Scientific Research and Essays Vol. 7(9), pp. 1051-1057, 9 March, 2012
Available online at http://www.academicjournals.org/SRE
DOI: 10.5897/SRE11.2055
ISSN 1992-2248 ©2012 Academic Journals

Full Length Research Paper

Quantum message exchanging network using entanglement swapping and decoy photons

Negin Fatahi and Mosayeb Naseri*

Department of Physics, Islamic Azad University, Kermanshah Branch, Kermanshah, Iran.

Accepted 17 February, 2012

We propose a scheme for secure quantum message exchanging network following the idea in entanglement swapping. In this scheme, the servers of the network provide the service for preparing the Greenberger-Horne-Zeilinger (GHZ) entangled states as quantum channels. For preventing the eavesdropping, a security checking method is suggested. After the security check, anyone of the authorized users can exchange his/her messages with another on the network securely and directly.

Key words: Quantum secure direct communication, entanglement swapping, quantum communication network PACS.

INTRODUCTION

The quantum key distribution (QKD) is an ingenious application of quantum mechanics, in which two remote legitimate users (Alice and Bob) can establish a shared secret key through the transmission of quantum signals. Since the first protocol of QKD has been proposed (Bennett and Brassard 1984), a number of QKD protocols have been proposed as well (Ekert, 1991; Bennett, 1992; Bennett et al., 1992; Gisin et al., 2002) and extended to quantum encryption (Boykin and Roychowdhury, 2003; Leung, 2002; Gisin et al., 2002; Zhou, et al., 2007), quantum identification authentication (Mihara, 2002; Li and Barnum, 2004; Zhou et al., 2005), quantum secret sharing (Hillery et al., 1999; Karlsson et al., 1999; Xiao et al., 2004) and quantum secure direct communication (QSDC) protocols (Long and Liu, 2002; Deng et al., 2003; Deng and Long, 2004; Wang et al., 2005; Wang et al., 2005; Li et al., 2006). Beige et al. (2002) presented the first QSDC scheme in which the message can be read after the transmission of classical information. Also, ping-pong protocol (PPP) was presented by Boström and Felbinger (2002), which allows the encoded bit to be decoded instantaneously in each respective transmission run. However, the PPP supports only one-way communication and contains in itself some limitations (Cai, 2003). A QSDC protocol has at least two important features. The first one is the security. That is to say, it requires the protocol and is secure. The second feature is the directness which requires that the receiver can read out the secret message directly. According to these two features (the definition), the quantum communication protocols shown in Cai (2003) is quantum direct communication protocol, but not secure ones as the receiver cannot check eavesdropping before the secret message is encoded on a qubit. It is worth to point out that Deng and Long (2007) gave a criteria for QSDC (Deng-Long criteria for QSDC as shown in their reviewing article (Long et al, 2007) and another article about QSDC network (Deng et al., 2006). According to Deng-Long criteria, a real secure QSDC scheme should satisfy four requirements: (1) The secret message can be read out by the receiver directly after the quantum states are transmitted through a quantum channel, and there is not additional classical information exchange by the sender and the receiver in principle except for those for checking eavesdropping and estimating the error rate. (2) The eavesdropper, Eve cannot obtain useful information about the secret message no matter what she does. (3) The two legitimate users can detect Eve before they encode the secret message on the quantum states. (4) The quantum states are transmitted in block by block way. Considering (Long et al., 2007; Deng et al., 2006) the quantum communication protocol by Beige et al.

*Corresponding author. E-mail: m.naseri@iauksh.ac.ir.

(2002) is not a QSDC. It is not based on the fact that the protocol is insecure, but just as the physical essence that the message can only be read out after at least one bit of classical information is exchanged for each qubit, not directly. There are some misunderstandings about the work. It is similar to a QKD working in a deterministic way. It is a modified BB84 QKD with 2° of freedom of single photons (that is, the polarization states and the spatial-mode stats of a single photon). As shown in the reviewing article about QSDC (Long et al., 2007; Deng et al., 2006), the quantum communication protocol by Beige et al. (2002) is a deterministic secure quantum communication (DSQC) protocol. So far some interesting DSQC protocols have been proposed (Yan and Zhang, 2004; Gao et al., 2005; Man et al., 2005; Gao, 2004; Gao and Yan, 2005; Gao et al., 2004; Gao et al., 2005; Man et al., 2005; Zhu et al., 2006; Li et al., 2006; Lee et al., 2006; Wang et al., 2006; Li et al., 2006; Wang et al., 2006; Wang et al., 2006; Wang et al., 2006; Ji et al., 2006; Cao and Song, 2006).

