Authenticated Multiparty Secret Key Sharing Using Quantum Entanglement Swapping

Muneer Alshowkan, Student Member, IEEE, Khaled Elleithy, Senior Member, IEEE

Abstract—In this paper 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.

Index Terms—cryptography, entanglement, EPR, multiparty, quantum swapping

I. INTRODUCTION

Quantum Mechanics unique properties and laws are the keystone to quantum computing and quantum information theory. Quantum computing have been providing promising solution to the difficult problems in classical computing. For instance, quantum teleportation, entanglement and quantum parallelism are contributing in quantum computing by providing new techniques that differ from the current techniques in classical computing [1-4].

Many protocols based on quantum entanglement and quantum teleportation have been proposed to provide solutions to the different challenges in classical computing networks and secure data transmission [5-11]. Quantum entanglement is the basic element in quantum teleportation which is a significant protocol in quantum cryptography for secure data transmission. The aim of the different protocols in quantum cryptography is to provide a new unconditional secure protocols instead of the current cryptographic protocols in the classical computing. Which are depending on the computation difficulty to compute the secret key.

In this protocol we assume that Alice and Bob want to share a secret key. However, a trust between Alice and Bob need to be established so Alice can share her secret state with Bob and Bob want to make sure that Alice is a legitimate user and not an intruder. Therefore, a trusted party for Alice and Bob will be required to authenticate them to each other’s. As a result, Alice will have enough trust to form and share a secret key to Bob. After the authentication process, the trusted party will create and EPR pair between Alice and Bob to be used in their communication. The communication between Alice and Bob will be based on Alice measurement to her qubit in the EPR.

The organization of this paper will be as follow. After we started with introduction in section I we will cover some of the basics and background of quantum computing in section II. Then we will cover the related work in the literature in section III. After that, the proposal protocol with the steps required to process it in section IV. Finally the conclusion and the
final remarks in section V.

II. QUANTUM COMPUTING PRELIMINARIES

A. Quantum bits

Quantum computing takes the advantages of the laws of quantum mechanics to efficiently solve the difficult problems in classical computing. Having the bit as the fundamental unit in classical computers to represent and store data. Where, the name of the same unit in quantum computing is called qubit. The difference between a bit and qubit is that a bit represents one of two different disjoined states such as a signal to be high or low, a switch to be on or off or logical value true or false. However, a qubit can represent one state or two states simultaneously such as a switch to be on and off or logical value to be true and false at the same time. The notation of one qubit is $|0\rangle$ for zero and $|1\rangle$ for one. When a qubit is in both states $|0\rangle$ and $|1\rangle$ it state is called a superposition and it can be represented as a linear combination of both stats as:

$$|\Psi\rangle = \alpha |0\rangle + \beta |1\rangle$$  \hspace{1cm} (1)

The coefficients $\alpha$ and the coefficient $\beta$ are complex numbers in $C^n$ and the states $|0\rangle$ and $|1\rangle$ are an orthonormal basis in the two-dimensional vector space. The value determination in classical and quantum computers are different. For instance, we can easily examine a classical bit and determine if it in state 0 or 1. However, in qubits we examine the coefficients $\alpha$ and $\beta$ instead. After measuring a qubit the result become either 0 with probability $|\alpha|^2$ or 1 with probability $|\beta|^2$ resulting in:

$$|\alpha|^2 + |\beta|^2 = 1$$  \hspace{1cm} (2)

Having both probabilities sums to one geometrically indicates that the qubit state must be normalized to length one in the two-dimensional vector space.

Two qubits in quantum systems can be represented by four states using classical bit for instance, $|00\rangle$, $|01\rangle$, $|10\rangle$, $|11\rangle$. At the other hand, two qubits can be represented by four basis states denoted by $|00\rangle$, $|01\rangle$, $|10\rangle$, $|11\rangle$. Moreover, the two qubits can also be in a superposition by forming a linear combination of states with their complex coefficient which often called an amplitude.

$$|\Psi\rangle = \alpha_{00}|00\rangle + \alpha_{01}|01\rangle + \alpha_{10}|10\rangle + \alpha_{11}|11\rangle$$  \hspace{1cm} (3)

After the measurement of this multi qubit state, the result will be similar to a system with only one qubit, as the probability of having one of the four states is can be donated by $|\alpha_x|^2$.

