Secret Key Sharing Using Entanglement Swapping and Remote Preparation of Quantum State

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

Department of Computer Science and Engineering
University of Bridgeport
Bridgeport, USA
malshowk@my.bridgeport.edu, elleithy@bridgeport.edu

***Abstract*—In this paper we propose a new algorithm for secret key sharing by utilizing quantum entanglement swapping and remote preparation of quantum state. This algorithm is used when two parties do not share an Einstein-Podolsky-Rosen (EPR) pair but one wishes to transmit a secret key to the other. In order to successfully accomplish this process, a third party who shares an EPR pair with both parties will help them build a new EPR pair. The new EPR pair will be used between the sender and the receiver to remotely prepare a quantum state. This process will provide a secure way to share secret keys between the two parties who do not share EPR pairs. Furthermore, the process doesn't require sending any physical quantum state, instead the sender prepares a known state and sends only one classical bit to the receiver to help build an intended quantum state.**

Keywords- remote preparation; quantum cryptography; EPR pairs; entangelemt swapping; secret key sharing;

I. INTRODUCTION

Quantum computing and quantum information theory have been providing promising solutions using quantum parallelism, teleportation and entanglement to efficiently solve difficult problems in classical computing [1-4]. Data and network security are of the most challenges in classical computing. Providing that, many quantum protocols have been proposed based on quantum entanglement to improve and provide more secure systems [5-10]. Moreover, quantum teleportation depends on quantum entanglement which is one of the most important protocols for data transmission in quantum computing.

Quantum teleportation is used to transmit an arbitrary unknown state from a sender (Alice) to receiver (Bob) with a spatial distance between them, using a quantum entanglement channel. However, a classical communication channel between the sender and the receiver will be required to help in transmitting and measuring the target state. In fact, in quantum teleportation the quantum state gets moved to a remote place while the original state gets eliminated because, the no-cloning theorem states that it is impossible to copy a quantum state [11].

Moreover, the teleportation process requires two kinds of channels; one being the quantum channel for creating EPR pair and the other the classical channel. Considering, an eavesdropper could try to make malicious activities on the transmission path. For this reason, such path might not be secure for sending and receiving data.[12, 13]. An interesting algorithm to transmit a known pure quantum state by taking the advantage of prior shared entanglement is known as remote state preparation (RSP). RSP was presented by Lo [14]. Further, RSP is similar to teleportation as in both algorithms entanglement state and classical channel are required to successfully send and receive the quantum state. However, the major difference between them is in RSP, Alice knows the state she intends to send to Bob. Where in teleportation, no one knows the state being transmitted. Furthermore, RSP was proved to be more economically efficient than teleportation by Pati [15]. Because using teleportation requires Alice to send two classical bits for each qubit she sends to Bob. Then Bob will have to perform specific operations based on these classical bits to make the necessary operations on the shared EPR to recover the state Alice is sending.

The trade-off in cost between the classical information required entanglement and RSP was provided by Bennett et al [16]. After that, many researchers studied and proposed different theoretical types of RSP [17-24] . On the other hand, Peng et al [19] have implement RSP using Nuclear magnetic resonance and Xiang et al [21] have implemented RSP using spontaneous parametric down-conversion, single photon detector and linear optical elements. Additionally, other RSP methods were proposed using different entanglement [25].

In this paper, we will use the properties of quantum systems to provide a secure method to create and share secret keys between Alice and Bob. We will take the advantage of entanglement swapping to remotely build an EPR pairs between the two nodes who do not share a prior entangled states by the help of the EPR generator. After that, Alice and Bob will have an entangled EPR pair. Then, using remote state preparation of quantum state, Alice can prepare a secret key and send it to Bob using the classical channel by only one classical bit for each qubit she prepared.

The organization of this paper will be as follows; Quantum computing preliminaries will be covered in section II, then the related work will be in section III. After that the proposal algorithm in section IV. Result and discussion in section V. Finally the conclusion and the final remarks will be covered in section VI.

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 disjointed 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:

$$|\Psi\rangle = \alpha|0\rangle + \beta|1\rangle \quad (1)$$

The coefficients α and the coefficient β 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 α and β instead. After measuring a qubit the result become either 0 with probability $|\alpha|^2$ or 1 with probability $|\beta|^2$ resulting in:

$$|\alpha|^2 + |\beta|^2 = 1 \quad (2)$$

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, 01, 10, 11. 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.