In fact, there are some confusion about QKD and QSDC. A QSDC can surely be used as a QKD: QSDC can transmit predetermined message securely, it can also transmit random numbers deterministically. Although the quantum communication protocol in Beige et al. (2002) is a QKD protocol as shown in the paper. However, by definition of QSDC, the property which can transmit secret message directly in a deterministic manner is a characteristic feature of QSDC. The efficient QKD protocol in Beige et al. (2002) can be considered as a QSDC protocol and it satisfies all the criteria of a QSDC protocol.

Nguyen (2004) presented the first quantum dialogue scheme using Einstein-Podolsky-Rosen (EPR) pairs, which can simultaneously transmit their secret message to each other in each quantum channel. Man et al. (2005) thought that it is insecure and modified the security check. Then, Ji and Zhang (2006) presented a quantum dialogue protocol based on single photon. Also, Xia et al. (2006, 2007) presented two quantum dialogue protocols using Greenberger-Horne-Zeilinger (GHZ) state. Unfortunately, it was pointed out that half of the secret message would be leaked through the classical channel in quantum dialogue protocols. However, the leaked message only describes the relation between the secret message of the two communicators, so the eavesdropper cannot gain any of the genuine secret messages between the two communicators (Tan and Cai, 2008; Gao et al., 2005). Recently, a quantum telephone protocol including the dialing process and the talking one has been proposed by Wen et al. (2007). Although, the security of secure quantum telephone has been analyzed (Naseri, 2009), where a fake entangled photons eavesdropping (FEP) attack on the secure quantum telephone protocol is presented, in which a dishonest server, an eavesdropper can gain full information of the communication with zero risk of being detected. Also the main source of the failure of the protocol is discussed. Finally, it is realized that to preserve the security of the secure quantum telephone protocol, the server of the protocol should be necessarily trusted.

More recently, a protocol for controlled quantum dialogue in the network using entanglement swapping, in which, any two users can exchange the secret message securely is with the cooperation of the other users (Deng et al., 2008). Also two protocols for multiparty quantum communication have been proposed (Deng et al., 2006; Li et al., 2007).

A practical quantum communication requires that anyone on a passive optical network can communicate another authorized user, similar to a classical communication network, such as the World Wide Web (that is, www) and the classical telephone network. Usually, there are some servers (the number of the servers is much less than that of the users), say $Alice_j$ who provide the service for preparing and measuring the quantum signal for the legitimate users on a passive optical network, which will reduce the requirements on the users devices for secure communication (not the servers) largely, same as the classical communication. In this paper, we will introduce a quantum secure message exchanging network scheme using the idea of entanglement swapping.

MATERIALS AND METHODS

Quantum message exchanging network using entanglement swapping

Before giving our protocol, let us review an entanglement swapping for two EPR states. The goal of entanglement swapping is to make quantum systems entangled, which are never interacted directly before, through certain physical process. Entanglement swapping plays an important role in quantum communications and quantum network. For example, entanglement swapping can be used to prepare new entanglement states and extend the distance of quantum communications. Suppose Alice shares two EPR pairs with Bob:

$$\left|\phi^{+}\right\rangle_{12}=\frac{1}{\sqrt{2}}\left(\left|00\right\rangle+\left|11\right\rangle\right)_{12},$$

$$\left|\phi^{+}\right\rangle_{34}=\frac{1}{\sqrt{2}}\left(\left|00\right\rangle+\left|11\right\rangle\right)_{34}, \quad (1)$$

The photons 1 and 4 are in the site of Alice and Bob owns the photons 2 and 3. The state of the whole system can be denoted as:

$$\left|\phi^{+}\right\rangle_{12}\left|\phi^{+}\right\rangle_{34}=\frac{1}{2}\left(\left|\phi^{+}\right\rangle_{14}\left|\phi^{+}\right\rangle_{23}+\left|\phi^{-}\right\rangle_{14}\left|\phi^{-}\right\rangle_{23}+\left|\psi^{+}\right\rangle_{14}\left|\psi^{+}\right\rangle_{23}+\left|\psi^{-}\right\rangle_{14}\left|\psi^{-}\right\rangle_{23}\right). \quad (2)$$

