Vol 14 No 5, May 2005
1009-1963/2005/14(05)/0893-05

Chinese Physics

Controlled quantum teleportation and secure direct communication*

Gao Ting(高　亭)[a)b)d)†], Yan Feng-Li(闫凤利)[c)d)], and Wang Zhi-Xi(王志玺)[b)]

[a)] *College of Mathematics and Information Science, Hebei Normal University, Shijiazhuang* 050016, *China*
[b)] *Department of Mathematics, Capital Normal University, Beijing* 100037, *China*
[c)] *College of Physics, Hebei Normal University, Shijiazhuang* 050016, *China*
[d)] *CCAST (World Laboratory), Beijing* 100080, *China*

(Received 30 August 2004; revised manuscript received 13 November 2004)

We present a controlled quantum teleportation protocol. In the protocol, quantum information of an unknown state of a 2-level particle is faithfully transmitted from a sender Alice to a remote receiver Bob via an initially shared triplet of entangled particles under the control of the supervisor Charlie. The distributed entangled particles shared by Alice, Bob and Charlie function as a quantum information channel for faithful transmission. We also propose a controlled and secure direct communication scheme by means of this teleportation. After ensuring the security of the quantum channel, Alice encodes the secret message directly on a sequence of particle states and transmits them to Bob supervised by Charlie using this controlled quantum teleportation. Bob can read out the encoded message directly by the measurement on his qubit. In this scheme, the controlled quantum teleportation transmits Alice's message without revealing any information to a potential eavesdropper. Because there is not a transmission of the qubit carrying the secret message between Alice and Bob in the public channel, it is completely secure for controlled and direct secret communication if perfect quantum channel is used. The special feature of this scheme is that the communication between two sides depends on the agreement of a third side to co-operate.

Keywords: controlled quantum teleportation, secure direct communication, measurement
PACC: 0365

1. Introduction

The goal of secure communication is to make two distant parties to exchange information but not to allow a third party to steal or alter the content of information. Before transmitting their secret messages the two distant parties must distribute secret key first. Since it is difficult to distribute secret key through a classical channel, people have paid a lot of attention to quantum key distribution. In 1984, Bennett and Brassard presented the first quantum cryptography protocol.[1] Up to now, there have already been several quantum key distribution schemes such as proposed in Refs.[2–17].

Recently, a novel quantum direct communication protocol has been proposed[18] that allows secure direct communication, i.e. the two parties communicate important messages directly without first establishing a shared secret key to encrypt them and the message is deterministically sent through the quantum channel, but can only be decoded after a final transmission of classical information. Boström and Felbinger[19] put forward a direct communication scheme, the "ping-pong protocol", which is insecure if it is operated in a noisy quantum channel, as indicated by Wójcik.[20] More recently, Deng *et al*[21] suggested a two-step quantum direct communication protocol using Einstein–Podolsky–Rosen pair block. However, in all these secure direct communication schemes it is necessary to send the qubits with secret messages in the public channel. Therefore, a third party, Eve, can attack the qubits in transmission. Yan and Zhang[22] presented a scheme for secure direct and confidential communication between Alice and Bob, using Einstein–Podolsky–Rosen pairs and teleportation.[23] We proposed a protocol for controlled and secure direct communication us-

---

*Project supported by the National Natural Science Foundation of China (Grant No 10271081), the Natural Science Foundation of Hebei Province (Grant No A2004000141) and the Key Natural Science Foundation of Hebei Normal University.

†E-mail: gaoting@heinfo.net

ing Greenberger–Horne–Zeilinger (GHZ) state and teleportation.[24] Because there is not a transmission of the qubits carrying the secret messages between Alice and Bob in the public channel, they are completely secure for direct secret communication if perfect quantum channel is used.

Quantum teleportation is commonly considered as one of the most striking progress of quantum information theory. In the original quantum teleportation scheme of Bennett *et al*,[23] quantum information of an unknown quantum state of a d-level particle is faithfully transmitted from a sender Alice to a spatially distant receiver Bob via an initially shared maximally entangled state with the help of classical communication. To date teleportation has been generalized to many cases.[25−39] In this paper, we present a controlled quantum teleportation protocol, in which a third side (the supervisor Charlie) is included, so that the quantum channel is controlled by this additional side, and quantum information of an unknown quantum state of a 2-level particle can not be transmitted unless all three sides agree to co-operate. We also propose another scheme for controlled secure direct communication with the aid of a three-particle entangled state and this controlled teleportation. After ensuring the security of the quantum channel, Alice encodes the secret messages directly on a sequence of particle states and transmits them to Bob supervised by Charlie using this controlled quantum teleportation. Bob can read out the encoded messages directly by the measurement on his qubit. In this scheme, the controlled quantum teleportation transmits Alice's message without revealing any information to a potential eavesdropper. Because there is not a transmission of the qubit carrying the secret messages between Alice and Bob in the public channel, it is completely secure for controlled and direct secret communication if perfect quantum channel is used. The special feature of this scheme is that the communication between two sides depends on the agreement of the third side.

