Many-Agent Controlled Teleportation of Multi-qubit Quantum Information via Quantum Entanglement Swapping

2005 Commun. Theor. Phys. 44 847

(http://iopscience.iop.org/0253-6102/44/5/847)

Commun. Theor. Phys. (Beijing, China) **44** (2005) pp. 847–850
© International Academic Publishers Vol. 44, No. 5, November 15, 2005

Many-Agent Controlled Teleportation of Multi-qubit Quantum Information via Quantum Entanglement Swapping*

ZHANG Zhan-Jun,[1,3,†] LIU Yi-Min,[2] and MAN Zhong-Xiao[3]

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

[2]Department of Physics, Shaoguan University, Shaoguan 512005, China

[3]Wuhan Institute of Physics and Mathematics, the Chinese Academy of Sciences, Wuhan 430071, China

(Received March 9, 2005; Revised April 26, 2005)

Abstract *We present a method to teleport multi-qubit quantum information in an easy way from a sender to a receiver via the control of many agents in a network. Only when all the agents collaborate with the quantum information receiver can the unknown states in the sender's qubits be fully reconstructed in the receiver's qubits. In our method, agents's control parameters are obtained via quantum entanglement swapping. As the realization of the many-agent controlled teleportation is concerned, compared to the recent method [C.P. Yang, et al., Phys. Rev. A* **70** *(2004) 022329], our present method considerably reduces the preparation difficulty of initial states and the identification difficulty of entangled states, moreover, it does not need local Hadamard operations and it is more feasible in technology.*

PACS numbers: 03.67.Lx, 03.65.-w, 42.50.Dv
Key words: quantum teleportation, quantum information, quantum entanglement swapping

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. In 1993, Bennett *et al.*[1] first proposed a method teleporting an arbitrary unknown quantum state in a qubit to a distant qubit with the aid of Einstein–Podolsky–Rosen (EPR) pair. Their work showed in essence the interchangeability of different resources in quantum mechanics. In 1998 Karlsson and Bourennane[2] generalized the teleportation idea of Bennett *et al.* by using a three-qubit Greenberger–Horne–Zeilinger (GHZ) state $|000\rangle + |111\rangle$ instead of an EPR pair. In thier work, only when conditioned on one receiver's measurement outcome can the arbitrary quantum state in the sender's qubit be successfully teleported to the other receiver's qubit. In 1999, Hillery, Buzek, and Berthiaume[3] first introduced a protocol of quantum secret sharing, which is a quantum version of classical sharing schemes.[4] In their work, they showed how a qubit of quantum information can be securely shared by two (three) agents via three-particle (four-particle) GHZ states. Later, a number of works on quantum secret sharing were also presented.[5−11] Since controlled teleportation is useful in networked quantum information processing and cryptographic conferences, how to implement it is a particular interesting topic.[10−13] Very recently, Yang *et al.*[11] have presented their extensive study on teleporting multi-qubit information from a sender to a distant receiver via the control of many agents in a network. In their work, they first briefly reviewed how to finish the task (i.e., let each agent have a control parameter and only when all the agents collaborate with the receiver Bob can Bob successfully reconstruct the unknown states in his qubits) by using the methods presented in Refs. [2] and [3] and then proposed their preponderant method. In their method, 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 intricate initial states (c.f., Eqs. (2), (21), and (29) in Ref. [12]) have to be prepared in advance, the sender Alice must perform Bell-state (GHZ state) measurements and publish the outcomes, Alice and each agent have to perform Hadamard operations, and classical communications between Alice and Bob and between each agent and Bob are necessary. Compared to the methods in Refs. [2] and [3], as Yang *et al.* claimed,[12] 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 is concerned, we think, the methods in Refs. [2], [3], and [12] are all very complicated, i.e., the task is completed in a complicated way. In this paper, by using quantum entanglement swapping we will present a method to deal with this issue in a much easier way.

Let us begin with a brief review of the general quantum teleportation using an EPR pair.[1] Define the four

*The project supported by National Natural Science Foundation of China under Grant No. 10304022
†Corresponding author, E-mail: zjzhang@ahu.edu.cn

Bell states as

$$|\psi^+\rangle=\frac{1}{\sqrt{2}}(|0\rangle|1\rangle+|1\rangle|0\rangle)\,,\quad |\psi^-\rangle=\frac{1}{\sqrt{2}}(|0\rangle|1\rangle-|1\rangle|0\rangle)\,,$$

$$|\phi^+\rangle=\frac{1}{\sqrt{2}}(|0\rangle|0\rangle+|1\rangle|1\rangle)\,,\quad |\phi^-\rangle=\frac{1}{\sqrt{2}}(|0\rangle|0\rangle-|1\rangle|1\rangle)\,,$$

respectively. An EPR pair can be in one of the four Bell states. Furthermore, we define $|\psi^+\rangle$, $|\psi^-\rangle$, $|\phi^+\rangle$ and $|\phi^-\rangle$ corresponding to two classical bits "00", "01", "10", and "11", respectively. 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 total state of the three photons 1, 2 and 3 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

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

If Alice performs a Bell-state measurement on the two photons 1 and 2 in her lab and tells Bob her measurement outcome, say, $|\psi^-\rangle$ ($|\psi^+\rangle, |\phi^-, |\phi^+\rangle$), i.e., "00" ("01", "10", "11"), 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 needs to be teleported, it can be accomplished via the above procedure repeatedly.