So when a Bell-state measurement is made on photons 1 and 4 by Alice, the photons 2 and 3 are projected onto one of the following states:

$$\left|\phi^{+}\right\rangle_{14}\left|\phi^{+}\right\rangle_{23},\left|\phi^{-}\right\rangle_{14}\left|\phi^{-}\right\rangle_{23},\left|\psi^{+}\right\rangle_{14}\left|\psi^{+}\right\rangle_{23},\left|\psi^{-}\right\rangle_{14}\left|\psi^{-}\right\rangle_{23}$$

That is to say, the entanglement swapping entangles two photons (2 and 3) that have never interacted before by performing a Bell-state measurement on the photons (1 and 4) which are from two different entangled pairs.

For each request of the users, If two users do exist in a same branch of the network, the server of the branch connect the user to another on the network or sending a sequence of photons to the user. If two users do not exist in a same branch of the network, they can agree that the server of the branch with the sender provides the service for preparing the quantum signal and charge the communicator who starts the communication, and the other servers cooperate to provide the service for connecting the two communicators and control the communication in some a time slot.

Now, let us describe our quantum message exchanging network scheme. In this scheme, the servers cooperate to provide the service of communication to the registered users. If anyone of the users wants to call other one privately, he/she asks the server of the branch to provide quantum channels. Once they have passed their server's authentication, they can talk with each other securely in the quantum talking process. Registered users apply for their respective N-bit network quantum keys from the servers. To obtain unconditional security, the quantum keys are distributed via QKD protocols, such as BB84 or B92 protocols. The quantum message exchanging in the network can be achieved in two phases, the connection phase and the communication phase.

Quantum connection and authentication phase

Here, we consider a general case, where, Bob_k wants to exchange his message with $Zack_m$. Suppose that the server of the branch with Bob_k is S_1 and the sever of the branch with $Zack_m$, is S_2. Suppose Bob_k asks Bob to provide quantum channels. Once Bob_k and $Zack_m$ have passed the authentications of S_1 and S_2, they can exchange their secret bits with each other securely in the quantum communication process. The connection phase including identification of Bob_k and $Zack_m$ is described as follows:

Step 1: Dialing process

The dialing process includes the authentication of Bob_k and S_2 (the server of the branch with the receiver) by S_1 (the server of the branch with the applier) and the authentication of $Zack_m$ by S_2 can be described as follows:

1) At the beginning of the communication Bob_k asks S_1 to provide quantum channels between $Zack_m$ and him. On receiving the request of Bob_k, S_1 prepares an ordered set of L qubits authentication sequence $[P_1(B_k), P_2(B_k),..., P_L(B_k)]$ using bases $B_Z = \left|0\right\rangle,\left|1\right\rangle$ or $B_X = \left|+\right\rangle,\left|-\right\rangle$ according to the network quantum key. If the i-th value of the quantum key is 1, S_1 prepares the i-th qubit of the authentication sequence using the bases $B_Z = \left|0\right\rangle,\left|1\right\rangle$, or else, S_1 prepares it using the bases $B_X = \left|+\right\rangle,\left|-\right\rangle$. To verify identity of Bob_k, he/she sends the authentication sequence $[P_1(B_k), P_2(B_k),..., P_L(B_k)]$ to Bob_k. The legitimate user Bob_k knows his authentication sequence. Therefore, he can accurately choose bases $B_Z = \left|0\right\rangle,\left|1\right\rangle$ or $B_X = \left|+\right\rangle,\left|-\right\rangle$ to measure the sequence according to his sequence. Then Bob_k announces S_1 the measuring results. Afterwards S_1 checks the measuring results of Bob_k. If the results are the same as he/she prepared, the authentication of Bob_k is succeeded and the protocol proceeds. Otherwise, he/she aborts the protocol. After the authentication of Bob_k, S_1 applies to connect to S_2 with the cooperation of other servers. Then he/she sends the authentication sequence $[P_1(Z), P_2(Z),..., P_L(Z)]$ to S_2 to verify his identity. So he/she verifies the identity of S_2 in a similar way to the method that is used by him/her to verify Bob_k. Afterwards S_1 announces S_2 that his/her user, Bob_k is willing to communicate with one of the S_2's users $Zack_m$. Then S_1 asks S_2 to connect the quantum line to $Zack_m$ after she verifies the identity of $Zack_m$.

