On Quantum 3-Pass Protocol

Ahmed E*

Department of Mathematics, Faculty of Science, Egypt

Submission: November 22, 2017; Published: February 01, 2018

*Corresponding author: Ahmed E, Department of Mathematics, Faculty of Science, Mansoura 35516, Egypt, Email: magd45@yahoo.com

Abstract

Some proposed 3-pass protocols in quantum cryptography assume that the qbits are 2-component. Here we propose a protocol without this assumption.

Keywords: cryptography; Three-pass protocol; Private decryption key; Three encrypted messages

Opinion

Three pass protocol [1,2]

In cryptography, the three-pass protocol for sending messages is a framework which allows one party to securely send a message to a second party without the need to exchange or distribute encryption keys. It is called the three-pass protocol because the sender and the receiver exchange three encrypted messages. The first three-pass protocol was developed by Adi Shamir circa 1980. The basic concept of the three-pass protocol is that each party has a private encryption key and a private decryption key. The two parties use their keys independently, first to encrypt the message, and then to decrypt the message.

The Three-Pass Protocol works as follows:

1. The sender chooses a private encryption key $es$ and a corresponding decryption key $ds$. The sender encrypts the message $m$ with the key $es$ and sends the encrypted message to the receiver.
2. The receiver chooses a private encryption key $er$ and a corresponding decryption key $dr$. The receiver encrypts the first message $E(es, m)$ with the key $dr$ and sends the doubly encrypted message $E(er, E(es, m))$ back to the sender.
3. The sender decrypts the second message with the key $ds$. Because of the commutativity property described above, $D(ds, E(er, E(es, m))) = E(er, m)$ which is the message encrypted with only the receiver’s private key. The sender sends this to the receiver.

The receiver can now decrypt the message using the key $dr$, namely $D(dr, E(er, m)) = m$ the original message. Notice that all of the operations involving the sender’s private keys $es$ and $ds$ are performed by the sender, and all of the operations involving the receiver’s private keys $er$ and $dr$ are performed by the receiver, so that neither party needs to know the other party’s keys.

Quantum 3-pass protocol

Recently quantum 3-pass protocol has been proposed [3]. It was assumed that the qbits are 2-component hence they use the fact that the group SO(2) is commutative. This is not true for SO(n), n>2. Here we propose the following protocol which does not make this assumption. Assume that sender A sends a string of qbits $\{qb(1), qb(2), ..., qb(s)\}$ to a receiver B. He receives them which causes some errors according to Uncertainty principle [4]. The receiver B sends back the Extended string $\{qb'(1), qb'(2), ..., qb'(s), qb(s+1), ..., qb(s+r)\}$. When the sender A receives it the correct subset of $\{qb'(1), qb'(2), ..., qb'(s)\}$ will form her key. The extended string is sent back to the receiver B and he gets $\{qb'(1), qb'(2), ..., qb'(s), qb'(s+1), ..., qb'(s+r)\}$. The correct subset of the string $\{qb'(s+1), ..., qb'(s+r)\}$ will be his key. No assumptions are made on the number of components used for each qbit.

References

2. 3-pass protocol, Wikipedia.