ISSN 1063-7761, Journal of Experimental and Theoretical Physics, 2007, Vol. 105, No. 6, pp. 1132–1135. © Pleiades Publishing, Inc., 2007.

ATOMS, MOLECULES, OPTICS

Multiparty-Controlled Quantum Secure Direct Communication[1]

X.-M. Xiu, L. Dong, Y.-J. Gao, and F. Chi

Physics Department, Bohai University, Jinzhou, 121000 People's Republic of China

e-mail: xiuxiaomingdl@126.com

Received July 12, 2007

Abstract—A theoretical scheme of a multiparty-controlled quantum secure direct communication is proposed. The supervisor prepares a communication network with Einstein–Podolsky–Rosen pairs and auxiliary particles. After passing a security test of the communication network, a supervisor tells the users the network is secure and they can communicate. If the controllers allow the communicators to communicate, the controllers should perform measurements and inform the communicators of the outcomes. The communicators then begin to communicate after they perform a security test of the quantum channel and verify that it is secure. The recipient can decrypt the secret message in a classical message from the sender depending on the protocol. Any two users in the network can communicate through the above processes under the control of the supervisor and the controllers.

PACS numbers: 03.67.Hk, 03.67.Dd, 03.65.Ud

DOI: 10.1134/S1063776107120047

1. INTRODUCTION

Cryptography [1] is an important branch of quantum information theory, which enables two communicators to communicate in privacy. Using the characteristics of quantum mechanics, for example, quantum entanglement, secret information can be securely transmitted between two users. Quantum key distribution (QKD) is a process whereby two legitimate users first establish a shared secret key by means of the transmission of a classical message and then use this key to encrypt (decrypt) a secret message. Since the first QKD scheme proposed in 1984 [2], many QKD schemes have been presented [3–8].

In 2002, a quantum secure direct communication (QSDC) scheme was proposed in [9], which permits messages to be communicated directly without first establishing a random key to encrypt them as QKD schemes do. Subsequently, the so-called "ping-pong protocol" was proposed in [10], allowing the encoded bit to be decoded instantaneously in each respective round of transmissions. However, it is insecure in a noisy quantum channel, as indicated in [11, 12]. Also, the ping-pong protocol can be attacked without eavesdropping [13, 14]. The ping-pong protocol was modified in [15] for transmitting a secret message with a single photon in a mixed state. A two-step QSDC protocol using blocks of Einstein–Podolsky–Rosen (EPR) pairs was proposed in [16], and a QSDC scheme with a quantum one-time pad using single photons in [17] was developed to enhance security of the communication. To date, many studies have been focused on QSDC schemes [9–24].

As a matter of fact, in the above schemes, the secret information to be sent can be read by the recipient only after the sender completes the transmission of classical information for each qubit. It is necessary for the sender to send the qubits carrying the secret message to the recipient. Therefore, an eavesdropper has the chance to attack the qubits in transmission to obtain the secret information or disturb the communication without being discovered. Some QSDC schemes are presented in which no qubit is transmitted, using entanglement and teleportation (EPR pairs [21, 22], W state [23]). A controlled quantum secure direct communication scheme using the GHZ state and teleportation was proposed in [24].

There are many QKD network schemes [7, 25–29], but a distrustful server can steal certain information without being detected in these schemes. Two QSDC network schemes with ordered N EPR photon pairs were proposed in [30]. An authorized user can communicate securely with any other in the network in these schemes. There are only two users (sender and receiver) and the server in the network; communication between the two users can only be controlled by the server. A multiparty-controlled quantum secure direct communication protocol is presented in [31] using single photons.

In this paper, a theoretical scheme for multiparty-controlled quantum secure direct communication using ordered EPR pairs and auxiliary particles is proposed. There are no qubits carrying a secret message to be transmitted; this scheme can avoid an eavesdropper's attack on the qubits in a transmission. Any two users in a communication network composed of many users can communicate in their protocol under the control of the supervisor and controllers.

There are three kinds of roles in this scheme. The supervisor is mainly responsible for the preparation of the communication network. Any two users in the net can communicate under the control of the other users.

[1] The text was submitted by the authors in English.