Step 2: Distribution process

Bob prepares a set of G groups n+2-particle GHZ states

$$\left|\phi\right\rangle = \bigotimes_{i=1}^{G}\frac{1}{\sqrt{2}}\left(\left|++\right\rangle_{B_k^i Z_m^i}\otimes_{j=1}^{m}\left|+\right\rangle_{S_i}+\left|--\right\rangle_{B_k^i Z_m^i}\otimes_{j=1}^{m}\left|-\right\rangle_{S_i}\right), \tag{3}$$

Lets Bob_k to exchange his 2G-bit message with $Zack_m$'s 2G-bit message, where S_i denotes the particle which is taken by i-th server $(S_1, S_2,\ldots,S_n)$. Then S_1 forms n+2 photon sequences:

$$B_K - Sequence = B_k^1, B_k^2,..., B_k^G ,$$

$$Z_m - Sequence = Z_m^1, Z_m^2,..., Z_m^G ,$$

$$S_m - Sequence = S_1^1, S_1^2,..., S_1^G ,$$

$$\vdots$$

$$S_n - Sequence = S_n^1, S_n^2,..., S_n^G . \tag{4}$$

Then S_1 keeps S_1-sequence with herself and sends S_2-sequence to $S_2,\ldots,S_n$-sequence to S_n. Also she sends B_k-sequence to Bob_k and Z_m-sequence to $Zack_m$, respectively. To insure the security of the communication, it is required that the length of the photon sequence is larger than the length of secret message. Also S_1 adds some decoy photons in sequences before she sends the sequence to the other severs and the communicators.

Step 3: Dialing acceptance

If the servers agree for Bob_k and $Zack_m$ to communicate, they perform the measurements and announce the measurement outcomes through classical channel. After the measurements, the photons of the servers are traced out of entanglement.

Step 4: Checking the honesty of the other servers with decoy photons

For ensuring the honesty of the other servers S_1 adds some decoy photons in sequences before she sends B_k-sequence to Z_m-sequence, S_2-sequence , . . ., S_n-sequence to Bob_k, $Zack_m$, $S_1,\ldots,S_n$ respectively. The decoy photon technique was proposed first by Li et al. (2005, 2006) in QKD network. The principle of the decoy photon technique is that S_1 prepares some photons which are randomly in one of the four non-orthogonal states $\left|+\right\rangle,\left|-\right\rangle,\left|1\right\rangle,\left|0\right\rangle,$ and then inserts them into the transmitted sequences. As the states and the positions of the decoy photons are unknown for all the parties of the communication, the

Table 1. The correlation of measurement results of the network's parties.

The outcome results of Bob_k	The outcome results of $Zack_m$	The outcome result of the servers
$\|+\rangle$	$\|+\rangle$	$_{All}\|+\rangle$
$\|-\rangle$	$\|-\rangle$	$_{All}\|-\rangle$
$\|0\rangle$	$\|0\rangle$	$_{Even}\|0\rangle$
$\|1\rangle$	$\|1\rangle$	$_{Even}\|1\rangle$
$\|0\rangle$	$\|0\rangle$	$_{Odd}\|0\rangle$
$\|1\rangle$	$\|1\rangle$	$_{Odd}\|1\rangle$

eavesdropping done by an eavesdropper will inevitably disturb these decoy photons and will be detected. The number of the decoy photons is not required to be very large, just large enough for checking eavesdropping.

Quantum communication phase

The communication phase process begins if the authentication to Bob_k, S_2 and $Zack_m$ has succeeded in the quantum connection phase and the honesty of the other servers is insured by S_1. This phase can be described as follows:

Step 1: Security check

Bob_k selects randomly a sufficiently large subset of photons from B_k-sequence as a checking group, which can be used to check whether there is eavesdropping in the network or not. And then, she tells $Zack_m$ which photons she selects through classical channel. Bob_k and $Zack_m$ measure the photons in their checking group under the same bases as the servers, respectively. After the measurements, they begin to compare their measurement outcomes publicly. If there is no eavesdropping, the measurement outcomes of Bob_k, $Zack_m$ and the servers should be correlative as shown in Table 1. If there exists eavesdropping, their measurement outcomes will not be correlative completely. Then they abandon this communication. Otherwise, they would continue.

