Vol 14 No 11, November 2005
1009-1963/2005/14(11)/2149-04

Chinese Physics

© 2005 Chin. Phys. Soc.
and IOP Publishing Ltd

Multi-agent controlled teleportation of multi-qubit quantum information via two-step protocol*

Yang Jie(杨 杰)†

School of Physics & Material Science, Anhui University, Hefei 230039, China

(Received 21 December 2004; revised manuscript received 3 June 2005)

Utilizing both the general quantum teleportation and the two-step protocol, a new method is presented by which multi-qubit quantum information can be teleported in a much easier way from a sender Alice to a receiver Bob via the control of many agents in a network than by Yang *et al*'s method. In this method, only all the agents collaborate with Bob can the unknown states in Alice's qubits be fully reconstructed in Bob's qubits. Comparisons between the method and *Yang et al*'s method are made. Results show that, in this method, the preparation difficulty of initial states and the identification difficulty of entangled states are considerably reduced, new method is more feasible in technique, and Hadamard operations are not needed at all.

Keywords: quantum teleportation, two-step protocol, quantum information
PACC: 0155, 0365B

The combination of quantum mechanics with information has produced many interesting and important developments in quantum secret communication[1−14] and quantum computing. Since no-cloning theorem forbids a copy of an arbitrary unknown state, how to interchange different resources has ever been a question in quantum computation and quantum information. Bennett *et al*'s pioneering work[15] on teleporting an unknown quantum state of a qubit from one party (Alice) to another (Bob) with the aid of long-range Einstein–Podolsky–Rosen (EPR) correlations, showed in essence the interchangeability of different resources in quantum mechanics. Since then, scientists have made dramatic progress in the field of quantum teleportation.[16−20,21−29] Since controlled teleportation is useful in networked quantum information processing and cryptographic conferences, how to implement it is a particularly interesting topic. Very recently Yang *et al*[30] have proposed a method to teleport multi-qubit quantum information to a remote place via the control of many agents. The quantum information are some unknown quantum states in the sender Alice's qubits. The many-agent control means that, only all the agents collaborate with the quantum information, receiver Bob can reconstruct the original states in his qubits, otherwise, even if one agent does not cooperate, the original states can not be fully recovered by Bob. In their work,[30] the basic purpose is to let each agent have a control parameter on Bob's reconstructions. To achieve this, they have designed a scheme, where (i) intricate initial states (see Eqs.(2), (21) and (29) in Ref.[30]) have to be prepared in advance; (ii) Alice has to perform Bell-state (GHZ state) measurements and publish the outcomes; (iii) Alice and each agent have to perform Hadamard operations; and (iv) classical communications between Alice and Bob and between each agent and Bob are necessary. Compared with the methods in Ref.[16] and Ref.[17], as Yang *et al* claimed,[30] their method is apparently simpler and economical, because the required auxiliary qubit resources, the number of local operations, and the quantity of classical communication are greatly reduced. However, as the accomplishment of the task (i.e., many-agent controlled teleportation of multi-qubit quantum information) is concerned, we think, Yang *et al*'s method is also very complicated: i.e., the task is completed in a complicated way. In this paper, we will present a new method to complete the same task in a much easier way. Alternatively, we will realize many-agent controlled tele-

*Project supported by the National Natural Science Foundation of China (Grant No 10304022).
†E-mail: yangjies@sina.com.cn

portation of multi-qubit quantum information by employing general quantum teleportation which use EPR pairs and a quantum secure direct communication protocol named the two-step protocol.[31]

