50%	50%	equal	50%	equal	Various	Various	equal
Qubit case	DV	DV	DV	DV	DV	DV	No	DV	DV
Classical channels	Yes	Yes	Yes	Yes	Yes	Yes	No	Yes	Yes
Decoy States	No	No	No	Yes	No	No	Yes	No	No
Sifting phase	Revealing Bases	Alice = 1 - Bob	Revealing non-orth. state	revealing the times 2k+1	determining the error rate	Bell's Inequality	No	Revealing Bases	No
Bell's inequality	No	No	No	No	No	Yes	No	No	No
PNS attack	Vulnerable	Vulnerable	It's better than BB84	Robust	Robust	N/A	N/A	N/A	Robust
IRUD attack	Vulnerable	Vulnerable	Vulnerable	Under Test	Under Test	Vulnerable	N/A	N/A	N/A
Beam-Splitting attack	Vulnerable	Vulnerable	Robust	Robust	Robust	Vulnerable	N/A	N/A	Robust
Denial of Service attack	Vulnerable	Vulnerable	Vulnerable	Vulnerable	Vulnerable	Vulnerable	N/A	N/A	Robust
Man-In-The-Middle attack	Vulnerable	Robust	Robust	Robust	Robust	Robust	Robust	N/A	Robust
IRA attack	Vulnerable	Vulnerable	Robust	Robust	Robust	Bell's inequality	Robust	N/A	Robust

These information were collected from different resources (journals, articles and conference paper) and whole information and data above have been based on either the original studies or the last improvement. Also, this paper just received nine of the most famous protocols that will be a base to quantum computer world. Furthermore, some of the details have been received from the original publication where it was not studied more than one or two; On the other hand, others were had the details from different studies such asBB84, which has plenty of studies in different approaches [24].

XII. THE COMPARISON BETWEEN QUANTUM PROTOCOLS

This paper has included many important approaches that have been extracted from each studied protocol and looked at the difference that could be a weak or a strong point in these operations of establishing the quantum connection between two parties. As shown above, some details that were collected from journals and papers reflect the major definition to each protocol, especially when a certain protocol receives a unique way than others such as what happened in Coherent One Way protocol that depends upon decoy states. Moreover, this comparison is based on the first or original scheme of each protocol, which some of these were improved by scientists to be more reliable and secure.

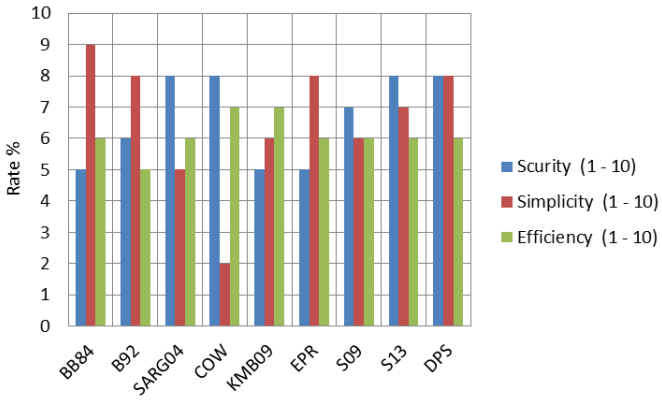

Figure (7) shows comparing the Quantum Key Distribution Protocols by security, simplicity and efficiency rate.

Furthermore, there are two protocols (BB84, B92) that were compared in the runtime to whole protocol by MATLAB, where this simulation shows the simplicity for B92 in creating more bits than BB84. This depends upon many aspects included in scheme each one of these protocols. Moreover, the paper presents the Run-Time simulation to the whole studied protocols in this paper by quantum libraries in MATLAB, where all these simulations show the simplicity and difficulty of running each protocol. Meanwhile, these simulations were done at 500 bits long of the secret key, where each protocol has independent scheme regarding how many bits can be sent by Alice to Bob and the complicity of the algorithm when it is sent.

After simulating the Run-Time execution function ***T(n)*** during each QKD protocol algorithm, it has seen that the complexity in each protocol will cause increasing in Run-Time execution. For instance, SARG04 protocol is similar to BB84 protocol, but SARG04 has a complexity higher than BB84, which means taking more time to generate a secret key. More precisely, many execution loops happen in SARG04; especially in reconciliation phase unlike BB84. Also, the simplicity reflects the Run-Time execution in easy mode, and the BB84 protocol is ranked at the top of this simulation.