Step 2: Message encoding

Bob_k and $Zack_m$ discard the checking group and retain a subset of other EPR states, which are the outcomes measured by the servers. They call them message group. Bob_k and $Zack_m$ also record the measurement outcome in the message group of the servers as k, which is 00 if even number of $|1\rangle$ is gained, or 01 if odd number of $|1\rangle$ is gained. Then the communicators encode their secret message x, y by performing unitary transformations $I, \sigma_x, i\sigma_y, \sigma_z$ on their own photons according to their previous agreement. In order to realize quantum message exchanging network, Bob_k and $Zack_m$ firstly come to an agreement that the encoding operations $I, \sigma_x, i\sigma_y, \sigma_z$ represent classical information 00, 01, 10 and 11, respectively.

Step 3: Message decoding

Finally to decode the encoded messages, Bob_k and $Zack_m$ perform Bell-state measurements on the photons in their own sites and announce the measurement outcomes p and q through classical channel, where Bell-state measurement outcomes $|\phi^+\rangle, |\phi^-\rangle, |\psi^+\rangle, |\psi^-\rangle$, corresponds to classical information 00, 11, 01 and 10, respectively. Then Bob_k and $Zack_m$ decode secret message simultaneously. Bob_k can decode the secret message of $Zack_m$ as x=|q-k-p-y| and $Zack_m$ can also decode the secret message of Bob_k as y=|p-k-q-x|, here "-" represents single-bit binary subtraction.

RESULTS

It is needless to say, every secure communication protocol, whether quantum or classical, needs an authenticated channel. User authentication (also called user identification) makes it possible for a communicator to prove his/her identity, often as the first step to log into a system. Usually, the authenticated channel is tacitly assumed. The need for an authenticated channel in any secure communication protocol can be seen immediately when asking: how can Bob_k be sure that it is $Zack_m$ he is talking to? In the presented scheme, if each server in a network is trusted for the users of her own branch, the server of the branch with the sender can check whether the receiver of the message is legitimate or not by authentication of the server of the branch with the receiver, and insures the sender of the message that the travel encoded photons are taken by the legitimate receiver, $Zack_m$.

DISCUSSION

In essence, the security of quantum communication is based on the principles of quantum mechanics, such as

the uncertainty principle (no-cloning theorem), quantum correlations, non locality and so on. These principles ensure that Eve cannot copy the quantum states freely, as her action will inevitably perturb the quantum systems, which will introduce some errors in the results. It is obvious that the present protocol is secure if the process for sharing the entangled states as quantum channels is secure. As we know the principle of the security in a quantum communication protocol depends on the fact that an eavesdropper's action can be detected by analyzing the error rate of the samples chosen randomly with statistical theory. Here, we consider two situations, in the first one we suppose that one of the servers is dishonest and the second case is the eavesdropping procedure in which the eavesdropper (Eve) who is outside the network wants to steal the content of the communication.

The dishonest servers may introduce the additional photons and make them entangle into the communication network, but it can be detected by the communicators in security check. Also, If anyone of the servers is dishonest and tells wrong information about measurement outcome, the action will be found in the security checking process by the server of the branch with the applier, furthermore it can be found exactly who did the error when the fake photon method is used.

In the second case, Eve may intercept the travel photons from S_2 to the others and measures the photons with the basis $|+\rangle,|-\rangle$ or $|0\rangle,|1\rangle$. Then she resents fake photons with state $|+\rangle$ or state $|-\rangle$.However, the procedure for analyzing the error rate of the samples in the first step of the quantum communication phase, guarantees the revealing of the Eve.

As it is mentioned in the work, the security of our quantum communication network scheme is based on the security of the process for preparing and distribution of the entangled states as quantum channels. On the other hand, the cost of the preparation of quantum states is too high to the common communicators. So in the presented scheme, similar to the telephone system in our real life, some servers agents are introduced, who are provide legitimate communicators a quantum channel, and play a role of authenticated channel.