We call them communicators. The rest of the users, who are the controllers, perform measurements on their particles to help control the communication between the communicators. The supervisor also fulfils the same control function as the controllers do.

This paper is organized as follows. The scheme of a multiparty controlled quantum secure direct communication is proposed in Section 2. Subsequently, in Section 3, we discuss the security of this scheme. Finally, conclusions are given in Section 4.

2. MULTIPARTY-CONTROLLED QUANTUM SECURE DIRECT COMMUNICATION

Multiparty-controlled quantum secure direct communication can be achieved via the following steps.

(1) Alice prepares ordered particle pairs (A_l, B_l), $(l = 1, 2, \ldots, N)$ in an EPR state $|\Phi^+\rangle_{A_lB_l}$ or $|\Psi^+\rangle_{A_lB_l}$,

$$|\Phi^+\rangle_{A_lB_l} = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)_{A_lB_l},$$
$$|\Psi^+\rangle_{A_lB_l} = \frac{1}{\sqrt{2}}(|01\rangle + |10\rangle)_{A_lB_l}. \quad (1)$$

The EPR state can be securely set up with entanglement purification protocols [32, 33], which provides a way of protecting quantum states from interaction with the environment.

Then, Alice introduces an auxiliary particle sequence $(C_l, D_l, \ldots)$, $(l = 1, 2, \ldots, N)$ in the initial state $|0\rangle$. Each sequence contain M particles. She then performs an H gate operation on them. Subsequently, Alice sends particles (C_l, A_l), particles (D_l, C_l), and particles (E_l, D_l), …, $(l = 1, 2, \ldots, N)$ through CNOT gates. In a CNOT gate, the state of the target bit changes if and only if the state of control bit is $|1\rangle$.

After these manipulations, the system state of particles $(A_l, B_l, C_l, \ldots)$ at Alice's location can be written as

$$|\Psi\rangle = \prod_{l=1}^{N}|\xi_{M+2,l}\rangle = \prod_{l=1}^{N}\frac{1}{\sqrt{2}}(|i_{M+1,i}\rangle|\xi_{M+1,l}\rangle + |\bar{i}_{M+1,l}\rangle|\xi'_{M+1,l}\rangle), \quad (2)$$

where $i_{1,l}, i_{2,l}, \ldots, i_{M+2,l} \in \{0, 1\}$, $\bar{i}_{1,l}, \bar{i}_{2,l}, \ldots, \bar{i}_{M+2,l}$ are the counterparts of the binary numbers $i_{1,l}, i_{2,l}, \ldots, i_{M+2,l}$, i.e., $\bar{i}_{1,l} = 1 - i_{1,l}$, $\bar{i}_{2,l} = 1 - i_{2,l}$, …, $\bar{i}_{M+2,l} = 1 - i_{M+2,l}$. The M-particle maximally entangled state $|\xi_{M,l}\rangle$ $(M \geq 2)$ satisfies the conditions

$$\langle\xi_{M,l}|\xi'_{M,l}\rangle = 0,$$
$$|\xi_{M,l}\rangle = \frac{1}{\sqrt{2}}(|i_{M-1,l}\rangle|\xi_{M-1,l}\rangle + |\bar{i}_{M-1,l}\rangle|\xi'_{M-1,l}\rangle),$$
$$|\xi_{2,l}\rangle = \frac{1}{\sqrt{2}}(|i_{1,l}\rangle|i_{2,l}\rangle + |\bar{i}_{1,l}\rangle|\bar{i}_{2,l}\rangle), \quad (3)$$
$$|\xi'_{2,l}\rangle = \frac{1}{\sqrt{2}}(|\bar{i}_{1,l}\rangle|i_{2,l}\rangle + |i_{1,l}\rangle|\bar{i}_{2,l}\rangle),$$

where $|\xi_{2,l}\rangle$ and $|\xi'_{2,l}\rangle$ are the two-particle Bell states. For example, if

$$|\xi_{2,l}\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle),$$

then

$$|\xi'_{2,l}\rangle = \frac{1}{\sqrt{2}}(|01\rangle + |10\rangle);$$

if

$$|\xi_{2,l}\rangle = \frac{1}{\sqrt{2}}(|01\rangle + |10\rangle),$$

then

$$|\xi'_{2,l}\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle).$$

(2) Alice sends the ordered particle sequence $(B_l, C_l, D_l, \ldots)$ $(l = 1, 2, \ldots, N)$ in sequence to the respective other users (Bob, Charlie, David, etc.) and keeps the particle sequence A_l herself. The other users tell Alice that they have received all the particle sequences through classical channels.

