Global Journal of Computer Science and Technology: E
Network, Web & Security
Volume 16 Issue 5 Version 1.0 Year 2016
Type: Double Blind Peer Reviewed International Research Journal
Publisher: Global Journals Inc. (USA)
Online ISSN: 0975-4172 & Print ISSN: 0975-4350

Simultaneous Initiating EPR and Quantum Channel by Quantum Key Distribution Protocol

By Abdulbast Abushgra & Khaled Elleithy
University of Bridgeport

Abstract- Cryptography is the background of protecting the flowed information between various communicated parties. Quantum cryptography gives the extreme trust to transferred information by creating a unique secret key that is based upon the law of physics. This paper will discuss a novel algorithm that is presented through quantum key distribution (QKD) protocol. This QKD protocol depends on parallel quantum communications between participants within EPR and quantum channels. The proposed protocol utilizes the EPR channel to prove the authentication while the quantum channel to transfer the shared key. Moreover, the proposed protocol initiates the verification of the participant's identity between the communicators by the EPR channel. After that the transferred data into quantum channel will create the secret key that contains a string of qubits as well as no need to communicate into classical channel.

Keywords: entangled states, epr pair paradox, intercept-resend attack (IRA), open-key string (OKS), and pauli-matrices measurement.

GJCST-E Classification : C.2.2 D.2.7

Strictly as per the compliance and regulations of:

© 2016. Abdulbast Abushgra & Khaled Elleithy. This is a research/review paper, distributed under the terms of the Creative Commons Attribution-Noncommercial 3.0 Unported License http://creativecommons.org/licenses/by-nc/3.0/), permitting all non-commercial use, distribution, and reproduction inany medium, provided the original work is properly cited.

Simultaneous Initiating EPR and Quantum Channel by Quantum Key Distribution Protocol

Abdulbast Abushgra [α] & Khaled Elleithy [σ]

Abstract- Cryptography is the background of protecting the flowed information between various communicated parties. Quantum cryptography gives the extreme trust to transferred information by creating a unique secret key that is based upon the law of physics. This paper will discuss a novel algorithm that is presented through quantum key distribution (QKD) protocol. This QKD protocol depends on parallel quantum communications between participants within EPR and quantum channels. The proposed protocol utilizes the EPR channel to prove the authentication while the quantum channel to transfer the shared key. Moreover, the proposed protocol initiates the verification of the participant's identity between the communicators by the EPR channel. After that the transferred data into quantum channel will create the secret key that contains a string of qubits as well as no need to communicate into classical channel.

Keywords: entangled states, epr pair paradox, intercept-resend attack (IRA), open-key string (OKS), and pauli-matrices measurement.

I. Introduction

According to several studies in the quantum cryptography, approving the stability of quantum key distribution protocol (QKDP) is based upon resisting the QKD protocol to quantum security attacks. These attacks have different algorithms and mechanisms that are generally used to tap or eavesdrop transferred data between various parties. The robust scenario in using quantum cryptography is its independency to utilize the law of physics through the quantum channel, which can detect an error as long as it occurs during an eavesdropper or fiber-optics noise. For instance, Intercept-Resend-Attack (IRA) is the well-known quantum attack that threatens the submitted photons from the sender to the receiver (Acín, Masanes, & Gisin, 2003; Curty & Lütkenhaus, 2005). In this scenario, Eve will mask itself as one of the legal parties where she will measure the first particle of the submitted entangled state, and she will try to resend the new created qubit back to Bob. First, the EPR pairs are anticipated to be located with Alice and Bob, but Eve will not be detected at first check. However, because of the property of EPR pairs, Eve will be detected during the second error check that is because EPR pairs have collapsed (Li & Zhang, 2006; Long & Liu, 2002).

The majority of QKD protocols face a difficulty of identity's determination, where the communicators sometimes are not exactly sure who is the sender (or the receiver). Several quantum attacks take this advantage of missed identification between the communicated parties. Therefore, the run time execution will suffer a delay due to much time to restart a new communication or errors correction, every time when the participants find a noise in the quantum channel. On the other hand, the shared data will be lacked if the connected parties ignore the error rate that usually happens during many quantum attacks.