B. Quantum gates

Classical systems depends on the wires and the logic gates in the digital circuits to carry and manipulate the information. For instance, the NOT gate in classical system perform a specific operation which is manipulating the stats 0 and 1 by interchanging their values in which state 0 to be 1 and state 1 to be 0. Similarly, the NOT gate in quantum systems interchange state $|0\rangle$ to state $|1\rangle$ and state $|1\rangle$ to state $|0\rangle$.

$$\alpha |0\rangle + \beta |1\rangle \rightarrow \text{ NOT } \rightarrow \alpha |1\rangle + \beta |0\rangle$$  \hspace{1cm} (4)

Moreover, another convenient way to represent quantum gates is in matrix form. For instance, quantum gates $I$, $X$, and $H$ which represent the Identity, NOT and Hadamard gates respectively can be represented in term of matrices as:

$$I = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}, \quad X = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}, \quad H = \frac{1}{\sqrt{2}} \begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix}$$  \hspace{1cm} (5)

C. Quantum Teleportation

Quantum teleportation [7] is a technique of transferring a quantum state from one location to another with the absence of physical quantum channel between the sender and the receiver [25]. However, this process of transferring the state from one location to another doesn’t conflict with the no-cloning which states that it is impossible to clone an exact state without destroying the original state. That means it is possible to move a state from one location to another but not copying. Providing that, the teleported state will necessarily be destroyed.

Teleportation uses the EPR pairs which is also called Bell states and Bell basis to archive its goal. Bell Basis consist of two entangled qubits in a noncanonical basis:

$$\left\{ \frac{|0\rangle + |1\rangle}{\sqrt{2}}, \frac{|0\rangle - |1\rangle}{\sqrt{2}} \right\}$$  \hspace{1cm} (6)

The Bell basis or the noncanonical basis consists of four entangled vectors as follow:

$$\left| \Psi^- \right\rangle = \frac{|01\rangle - |10\rangle}{\sqrt{2}}$$  \hspace{1cm} (7)

$$\left| \Phi^- \right\rangle = \frac{|00\rangle + |11\rangle}{\sqrt{2}}$$  \hspace{1cm} (8)

By using Bell basis, if Alice would like to teleport a qubit to Bob and the qubit is in an arbitrary state $|\psi\rangle = \alpha |0\rangle + \beta |1\rangle$. To accomplish the teleportation process Alice perform some operations denoted in the quantum circuit in Fig 1.

![Quantum Teleportation Circuit](image)

After applying the required operations Alice qubits will be result to one of the four states $|00\rangle$, $|01\rangle$, $|10\rangle$ or $|11\rangle$ which will indicate the state of Bob’s qubit as follows:
Quantum direct communication (QDC) for mutual authentication based on entanglement swapping was proposed in [30]. There are two phases in this protocol. First phase is used to provide mutual authentication and the second phase is used for direct communication. The identification between Alice and Bob can be performed by testing the Einstein-Podolsky-Rosen (EPR) pairs. Moreover, the properties of entanglement swapping allows Bob to decode Alice’s message by just performing exclusive-or operation on both of Alice’s public key and Bob’s measurement. Further, the authentication process and the direct communication process are proved to be secure because there is no physical transmitting of qubits in both operations. The public key for Alice will consist of two classical bits. Alice will have to send it to Bob using the public classical channel. However, that will not reveal any information about the secret key Alice holds because they are irrelevant to each other.

In [31] a study of quantum cryptography was conducted including in details description of protocol BB84. Also, described key reconciliation, distillation, security measure and level of security. Security measure is a probability that indicates if the distributed key was intercepted or not by unauthorized third party. Two security measures were defined as in (14) and (15) where log is the natural logarithm, k is the number of the compared bits in the public channel and n is the length of the key.

\[
J(k) = \log_{\frac{k}{n}} \quad (14)
\]

\[
S(k) = -\frac{k}{n} \log_{\frac{k}{n}} \quad (15)
\]

In J(k) the first 20% of bits have more effect on the result compared to the last 30% of the bits in the key. And dividing S(k) by n gives maximum value of 0.1 which is equivalent to 37% of the bits in the key.

Travis Humble discussed securing quantum communication in the link layer [32]. Besides, describing the basics of quantum communications and quantum optical communication. As well as, described the quantum seal Fig. 2 to provide integrity and monitoring to quantum communication.
any violation will be by setting threshold stating if the
communication is safe or not when the threshold value will be
the result of quantum seal process.

