Initiated decoy States in Quantum Key Distribution Protocol by 3 ways channel

Abdulbast Abushgra
aabushgr@my.bridgeport.edu
Department of Computer Science & Engineering
University of Bridgeport, CT USA

Khaled Elleithy
elleithy@bridgeport.edu

Abstract—After decades of research, computer scientists have in recent years come close to reaching substantive results which prove the usability of quantum key distribution (QKD). Several QKD protocols and different schemes have surfaced since the last century. Additionally, some of these protocols were created in new algorithms and up until now, have been proven to be secure; however, other scientists only made modifications to previous original protocols. This paper seeks to create a new scheme in QKD that will communicate between two parties and will give them a high level of security against any well-known attacks while handling both of parties in a manner that will reduce their dependency on both classic communication and the classical channel.

Index Terms—Quantum key distribution, EPR pair, Entanglement state, QKD attacks.

I. INTRODUCTION

For several centuries, cryptography has been, and still remains, a challenge to many computer scientists as well as physicists. As long as more information and data are transferred from one party to another, there is the need for even more security for the data and information being transferred. With regards to security, several schemes were proven to be either new complicated computing algorithms or improving existing ones. Cryptography is considered as the art of encoding and decoding messages, and will remain necessary as long as cyber eavesdroppers exist. Therefore, the science of cryptography deals with keeping these information secure [1].

Today, majority of the biggest systems and applications are still being run using conventional cryptography, which is still powerful enough to keep attackers away from stealing or tapping into any important information. As compared to quantum computing, classical security systems that depend upon complicated computing algorithms are extremely weak. Furthermore, if quantum cryptography became tangible and useable, conventional cryptography would easy to break [2].

Classical security is still in wide use and several schemes have shaken up the whole community of security. One of these schemes was invented by Shor in 1994 and is not only based on the factorization of prime numbers but still occupies a top rank in classical cryptography. Also, most encryption theories are based on mathematical operations, which are usually capable of being attacked [3]. Quantum Mechanics is a ray of hope which seeks to change several weaknesses in the classical system.

II. QUANTUM KEY DISTRIBUTION

A. BB84 protocol

Quantum key Distribution permits in general two parties so-named Alice (the sender) and Bob (the receiver) to communicate over the quantum channel with the ability to realize the occurrence of any form of eavesdropping as Eve (the eavesdropper), may or may not disturb the established connection [4]. BB84 protocol, which is still a unique QKD protocol, is the first step in this approach. Most of today’s protocols have been designed on the same idea. Bennett and Brassard in [5] came up with an innovative protocol that uses the polarization of photons. They also divided the communication between Alice and Bob into two channels (Quantum and public channel).

In 2000, Shor and Preskill in [6] proved the BB84 protocol to be a secure quantum protocol. In [7] Gottesman and others again proved that the security of the BB84 is the source and detector under a limit control of an adversary. Also, the above mentioned protocol is still considered as one of spotlights in the last two decades and has seen unique transformations between the two parties. Additionally, [8] proved the BB84 as still standing against the King Mean Problem that was created by J. Bub in 2001. Most scientists are of the conviction that quantum computing is the future for this field. In QKD, if for any reason interruption occurs, the system will in turn realize it immediately.

Even though in recent times certain protocols have been created because the authors mentioned above announced that the BB84 is unsecure, the BB84 and other protocols started as first a generation commercial system [9]. In [10] Scarani et al. implemented another QKD protocol that was extracted from the previous protocol BB84. SARG04 has the same features as the BB84 protocol except in a classical sifting procedure, in which the SARG04 is considered as robust against the optimal individual eavesdropping as well as photon-number splitting (PNS) attacks. The existence of PNS will result in dramatic consequences in security analysis [11].

This paper will discuss the advantages of BB84 and EPR in order to improve the new scheme. The new scheme derives its robustness from the advantages that have already been discovered in either the BB84 or EPR.
B. EPR Protocol

EPR in [12] was invented by Einstein, Podolsky, and Rosen, who presented the EPR paradox in 1935. In their paper, they argued about the completeness of physical theory in quantum mechanics. Basically, the EPR protocol is defined by EPR pair as:

\[ |0\rangle = \frac{1}{\sqrt{2}}(|00\rangle \mp |11\rangle), \]
\[ |\varphi\rangle = \frac{1}{\sqrt{2}}(|01\rangle \mp |10\rangle). \]

Where \(|0\rangle\) and \(|1\rangle\) are the eigenvectors of the Pauli operator, which the single photon will be measured by one of the legitimate parties that end up destroying the measurement state, and also determine the measurement of a particular state. For instance, measuring one of the created photons in the Bell’s state \(|\varphi\rangle\) and getting \(|1\rangle\) that means the other photon will collapse to the state \(|0\rangle\) [13]. To authenticate the communication, Alice can follow this scenario by using redundant coding, which she can encode one bit by two qubits [14].