It is worth pointing that if there is no authenticated channel then a man-in-the-middle attack is always possible, resulting in a complete loss of security. For example, suppose that the public channel in BB84 was not authenticated. Then Eve could simply slip into the role of Bob, capture all qubits and receive all measurement results from Alice, perform her own measurements, compare some of them publicly with Alice and finally establish a shared secret key between her and Alice. In the meanwhile, Bob can do nothing but inform Alice (via public channel) that it is not him who she is talking to all the time. But since the public channel is not authenticated, why should Alice trust Bob more than Eve? To prevent the active attack strategy in the quantum key distribution, classical identity authentication (CIA) protocols such as Wegman-Carter protocol are naturally available (Carter and Wegman, 1979; Wegman and Carter, 1981).

In essence, the present topic has been discussed in detail by some groups (Phoenix et al., 1995; Townsend, 1997; Biham et al., 1996; Deng et al., 2002; Li et al., 2005; Li et al., 2006; Deng et al., 2006; Deng et al., 2007; Deng et al., 2007). Compared with previous protocol, the presentation of quantum authentication method in our scheme is one of the advantages of the protocol. The other advantage of the presented scheme is that the communicators must pay for the server to rent the quantum channel and the cost of using the quantum network depends on the order of the GHZ states which are prepared by the server of the branch with the applier, which directly depends on the number of the servers between the communicators.

Conclusion

A new feasible scheme for quantum message exchanging network with entanglement swapping only needs single-photon operations, and Bell-state measurements is proposed. In this scheme, if each user trust on the server of the branch with himself/herself once he/she have passed authentication of the server, a quantum channel is provided to him/her, and communication phase will begins. After confirming the security of the transmission, an authorized user on the network can communicate another one securely.

ACKNOWLEDGMENTS

It is a pleasure to thank the reviewers and the editor for their many fruitful discussions about the topic. The authors would like to thank Alimorad Ahmadi for his helpful comments with English and also Soheila Gholipour and Yasna Naseri for their interest in this work. This work is supported by Islamic Azad University, Kermanshah Branch, Kermanshah, Iran.

REFERENCES

Beige *A,* Englert B G, Kurtsiefer C H, Weinfurter H (2002). Secure communication with a publicly known key. Acta Phys. Pol. A, 101*:* 357

Bennett CH (1992). Quantum cryptography using any two nonorthogonal states. Phys. Rev. Lett., 68*:* 3121-3124.

Bennett CH, Brassard G (1984). Quantum Cryptography: Public key distribution and coin tossing. Proceedings of the IEEE International Conference on Computers, Systems and Signal Processing, Bangalore, India., pp. 175-179.

Bennett CH, Brassard G, Mermin ND (1992). Quantum cryptography without bell's theorem. Phys. Rev. Lett*.,* 68*:*557-569.