Quantum determined key distribution scheme was proposed
in [33] and it is based on quantum teleportation. In this
protocol the sender and the receiver will share predetermined
key by taking advantage of quantum teleportation instead
of random string as in the other key distribution protocols.
Moreover, because of quantum mechanics properties, the
system will be unconditionally secure. In fact, the protocol
consists of two major steps. First step, building the shared
EPR pairs. Second step, building the secret key. In the first
step Alice create EPR pairs in state $|\Phi^+\rangle$ and share them with
Bob.

$$|\Phi^+\rangle_{AB} = \frac{1}{\sqrt{2}}(|0\rangle_A|0\rangle_B + |1\rangle_A|1\rangle_B)$$

(16)

First qubit $A$ will belong to Alice and the second qubit $B$
will belong to Bob. Then, Bob measures his qubit in one of
three basis. After that Alice and Bob declare the basis they
used in their measurements and compare their results. If both
used different basis they discard the EPR pair. However, if
they find they are many disagreement when they used the
same basis, they can conclude that there is an eavesdropper on
the channel. Building the will be based on quantum
teleportation using the EPR pairs were previously built.

IV. PROPOSED ALGORITHM

In this process we assume that each party shares $N$ EPR
pairs with the trusted party named Charlie and not sharing
EPR pairs with the other parties. The first step in this
protocol will be establishing an EPR-pair between the sender
and the receiver by the help of the trusted node Charlie. After
that Charlie will act as generator for EPR-pairs between the
sender and the receiver to allow them to communicate with
each other’s. The first step require Charlie to help the sender
(Alice) and the receiver (Bob) to form an EPR pair. The
shared EPR pair between Alice and Charlie will be as follows:

$$AC = \frac{|0\rangle_A|0\rangle_C + |1\rangle_A|1\rangle_C}{\sqrt{2}}$$

(17)

And the shared EPR pair between Charlie and Bob is as
follows:

$$CB = \frac{|0\rangle_C|0\rangle_B + |1\rangle_C|1\rangle_B}{\sqrt{2}}$$

(18)

$$AC \otimes CB = \frac{|0\rangle_A|0\rangle_C + |1\rangle_A|1\rangle_C}{\sqrt{2}} \otimes \frac{|0\rangle_C|0\rangle_B + |1\rangle_C|1\rangle_B}{\sqrt{2}}$$

(19)

Applying CNOT to C:

$$= \frac{1}{2} \{ |0\rangle_A|0\rangle_C (|0\rangle_C|0\rangle_B + |1\rangle_C|1\rangle_B) \}$$

(20)

$$+ \frac{1}{2} \{ |1\rangle_A|1\rangle_C (|1\rangle_C|0\rangle_B + |0\rangle_C|1\rangle_B) \}$$

(21)

Applying Hadamard gate to C in the first EPR-pair:

$$= \frac{1}{\sqrt{2}} \{ |0\rangle_A(|0\rangle_C + |1\rangle_C) (|0\rangle_C|0\rangle_B + |1\rangle_C|1\rangle_B) \}$$

(22)

Rearrange and group C:

$$= \frac{1}{\sqrt{2}} \{ |0\rangle_A|0\rangle_C|0\rangle_B + |1\rangle_A|1\rangle_C|1\rangle_B \}$$

(23)

Depending on the result of Charlie’s measurement, Alice
and Bob can build their entangled qubits after applying Pauli-
X, Pauli-Z, both or no gate. For the particles in Alice’s and
Bob’s possessions, the result of the process will be one of the
following EPR pairs:

$$|\Psi^-\rangle_{AB} = \frac{1}{\sqrt{2}}(|0\rangle_A|1\rangle_B - |1\rangle_A|0\rangle_B)$$

(24)

$$|\Psi^+\rangle_{AB} = \frac{1}{\sqrt{2}}(|0\rangle_A|1\rangle_B + |1\rangle_A|0\rangle_B)$$

(25)

$$|\Phi^-\rangle_{AB} = \frac{1}{\sqrt{2}}(|0\rangle_A|0\rangle_B - |1\rangle_A|1\rangle_B)$$

(26)

$$|\Phi^+\rangle_{AB} = \frac{1}{\sqrt{2}}(|0\rangle_A|0\rangle_B + |1\rangle_A|1\rangle_B)$$

(27)

After forming the EPR pair between Alice and Bob, they
have the option to measure their EPR pair using one of the
basis $|+\rangle,|−\rangle,|0\rangle$ or $|1\rangle$. When Alice measure her qubit
(first qubit in the EPR pair) using one of these basis, Bob’s
qubit (second qubit in the EPR pair) will be collapsed to the
opposite of the result of Alice’s state. However, for Bob to
have the correct opposite state, he needs to measure his qubit
using the same basis Alice used to measure her qubit.