Let us begin with a brief review of quantum teleportation by using an EPR pair.[15] Define the four Bell states as $|\psi^+\rangle = \frac{1}{\sqrt{2}}(|0\rangle|1\rangle + |1\rangle|0\rangle)$, $|\psi^-\rangle = \frac{1}{\sqrt{2}}(|0\rangle|1\rangle - |1\rangle|0\rangle)$, $|\phi^+\rangle = \frac{1}{\sqrt{2}}(|0\rangle|0\rangle + |1\rangle|1\rangle)$ and $|\phi^-\rangle = \frac{1}{\sqrt{2}}(|0\rangle|0\rangle - |1\rangle|1\rangle)$ respectively. An EPR pair can be in one of the four Bell states. Suppose Alice wants to send an unknown quantum state $|u\rangle_1 = \alpha_1|0\rangle_1 + \beta_1|1\rangle_1$ in her photon 1 to Bob. She prepares a photon pair in the Bell state, say, $|\psi^-\rangle_{23} = (|0\rangle_2|1\rangle_3 - |1\rangle_2|0\rangle_3)/\sqrt{2}$, and sends the photon 3 to Bob. The complete state of the three photons is $|F\rangle_{123} = |u\rangle_1|\psi^-\rangle_{23}$. It can be rewritten in terms of the Bell states of both photon 1 and photon 2 as follows

$$\begin{aligned}|F\rangle_{123} =& \frac{1}{2}[|\psi^-\rangle_{12}(-\alpha|0\rangle_3 - \beta|1\rangle_3) \\ &+ |\psi^+\rangle_{12}(-\alpha|0\rangle_3 + \beta|1\rangle_3) \\ &+ |\phi^-\rangle_{12}(\alpha|1\rangle_3 + \beta|0\rangle_3) \\ &+ |\phi^+\rangle_{12}(\alpha|1\rangle_3 - \beta|0\rangle_3)].\end{aligned}$$

If Alice performs a Bell-state measurement on the two photons 1 and 2 in her laboratory and tells Bob her measurement outcome, say, $|\psi^-\rangle$ ($|\psi^+\rangle, |\phi^-\rangle, |\phi^+\rangle$), then Bob can perform a corresponding unitary operation $U_1 = |0\rangle\langle 0| + |1\rangle\langle 1|$ ($U_2 = |0\rangle\langle 0| - |1\rangle\langle 1|, U_3 = |1\rangle\langle 0| + |0\rangle\langle 1|, U_4 = |0\rangle\langle 1| - |1\rangle\langle 0|$) to reconstruct the original quantum state in photon 3. Similarly, if multi-qubit quantum information are needed to teleport, it can be accomplished via the above procedure repeatedly.

From the above brief review of quantum teleportation, one can see that Alice's notices of her Bell-state measurement outcomes to Bob are necessary and they are in essence control parameters on Bob's correct reconstructions. Hence, if Alice is able to transform her control parameters into agents' control parameters, then only all the agents collaborate with Bob can Bob reconstruct the unknown state in his photon 3. As mentioned previously, Yang *et al*[30] have designed a complicated scheme to achieve this goal. In this paper we will utilize a quantum secure direct communication protocol named two-step protocol proposed by Deng *et al*[31] to transform the so-called Alice's control parameters to each agent's control parameter. Incidentally, the two-step protocol can securely transmit secret messages from one legitimate user to another and its security has been proven. Note that within the framework of the two-step protocol even classical secret bits are transmitted in each run because the dense coding has been introduced.

Suppose in Alice's m photons there are m-qubit quantum information $\{|u\rangle_i = \alpha_i|0\rangle_i + \beta_i|1\rangle_i, (i = 1, \ldots, m)\}$. Alice wants to send this m-qubit quantum information to Bob via the control of n agents such that Bob can fully get the quantum information if and only if all the agents cooperate with him. This can be done by the following procedure.

(1) Alice prepares m ordered EPR pairs, each in the state $|\psi^-\rangle_{i'i''}$ $(i = 1, \ldots, m)$. Then she takes one particle from each EPR pair to form an ordered particle sequence called B-sequence, say, $\{1'', 2'', \ldots, m''\}$, the remaining particles compose another ordered sequence called A-sequence, i.e., $\{1', 2', \ldots, m'\}$. She sends the B-sequence to Bob and stores the A-sequence in her laboratory.