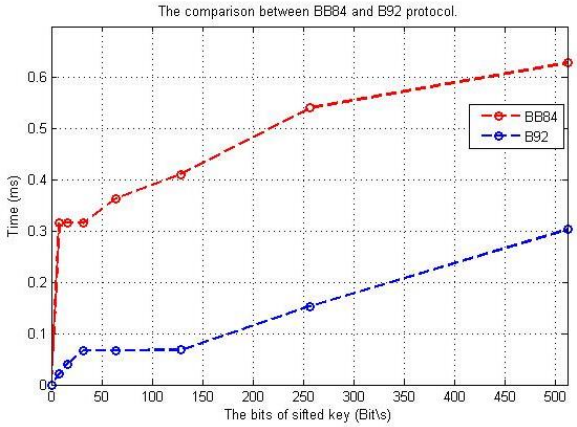

Figure (8) shows the comparison between BB84 and B92.

The shown graphs in [9-10-11-12-13-14-15-16-17] explain each protocol was studied in this paper, and the graphs show how much time it takes each protocol to execute 500 bits from Alice side to Bob. Basically the gaps between each execution time depend on which states and bases used in the protocol as explained above. Also, it has relation with the type of connections between two parties (e.g. quantum channel, public channel). The result in these measurements exactly was done in absence of Eve and also it was considered to run a connection without any error that usually would be characterized either in current fibre-optics or free-space link.

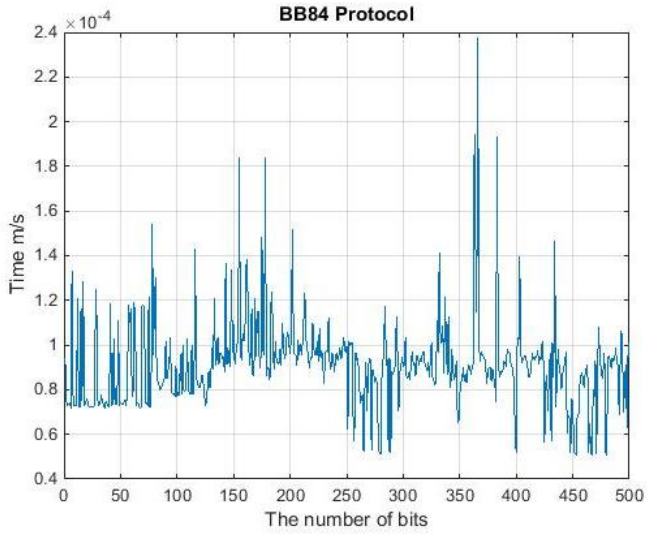

Figure (9) shows the run time execution for BB84 Protocol.

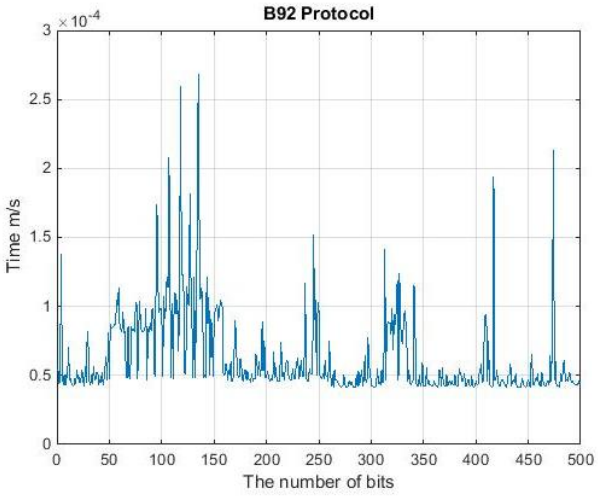

Figure (10) shows the run time execution for B92 Protocol.

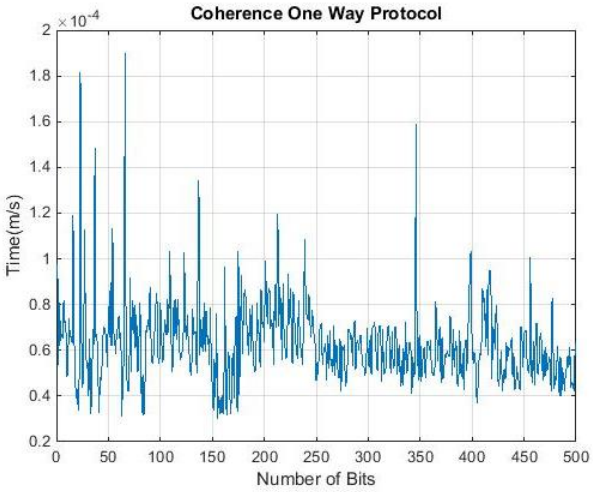

Figure (13) shows the run time execution for COW Protocol.