$$|+\rangle = \frac{|0\rangle+|1\rangle}{\sqrt{2}}$$

(28)

$$|−\rangle = \frac{|0\rangle−|1\rangle}{\sqrt{2}}$$

(29)

$$|0\rangle = \frac{|+\rangle+|−\rangle}{\sqrt{2}}$$

(30)

$$|1\rangle = \frac{|+\rangle−|−\rangle}{\sqrt{2}}$$

(31)

Alice and Bob can start to measure her qubit in one of these
basis randomly and get the measurement result. After that
Alice can meet Bob on the classical channel and compare with
him about the basis they used in measuring their qubit without
disclosing her measurement result. The result of Bob’s
measurement will be the opposite of Alice’s result in the same
basis. For example, if Alice used basis $|+\rangle,|−\rangle$ and her
measurement results state $|+\rangle$ then the result of Bob
measurement will be $|−\rangle$. And if Alice used basis $|0\rangle,|1\rangle$ for

[Type text]
her measurement, if the result of her first qubit is \( |1 \rangle \) then the result of Bob’s second qubit will be \( |0 \rangle \). Alice and Bob perform this process until they meet their key length. Once they finish with the process of measurement, Bob can start to reverse all of his measurement result which will make his measurement result identical to Alice’s measurement results and this will be the secret key.

A. The steps of the Protocol:
Step 1: When Alice want to securely communicate with Bob, Alice contact Charlie. Since Charlie have prior entangled pairs with Alice Charlie can authenticate Alice’s identity.

Step 2: Charlie also authenticate Bob’s identity as they share prior entangled pairs. Further, Charlie communicate with Bob and inform him about Alice request. Bob can accept or reject Alice’s request.

Step 3: If Bob accept to securely communicate with Alice, Charlie start the entanglement swapping process and inform both Alice and Bob when the process is successful and provide the gate code so Alice and Bob make the correction to their EPR pair. On the other hand, if Bob rejected the request. Charlie inform Alice and do not process the entanglement swapping.

Step 4: When Alice receive the confirmation from Charlie, Alice start the measurement of her qubit using one of the basis randomly.

Step 5: Bob also randomly select one of the basis and start measuring his qubit.

Step 6: When they measures all of their qubits, Alice and Bob will have to meet on the classical channel and compare the basis they used. Both will discard the result of the mismatch basis. This process will make Bob’s state identical to Alice’s states and will be the key they can use to encrypt their information.

Alice and Bob will not use any quantum channels to transmit the physical quantum states. Instead, they will depend on the EPR pair that Charlie will help them to form. Once Charlie authenticate the identity of both parties in the beginning of the process then they can have confidence that the following process will be secured because the states will not be able to intercepted and compromised.

V. 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. This protocol requires each party to have an EPR pair shared with the trusted party. However, EPR pair between the parties themselves will not be required. For a sender to share a secret key with the another party who shares only EPR pair with the trusted party, the sender will request a permission to contact the receiver and the trusted party will handle the authentication process with the receiver as they share and EPR pair and they can be verified using their entangled qubits. Once the authentication process is completed, the trusted party perform the entanglement swapping process and have both parties to share an EPR pair. The sender measures his own qubit in the entangled state using one of the basis randomly. Also, the receiver perform measure on the entangled state randomly using one of the basis. When the sender and receiver measure their qubits. They meet on the classical channel and discard the mismatch basis result. The sender and the receiver will not use any quantum channel to send and receive quantum states and will only depend on classical channel to compare the basis without sharing the results. Comparing the basis wouldn’t affect the security and no quantum medium will be used for intercepting the quantum states. Thus, this protocol is secure.

REFERENCES


Muneer Alshowkan is currently pursuing a Ph.D. degree in Computer Science and Engineering at the University of Bridgeport. In 2011, he received his Master's degree in Information, Network and Computer Security at New York Institute of Technology, and received his B.S. in Computer and Management Information Systems at King Faisal University in Kingdom of Saudi Arabia. His research interest in Quantum Computing, Computer Networks Security and Wireless Communication. He is currently an active member of IEEE.

Dr. Khaled Elleithy is the Associate Dean for Graduate Studies in the School of Engineering at the University of Bridgeport. He has research interests are in the areas of network security, mobile communications, and formal approaches for design and verification. He has published more than two hundred fifty research papers in international journals and conferences in his areas of expertise. Dr. Elleithy is the co-chair of the International Joint Conferences on Computer, Information, and Systems Sciences, and Engineering (CISSE). CISSE is the first Engineering/Computing and Systems Research e-Conference in the world to be completely conducted online in real-time via the internet and was successfully running for four years. Dr. Elleithy is the editor or co-editor of 10 books published by Springer for advances on Innovations and Advanced Techniques in Systems, Computing Sciences and Software.