\[ |0\rangle \rightarrow 0', \quad |1\rangle \rightarrow 'illgal' \]
\[ |\varphi\rangle \rightarrow 1', \quad |\varphi\rangle \rightarrow 'illgal' \]

EPR protocol has been modified in several researches and papers as [15] where Hwang and Lee tried to add more efficiency to the protocol. Both Alice and Bob are able to generate the EPR pair which the receiver can preserve. One of the assumptions here is that no collision occurs between the photon states, and the used measurement system is polarization as described above. Moreover, Dong and others in [16] presented a multiparty Quantum Secret Sharing (QSS) protocol that is based on entanglement swapping and random EPR selection, which has raised the probability of detecting the eavesdropper to 95.8%, which means more efficiency.

III. THE NEW QUANTUM KEY SCHEME

As mentioned above, the new scheme can be reflected on one of the protocols that are extracted by BB84, or more precisely the new scheme can be transmitted into the quantum channel initializing two, four, or six states. Generally, computer scientists believe quantum mechanics is not the whole solution but rather part of it. They also know that the law of physics can be a major aspect of creating a security system, where QKD protocols have proved two parties as being able to establish a communication under generating a secret binary string that is totally random [17]. Now as cryptography, we still need more of complicated computing as well as some tricks to provide perfection to our protocols.

In this paper, we provide a new QKD protocol that will use different systematic processes of submitting channels, where we try to capitalize on the advantage of the law of physics, the variety of BB84 and EPR protocol.

A. Proposal Scheme

The new protocol practically utilizes the features of EPR pairs to ensure the authentication of the initiated communication between the two parties that generally raises the reliability and the accuracy of the protocol to more than 50% as compared to the other protocols such as regular BB84. Moreover, The BB84 is used in this scheme as fundamental polarization, in which the sender party can create the electron (photon) in four bases by sending the photon randomly in different states. Also, the length of the code depends upon the text that Alice wants to share with Bob. Here, the steps of the proposed protocol are explained in sequentially as follows:

- **Step 1**: Alice creates \( n \) EPR pair, keeps photon A and sends photon B to Bob as shown in [18],
[19] and [20], this string of photons includes the authentication key, the length (includes the dimension of the matrix) of next sent qubits and the time when Alice starts submitting the first qubit (giving the signature and confidentiality to Bob).

\[ |0\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle), \]
\[ |\varphi\rangle = \frac{1}{\sqrt{2}}(|00\rangle - |11\rangle), \]
\[ |\varphi\rangle = \frac{1}{\sqrt{2}}(|01\rangle + |10\rangle), \]
\[ |\varphi\rangle = \frac{1}{\sqrt{2}}(|01\rangle - |10\rangle). \]

- **Step 2**: Bob resends the authentication key and the bases code into the first channel (orthogonal basis = 0, and orthonormal = 1) this is done by creating an auxiliary qubit and which is then transferred into CNOT gate.

- **Step 3**: Alice starts preparing the bits and passes them through the polarization device. This process will be done by entering the code bits randomly in lower triangle (\( l \)) and filling in the upper triangle (\( u \)) sequentially. After this, she modifies every row to be even by filling the diagonal with (0 or 1); hence, making the rows even.

![Figure (1) shows the table that prepared by Alice](image-url)
- **Step 4**: Alice submits the rows of prepared matrix in random selections, where she picks up different indices every time, and then submits the whole string of photons to Bob. Here, I would mention to Eve that she cannot figure out the submitted qubits because they have been submitted in the rows randomly.

\[
\sigma_x = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}, \quad \sigma_z = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}
\]

- **Step 5**: Bob at the other side measures the upcoming qubits from Alice that are supposed to be in either \(|0\rangle\), \(|1\rangle\), \(|+\rangle\), \(|-\rangle\) in random bases \((+\text{ or } \times)\). He measures the qubits into Pauli-Matrices operators \((z, x)\). Next, he places the measured qubits in the well-known matrix and then starts to sort the matrix as Alice mentioned in EPR communication.

- **Step 6**: Bob sends just the upper triangle to Alice in a sorted string of one basis (the agreement was fulfilled since the first communication). If Alice agreed to the received photons, she will end the quantum communication and start the classical channel. On the other hand, if Alice does not accept the upper triangle that was sent by Bob, she will send the measured bases in sequence to Bob by classical channel \((1\text{ and } 0)\).

\[
\theta = \begin{pmatrix} d_{11} & \cdots & u_{ij} \\ \vdots & \ddots & \vdots \\ l_{ij} & \cdots & d_{ij} \end{pmatrix}
\]

Where \(\theta\) is the whole qubits that are represented in one matrix and should be sent to Bob row by row.

