Authenticated Multiparty Secret Key Sharing Using Quantum Entanglement Swapping

Muneer Alshowkan, Khaled Elleithy
Department of Computer Science and Engineering
University of Bridgeport, Bridgeport, CT

Abstract

In this research we propose a new protocol for multiparty secret key sharing by using quantum entanglement swapping. Quantum Entanglement swapping is a process that allows two non-interacting quantum systems to be entangled. Further, to increase the security level and to make sure that the users are legitimate, authentication for both parties will be required by a trusted third party. In this protocol, a trusted third party will authenticate the sender and the receiver and help them forming a secret key. Furthermore, the proposed protocol will perform entanglement swapping between the sender and the receiver. The result from the entanglement swapping will be an Einstein-Podolsky-Rosen (EPR) pair that will help them in forming and sending the secret key without having the sender to send any physical quantum states to the receiver. This protocol will provide the required authentication of all parties to the trusted party and it will provide the required secure method in transmitting the secret key

Introduction

Bell States

The canonical basis consist of only one single qubit such as:

$$\{|0\rangle, |1\rangle\}$$

Bell states which also called EPR (Einstein-Podolsky-Rosen) pairs consist of two entangled qubits in a noncanonical basis as:

$$\{|0\rangle+|1\rangle/\sqrt{2}\ ,\ |0\rangle-|1\rangle/\sqrt{2}\ \}$$

The Bell basis consists of four entangled vectors as following

$$|\Psi^{+}\rangle = |01\rangle+|10\rangle/\sqrt{2} \qquad |\Psi^{-}\rangle = |01\rangle-|10\rangle/\sqrt{2}$$

$$|\Phi^{+}\rangle = |00\rangle+|11\rangle/\sqrt{2} \qquad |\Phi^{-}\rangle = |00\rangle-|11\rangle/\sqrt{2}$$

Forming Bell basis in two-dimensional case requires applying Hadamard matrix which performs the following:

$$|0\rangle\rightarrow|0\rangle+|1\rangle/\sqrt{2}\ ,\quad |1\rangle\rightarrow|0\rangle-|1\rangle/\sqrt{2}$$

Applying some input in the quantum circuit in Fig 1. result in creating one of Bell basis:

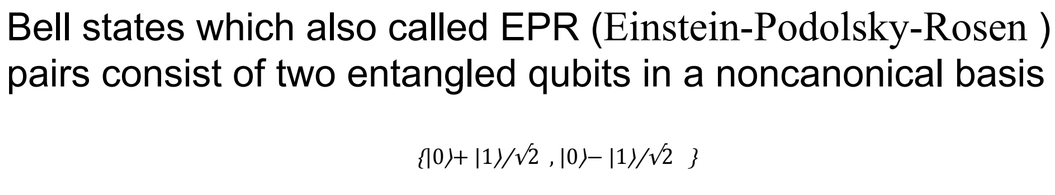

Fig 1. Quantum Circuit to Create Bell State

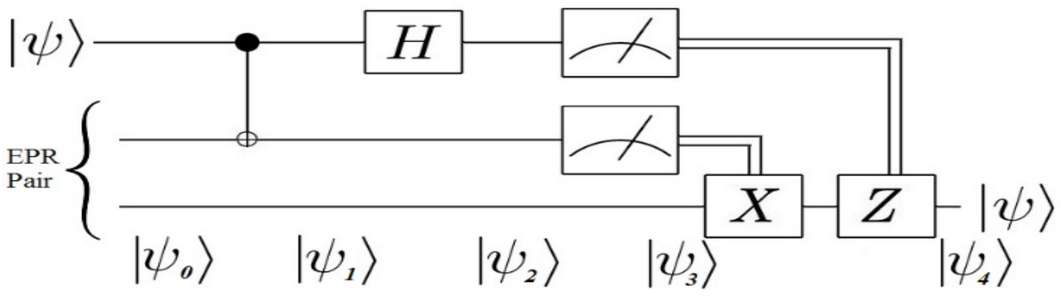

Fig 2. Quantum Teleportation Circuit

Proposed Algorithm

In this algorithm we assume that each party shares N EPR pairs with the trusted party Charlie and not sharing EPR pairs with the other parties. The first process in this protocol will be establishing an EPR-pair between the sender and the receiver by the help of the trusted node Charlie using quantum entanglement swapping Fig. 3