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

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 stae $|0\rangle$.

$$\alpha|0\rangle + \beta|1\rangle \longrightarrow NOT \longrightarrow \alpha|1\rangle + \beta|0\rangle \quad (4)$$

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:

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

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[26]. 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:

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

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

$$\frac{|\Psi^{\mp}\rangle = |01\rangle \mp |10\rangle}{\sqrt{2}} \quad (7)$$

$$\frac{|\Phi^{\mp}\rangle = |00\rangle \mp |11\rangle}{\sqrt{2}} \quad (8)$$

By using Bell basis, if Alice would like to teleport a qubit to Bab 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.

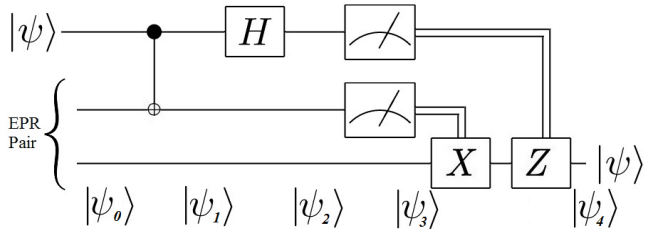

Figure 1. Quantum Teleportation Circuit

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:

$$|00\rangle \longrightarrow [\alpha|0\rangle + \beta|1\rangle] \quad (9)$$

$$|01\rangle \longrightarrow [\alpha|1\rangle + \beta|0\rangle] \quad (10)$$

$$|10\rangle \longrightarrow [\alpha|0\rangle - \beta|1\rangle] \quad (11)$$

$$|11\rangle \longrightarrow [\alpha|1\rangle - \beta|0\rangle] \quad (12)$$

Alice will sends to Bob her measurement and depending on Alice's qubits Bob will have to fix the state in his

possession by applying one of the quantum gates. Receive state $|00\rangle$ will require Bob to apply I gate, receiving state $|01\rangle$ will require him to apply X gate, receiving state $|10\rangle$ will require him to apply the Z gate and receiving state $|11\rangle$ will require Bob to apply X and Z gates which is often called Y gate.

$$Z = \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix} \quad Y = \begin{bmatrix} 0 & -i \\ i & 0 \end{bmatrix} \tag{13}$$

III. Related Work

An enhancement of multiparty quantum secret sharing (QSS) algorithm [27] was proposed in [28]. The authors proposed two algorithms taking advantage of the entanglement swapping operation. The first proposed algorithm requires the sender to release the encoded classical bits to help the receiver to deduce intended classical bits from a qubit state. However, in the second proposed scheme the sender and the receiver need to physically meet and exchange the classical bits. However, the new algorithms improve the amount of data the original QSS protocol transmit by the reducing it twice. Further, the new algorithms are more efficient in term of the performance compared to the original QSS. In addition, a reused scheme was also proposed to reuse some qubits from previous round in new round.

A protocol for quantum authentication using entanglement swapping was proposed in [12]. The aim in this paper is to securely exchange messages between the participating parties. The proposed protocol provides mutual authentication for the sender and the receiver when using unsecure routing path. Further, the authentication protocol depends on four sequence numbers called S_i generated by a third party with the following functions for each number: Quantum key generation by S_1, eavesdropping detection by S_2, identity identification by S_3 and message transferring using S_4 . In order to obtain the secret key, the eavesdropper on the channel need to successfully break S_3. However, the eavesdropped on the routing path cannot break the entanglement swapping technique and cannot have access to the controlled qubits.

Network cryptographic protocol based on entanglement swapping key management center was proposed in [29]. The goal was to securely distribute the secret keys between parties with prior sharing of entanglement pairs. However, this protocol only requires channels between the users and the key manger center and not between the users themselves. This protocol preserve the networks resource by only allowing the physical communication channels between the users and the key management center and eliminating user-to-user channels. Also, this protocol performs well even if the users are far away from each other's.

Quantum direct communication (QDC) for mutual authentication based on entanglement swapping was proposed in [13]. 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 irrelative to each other.