In Section 2 of the paper we present a protocol for controlled quantum teleportation. In the protocol, quantum information of an unknown state of a 2-level particle is faithfully transmitted from a sender Alice to a remote receiver Bob via an initially shared triplet in an entangled state under the control of the supervisor Charlie. The distributed entangled particles shared by Alice, Bob and Charlie function as a quantum information channel for faithful transmission. In Section 3 we also propose a controlled and secure direct communication scheme by means of this teleportation. A summary is given in Section 4.

2. Controlled quantum teleportation

In Ref.[38], Zhou *et al* proposed a controlled quantum teleportation scheme, where the entanglement property of GHZ state is utilized. Here we present another controlled quantum teleportation protocol in which a triplet in an entangled state (different from GHZ state) initially shared by the sender Alice, the receiver Bob and the supervisor Charlie functions as a quantum channel with the help of a classical information channel.

We suppose that the sender Alice, the receiver Bob and the supervisor Charlie are spatially separated from each other. The original unknown quantum state of a 2-level particle Alice wishes to teleport to Bob is

$$|\psi\rangle_{\rm M}=a|0\rangle_{\rm M}+b|1\rangle_{\rm M}, \tag{1}$$

where $|a|^2+|b|^2=1$. The quantum channel initially shared by Alice, Bob and Charlie is a three-particle entangled state:

$$|\xi\rangle_{\rm ABC}=\frac{1}{2}(|000\rangle+|110\rangle+|011\rangle+|101\rangle)_{\rm ABC}. \tag{2}$$

The joint state of the system is

$$\begin{aligned}|\psi\rangle_{\rm M}|\xi\rangle_{\rm ABC}=&(a|0\rangle+b|1\rangle)_{\rm M}\\&\otimes\frac{1}{2}(|000\rangle+|110\rangle\\&+|011\rangle+|101\rangle)_{\rm ABC}.\end{aligned} \tag{3}$$

If Charlie wants to help Alice for the quantum teleportation, he just measures his portion of ABC, namely qubit C, in the basis $\{|0\rangle_{\rm C},|1\rangle_{\rm C}\}$, and transfer the result of his measurement to Alice and Bob via a classical channel. Then the particles M, A and B would become one of the states:

$$\begin{aligned}|\phi_1\rangle_{\rm MAB}=&{}_{\rm C}\langle 0|\psi\rangle_{\rm M}|\xi\rangle_{\rm ABC}=(a|0\rangle+b|1\rangle)_{\rm M}\\&\otimes\frac{1}{\sqrt{2}}(|00\rangle+|11\rangle)_{\rm AB},\end{aligned} \tag{4}$$

$$\begin{aligned}|\phi_2\rangle_{\rm MAB}=&{}_{\rm C}\langle 1|\psi\rangle_{\rm M}|\xi\rangle_{\rm ABC}=(a|0\rangle+b|1\rangle)_{\rm M}\\&\otimes\frac{1}{\sqrt{2}}(|01\rangle+|10\rangle)_{\rm AB},\end{aligned} \tag{5}$$

which can be rewritten as

$$\begin{aligned}|\phi_1\rangle_{\mathrm{MAB}} =&\frac{1}{2}[|\varPhi^+\rangle_{\mathrm{MA}}(a|0\rangle+b|1\rangle)_{\mathrm{B}}\\&+|\varPsi^+\rangle_{\mathrm{MA}}(a|1\rangle+b|0\rangle)_{\mathrm{B}}\\&+|\varPhi^-\rangle_{\mathrm{MA}}(a|0\rangle-b|1\rangle)_{\mathrm{B}}\\&+|\varPsi^-\rangle_{\mathrm{MA}}(a|1\rangle-b|0\rangle)_{\mathrm{B}}], \qquad (6)\end{aligned}$$

$$\begin{aligned}|\phi_2\rangle_{\mathrm{MAB}} =&\frac{1}{2}[|\varPhi^+\rangle_{\mathrm{MA}}(a|1\rangle+b|0\rangle)_{\mathrm{B}}\\&+|\varPsi^+\rangle_{\mathrm{MA}}(a|0\rangle+b|1\rangle)_{\mathrm{B}}\\&+|\varPhi^-\rangle_{\mathrm{MA}}(a|1\rangle-b|0\rangle)_{\mathrm{B}}\\&+|\varPsi^-\rangle_{\mathrm{MA}}(a|0\rangle-b|1\rangle)_{\mathrm{B}}]. \qquad (7)\end{aligned}$$