Furthermore, using an authentication procedure at the beginning of the communication between two or more parties will rise the security rate of data transmission. It can also avoid the Intercept-Resend Attack (IRA) or Man-In-Middle Attack (MIM) (Gao, Qin, Guo, & Wen, 2011; Peev et al., 2005) that are based upon impersonating the sender or receiver or both. On the other hand, making a separation between the authentication phase (e.g. EPR channel) and the data submission stage (e.g. Quantum channel) will increase the live time execution that causes a chance for Eve to catch or interrupt even a few communication qubits. Therefore, merging the authentication and the submission of data have the possibility to reduce any eavesdropping chance.

This paper will introduce a new quantum key distribution algorithm, which uses the two quantum channels to ful fil the authentication between the participants by EPR channel. Then the quantum channel will be prepared at the same time of EPR communications to submit a qubits (secret key data). There will be early decision available to both communicators to finish or keep the connection. First part of this paper will demonstrate the initiation of EPR and Quantum channels, and then will show the measurement techniques that will be used at the receiver side.

II. The Initiation of the EPR Connection

In 2015, a quantum key distribution algorithm (Abushgra &Elleithy, 2015) was presented, where it was designed to be robust against common quantum attacks. One such quantum attack was the Man-In-Middle (MIM) attack, which causes an enormous leak of

Author α: He is PhD candidate at Computer Science and Engineering Department, University of Bridgeport.
e-mail: aabushgr@my.bridgeport.edu
Author σ: He is Professor at Computer Science and Engineering Department, University of Bridgeport. e-mail: elleithy@bridgeport.edu

© 2016 Global Journals Inc. (US)

data into the quantum communication between Alice and Bob. The proposed protocol prevents the MIM attack according to the rules of MIM attacks. The MIM attack relies on the fact that the MIM attack will lie or pretend to be a sender or a receiver to both legitimate parties (Yong, Huadeng, Zhaohong, &Jinxiang, 2009). Moreover, the MIM attacker plays on the weaknesses of verification identities between the communicated participants.

The proposed protocol is initiated by a communication into the EPR channel, where Alice (or third party) submits a string of entangled states $|\vdash\Psi\pm\rangle$ or $|\vdash\Phi\pm\rangle$ as well as an unknown state$|\vdash\varphi\rangle$. The unknown state is considered to be the identification state, where the identification state includes initiated strings of time t_1, size of matrix m, and number of matrices n, parity strings p, number of states s, raw index R, and determinate time t_2. The EPR communication will not take a long time of execution because the string of entangled states should be sent in short. After that Bob measures the upcoming string based on EPR theory (Entangled states) (Bell, 1964; Ekert, 1991; Li & Chen, 2007), and then after tensor EPR state (in random) with unknown state (Alice knows) Bob receives a separate code to apply the proper gate, which are one of the quantum gate (x, y, and z gates). Bob will use these gates to measure the states in the superposition. Next, Alice now knows that Bob had received a portion of the right qubits if the percentage of matched qubits is over 70%. Hence, Alice starts

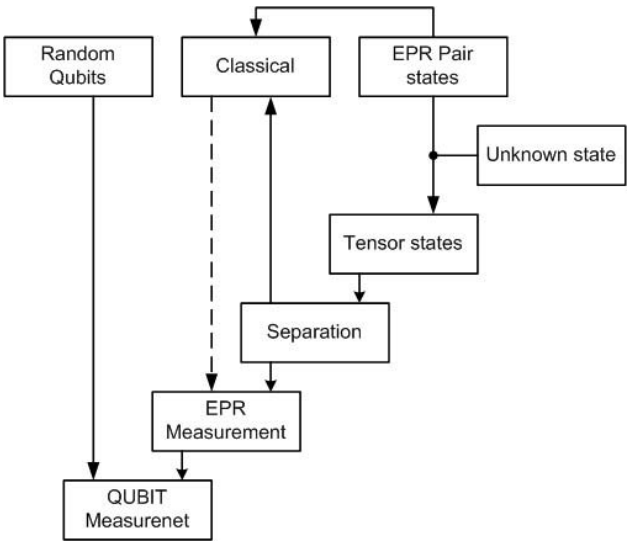

Fig. 2 : Shows the proposed scheme between two legitimate parties (A and B).