In [30] 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.

$$J(k) = \log \frac{k}{n} \tag{14}$$

$$S(k) = -\frac{k}{n} * log \frac{k}{n} \tag{15}$$

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 [31]. 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. As illustration, an entangled pair of photons are created by SPDC and passed through an active and reference fiber channels. An attempt to change a photon by an attacker will result in destroying the correlation between these two photons and will result in losing the entanglement. On the other hand, Cyber-Physical security is implement using quantum seal. Detecting 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.

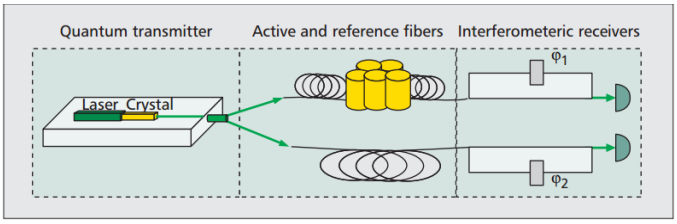

Figure 2. Quantum Seal [31]

Quantum determined key distribution scheme was proposed in [32] and it is based on quantum teleportation. In this protocol the sender and the receiver will share predetermined key by taking the 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.

$$|\Phi^+\rangle_{AB} = \frac{1}{\sqrt{2}}(|0\rangle_A|0\rangle_B + |1\rangle_A|1\rangle_B) \quad (16)$$

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

Our proposed algorithm is based on two important algorithms in quantum computing. The first algorithm is entanglement swapping [33] and the second algorithm is the remote state preparation [15] In this Algorithm we establish an EPR-pair between source Alice and destination Bob where Alice and Bob share EPR-pairs with an intermediate node called Charlie. Charlie will be acting as a trusted generator for EPR pair between Alice and Bob. The shared EPR pair between Alice and Charlie is as follows:

$$AC = \frac{|0\rangle_A|0\rangle_C + |1\rangle_A|1\rangle_C}{\sqrt{2}} \quad (17)$$

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

$$CB = \frac{|0\rangle_C|0\rangle_B + |1\rangle_C|1\rangle_B}{\sqrt{2}} \quad (18)$$

$$AC \otimes CB = \frac{|0\rangle_A|0\rangle_C + |1\rangle_A|1\rangle_C}{\sqrt{2}} \otimes \frac{|0\rangle_C|0\rangle_B + |1\rangle_C|1\rangle_B}{\sqrt{2}} \quad (19)$$

$$= \frac{1}{2}\begin{Bmatrix} |0\rangle_A|0\rangle_C\,(|0\rangle_C|0\rangle_B + |1\rangle_C|1\rangle_B) \\ +|1\rangle_A|1\rangle_C\,(|0\rangle_C|0\rangle_B + |1\rangle_C|1\rangle_B) \end{Bmatrix} \quad (20)$$

Applying CNOT to C:

$$= \frac{1}{2}\begin{Bmatrix} |0\rangle_A|0\rangle_C\,(|0\rangle_C|0\rangle_B + |1\rangle_C|1\rangle_B) \\ +|1\rangle_A|1\rangle_C\,(|1\rangle_C|0\rangle_B + |0\rangle_C|1\rangle_B) \end{Bmatrix} \quad (21)$$

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

$$= \frac{1}{2\sqrt{2}}\begin{Bmatrix} |0\rangle_A(|0\rangle_C + |1\rangle_C)\,(|0\rangle_C|0\rangle_B + |1\rangle_C|1\rangle_B) \\ +|1\rangle_A(|0\rangle_C - |1\rangle_C)\,(|1\rangle_C|0\rangle_B + |0\rangle_C|1\rangle_B) \end{Bmatrix} \quad (22)$$

Rearrange and group C:

$$= \frac{1}{2\sqrt{2}}\begin{Bmatrix} |00\rangle_C|0\rangle_A|0\rangle_B + |1\rangle_A|1\rangle_B \\ |01\rangle_C|0\rangle_A|1\rangle_B + |1\rangle_A|0\rangle_B \\ |10\rangle_C|0\rangle_A|0\rangle_B - |1\rangle_A|1\rangle_B \\ |11\rangle_C|0\rangle_A|1\rangle_B - |1\rangle_A|0\rangle_B \end{Bmatrix} \quad (23)$$