Here $|\varPhi^\pm\rangle_{\mathrm{MA}} = \frac{1}{\sqrt{2}}(|00\rangle \pm |11\rangle)_{\mathrm{MA}}, |\varPsi^\pm\rangle_{\mathrm{MA}} = \frac{1}{\sqrt{2}}(|01\rangle \pm |10\rangle)_{\mathrm{MA}}$. Now Alice performs a Bell state measurement on her two particles M and A and sends the result to Bob through a classical communication channel. Depending on both Charlie and Alice's eight possible measurement outcomes $|0\rangle_{\mathrm{C}}|\varPhi^+\rangle_{\mathrm{MA}}$, $|0\rangle_{\mathrm{C}}|\varPsi^+\rangle_{\mathrm{MA}}$, $|0\rangle_{\mathrm{C}}|\varPhi^-\rangle_{\mathrm{MA}}$, $|0\rangle_{\mathrm{C}}|\varPsi^-\rangle_{\mathrm{MA}}$, $|1\rangle_{\mathrm{C}}|\varPhi^+\rangle_{\mathrm{MA}}$, $|1\rangle_{\mathrm{C}}|\varPsi^+\rangle_{\mathrm{MA}}$, $|1\rangle_{\mathrm{C}}|\varPhi^-\rangle_{\mathrm{MA}}$ and $|1\rangle_{\mathrm{C}}|\varPsi^-\rangle_{\mathrm{MA}}$, Bob applies the corresponding unitary operators I, X, Z, ZX, X, I, ZX and Z, respectively, on his particle in order to recover the initial state $|\psi\rangle_{\mathrm{B}} = a|0\rangle_{\mathrm{B}} + b|1\rangle_{\mathrm{B}}$. Here $I = |0\rangle\langle 0| + |1\rangle\langle 1|$, $X = |0\rangle\langle 1| + |1\rangle\langle 0|$, $Z = |0\rangle\langle 0| - |1\rangle\langle 1|$. So an initial state $|\psi\rangle_{\mathrm{M}}$ is faithfully transmitted to Bob's particle via the quantum channel.

The feature of this scheme is that teleportation between two sides depends on the agreement of the third side. It is therefore another kind of "controlled quantum teleportation" different from that in Ref.[38].

3. Controlled and secure direct communication

Next we present a controlled and secure direct communication scheme (different from that in Ref.[24]) by the above controlled teleportation. The special feature of this scheme is that the communication between two sides depends on the agreement of the third side.

Consider the following scenario. Suppose that the administrative personnel of the server, Charlie, wishes to control the correspondence between users. This means that if and only if Charlie gives his permission, Alice and Bob can correspond with each other. However, the users want their communication to be secret to Charlie and not altered during transmission. What can they do? Our following scheme will suit this task. In our scheme, there are three parties: the controller Charlie and the users Alice and Bob. How does this new scheme work?

3.1. Preparing quantum channel

Suppose that Alice, Bob and Charlie share a set of triplets of qubits in an entangled state $|\xi\rangle_{\mathrm{ABC}}$ which function as quantum channel. Obtaining these triplets in an entangled state could have come about in many different ways; for example, Charlie prepares a sequence of three-particles in an entangled state $|\xi\rangle_{\mathrm{ABC}}$ and then sends particles A to Alice and particles B to Bob, and keeps the corresponding particles C. Alternatively, a fourth party could prepare an ensemble of particles in $|\xi\rangle_{\mathrm{ABC}}$, and ask Alice, Bob and Charlie each to take a particle (A, B, C, respectively) in each triplet. Or they could have met long time ago and shared them, storing them until the present. Alice, Bob and Charlie then choose randomly a subset of qubits in an entangled state $|\xi\rangle_{\mathrm{ABC}}$, and do some appropriate tests of fidelity. For example, they can test whether $|\xi\rangle_{\mathrm{ABC}}$ is the simultaneous eigenstate of the operators $\sigma_x \otimes \sigma_x \otimes I$, $\sigma_x \otimes I \otimes \sigma_x$, $I \otimes \sigma_x \otimes \sigma_x$ and $\sigma_z \otimes \sigma_z \otimes \sigma_z$ with the eigenvalue 1. Passing the test certifies that they continue to hold sufficiently pure, entangled quantum states (i.e. the quantum channel is perfect). However, if tampering has occurred, Alice, Bob and Charlie discard these triplets, and a new sequence of qubits in $|\xi\rangle_{\mathrm{ABC}}$ should be reproduced.