- **Step 7**: Bob compares the measured qubits with those sent by Alice. If the measured qubits contains differences, he will then know that a third party was existent and tapping or eavesdropping. In this case he informs Alice to ignore the interrupted ones or rejects the whole communication if the rate of interrupted qubits is over 50%.

The new scheme demonstrates a protocol that contains three ways of communication between two parties. It begins by affirming the authentication prior to starting the transfer of the encoded qubits by quantum channel. The first communication will be processed by the EPR channel where both of the legitimate parties do not need to keep their information in the memory for a long time. In addition, this information should be short and effective. The second scenario of the communication is transferring the encoded information into the two bases quantum system, which is considered as BB84 in the polarization system. One of the advantages in this protocol is the reduction of classical communication to the last station in order to confirm the previous transfers, and to combine the reconciliation and error correction in the connection steps.

### B. The simulation

The new protocol has been examined to have certain common features with protocols such as the BB84. This was done by creating a certain level of noise in the channels of both protocols. The created noises comprised White Gaussian Noise, Intercept-Resend (IRA) Attack and others. Our protocol recorded a high ability to stand resist the IRA attack when it was applied and measured with BB84. It also recorded a higher ratio as compared to BB84 as shown in table [1]:

<table>
<thead>
<tr>
<th>Qubits\ Ratio</th>
<th>BB84</th>
<th>New Protocol</th>
</tr>
</thead>
<tbody>
<tr>
<td>32</td>
<td>0.4063</td>
<td>0.5200</td>
</tr>
<tr>
<td>64</td>
<td>0.5000</td>
<td>0.5278</td>
</tr>
<tr>
<td>128</td>
<td>0.5703</td>
<td>0.5714</td>
</tr>
</tbody>
</table>

Therefore, as shown in Figure (4), the applied correlation between the submitted and received photons is shown to be more linear in BB84’s figure unlike new scheme. On the other hand, the measurements were timed before exchanging channels. This means, whereas in the BB84, the attacker can gain some data by IRA, in the new scheme, it is very difficult to monitor any data.
Even though noise was created in both protocols, the BB84 protocol demonstrated more weakness as compared to the new scheme. This is because the new protocol is not affected by noise that is either caused by the environment, dark count probability or by an attacker. Reason being, Alice and Bob ensure that both of them are the legitimate parties; hence, making the next mechanism unknown except to one of them.

IV. SECURITY ANALYSIS

This section discusses the scenario of the proposal protocol and how the protocol is able to fight against many different types of quantum attacks. As known, the fake-signal attack is commonly seen in quantum security [21]. Supposing Eve is able to copy some of these photons $\emptyset \pm$ and $\varphi \pm$ and sends fake-photons to Bob, the proposal scheme in turn will ensure the inability of reaching Eve to the desired secret key. This is due to the asymmetric decoy states that are embedded in the submitted photons between Alice and Bob.

Men-In-Middle attack is a form of quantum attack [22], and this attack depends totally on measuring the pulse that is created with more than one photon, where Eve just keeps one of these photons and leaves the other without any interruption. The new scheme leaves MIM attack with nothing even if Eve catches some photons. Next, due to the use of the asymmetric decoy states in the new scheme, the Denial-Of-Service attack (DoS) suffers strict processes that have been explained above. The point here is when Bob measures the submitted photons in sequence, he will realize whether Eve interrupted the connection or not.

To increase the security of the proposed scheme, Alice and Bob share the only function that forms the density of the matrix $(\log_2 n)$, where $n$ is the length of text that is needed to be encoded as well as this length is invisible except Alice and Bob. As mentioned in [23] the Photon Number Splitting (PNS) attack can be computed, and its efficiency determined by computing the density matrices is associated with $n$ photon-pulses. Furthermore, PNS is still unable to be processed or completely efficient by Eve without establishing another attack that so-called Intercept-resend with unambiguous discrimination (IRUD) attack, which is still possible in our scheme; however, fortunately without gaining any information.

V. THE CONCLUSION

The proposed scheme is proved to be more secure than BB84, where the eavesdropper cannot realize the secret key even with caching some of the photons and resending others. Additionally, requesting the authentication at the beginning increases the level of security, where at the first channel the legitimate party can ignore the communication or resume it and then move to the next step. Therefore, the protocol has been designed for resisting attacks even in weak scenarios, where Eve will not have any useful combination of submitted data.
vi. references


VIII. BIOGRAPHY

Abdulast 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 cryptography, and how to make a sharing secret key by Quantum Mechanics is possible in our classical 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 hundred research papers in international journals and conferences in his areas of expertise.