The submitted Open-Key (OK) string provides the authentication by EPR entangled states, where each photon is prepared by the sender or third party to be merged with an unknown state (e.g. two dimension state). Measuring an electron at the same time gives an negotiations with Bob to make sure there is no eavesdropper. If Alice finds the matched qubits less than 70%, she will announce Bob to restart another communication.

In case, Alice accepts the EPR communication outcomes, she will submit the string of qubits (data) as in (Abushgra & Elleithy, 2015) into the quantum channel. When Alice initiates the quantum communication within the quantum channel, she knows that Bob has already produced Open-Keys such as (t1, n, m, s, p, R, and t2). On the other side, Bob measures the upcoming qubits based on the number of states (s). He will have enormous amount of measured qubits, where these qubits will be reset in a number of matrices (n) based upon the raw index (R). After that Bob inserts the parity diagonal string (p) into the matrix to start correcting the error phase. If the total of matrix raw summation was even, it means there is no interruption. On the other hand, if the total of the matrix raw was odd, Bob will initiate reconciliation phase.

$$A_{string} = \{t_1,\ \ m,\ \ n,\ \ p,\ \ s,\ \ R,\ \ t_2\}.$$

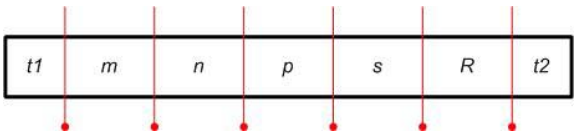

Fig. 1 : Shows the initiated open-key string that will be submitted by Alice to Bob through EPR channel.

opposite result at each participant's side by conservation of linear momentum (Hwang & Lee, 2007). Therefore, these electrons are employed in the authentication phase because physically the photons that represent the Open-Key travel faster than the light speed. Moreover, the Open-Key string in the proposed protocol includes the following characters that are used to authenticate the communication between Alice and Bob as follows:

- t_1 is the initiated time.
- n is the used matrices that can be any number (i = 1, 2,… N).
- m represents the size of the matrix (or matrices) that must be (a = b).
- p is the string of parity diagonal, which it should be prepared simultaneously with EPR connection.
- s is the number of states that are bounded in two types: orthogonal states, or non-orthogonal states.
- R is the row indices sequentially.
- t_2 is termination time.

These characters must be submitted into the Open-Key (OK) string by the EPR channel, and both of the participants should know the included qubits by the theory of entangled states. To measure the upcoming qubits, it is necessary to use the Pauli-Matrices $(\sigma_x, \sigma_y, and \sigma_z)$(Shor & Preskill, 2000) in Bob's circuit's

© 2016 Global Journals Inc. (US)

side. Moreover, when Alice desires to share a classical bit 0 with Bob, she initiates the EPR pairs in the state of $|\Phi \mp\rangle$. Also, Alice creates $|\Psi \mp\rangle$ state, if she wants to share classical bit 1(Li & Zhang, 2006).

$$|\varphi\rangle = \alpha|0\rangle + \beta|1\rangle \qquad Unknown\ state$$
$$|\Psi \mp\rangle = \frac{1}{\sqrt{2}}(|0\rangle \otimes |0\rangle \mp |1\rangle \otimes |1\rangle) \quad Entangled\ state$$
$$|\Phi \mp\rangle = \frac{1}{\sqrt{2}}(|0\rangle \otimes |1\rangle \mp |1\rangle \otimes |0\rangle) \quad Entagled\ state.$$

Hence, the submitted particle should be initiated in the previous entangled state, where the position of eigenstate in the $|\emptyset \mp\rangle$ are first $|0\rangle, |1\rangle$ and second $|0\rangle, |1\rangle$. Then Alice keeps one of the qubits in her quantum memory and submits the other qubits into EPR channel. To figure out how the size of the used matrix (or matrices), Bob must calculate the upcoming qubits during the EPR channel in the equation as follows:

$$M_{xy} = \frac{\sum_{i=1} |\varphi_i\rangle}{R} \times n.$$

Based on the received qubits, Bob can organize the qubits into a matrix (or matrices) by the above equation of M_{xy} where the whole received qubits are put in the number of matrices n. Also, the$\sum_{i=1} |\varphi_i\rangle$is an Open-Key string that represents the tensor of all received qubits. Then Bob begins multiple sequential steps to decide if the qubits are zero eavesdropping or there was a noise during the communication.