(3) Alice randomly selects a sufficiently large subset of particles from the particle sequence as the checking sequence to test the security of the communication network; the other particles are the communication sequence used to communicate between the communicators. This is the first security test (the security test of the communication network). She asks the other users to measure the checking sequence using one of two measurement bases, $\{|0\rangle, |1\rangle\}$ or $\{|+\rangle, |-\rangle\}$, which are appointed by her at random. The other users perform measurements along the same basis on the same ordered particles and then transmit their measurement outcomes to Alice. Alice tests the security of the communication network depending on the measurement outcomes of all the users including herself. When the original EPR state is $|\Phi^+\rangle$, the measurement outcome $|1\rangle$ should be even. When the original EPR state is $|\Psi^+\rangle$, the measurement outcome $|1\rangle$ should be odd. The measurement outcomes of all the users should be the same when $\{|+\rangle, |-\rangle\}$ is adopted as the measurement basis. If the error rate of the checking sequence is reasonably low, Alice can trust the communication network; otherwise, she abandons the processing.

(4) Any two users in the network may communicate under the control of the other users. We suppose that

Bob and Charlie communicate with each other. If the controllers agree to cooperate with the communicators, they (including the supervisor) should perform measurements on their own particles in the communication sequence. After the measurements, they tell Bob and Charlie their measurement outcomes.

(5) After receiving the measurement outcomes, Bob and Charlie ask Alice to tell them the original EPR pairs that were adopted to prepare the communication network. If the original EPR state is $|\Phi^+\rangle$, Alice transmits 0 to Bob and Charlie. If the original EPR state is $|\Psi^+\rangle$, Alice transmits 1 to them. For the security of communication in privacy between them, Bob and Charlie should test the security of the quantum channel. This is the second security test (the security test of the quantum channel). Bob and Charlie randomly select particles from the communication sequence that suffice for testing the security of the quantum channel. We say that these particles are the checking sequence of the communicators and the rest of the particles are the coding sequence. Bob and Charlie perform a local measurement on the checking sequence in their hands using one of the two measurement bases $\{|0\rangle, |1\rangle\}$ or $(|+\rangle, |-\rangle\}$ randomly. Depending on Alice and controllers' classical information, Bob and Charlie can test the security of the quantum channel. If the error rate of the checking sequence is low enough, Bob and Charlie continue to communicate. Otherwise, they abandon this communication.

(6) If the security of the quantum channel is ensured, the communicators may communicate by their protocol. For instance, they agree that if the sender's measurement outcome is identical to the secret message to be transmitted, the sender sends 0 to the recipient; otherwise, the sender sends 1 to the recipient. We assume that Charlie is the recipient and Bob is the sender. Bob performs measurements on his particles in the coding sequence and sends the corresponding classical information to Charlie through classical channels. That is, if Bob's measurement outcome is $|0\rangle$ and the message to be sent is 0, or the measurement outcome is $|1\rangle$ and the message to be sent is 1, Bob sends 0 to Charlie. Otherwise, Bob sends 1 to Charlie.

(7) Charlie can deduce the measurement outcomes of Bob depending on his measurement outcomes. Consequently, Charlie can deduce the secret message that Bob wants to transmit to him depending on the classical message from Bob. For instance, if the classical information about the original EPR state is 00110101 and the outcome from the controllers is 11010110 (the signal "1" indicates that the number of the measurement outcomes $|1\rangle$ is odd, and the signal "0" that the number of the measurement outcomes $|1\rangle$ is even), Bob's classical information is 00011011. If Charlie's measurement outcome is $|1\rangle, |0\rangle, |1\rangle, |0\rangle, |1\rangle, |0\rangle, |0\rangle, |1\rangle$, he can deduce that Bob's outcome is $|0\rangle, |1\rangle, |0\rangle, |0\rangle, |1\rangle, |0\rangle, |1\rangle, |0\rangle$. Therefore, the secret message that Bob wishes to send to Charlie is 01010001.