Form the above brief review of the general 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's control parameters, then only when all the agents collaborate with Bob can Bob reconstruct the unknown state in his photon 3. As mentioned previously, Yang *et al.*[10] have designed a complicated scheme to achieve this goal. In fact, such a task to let each agent own a control parameter can be achieved in a much easier way. Our method is to let Alice uniformly encrypt the message of her Bell-state measurement outcomes before she publishes the encrypted message and then let each agent have a control parameter from Alice's uniform encryption via quantum entanglement swapping.

Suppose in Alice's m photons there is 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.

(i) Alice prepares m ordered EPR pairs, each in the state $|\psi^-\rangle_{i'i''}$ ($i=1,2,\ldots,m$). Then she takes one particle from each EPR pair to form an ordered particle sequence called B-sequence, say, $\{1'',2'',3'',\ldots,m''\}$, and the remaining particles compose another ordered sequence called A-sequence, i.e., $\{1',2',3',\ldots,m'\}$. She sends the B-sequence to Bob and stores the A-sequence in her lab.

(ii) After knowing Bob's confirmation of receiving the B-sequence, Alice performs Bell-state measurement on each pair $\{i,i'\}$ and records the measurement outcome. Without loss of generality, we suppose that she obtains $\{\psi^+_{11'},\phi^-_{22'},\phi^+_{33'},\ldots,\psi^-_{mm'}\}$ corresponding to classical bits $\{(10)_{11'},(01)_{22'},(00)_{33'},\ldots,(11)_{mm'}\}$.

By the way, if Alice publicly announces her measurement outcomes, then Bob can fully reconstruct all the unknown states in his qubits by performing correct unitary operations, that is, Bob can in turn perform unitary operations U_3, U_2, U_1, $\ldots$, U_4 on his photons $1''$, $2''$, $3''$,..., m'' to reconstruct the unknown states $|u\rangle_1,|u\rangle_2,|u\rangle_3,\ldots,|u\rangle_m$.

(iii) Alice uniformly encrypts the message of these outcomes by using a secret key, say, 01. Then according to the Table 1 she publicly announces $\{(11)_{11'}$, $(00)_{22'},(01)_{33'},\ldots,(10)_{mm'}\}$.

Table 1 Relation among Alice's different measurement outcomes, her different encryption bits (EB) and her corresponding public announcements after her encryptions. Different measurement outcomes are listed in the first line. Different EBs are listed in first column.

	$\phi^+(00)$	$\phi^-(01)$	$\psi^+(10)$	$\psi^-(11)$
00	00	01	10	11
01	01	00	11	10
10	10	11	00	01
11	11	10	01	00

(iv) Alice and n agents (Charlie, Dick, Ellen, ..., Zeck) each prepare a photon pair in one Bell state, say, ϕ^+.

(v) From her photon pair (a_1,a_2) in the Bell state ϕ^+, Alice selects one photon, say a_2, and sends it to the first agent Charlie. Similarly, Charlie sends his second photon c_2 to the second agent Dick, and so on. The n-th agent Zeck sends his second photon z_2 to Alice.

(vi) After all the transmissions, Alice performs unitary operation u_2 (u_1,u_2,u_3) corresponding to her secret key 01 (00, 10, 11) on her photon a_1. Then she performs a Bell-state measurement on the photons a_1 and z_2 in her lab and publicly announces her measurement outcome.

(vii) After knowing Alice's announcement, Charlie, Dick, . . ., Zeck perform in turn on the two photons in their respective lab. Note that the ordering is very important.

Incidentally, the steps (iv)–(vii) ensure each agent to have a control parameter from Alice's secret key 01 via quantum entanglement swapping. They form in essence a quantum secret sharing of classical messages.

(viii) If All the agents collaborate with each other, then they can extract Alice's encryption bits (i.e., the secret key) 01 in a recursive way according to Table 2.

(ix) If all agents collaborate with Bob further, then Bob can obtain the secret key from all the agents. Further, he can extract Alice's exact initial Bell-state measurement outcomes from Alice's public announcements and performs correct unitary operations on his photons to reconstruct the unknown states. In contrast, if one agent is not willing to collaborate at very beginning, then Bob cannot fully reconstruct the unknown states.

Table 2 The corresponding relations between the two initial Bell states (TIBSs) and the two possible output Bell states (TPOBSs) after the quantum entanglement swapping.