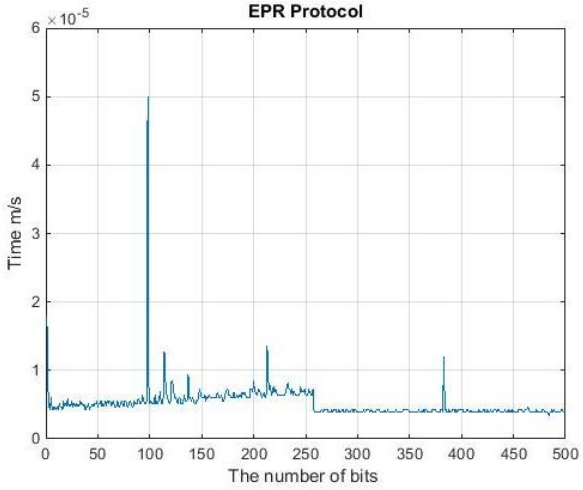

Figure (11) shows the run time execution for EPR Protocol.

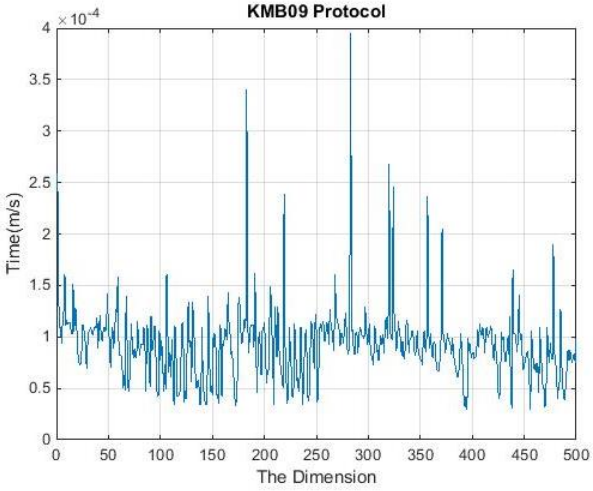

Figure (14) shows the run time execution for KMB09 Protocol.

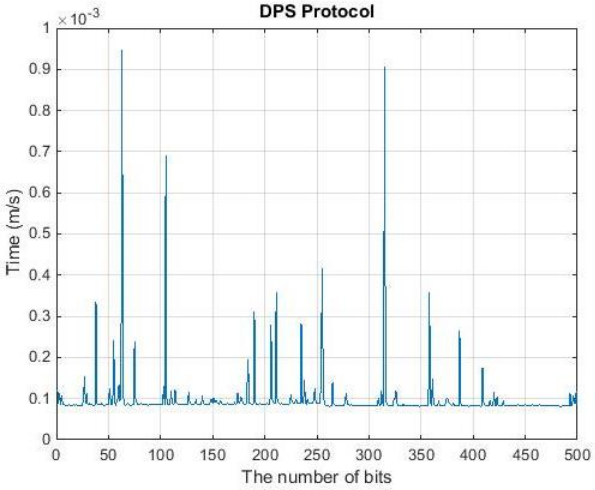

Figure (12) shows the run time execution for DPS Protocol.

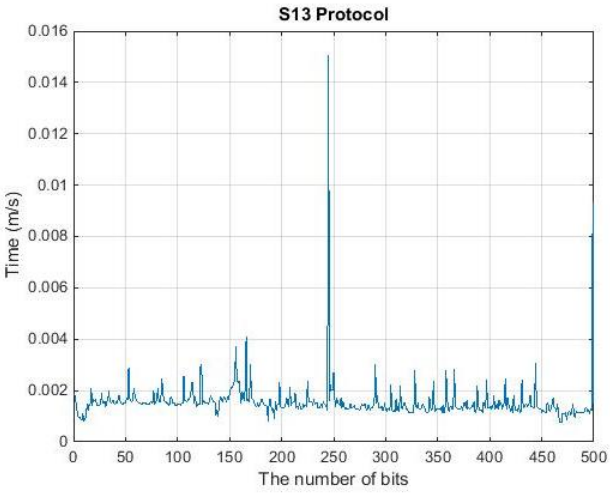

Figure (15) shows the run time execution for S13 Protocol.