III. The Measured Qubits Into EPR Channel

To re-sort the proper indices in their positions, Bob should match the measured indices (R_j) with the OKP (R_i) indices, which usually will be raw by raw. The concluded matrix will be filled in by qubits either $|\emptyset \mp\rangle$ or $|\varphi \mp\rangle$ as well as the diagonal of the matrix (LEFT to RIGHT) that will be filled by a parity string. The parity string (p) is the qubits that should be located at the matrix's diagonal (UP to DOWN). Later, Bob sums the qubits in each raw; if the summation is (0) that means the first correcting phase is secure. Otherwise, Bob will know that there is a noise or an eavesdropping when he finds (1) as a summation of the matrix raw.

$$R_{(i)} = R^*_{(j)}$$

where R is the index number of the matrix, and $i and j \in \{1, 2 \dots n\}$).

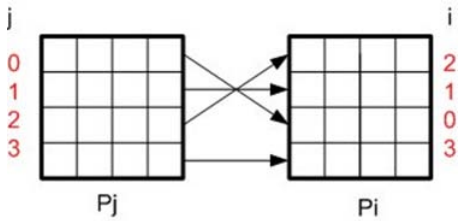

Fig. 3 : Shows re-sorting the received rows by Bob in the proposed protocol between two matrices, where these rows were received such as one string and sequentially resorted in equal matrix.

The abovementioned security checks are not the only security procedures into the proposed protocol, where the implemented decoy states during Alice's preparation is a type of security protection against MIM attacks. The decoy states are located in the upper-triangle of the matrix ($\mu_{ij} \in \{|0\rangle, |1\rangle, |\varphi\rangle, and\ |\emptyset\rangle\}$), where it has a limited tolerance to lose some qubits through the communication phase.

$$\begin{pmatrix} \omega_{11} & \cdots & \mu_{1j} \\ \vdots & \ddots & \vdots \\ \varphi_{i1} & \cdots & \omega_{ii} \end{pmatrix} \times Open - Key = \begin{pmatrix} \delta_{11} & \cdots & \delta_{1j} \\ \vdots & \ddots & \vdots \\ \delta_{i1} & \cdots & \delta_{ii} \end{pmatrix},$$

where $|\varphi_{ij}\rangle$ is the real qubits that will create the key, $|\omega_{ii}\rangle$ is the parity states that are placed diagonally in the matrix, $|\mu_{ij}\rangle$ is decoy states that usually are created similar to real data in random, and $|\delta_{ij}\rangle$ is the resorted matrix's rows after the measurement by Bob ($i \neq j \in \{1, 2 \dots n\}$) as shown in figure (3).

The submitted qubits will not be effected by eavesdroppers, in case, Eve tried to interrupt the channel. The reason of standing against any Eve's interruption is involved through inability of realizing the real qubits of the decoy qubits. Moreover, the string of qubits will be such as one string of data, and there is no variation between each photon.

$\|\omega_{ij}\rangle$	$\|\varphi_{ij}\rangle$	$\|\varphi_{ij}\rangle$	$\|\varphi_{ij}\rangle$	$\|\varphi_{ij}\rangle$
$\|\Psi_{ij}\rangle$	$\|\omega_{ij}\rangle$	$\|\varphi_{ij}\rangle$	$\|\varphi_{ij}\rangle$	$\|\varphi_{ij}\rangle$
$\|\Phi_{ij}\rangle$	$\|\Psi_{ij}\rangle$	$\|\omega_{ij}\rangle$	$\|\varphi_{ij}\rangle$	$\|\varphi_{ij}\rangle$
$\|\Psi_{ij}\rangle$	$\|\Phi_{ij}\rangle$	$\|\Psi_{ij}\rangle$	$\|\omega_{ij}\rangle$	$\|\varphi_{ij}\rangle$
$\|\Phi_{ij}\rangle$	$\|\Psi_{ij}\rangle$	$\|\Phi_{ij}\rangle$	$\|\Phi_{ij}\rangle$	$\|\omega_{ij}\rangle$

Fig. 4 : Shows the prepared qubits in one matrix by three classifications, shared data, decoy states, and parity states resorted from up to down and left to right sequentially, where $|\omega\rangle$ is the parity diagonal states, $|\varphi\rangle$ is the data thatwill build the secret key, and $|\mu\rangle$ is the decoy states. ($i = j \in \{1,2 \dots N\}$).