3.2. Secure direct communication using the above controlled teleportation

After ensuring the security of the quantum channel, they begin controlled and secure direct communication.

First Alice makes his particle sequence in the states, composed of $|+\rangle$ and $|-\rangle$, according to the message sequence. For example if the message to be transmitted is 101001, then the sequence of particle states should be in the state $|+\rangle|-\rangle|+\rangle|-\rangle|-\rangle|+\rangle$, i.e. $|+\rangle$ and $|-\rangle$ correspond to 1 and 0, respectively. Here

$$\begin{aligned}|+\rangle &= \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle),\\|-\rangle &= \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle). \qquad (8)\end{aligned}$$

The signal state carrying secret message that Alice wants to teleport is represented as

$$|\varphi\rangle_{\mathrm{M}} = \frac{1}{\sqrt{2}}(|0\rangle + b|1\rangle)_{\mathrm{M}}, \qquad (9)$$

where $b = 1$ and $b = -1$ correspond to $|+\rangle$ and $|-\rangle$, respectively. The quantum state of the whole system (the four qubits) reads

$$|\varphi\rangle_{\rm M}|\xi\rangle_{\rm ABC} = \frac{1}{\sqrt{2}}(|0\rangle + b|1\rangle)_{\rm M} \otimes \frac{1}{2}(|000\rangle + |110\rangle + |011\rangle + |101\rangle)_{\rm ABC}. \quad (10)$$

If Charlie allows the communications between the two users, he performs measurements on his qubit C and classically (and publicly) broadcasts the measurement outcome (on which basis state of $\{|0\rangle_{\rm C}, |1\rangle_{\rm C}\}$ he obtained by projection) to the users Alice and Bob. After that, Alice makes a Bell state measurement on her particles M and A and informs Bob of the result of measurement also publicly over a classical channel. Once Bob has learned the broadcast results of Charlie and Alice, Bob can 'fix up' his state, recovering the signal state $|\varphi\rangle_{\rm B} = \frac{1}{\sqrt{2}}(|0\rangle + b|1\rangle)_{\rm B}$, by applying appropriate quantum gate. Then Bob measures the basis $\{|+\rangle, |-\rangle\}$ and reads out the messages that Alice wants to transmit to him.

It is undeniable that this process of controlled quantum teleportation has similar notable features of the original quantum teleportation[23] which was mentioned in Refs.[22, 24]. For instance, the process is entirely unaffected by any noise in the spatial environment between each other, and the controlled teleportation achieves perfect transmission of delicate information across a noisy environment and without even knowing the locations of each other. In the process Bob is left with a perfect instance of $|\varphi\rangle$ and hence no participants can gain any further information about its identity. So in our scheme controlled quantum teleportation transmits Alice's message without revealing any information to a potential eavesdropper, if the quantum channel is in the perfect state in Eq.(2) (perfect quantum channel).

The security of this protocol only depends on the perfect quantum channel (pure state in Eq.(2)). Thus as long as the quantum channel is perfect, our scheme is absolutely reliable, deterministic and secure.

4. Summary

In summary, we present a controlled quantum teleportation protocol. In the protocol, quantum information of an unknown state of a 2-level particle is faithfully transmitted from a sender Alice to a remote receiver Bob via an initially shared triplet in an entangled state under the control of the supervisor Charlie. The distributed entangled particles shared by Alice, Bob and Charlie function as a quantum information channel for faithful transmission. We also propose a controlled and secure direct communication scheme by means of this controlled teleportation. After ensuring the security of the quantum channel, Alice encodes the secret messages directly on a sequence of particle states and transmits them to Bob by teleportation supervised by Charlie. Evidently the controlled teleportation transmits Alice's messages without revealing any information to a potential eavesdropper. Bob can read out the encoded messages directly by the measurement on his qubits. Because there is not a transmission of the qubit which carries the secret message between Alice and Bob, it is completely secure for controlled and direct secret communication if perfect quantum channel is used. The special feature of this scheme is that the communication between two sides depends on the agreement of the third side.