Biham E, Huttner B, Mor T (1996). Quantum cryptographic network

based on quantum memories. Phys. Rev. A, 54: 2651.
Boykin PO, Roychowdhury V (2003). Optimal encryption of quantum bits. Phys. Rev. A, 67: 42317-042322.
Cai Q (2003). The “Ping-Pong” Protocol Can Be Attacked without Eavesdropping. Phys. Rev. Lett., 91: 109801.
Cao HJ, Song HS (2006). Quantum Secure Direct Communication with W State. Chin. Phys. Lett., 23: 290.
Carter JL, Wegman MN (1979). Universal classes of hash functions. J. Comput. Syst. Sci., 18: 143.
Deng FG, Li X H, Li CY, Zhou P, Zhou Y (2006). Multiparty quantum secret splitting and quantum state sharing. Phys. Lett. A, 359: 359.
Deng FG, Li X H, Li CY, Zhou P, Zhou HY (2006). Multiparty quantum secret splitting and quantum state sharing. Phys. Lett. A, 354(3): 190-195.
Deng FG, Li XH, Li CY, Zhou P, Liang YJ, Zhou HY (2006). Multiparty quantum secret report. Chin. Phys. Lett., 23 : 1676.
Deng FG, Li XH, Li CY, Zhou P, Zhou HY (2008). Economical Quantum Secure Direct Communication. Optics Commun., 281: 6135-6138.
Deng FG, Li XH, Li CY, Zhou P, Zhou Y (2007). Economical quantum secure direct communication network with single photons Chin. Phys., 16: 3553.
Deng FG, Li XH, Li CY, Zhou P, Zhou Y (2007). Quantum secure direct communication network with superdense coding and decoy photons. Phys. Scr., 76: 25.
Deng FG, Liu XS, Ma YJ, Xiao L, Long GL (2002) Theoretical Scheme for Multi-user Quantum Key Distribution with N Einstein-Podolsky-Rosen Pairs on a Passive Optical Network. *Chin. Phys. Lett.,* 19: 893.
Deng FG, Long GL (2004). Secure direct communication with a quantum one-time pad. Phys. Rev. A, 69: 052319.
Deng FG, Long GL, Liu XS (2003). Optimal encryption of quantum bits. Phys. Rev. A, 68: 042317.
Ekert AK (1991). Quantum cryptography based on Bell's theorem. Phys. Rev. Lett., 67: 661-663.
Gao F, Guo FZ, Wen QY, Zhu FC (2005). Revisiting the security of quantum dialogue and bidirectional quantum secure direct communicationSci. China G Phys. Mech. Astron., 48: 237.
Gao T (2004) . Controlled and Secure Direct Communication Using GHZ State and Teleportation. Naturforsch A 59 (2004) 597.
Gao T, Yan FL, Wang ZX (2004). Quantum secure direct communication by EPR pairs and entanglement swapping. Nuovo Cimento B, 119: 313.
Gao T, Yan FL, Wang ZX (2005). Controlled quantum teleportation and secure direct communication. Chin. Phys., 14: 893.
Gao T, Yan FL, Wang ZX (2005). Deterministic secure direct communication using GHZ states and swapping quantum entanglement. J. Phys. A: Math. Gen, 38: 5761.
GaoT, Yan FL, Wang ZX (2005). Deterministic secure direct **...** using GHZ states and swapping quantum entanglement. J. Phys. A,: 5761.
Gisin N, Ribordy G, Tittel W, Zbinden H (2002), Quantum cryptography. Rev. Mod. Phys., 74:145-195.
Hillery M, Buzek V, Berthiaume A (1999). Quantum secret sharing. Phys. Rev. A, 59: 1829-1834.
Ji X, Zhang S (2006). Secure quantum dialogue based on single-photon.. Chin. Phys., 15: 1418.
Karlsson A, Koashi M, Imoto N (1999). Quantum entanglement for secret sharing and secret splitting. Phys. Rev. A, 59: 162-168.
Lee H, Lim J, Yang H (2006). Quantum direct communication with authentication.. Phys. Rev. A 73: 042305.
Leung D (2001). Quantum vernam cipher. Quantum Inf. Comput., 2: 14-34.
Li C Yan, Zhou HY, Wang Y, Deng FG (2005). Secure Quantum Key Distribution Network with Bell States and Local Unitary Operations. *Chin. Phys. Lett.,* 22 : 1049.
Li CY, Li XH, Deng FG, Zhou P, Liang YJ, Zhou HY (2006). Efficient Quantum Cryptography Network without Entanglement and Quantum Memory. Chin. Phys. Lett., 23: 2896.
Li CY, Zhou HY, Wang Y, Deng FG (2005). Secure Quantum Key
Distribution Network with Bell States and Local Unitary Operations. Chin. Phys. Lett., 22: 1049.
LI X H, ZHOU P, LIANG Y J, LI C Y, ZHOU H Y, DENG F G (2006). Quantum Secure Direct Communication Network with Two-Step Protocol. Chinese Physics Letters 23 (5): 1080-1083.
Li X, Barnum H (2004). Quantum Authentication Using Entangled States. Int. J . Foundations Comput. Sci., 15: 609-618.