(2) After knowing Bob's confirmation of receiving the B-sequence, Alice performs Bell-state measurement on each pair of $\{i, i'\}$ and records the measurement outcome.

(3) To let each agent have a control parameter, this step is classified into three cases.

(3a) Since the two-step protocol can securely transmit secret messages from one legitimate user to another, it is obvious that if there is only one agent, Alice can take advantage of the two-step protocol to inform the agent her control parameters. If so, then the purpose of one-agent control can be easily achieved by directly using the two-step protocol.

(3b) However, when the number n of the agents is more than one, the case is different. When $1 < n \leq m$, then Alice can split the messages of her measurement outcomes into n pieces and informs each agent a piece via the two-step protocol.

(3c) When $n > m$, the m messages of Alice's Bell-state measurement outcomes can not be split into n pieces, then the method in (3b) is invalid. In the following we will present a general method to solve this problem. Of course, as a quantum secure direct communication protocol, it is obvious that the two-step protocol can be used to distribute secret key between two legitimate users. Hence, Alice and each agent can securely share a secret key by using the two-step protocol. After sharing, Alice uniformly encrypts the messages of her Bell-state measurement outcomes via a

shared secret key between Alice and an agent. This encryption procedure is repeated until each of the shared keys between Alice and each agent is used one time. After the encryptions, Alice publishes the encrypted messages. Although Bob gets the encrypted messages, he cannot extract the correct messages without all the agents' collaborations. Hence the purpose to let each agent have a control parameter is achieved. In particular, this method is always valid for any large n agents.

(4) Only all the agents collaborate with Bob can Bob obtain Alice's exact initial messages of her Bell-state measurement outcomes and accordingly he can reconstruct the unknown states by performing correct unitary operation on each of his photons $\{1'', 2'', \ldots, m''\}$.

So far we have shown a new method which can realize n-agent controlled teleportation of m qubits by utilizing the general quantum teleportation and the two-step quantum communication protocol.

Let us analyse simply the security of the present method. Bob is the receiver of all the quantum information. Alice only wants to let him get these quantum information under the n agents' control. Therefore, the possible attack originates only from Bob if Bob wants to throw off all agents' control. In this case, the strategy Bob can adopt is to steal each agent's control parameter via eavesdropping attacks. Since the two-step protocol has been proven to be secure, when Alice transforms her measurement outcomes or her encryption key into each agent's control parameter, Bob's any eavesdropping attack will be detected in the framework of the two-step protocol. Hence the acquirement of the control parameter for each agent can be securely realized according to the present method.

It is necessary for us to compare our present method with the recent method.[30] From the description above, one can see that (a) Bell states are sufficient for use in the present method, however, in Yang *et al*'s method,[30] the complicated initial entangled states are needed to be prepared (see Eqs.(2), (21) and (29) in Ref.[30]), hence, the present method greatly reduces the preparation difficulty of initial states; (b) in our method only the Bell states are needed to be identified by Alice whenever how many agents are, however, according to Yang *et al*'s method the identification of multi-particle GHZ states should be completed by Alice when the number of agents is not less than 2, it is obvious in the present method the difficulty of Alice's identification on her entangled states is reduced; (c) to our knowledge, so far preparation of five-photon entangled states has been achieved in experiment,[32] however, preparation more-photon entanglement is still desired, alternatively, when the number n of the agents is large, it is impossible to prepare n-photon GHZ states according to the present-day technologies, hence, in the case that n is large, Yang *et al*'s method is impossible in reality, in contrast, according to the present method, for any large number of the agents, the efficient controls of all agents can be realized, this is because Bell states are sufficient for use in the present method, hence the present method is more feasible in technique; (d) local operations (i.e., the Hadamard operations in Ref.[30]) on Alice's qubit and on the agents' qubits are not needed in the present method at all.