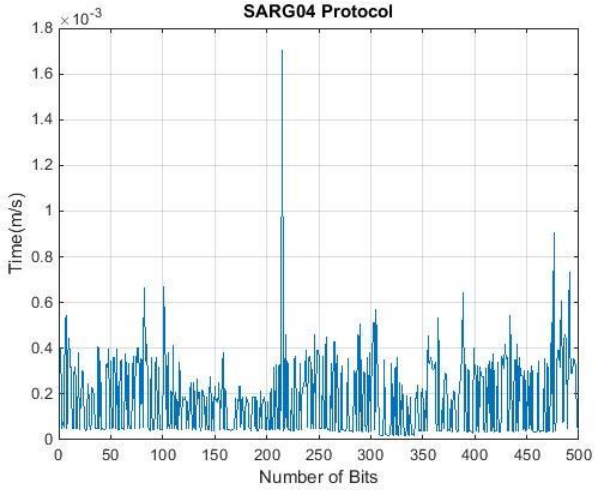

Figure (16) shows the run time execution for SARG04 Protocol.

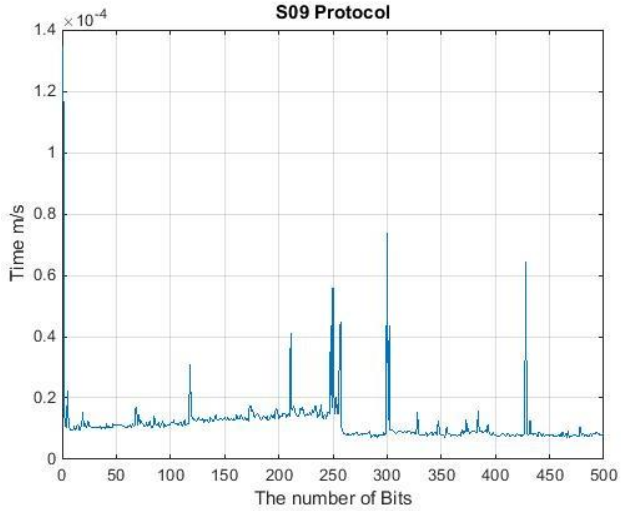

Figure (17) shows the run time execution for S09 Protocol.

XIII. CONCLUSION

This paper presents the quantum key distribution protocols (QKDP) in a period of time, where it considers as converted point in the computer science world. Moreover, through this paper we can follow what has been done, and also shown the variation between these protocols to be clear to see the efficiency to each one of them. Furthermore, it helps to start thinking in an efficient quantum protocol scheme that is based on the factors and situations that the protocol scheme built in. Further, one of the most important issues that discovered here is quantum key distribution protocols are still under study and experimental work, which it can be seen clearly in each protocol where no one of them has completely been finished and in contrast many of the weak points found each time. Finally, QKD protocol is a wide area that contains many considered specifications such as quantum information, quantum memory, quantum architecture, and quantum cryptography. All of these need to be done so that the quantum system works correctly and efficiently.

REFERENCES

[1] L. Oesterling, D. Hayford, and G. Friend, "Comparison of commercial and next generation quantum key distribution: Technologies for secure communication of information," in *Homeland Security (HST), 2012 IEEE Conference on Technologies for*, 2012, pp. 156-161.

[2] N. Walk, T. C. Ralph, T. Symul, and L. Ping Koy, "Security of post-selection based continuous variable quantum key distribution against arbitrary attacks," in *Lasers and Electro-Optics (CLEO), 2011 Conference on*, 2011, pp. 1-2.

[3] R. T. Possignolo and C. B. Margi, "A Quantum-classical Hybrid Architecture for Security Algorithms Acceleration," in *Trust, Security and Privacy in Computing and Communications (TrustCom), 2012 IEEE 11th International Conference on*, 2012, pp. 1032-1037.

[4] N. S. Y. a. M. A. Mannucci, "Quantum Computing for Computer Science " 2008.

[5] M. Yoshida, T. Miyadera, and H. Imai, "On the security of the quantum key distribution using the Mean King Problem," in *Information Theory and its Applications (ISITA), 2010 International Symposium on*, 2010, pp. 917-912.