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:

$$|\Psi^-\rangle_{AB} = \frac{1}{\sqrt{2}}(|0\rangle_A|1\rangle_B - |1\rangle_A|0\rangle_B) \quad (24)$$

$$|\Psi^+\rangle_{AB} = \frac{1}{\sqrt{2}}(|0\rangle_A|1\rangle_B + |1\rangle_A|0\rangle_B) \quad (25)$$

$$|\Phi^-\rangle_{AB} = \frac{1}{\sqrt{2}}(|0\rangle_A|0\rangle_B - |1\rangle_A|1\rangle_B) \quad (26)$$

$$|\Phi^+\rangle_{AB} = \frac{1}{\sqrt{2}}(|0\rangle_A|0\rangle_B + |1\rangle_A|1\rangle_B) \quad (27)$$

After creating the EPR pair between the Alice and Bob, Alice can remotely prepare a known quantum state and share it with the Bob. For example, if Alice wants to transmit a qubit in pure state:

$$|\Psi\rangle = \alpha|0\rangle + \beta|1\rangle \quad (28)$$

And since Alice and Bob share an EPR pair, let's consider it in state $|11\rangle$ from the previous step. The EPR will as follows:

$$|\Psi^-\rangle_{AB} = \frac{1}{\sqrt{2}}(|0\rangle_A|1\rangle_B - |1\rangle_A|0\rangle_B) \quad (29)$$

As the particle A is related to Alice and particle B is related to Bob. Now Alice wants to transmit a known state $|\Psi\rangle$ to Bob. So Alice can chose to measure the state in any qubit basis such as $|\Psi\rangle$ which is related to basis $|0\rangle_A$ as:

$$|0\rangle_A = \alpha|\Psi\rangle - \beta|\Psi\perp\rangle \quad (30)$$

Or state $|\Psi\perp\rangle$ which is related to basis $|1\rangle_A$ as:

$$|1\rangle_A = \beta^*|\Psi\rangle + \alpha|\Psi\perp\rangle \quad (31)$$

Writing the state $|\Psi^-\rangle_{AB}$ with these basis will result in:

$$|\Psi^-\rangle_{AB} = \frac{1}{\sqrt{2}}(|\Psi\rangle_A|\Psi\perp\rangle_B - |\Psi\perp\rangle_A|\Psi\rangle_B) \quad (32)$$

After Alice applies Von Neumann measurement on single particle, let's consider Alice's particle result to be in state $|\Psi\perp\rangle$. Then the total state will be as follows:

$$|\Psi\perp\rangle_A\langle\Psi\perp|\Psi^-\rangle_{AB} = -\frac{1}{\sqrt{2}}|\Psi\perp\rangle_A \otimes |\Psi\rangle_B \quad (33)$$

When Alice sends the measurement result to Bob by sending only one classical bit, Bob will find the particle in state $\alpha|0\rangle_B + \beta|1\rangle_B$. However, when the measurement of Alice's particle is $|\Psi\rangle_A$ then Bob will find it in state:

$$|\Psi\perp\rangle = \beta^*|\Psi\rangle + \alpha|\Psi\perp\rangle \quad (34)$$

Which is the complement to the original state.

This method works on any EPR pair result from the entanglement swapping from the basis $\{|\Psi^\pm\rangle_{AB}, |\Phi^\pm\rangle_{AB}\}$. However, applying Pauli matrices ($\sigma_z, i\sigma_y, \sigma_x$) will be required to form the correct state based on the EPR pair used between Alice and Bob.

V. Results and Discusison

The proposed algorithm provides a secure way to transmit the secret key between a sender and receiver at a minimum cost. For instance, the Teleportation protocol requires two classical bits and one bit of entanglement to transmit a quantum state. However, in the proposed protocol the cost of transmitting a quantum state from a sender to a receiver only requires one classical bit and one bit of entanglement. That is, the sender transmits each qubit by only one classical bit instead of two classical bits. Further, the proposed protocol does not require the sender and the receiver to have a physical quantum communication channel for date transmission as in quantum key distribution protocols based on BB84 and B92. Instead, it take the advantages of quantum entanglement. For example the protocol in [34] is based on protocol BB84. To form a secret key, the parties are required to send the physical quantum state through quantum communication channel to the trusted center. Then, the trusted center will form a key based on the received states from both parties. However, in the proposed protocol we do not use the quantum channels to transmit physical quantum states between the sender and the receiver. Instead we depend on the EPR pairs between each party, coupled with the EPR generator, to securely form EPR pairs between the other parties.