This completes the process whereby Bob transmits the secret message to Charlie. Of course, Charlie can also transmit a secret message to Bob to realize communication.

Any two users can communicate if the other users agree to cooperate with them in the scheme. The communication can be performed under the control of the supervisor and the controllers. If they have no cooperation, the communications cannot be made.

3. SECURITY OF THE SCHEME

There are two security tests in this scheme.

In the first security test, we suppose that an eavesdropper, who is outside the communication network, wants to steal the secret message. The eavesdropper intercepts the particles transmitted to other users by the supervisor and resends her own particles to them to imitate the particles she intercepted previously; however, the vicious action can be detected efficiently after Alice analyzes the measurement outcomes from the other users in the communication network.

If the first security test shows that the communication network is secure, the dishonesty of other users (the controllers) can be found in the second security test. If the controllers know all the classical information in the transmission in the scheme, they can deduce that the quantum channel between the communicators is being used. However, the information cannot help them obtain the secret message between two communicators, because they have no information on the measurement outcomes on EPR pairs by either of the two communicators. If the controllers want to steal the secret message or disturb a communication, their action can be found by the communicators in the second security test. If all the controllers want to disturb the communication collectively, the result does so.

There is a certain difference between the supervisor and the controllers. The supervisor knows the original EPR pairs and her own measurement outcome. Can she make the sender and the recipient deduce the error information about the quantum channel between them by giving them the wrong classical information? For example, if the original EPR pair is $|\Phi^+\rangle$ and the computational basis measurement outcome of Bob is $|0\rangle$, she tells the corresponding outcome to Charlie. This cannot allow the sender and the recipient to deduce a wrong verdict from the above analysis in Eq. (3). If Alice gives wrong classical information about the original EPR pairs, this can allow the sender and the recipient to deduce wrong information about the quantum channel. However, this can be found out by the sender and the recipient by comparing the measurement outcome in the second security test.

If the quantum channel is perfect and the controller is friendly and cooperative, the second security test is not necessary and an eavesdropper can be detected by the first security test.

To summarize, two communicators can detect an eavesdropper and ensure the security of private communication between them via the above security tests.

4. CONCLUSIONS

In summary, a theoretical scheme of multiparty-controlled quantum secret direct communication is proposed. Any two users in the communication network can communicate under the control of the supervisor and the controllers.

The communicators can communicate after the supervisor and the controllers agree to cooperate with them; they must know the original EPR states adopted to prepare the communication network and the measurement outcomes of all the controllers. If any one of them does not cooperate with the communicators, that is, he performs no measurement or tells the communicators a wrong measurement outcome, this communication between the communicators has no way of being completed.

The features of the scheme are as follows. Some simple manipulations are necessary in the scheme, which are only a few quantum CNOT gate operations and single-qubit operations, which could be implemented using technology that is currently being developed. The measurement order of each controller may be random when they begin to perform measurement after all the users receive the particles distributed earlier by the supervisor. The supervisor can increase the number of users by increasing the number of auxiliary particles and distributing corresponding particles to them. That is, the supervisor can increase the number of controllers before the communicators begin to communicate. The security tests ensure that this scheme is secure and the secret message has not leaked to another person. Since no qubit carries the secret message to be transmitted, this scheme can avoid an attack on the transmitted qubit, but the capacity is restricted: an entangled state as a quantum channel only carries one bit of classical information except for those used as the security test.

In reality, noise always exists in a quantum channel, which gives an eavesdropper a chance to steal the communication content between the communicators. The sender and the recipient can adopt quantum privacy amplification [34, 35] for improving security in a noisy channel to realize the quantum secure direct communication.

From the above analysis, we may deduce that the theoretical scheme can be realized in the near future.

ACKNOWLEDGMENTS

This study was supported by the National Natural Science Foundation of China (grant no. 10647101).