[6] M. S. Sharbaf, "Quantum cryptography: An emerging technology in network security," in *Technologies for Homeland Security (HST), 2011 IEEE International Conference on*, 2011, pp. 13-19.

[7] M. Niemiec and A. R. Pach, "Management of security in quantum cryptography," *Communications Magazine, IEEE*, vol. 51, 2013.

[8] D. G. a. H.-K. Lo, "From Quantum Cheating to Quantum Security," *Physics Today*, vol. 53, p. 22, November 2000.

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

[10] P. W. Shor, "Polynomial-Time Algorithms for Prime Factorization and Discrete Logarithms on a Quantum Computer," *Society for Industrial and Applied Mathematics*, vol. 41, pp. 303 - 332, Jun. 1999 1999.

[11] C. Zhengjun and L. Lihua, "Improvement of one quantum encryption scheme," in *Intelligent Computing and Intelligent Systems (ICIS), 2010 IEEE International Conference on*, 2010, pp. 335-339.

[12] Z. Sheng-Mei, L. Fei, and Z. Bao-yu, "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 vol.2.

[13] R. D. Sharma and A. De, "A new secure model for quantum key distribution protocol," in *Industrial and Information Systems (ICIIS), 2011 6th IEEE International Conference on*, 2011, pp. 462-466.

[14] M. B. Nicolas J. Cerf, Anders Karlsson, and Nicolas Gisin, "Security of Quantum Key Distribution Using d-Level Systems," *The American Physical Society*, vol. 88, p. 4, 25 March 2002 2002.

[15] D. N. Kartheek, G. Amarnath, and P. V. Reddy, "Security in quantum computing using quantum key distribution protocols," in *Automation, Computing, Communication, Control and Compressed Sensing (iMac4s), 2013 International Multi-Conference on*, 2013, pp. 19-25.

[16] X. W. Guihua Zeng "Quantum key distribution with authentication," *Article*, p. 15, DEC 10. 1998 1998.

[17] 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.

[18] P. W. S. a. J. Preskill, "Simple Proof of Security of the BB84 Quantum Key Distribution Protocol," p. 5, Februry 1, 2008 2008.

[19] 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.

[20] R. Djellab and M. Benmohammed, "Securing Encryption Key Distribution in WLAN via QKD," in *Cyber-Enabled Distributed Computing and Knowledge Discovery (CyberC), 2012 International Conference on*, 2012, pp. 160-165.

[21] M. Stipcevic, "How secure is quantum cryptography?," in *MIPRO, 2012 Proceedings of the 35th International Convention*, 2012, pp. 1529-1533.
[22] S. Rass, P. Schartner, and M. Greiler, "Quantum Coin-Flipping-Based Authentication," in *Communications, 2009. ICC '09. IEEE International Conference on*, 2009, pp. 1-5.
[23] D. Gottesman, L. Hoi-Kwong, Lu, x, N. tkenhaus, and J. Preskill, "Security of quantum key distribution with imperfect devices," in *Information Theory, 2004. ISIT 2004. Proceedings. International Symposium on*, 2004, p. 136.
[24] H. Singh, D. Gupta, and A. Singh, "Quantum Key Distribution Protocols: A Review."
[25] K. Inoue, E. Waks, and Y. Yamamoto, "Differential phase-shift quantum key distribution," in *Photonics Asia 2002*, 2002, pp. 32-39.
[26] E. E. a. H. Serna, "Quantum Key Distribution Protocol with Private-Public Key," *Quantum Physics*, p. 3, May 12 2014 2012.
[27] 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.
[28] E. H. SERNA, "QUANTUM KEY DISTRIBUTION FROM A RANDOM SEED," *Quantum Physics*, p. 3, Nov. 12 2013 2013.

BIOGRAPHY

Abdulbast A. Abushgra, He is a PhD candidate in Computer Science & Engineering at University of Bridgeport. He has served as professor assistant at Al-Mergib University in Libya since 2007. Also, he has worked in the Railroad Company for 10 years as an advisor. Now, his work focuses on the quantum cryptosystem, and how to make a sharing secret key by Quantum Mechanics possible in classical cryptographic system.

Khaled Elleithy, He is the Associate Vice President for Graduate Studies and Research at the University of Bridgeport. He is a professor of Computer Science and Engineering. He has research interests in the areas of wireless sensor networks, mobile communications, network security, quantum computing, and formal approaches for design and verification. He has published more than three hundreds research papers in international journals and conferences in his areas of expertise.