VI. Conclusion

In this paper we presented a secure algorithm based on entanglement swapping and remote state preparation of quantum state. Initially, Alice and Bob do not share an entanglement EPR pairs and ask for Charlie's help to create one. After forming the EPR pairs Between Alice and Bob by Charlie's help, Alice can prepare a quantum state and then help Bob to create it. However, before Alice will be able to help Bob to create the intended state, Alice will need to fully know the state by measuring it first using one of the bases as aforementioned. Once Alice becomes fully aware of her state, she can just send her one classical bit measurement result to Bob and Bob will have to be able to construct Alice's state because it will be the complement of the original state. We assume Charlie's system is secure and therefore, it will be impossible for any third party to manipulate the entanglement between Alice and Bob because Charlie will process the entanglement swapping there will not be transmission of any physical quantum state. Moreover, the one classical bit that Alice will send to Bob will not reveal any information about the target state Alice prepared to Bob and also, Alice did not send any physical quantum to Bob.

References

[1] L. K. Grover, "A fast quantum mechanical algorithm for database search," in *Proceedings of the twenty-eighth annual ACM symposium on Theory of computing*, 1996, pp. 212-219.

[2] M. A. Nielsen and I. L. Chuang, *Quantum computation and quantum information*: Cambridge university press, 2010.

[3] P. W. Shor, "Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer," *SIAM journal on computing,* vol. 26, pp. 1484-1509, 1997.

[4] R. Ratan and A. Y. Oruc, "Self-Routing Quantum Sparse Crossbar Packet Concentrators," *Computers, IEEE Transactions on,* vol. 60, pp. 1390-1405, 2011.

[5] L. Yi-MIn, W. Zhang-Yin, L. Jun, and Z. Zhan-Jun, "Remote Preparation of Three-Particle GHZ Class States," *Communications in Theoretical Physics,* vol. 49, p. 359, 2008.

[6] Z.-J. Zhang, "Multiparty quantum secret sharing of secure direct communication," *Physics Letters A,* vol. 342, pp. 60-66, 2005.

[7] C. H. Bennett, G. Brassard, C. Crépeau, R. Jozsa, A. Peres, and W. K. Wootters, "Teleporting an unknown quantum state via dual classical and Einstein-Podolsky-Rosen channels," *Physical Review Letters,* vol. 70, p. 1895, 1993.

[8] D. Wang, Y.-m. Liu, and Z.-j. Zhang, "Remote preparation of a class of three-qubit states," *Optics Communications,* vol. 281, pp. 871-875, 2008.

[9] N. Gisin, G. Ribordy, W. Tittel, and H. Zbinden, "Quantum cryptography," *Reviews of modern physics,* vol. 74, pp. 145-195, 2002.

[10] Z.-j. Zhang, Y. Li, and Z.-x. Man, "Multiparty quantum secret sharing," *Physical Review A,* vol. 71, p. 044301, 2005.

[11] W. K. Wootters and W. H. Zurek, "A single quantum cannot be cloned," *Nature,* vol. 299, pp. 802-803, 1982.

[12] C. Chia-Hung, L. Tien-Sheng, C. Ting-Hsu, Y. Shih-Yi, and K. Sy-Yen, "Quantum authentication protocol using entanglement swapping," in *Nanotechnology (IEEE-NANO), 2011 11th IEEE Conference on*, 2011, pp. 1533-1537.

[13] L. Zhihao, C. Hanwu, L. Wenjie, and X. Xiling, "Mutually Authenticated Quantum Key Distribution Based on Entanglement Swapping," in *Circuits, Communications and Systems, 2009. PACCS '09. Pacific-Asia Conference on*, 2009, pp. 380-383.

[14] H.-K. Lo, "Classical-communication cost in distributed quantum-information processing: A generalization of quantum-communication complexity," *Physical Review A,* vol. 62, p. 012313, 2000.