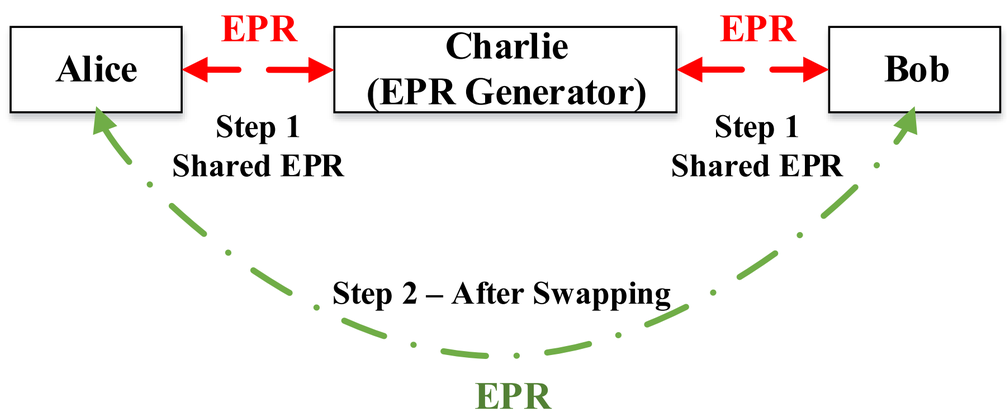

Fig 3. Creating EPR pair between Alice and Bob

The EPR pair between Charli-Alice and Charlie-Bob is as follow:

$$AC=|0\rangle\downarrow A\,|0\rangle\downarrow C+|1\rangle\downarrow A\,|1\rangle\downarrow C\,/\sqrt{2} \qquad CB=|0\rangle\downarrow C\,|0\rangle\downarrow B+|1\rangle\downarrow C\,|1\rangle\downarrow B\,/\sqrt{2}$$

After applying the entanglement swapping, Alice and Bob can build their entangled qubits after applying Pauli-X, Pauli-Z, both or no gate one the result of Charlie's swapping result to be in state:

$$|\Psi\uparrow-\rangle\downarrow AB=1/\sqrt{2}\ (|0\rangle\downarrow A\,|1\rangle\downarrow B-|1\rangle\downarrow A\,|0\rangle\downarrow B)$$
$$|\Psi\uparrow+\rangle\downarrow AB=1/\sqrt{2}\ (|0\rangle\downarrow A\,|1\rangle\downarrow B+|1\rangle\downarrow A\,|0\rangle\downarrow B)$$
$$|\Phi\uparrow-\rangle\downarrow AB=1/\sqrt{2}\ (|0\rangle\downarrow A\,|0\rangle\downarrow B-|1\rangle\downarrow A\,|1\rangle\downarrow B)$$
$$|\Phi\uparrow+\rangle\downarrow AB=1/\sqrt{2}\ (|0\rangle\downarrow A\,|0\rangle\downarrow B+|1\rangle\downarrow A\,|1\rangle\downarrow B)$$

After forming the EPR pair between Alice and Bob, they have the option to measure their EPR pair using one of the basis in Fig 4.

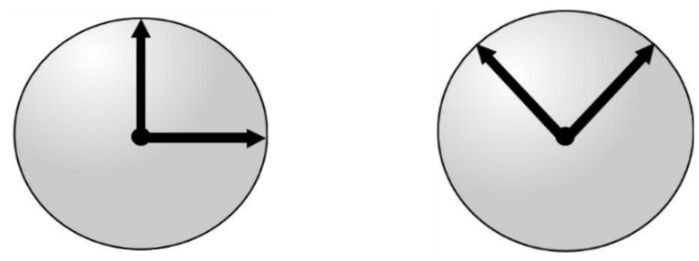

Fig 4. Quantum Orthogonal Basis

Alice can start to measure her qubit in one of these basis and get the measurement result. Then she can ask Bob to measure his qubit in the same basis. The result of Bob's measurement will be the opposite of Alice's result. For example:
Alice basis $|+\rangle,|-\rangle$ and her result is $|+\rangle$ then Bob's $|-\rangle$
Alice basis $|0\rangle,|1\rangle$ and her result is $|0\rangle$ then Bob's $|1\rangle$.

Conclusion

We have presented a multiparty quantum secret key sharing using quantum entanglement swapping. This protocol solves the problem of trust between sender and receiver. Where there will be a trusted third party who can authenticate each party to the other. Sender and receiver exchange data without having prior entangled state between. Also, quantum medium is not required and will take the advantage of quantum entanglement instead.