REFERENCES

1. N. Gisin, G. Ribordy, W. Tittel, and H. Zbinden, Rev. Mod. Phys. **74**, 145 (2002).
2. C. H. Bennett and G. Brassard, in *Proceedings of IEEE International Conference on Computer, Systems, and Signal Processing, Bangalore, India* (IEEE, New York, 1984), p. 175.
3. A. K. Ekert, Phys. Rev. Lett. **67**, 661 (1991).
4. C. H. Bennett, G. Brassard, and N. D. Mermin, Phys. Rev. Lett. **68**, 557 (1992).
5. D. Bruß, Phys. Rev. Lett. **81**, 3018 (1998).
6. G. L. Long and X. S. Liu, Phys. Rev. A **65**, 032302 (2002).
7. P. Xue, C. F. Li, and G. C. Guo, Phys. Rev. A **65**, 022317 (2002).
8. A. Acín, N. Gisin, and L. Masanes, Phys. Rev. Lett. **89**, 187902 (2002).
9. A. Beige, B. G. Englert, C. Kurtsiefer, and H. Weinfurter, Acta Phys. Pol. A **101**, 357 (2002).
10. K. Boström and T. Felbinger, Phys. Rev. Lett. **89**, 187902 (2002).
11. A. Wójcik, Phys. Rev. Lett. **90**, 157901 (2003).
12. Z. J. Zhang, Z. X. Man, and Y. Li, Phys. Lett. A **333**, 46 (2004); **341**, 385 (2005).
13. Q. Y. Cai, Phys. Rev. Lett. **91**, 109801 (2003).
14. Z. J. Zhang, Z. X. Man, and Y. Li, Int. J. Quantum Inf. **2**, 521 (2004).
15. Q. Y. Cai and B. W. Li, Chin. Phys. Lett. **21**, 601 (2004).
16. F. G. Deng, G. L. Long, and X. S. Liu, Phys. Rev. A **68**, 042317 (2003).
17. F. G. Deng and G. L. Long, Phys. Rev. A **69**, 052319 (2004).
18. B. A. Nguyen, Phys. Lett. A **328**, 6 (2004).
19. Z. X. Man, Z. J. Zhang, and Y. Li, Chin. Phys. Lett. **22**, 18 (2005).
20. Z. X. Man and Y. J. Xia, Chin. Phys. Lett. **23**, 1973 (2006).
21. F. L. Yan and X. Q. Zhang, Eur. Phys. J. B **41**, 75 (2004).
22. T. Gao, F. L. Yan, and Z. X. Wang, Int. J. Mod. Phys. C **16**, 1293 (2005).
23. H. J. Cao and H. S. Song, Phys. Scr. **74**, 572 (2006).
24. T. Gao, F. L. Yan, and Z. X. Wang, Chin. Phys. **14**, 0893 (2005).
25. P. D. Townsend, Nature **385**, 47 (1997).
26. E. Biham, B. Huttner, and T. Mor, Phys. Rev. A **54**, 2651 (1996).
27. F. G. Deng, X. S. Liu, Y. J. Ma, et al., Chin. Phys. Lett. **19**, 893 (2002).
28. C. Y. Li, H. Y. Zhou, Y. Wang, and F. G. Deng, Chin. Phys. Lett. **22**, 1049 (2005).
29. X. H. Li, P. Zhou, Yu-Jie Liang, et al., Chin. Phys. Lett. **23**, 1080 (2006).
30. F. G. Deng, X. H. Li, C. Y. Li, et al., Phys. Lett. A **359**, 359 (2006).
31. J. Wang, H. Q. Chen, Q. Zhang, and C. J. Tang, Acta Phys. Sin. **56**, 0673 (2007).
32. C. H. Bennett, G. Brassard, S. Popescu, et al., Phys. Rev. Lett. **76**, 722 (1996).
33. C. H. Bennett, D. P. DiVincenzo, J. A. Smolin, and W. K. Wootters, Phys. Rev. A **54**, 3824 (1996).
34. D. Deutsch, A. Ekert, R. Jozsa, et al., Phys. Rev. Lett. **77**, 2818 (1996).
35. F. G. Deng and G. L. Long, quant-ph/0408102.