[15] A. K. Pati, "Minimum classical bit for remote preparation and measurement of a qubit," *Physical Review A,* vol. 63, p. 014302, 2000.

[16] C. H. Bennett, D. P. DiVincenzo, P. W. Shor, J. A. Smolin, B. M. Terhal, and W. K. Wootters, "Remote state preparation," *Physical Review Letters,* vol. 87, p. 077902, 2001.

[17] M.-Y. Ye, Y.-S. Zhang, and G.-C. Guo, "Faithful remote state preparation using finite classical bits and a nonmaximally entangled state," *Physical Review A,* vol. 69, p. 022310, 2004.

[18] I. Devetak and T. Berger, "Low-entanglement remote state preparation," *Physical review letters,* vol. 87, pp. 197901-197901, 2001.

[19] X. Peng, X. Zhu, X. Fang, M. Feng, M. Liu, and K. Gao, "Experimental implementation of remote state preparation by nuclear magnetic resonance," *Physics Letters A,* vol. 306, pp. 271-276, 2003.

[20] S. Babichev, B. Brezger, and A. Lvovsky, "Remote preparation of a single-mode photonic qubit by measuring field quadrature noise," *Physical review letters,* vol. 92, p. 047903, 2004.

[21] G.-Y. Xiang, J. Li, B. Yu, and G.-C. Guo, "Remote preparation of mixed states via noisy entanglement," *Physical Review A,* vol. 72, p. 012315, 2005.

[22] A. Hayashi, T. Hashimoto, and M. Horibe, "Remote state preparation without oblivious conditions," *Physical Review A,* vol. 67, p. 052302, 2003.

[23] Y. Xia, J. Song, and H.-S. Song, "Multiparty remote state preparation," *Journal of Physics B: Atomic, Molecular and Optical Physics,* vol. 40, p. 3719, 2007.

[24] B. A. Nguyen and J. Kim, "Joint remote state preparation," *Journal of Physics B: Atomic, Molecular and Optical Physics,* vol. 41, p. 095501, 2008.

[25] N. A. Peters, J. T. Barreiro, M. E. Goggin, T.-C. Wei, and P. G. Kwiat, "Remote state preparation: arbitrary remote control of photon polarization," *arXiv preprint quant-ph/0503062,* 2005.

[26] N. S. Yanofsky and M. A. Mannucci, *Quantum computing for computer scientists* vol. 20: Cambridge University Press Cambridge, 2008.

[27] Z.-j. Zhang and Z.-x. Man, "Multiparty quantum secret sharing of classical messages based on entanglement swapping," *Physical Review A,* vol. 72, p. 022303, 2005.

[28] Y. H. Chou, C. Y. Chen, R. K. Fan, H. C. Chao, and F. J. Lin, "Enhanced multiparty quantum secret sharing of classical messages by using entanglement swapping," *Information Security, IET,* vol. 6, pp. 84-92, 2012.

[29] Z. Dexi, Z. Qiuyu, and L. Xiaoyu, "Quantum Cryptographic Network Using Entanglement Swapping," in *Networks Security Wireless Communications and Trusted Computing (NSWCTC), 2010 Second International Conference on*, 2010, pp. 373-376.

[30] M. Niemiec and A. R. Pach, "Management of security in quantum cryptography," *Communications Magazine, IEEE,* vol. 51, pp. 36-41, 2013.

[31] T. S. Humble, "Quantum security for the physical layer," *Communications Magazine, IEEE,* vol. 51, pp. 56-62, 2013.

[32] L. Xiaoyu, W. Nianqing, and Z. Dexi, "Quantum Determined Key Distribution Scheme Using Quantum Teleportation," in *Software Engineering, 2009. WCSE '09. WRI World Congress on*, 2009, pp. 431-434.

[33] C. Sheng-Tzong, W. Chun-Yen, and T. Ming-Hon, "Quantum communication for wireless wide-area networks," *Selected Areas in Communications, IEEE Journal on,* vol. 23, pp. 1424-1432, 2005.

[34] M. Alshowkan, K. Elleithy, A. Odeh, and E. Abdelfattah, "A new algorithm for three-party Quantum key distribution," in *Innovative Computing Technology (INTECH), 2013 Third International Conference on*, 2013, pp. 208-212.