Teleportation has been realized in experiments,[40−42] therefore we hope that our protocols for controlled quantum teleportation and secure direct communication will be realized by experiment in the near future.

References

[1] Bennett C H and Brassard G 1984 *Proc. IEEE Int. Conf. on Computers, Systems and Signal Processing* (New York: IEEE Press) p175
[2] Ekert A K 1991 *Phys. Rev. Lett.* **67** 661
[3] Bennett C H, Brassard G and Mermin N D 1992 *Phys. Rev. Lett.* **68** 557
[4] Bennett C H 1992 *Phys. Rev. Lett.* **68** 3121
[5] Bennett C H and Wiesner S J 1992 *Phys. Rev. Lett.* **69** 2881
[6] Goldenberg L and Vaidman L 1995 *Phys. Rev. Lett.* **75** 1239
[7] Huttner B, Imoto N, Gisin N and Mor T 1995 *Phys. Rev.* A **51** 1863
[8] Koashi M and Imoto N 1997 *Phys. Rev. Lett.* **79** 2383
[9] Bruß D 1998 *Phys. Rev. Lett.* **81** 3018
[10] Hwang W Y, Koh I G and Han Y D 1998 *Phys. Lett.* A **244** 489
[11] Cabello A 2000 *Phys. Rev. Lett.* **85** 5635
[12] Cabello A 2000 *Phys. Rev.* A **61** 052312
[13] Long G L and Liu X S 2002 *Phys. Rev.* A **65** 032302
[14] Xue P, Li C F and Guo G C 2002 *Phys. Rev.* A **65** 022317

[15] Phoenix S J D, Barnett S M, Townsend P D and Blow K J 1995 *J. Modern Optics* **42** 1155

[16] Lo H K, Chan H F and Ardehali M 2000 quant-ph/0011056

[17] Yang L, Wu L A and Liu S H 2002 *Acta Phys. Sin.* **51** 1163 (in Chinese)

[18] Beige A *et al* 2002 *Acta Phys. Pol.* A **101** 357

[19] Boström K and Felbinger T 2002 *Phys. Rev. Lett.* **89** 187902

[20] Wójcik A 2003 *Phys. Rev. Lett.* **90** 157901

[21] Deng F G, Long G L and Liu X S 2003 *Phys. Rev.* A **68** 042317

[22] Yan F L and Zhang X Q 2004 *Eur. Phys. J.* B **41** 75

[23] Bennett C H *et al* 1993 *Phys. Rev. Lett.* **70** 1895

[24] Gao T 2004 *Z. Naturforsch.* **59a** 597

[25] Murao M, Plenio M B and Vedral V 2000 *Phys. Rev.* A **61** 032311

[26] Ikram M, Zhu S Y and Zubairy M S 2000 *Phys. Rev.* A **62** 022307

[27] Li W L, Li C F and Guo G C 2000 *Phys. Rev.* A **61** 034301

[28] Gorbachev V N and Trubilko A I 2000 *J. Exp. Theor. Phys.* **91** 894

[29] Lu H and Guo G C 2000 *Phys. Lett.* A **276** 209

[30] Zeng B, Liu X S, Li Y S and Long G L 2002 *Commun. Theor. Phys.* **38** 537

[31] Shi B S *et al* 2000 *Phys. Lett.* A **268** 161

[32] Yan F L, Tan H G and Yang L G 2002 *Commun. Theor. Phys.* **37** 649

[33] Yan F L and Bai Y K 2003 *Commun. Theor. Phys.* **40** 273

[34] Yan F L and Wang D 2003 *Phys. Lett.* A **316** 297

[35] Gao T, Wang Z X and Yan F L 2003 *Chin. Phys. Lett.* **20** 2094

[36] Gao T, Yan F L and Wang Z X 2004 *Quantum Information and Computation* **4** 186

[37] Gao T 2004 *Commun. Theor. Phys.* **42** 223

[38] Zhou J D, Hou G, Wu S J and Zhang Y D 2000 quant-ph/0006030

[39] Cai X H 2003 *Chin. Phys.* **12** 1066

[40] Bouwmeester D *et al* 1997 *Nature* **390** 575

[41] Boschi D *et al* 1998 *Phys. Rev. Lett.* **80** 1121

[42] Nielsen M A *et al* 1998 *Nature* **396** 52