IV. Transferred Qubits Into the Quantum Channel

Alice initiates the qubits that she desires to share with Bob at the same time while preparing the EPR channel. Also, Alice should have the created qubits in her memory to start submitting one by one in a string mode. Although the participants are looking to exchange secure data, the EPR connection, at first, is used to solve the authentication phase. Moreover, both

© 2016 Global Journals Inc. (US)

parties now attempt to obtain correct data rather than interrupted qubits by the eavesdropper or environment noise. The submitted qubits will be in four states and two non-orthogonal bases.

$$|\varphi\rangle = \frac{1}{\sqrt{2}}(\alpha|0\rangle + \beta|1\rangle),$$

$$|\emptyset\rangle = \frac{1}{\sqrt{2}}(\alpha|0\rangle + \beta|1\rangle).$$

There are multiple options available to transfer a qubit through quantum channel and make the submission secure. One such option is that Alice can communicate with Bob in multi-states $\oplus|s_k\rangle$, where Alice decides through the EPR channel the dimension of the used photon that will be submitted to Bob (e.g. two dimension or more). This is an optional technique that is used; especially, when the secret key should be created to match big data such as in OTP.

Therefore, the proposed algorithm proved its stand against two common quantum attacks. These attacks as mentioned above are IRA and MIM attacks, which both of these attacks are still considered the most concerns around submitting a data through a quantum channel. Also, there is ability to create a huge secret key to match the whole data as long as the quantum memory is available.

V. Conclusion

The proposed QKD algorithm has proved its stability of trusted communication through the quantum channel as well as it is robust against MIM and IRA attacks. The protocol was built, in general, to fulfill the authentication between the communicated parties through the quantum channel. Moreover, the QKD protocol has employed simultaneous exchanges either into the EPR channel (authentication) or quantum channel (sharing a secret key) that maximally sustains the flowing of data into secure phase. As a result, the proposed protocol has been tested and simulated mathematically by MATLAB in classical system and has proved its security against common quantum attacks. Therefore, the proposed protocol is specified by using two parallel quantum channels to prove the authentication between the communicated parties before exchanging secret key plain-text.

References Références Referencias

1. Curty, M., & Lütkenhaus, N. (2005). Intercept-resend attacks in the Bennett-Brassard 1984 quantum-key-distribution protocol with weak coherent pulses. Physical Review A, 71(6), 062301.
2. Ekert, A. K. (1991). Quantum cryptography based on Bell's theorem. Physical Review Letters, 67(6), 661.
3. Gao, F., Qin, S.-J., Guo, F.-Z., & Wen, Q.-Y. (2011). Dense-coding attack on three-party quantum key distribution protocols. Quantum Electronics, IEEE Journal of, 47(5), 630-635.
4. Hwang, T., & Lee, K.-C. (2007). EPR quantum key distribution protocols with potential 100% qubit efficiency. Information Security, IET, 1(1), 43-45.
5. Li, X., & Chen, L. (2007). Quantum authentication protocol using bell state. Paper presented at the Data, Privacy, and E-Commerce, 2007. ISDPE 2007. The First International Symposium on.
6. Li, X., & Zhang, D. (2006). Quantum information authentication using entangled states. Paper presented at the Digital Telecommunications,, 2006. ICDT'06. International Conference on.
7. Long, G.-L., & Liu, X.-S. (2002). Theoretically efficient high-capacity quantum-key-distribution scheme. Physical Review A, 65(3), 032302.
8. Peev, M., Nölle, M., Maurhardt, O., Lorünser, T., Suda, M., Poppe, A., . .Zeilinger, A. (2005). A novel protocol-authentication algorithm ruling out a man-in-the middle attack in quantum cryptography. International Journal of Quantum Information, 3(01), 225-231.
9. Shor, P. W., &Preskill, J. (2000). Simple proof of security of the BB84 quantum key distribution protocol. Physical Review Letters, 85(2), 441.
10. Yong, W., Huadeng, W., Zhaohong, L., &Jinxiang, H. (2009). Man-in-the-Middle Attack on BB84 Protocol and its Defence. Paper presented at the Computer Science and Information Technology, 2009. ICCSIT 2009. 2nd IEEE International Conference on.

© 2016 Global Journals Inc. (US)