Li XH, Li CY, Deng FG, Zhou P, Liang YJ, Zhou HY (2007). Multiparty Quantum Remote Secret Conference. Chin. Phys. Lett., 24: 23-26.
Li XH, Deng FG, Li CY, Liang YJ, Zhou P, Zhou HY (2006). Deterministic Secure Quantum Communication Without Maximally. Entangled States. J. Korean Phys. Soc., 49: 1354.
Li XH, Deng FG, Zhou HY (2006). Improving the security of secure direct communication based on the secret transmitting order of particles. Phys. Rev. A, 74: 054302.
Li XH, Zhou P, Liang YJ, Li CY, Zhou HY, Deng FG (2006). Quantum Secure Direct Communication Network with Two-Step Protocol. *Chin. Phys. Lett.* 23 : 1080.
Long GL, Deng FG, Wang C, Li XH, Wen K, Wang WY (2007). Quantum secure direct communication and deterministic secure quantum communication. Front. Phys. Chin., 2: 251.
Long GL, Liu XS (2002). Theoretically efficient high-capacity quantum-key-distribution scheme. Phys. Rev. A 65: 032302.
Man Z X, Zhang ZJ, Li Y(2005). Deterministic secure direct communication by using swapping quantum entanglement and local unitary operations. Chin. Phys. Lett., 22: 22.
Man ZX, Zhang ZJ, Li Y (2005). Deterministic Secure Direct Communication by Using Swapping Quantum Entanglement and Local Unitary Operation. Chin. Phys. Lett., 22 : 18.
Man ZX, Zhang ZJ, Li Y (2005). Deterministic secure direct communication by using swapping quantum entanglement and local unitary operations. Chin. Phys. Lett., 22: 22.
Mihara T (2002). Quantum identification schemes with entanglements. Phys Rev A, 65: 052326- 052329.
Naseri M (2009). Eavesdropping on secure quantum telephone protocol with dishonest server. Optics Commun., 282 : 3375-3378.
Nguyen BA (2004). Quantum exam. Phys. Lett. A, 328: 6.
Phoenix SJD, Barnett SM, Townsend PD, Blow KJ (1995). Multi-user Quantum Cryptography on Optical Networks. J. Mod. Opt., 42: 1155-1163.
Tan YG, Cai QY (2008). classical correlation in quantum dialogue. Int. J. Quant. Inf., 6: 325.
Townsend PD (1996). Quantum cryptography on multiuser optical fibre networks. *Nature,* 385: 47.
Wang C, Deng F G, Long G L (2005). Multi-step quantum secure direct communication. Opt. Commun., 253 : 15-20.
Wang C, Deng FG, Li YS, Liu XS, Long GL (2005). Quantum secure direct communication with high-dimension quantum superdense coding. Phys. Rev. A, 71: 044305.
Wang HF, Zhang S, Yeon KH, Um CI (2006). Quantum secure direct communication by using a GHZ state. J. Korean Phys.Soc., 49 : 459.
Wang J, Zhang Q, Tang C J (2006). quantum secure direct communication without a pre-established secure quantum channel Int. J. Quantum inf., 4: 925.
Wang J, Zhang Q, Tang C J (2006). Quantum secure direct communication without using perfect quantum channel. Int. J. Mod. Phys. C, 17: 685.
Wang J, Zhang Q, Tang CJ (2006). Quantum secure direct communication based on order rearrangement of single photons. Phys. Lett. A, 358: 256.
Wegman MN, Carter JL (1981). New hash functions and their use in authentication and set equality. J. Comput. Syst. Sci., 22: 265.
Wen X, Liu Y, Zhou N (2007). Secure quantum telephone. Optics Commun., 275: 278-282.
Xia Y, Fu CB, Zhang S (2006). Quantum dialogue by using the GHZ state. J. Korean. Phys. Soc., 48: 24-27.
Xia Y, Song J, Nie J, Song HS (2007). Controlled Secure Quantum Dialogue Using a Pure Entangled GHZ States Comm. Theor. Phys., 48: 841.
Xiao L, Long GL, Deng FG, Pan JW (2004). Efficient multiparty quantum-secret-sharing schemes. Phys. Rev. A, 69 : 052307.
Yan F L, Zhang X (2004). A scheme for secure direct communication using EPR pairs and teleportation. Euro. Phys. J. B, 41: 75.
Zhou N, Liu Y, Zeng G, Xiong J (2007). Novel qubit block encryption algorithm with hybrid keys. Physica A, 375: 693-698.

Zhou N, Zeng G, Zeng W, Zhu F (2005). Cross-center quantum identification scheme based on teleportation and entanglement swapping. *Optics* Commun., 254*:* 380-*388.*

Zhu AD, Xia Y, Fan QB, Zhang S (2006). Secure direct communication based on secret transmitting order of particles. Phys. Rev. A, 73: 022338.