To summarize, in this paper, a new method of teleporting multi-qubit quantum information from one place to another via the control of many agents in a network is proposed. Compared with Yang *et al*'s method, it works in a much easier way. Our method has several advantages: it greatly reduces the preparation difficulty of initial states and Alice's identification difficulty on her entangled states; for any large n agents it works and it is more feasible in reality; it does not need Hadamard operations.

Acknowledgement

I am very grateful to Professor Zhang Zhanjun for his instructive discussions and helps.

References

[1] Ekert A K 1991 *Phys. Rev. Lett.* **67** 661

[2] Bennett C H, Brassard G and Mermin N D 1992 *Phys. Rev. Lett.* **68** 557

[3] Goldenberg L and Vaidman L 1995 *Phys. Rev. Lett.* **75** 1239

[4] Xue P, Li C F and Guo G C 2002 *Phys. Rev.* A **65** 022317

[5] Deng F G and Long G L 2004 *Phys. Rev.* A **69** 052319

[6] Pasquinucci H Bechmann and Gisin N 1999 *Phys. Rev.* A **59** 4238

[7] Cabello A 2001 *Phys. Rev.* A **61** 052312
Cabello A 2000 *Phys. Rev.* A **64** 024301

[8] Guo G P, Li C F, Shi B S *et al* 2001 *Phys. Rev.* A **64** 042301

[9] Bostrom Kim and Felbinger Timo 2002 *Phys. Rev. Lett.* **89** 187902

[10] Zhang Z J, Man Z X and Li Y 2004 *Int. J. Quantum Information* **2** 521
[11] Zhang Z J, Man Z X and Li Y 2004 *Phys. Lett.* A **333** 46
[12] Long G L and Liu X S 2002 *Phys. Rev.* A **65** 032302
[13] Man Z X, Zhang Z J and Li Y 2005 *Chin. Phys. Lett.* **22** 18
[14] Man Z X, Zhang Z J and Li Y 2005 *Chin. Phys. Lett.* **22** 22
[15] Bennett C H, Brassard G, Crepeau C, Jozsa R, Peres A and Wotters W K 1993 *Phys. Rev. Lett.* **70** 1895
[16] Karlsson A and Bourennane M 1998 *Phys. Rev.* A **58** 4394
[17] Hillery M, Buzk V and Berthiaume A 1999 *Phys. Rev.* A **59** 1829
[18] Cleve R, Gottesman D and Lo H K 1999 *Phys. Rev. Lett.* **83** 648
[19] Li Y M, Zhang K S and Peng K C 2004 *Phys. Lett.* A **324** 420
[20] Zhang Z J and Man Z X 2005 *Phys. Rev.* A **72** 022303
[21] Zhang Z J, Li Y and Man Z X 2005 *Phys. Rev.* A **71** 044301
[22] Zhang Z J and Man Z X 2005 *Chin Phys. Lett.* **22** 1588
[23] Li Y, Zhang T C, Zhang J X and Xie C D 2003 *Chin Phys.* **12** 861
[24] Liu J M, Zhang Y S and Guo G C 2003 *Chin Phys.* **12** 251
[25] Dai H Y, Li C Z and Cheng P X 2003 *Chin Phys.* **12** 1354
[26] Zhan Y B 2003 *Chin Phys.* **13** 1801
[27] Zhang Z J and Man Z X 2005 *Phys. Lett.* A **341** 55
[28] Zhang Z J 2005 *Phys. Lett.* A **342** 60
[29] Zhang Z J, Li Y and Man Z X 2005 *Phys. Lett.* A **341** 385
[30] Yang C P, Chu S I and Han S 2004 *Phys. Rev.* A **70** 022329
[31] Deng F G, Long G L and Liu X S 2003 *Phys. Rev.* A **68** 042317
[32] Zhao Z, Chen Y A, Zhang A N, Yang T, Briegel H J and Pan J W 2004 *Nature* (London) **430** 54