SIMULTANEOUS INITIATING EPR AND QUANTUM CHANNEL BY AK15 PROTOCOL

Abdulbast Abushgra, Advisor: Pro. Khaled Elleithy
Computer Science & Engineering Department
University of Bridgeport, Bridgeport, CT

FRD

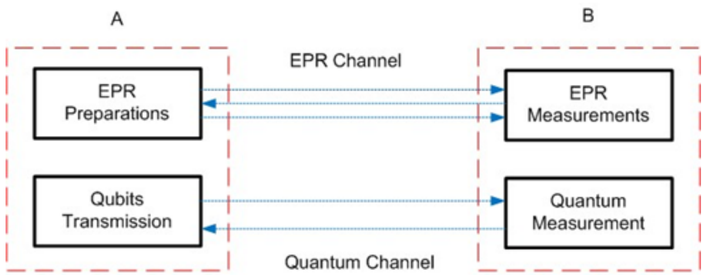
Introduction:

The Quantum Key Distribution is a technique to create a secret key, which is used to encode and decode the transferred data between sender and receiver. AK15 protocol was presented to stand against some quantum attacks. One of these attacks is Man-In-The-Middle Attack (MIMA), where it takes an advantage of missing the authentication between the communicated parties. The AK15 sets up a confidence connection by submitting an EPR pair before using a quantum channel.

The AK15 has ability to utilize a classical channel in limited usage. Also, the data that should be sent by the classical channel is unknown even an eavesdropper compromised it. The reality of robust this technique because the data submitted by the classical channel represents the type of gate that gives the receiver a chance to figure the qubits without extra communications.

AK15 Protocol:

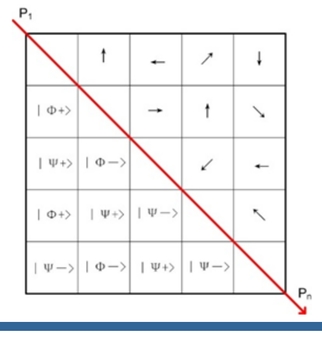
AK15 is a quantum key distribution that was designed to fulfil the authentication before exchanging any important data. The protocol uses a classical channel in narrow submissions.



The authentication requires an establishment of EPR channel that includes a classical communication in one way.

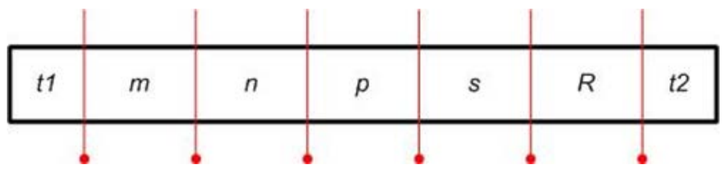
$$|\emptyset \mp\rangle = \frac{1}{\sqrt{2}}\,(|0\rangle \otimes |0\rangle \mp |1\rangle \otimes |1\rangle),$$
$$|\varphi \mp\rangle = \frac{1}{\sqrt{2}}\,(|0\rangle \otimes |1\rangle \mp |1\rangle \otimes |0\rangle).$$

The sender preparation is made by a matrix formulation.



AK15 Mechanism:

The AK15 protocol was designed to provide an authentication, where it is required to open a quantum communications. The sender starts EPR pair paradox photons into certain style, which is a string of qubits contains sorted needed data as shown in the figure.



The content of Qubit string:

t1- 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 raw indices sequentially. $R_{(i)} = R^{*}_{(j)}$
t2- is terminate time.
These component of qubits is based on inserting qubits into one matrix or more.

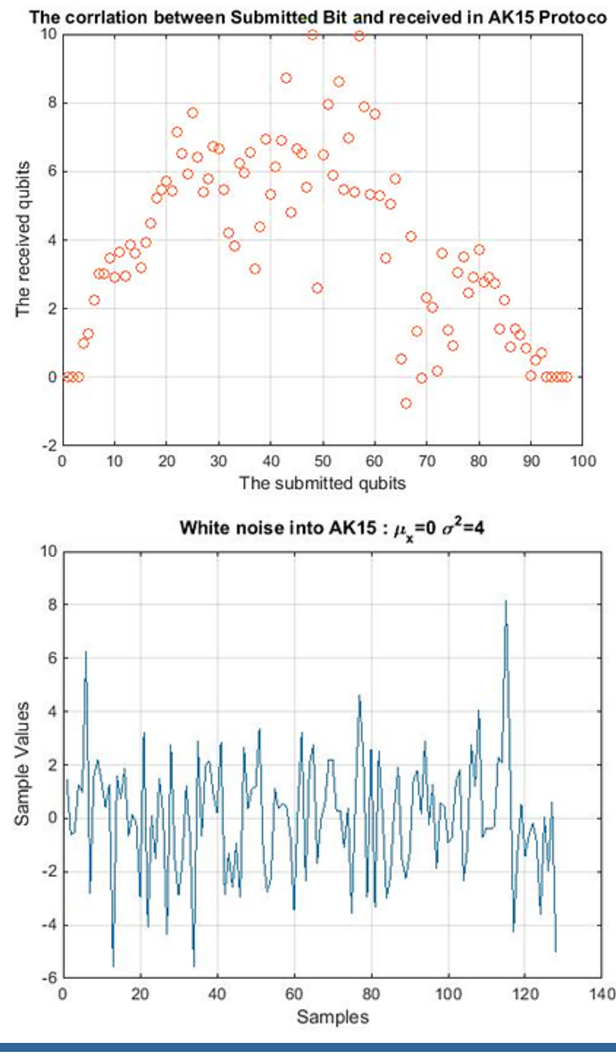
Decrypting Qubits:

The receiver should confirm the Open-Key into EPR channel. When the receiver gets the whole qubits, he already knows after the calculation, for instance, how many matrices the sender used by this formula.

$$M_{xy} = \frac{Open - Key\ string\ (OK)}{R} \times n$$

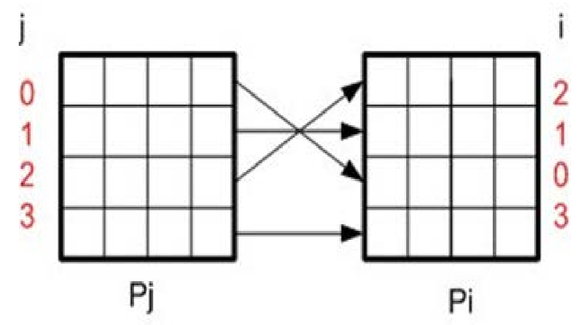
Based on the calculation, the receiver does not need any communication to correct any errors happened during the submission.

Simulations:



Result:

- The designed protocol is approved to be robust against Intercept-Resend-Attack (IRA), MIMA, and Wasting time



- Exchanging qubits occurs into quantum channel that is impossible to be tapped without interrupting the system, or formatting the upcoming data without the Open-Key.
- Employing decoy states into the qubit string makes an eavesdropper unable to relies the contents.
- The parity state diagonal is the key that is used to correct any errors without starting a communication or using difficult algorithms such as in many quantum protocols.

References:

- A. Abushgra and K. Elleithy, "*Initiated decoy states in quantum key distribution protocol by 3 ways channel*," in Systems, Applications and Technology Conference (LISAT), 2015 IEEE Long Island, 2015, pp. 1-5.
- Abushgra and K. Elleithy, "*Security of Quantum Key Distribution*," 2015.
- C. H. Bennett, "*Quantum cryptography using any two non-orthogonal states*," Physical Review Letters, vol. 68, p. 3121, 1992.
- 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