TIBSs	TPOBSs	TPOBSs	TPOBSs	TPOBSs
$\{\phi^+_{12},\phi^+_{34}\}$ $(\{\phi^-_{12},\phi^-_{34}\},\{\psi^+_{12},\psi^+_{34}\},\{\psi^-_{12},\psi^-_{34}\})$	$\{\phi^+_{13},\phi^+_{24}\}$	$\{\phi^-_{13},\phi^-_{24}\}$	$\{\psi^+_{13},\psi^+_{24}\}$	$\{\psi^-_{13},\psi^-_{24}\}$
$\{\phi^-_{12},\phi^+_{34}\}$ $(\{\phi^+_{12},\phi^-_{34}\},\{\psi^-_{12},\psi^+_{34}\},\{\psi^+_{12},\psi^-_{34}\})$	$\{\phi^+_{13},\phi^-_{24}\}$	$\{\phi^-_{13},\phi^+_{24}\}$	$\{\psi^+_{13},\psi^-_{24}\}$	$\{\psi^-_{13},\psi^+_{24}\}$
$\{\psi^+_{12},\phi^+_{34}\}$ $(\{\psi^-_{12},\phi^-_{34}\},\{\phi^+_{12},\psi^+_{34}\},\{\phi^-_{12},\psi^-_{34}\})$	$\{\phi^+_{13},\psi^+_{24}\}$	$\{\phi^-_{13},\psi^-_{24}\}$	$\{\psi^+_{13},\phi^+_{24}\}$	$\{\psi^-_{13},\phi^-_{24}\}$
$\{\psi^-_{12},\phi^+_{34}\}$ $(\{\psi^+_{12},\phi^-_{34}\},\{\phi^-_{12},\psi^+_{34}\},\{\phi^+_{12},\psi^-_{34}\})$	$\{\phi^+_{13},\psi^-_{24}\}$	$\{\phi^-_{13},\psi^+_{24}\}$	$\{\psi^+_{13},\phi^-_{24}\}$	$\{\psi^-_{13},\phi^+_{24}\}$

So far we have presented our method to realize n-agent controlled teleportation of m-qubit in a network. To well understand our method, let us show a simple example as follows. Suppose there are four agents, i.e. Charlie, Dick, Ellen and Zech. Without loss of generality, one can suppose that Alice's (Charlie's, Dick's) Bell-state measurement outcomes are in turn $\phi^+_{a_1z_2}$, $\phi^-_{c_1a_2}$, and $\psi^+_{d_1c_2}$ respectively and Alice has published her measurement outcome $\phi^+_{a_1z_2}$. In this case, the state of the whole system evolves as

$$\begin{aligned} & u_2\phi^+_{a_1a_2}\phi^+_{c_1c_2}\phi^+_{d_1d_2}\phi^+_{e_1e_2}\phi^+_{z_1z_2} \\ \to\ & \phi^-_{a_1a_2}\phi^+_{c_1c_2}\phi^+_{d_1d_2}\phi^+_{e_1e_2}\phi^+_{z_1z_2} \\ \to\ & \phi^+_{a_1z_2}\phi^+_{c_1c_2}\phi^+_{d_1d_2}\phi^+_{e_1e_2}\phi^-_{z_1a_2} \\ \to\ & \phi^+_{a_1z_2}\phi^-_{c_1a_2}\phi^+_{d_1d_2}\phi^+_{e_1e_2}\phi^+_{z_1c_2} \\ \to\ & \phi^+_{a_1z_2}\phi^-_{c_1a_2}\psi^+_{d_1c_2}\phi^+_{e_1e_2}\psi^+_{z_1d_2}\,. \end{aligned}$$

Since $\phi^+_{e_1e_2}$ and $\psi^+_{z_1d_2}$ are determined after Alice's, Charlie's, and Dick's Bell-state measurements, according to Table 2, Ellen's, and Zeck's Bell-state measurements can produce any one of the four possible outcomes $\{\phi^+_{e_1d_2}$, $\psi^+_{z_1e_2}\}$, $\{\phi^-_{e_1d_2}$, $\psi^-_{z_1e_2}\}$, $\{\psi^+_{e_1d_2}$, $\phi^+_{z_1e_2}\}$, and $\{\psi^-_{e_1d_2}$, $\phi^-_{z_1e_2}\}$, say $\{\psi^+_{e_1d_2}$, $\phi^+_{z_1e_2}\}$, then the final state of the whole system is $\phi^+_{a_1z_2}\phi^-_{c_1a_2}\psi^+_{d_1c_2}\psi^+_{e_1d_2}\phi^+_{z_1e_2}$. Hence, if Charlie, Dick, Ellen, and Zeck collaborate with each other, since they have known the outcome $\phi^+_{a_1z_2}$ of Alice's measurement on the photons a_1 and z_2, then in a recursive way they can deduce Alice's operation, which is also taken as the uniform encryption on Alice's measurement outcomes. This is completely the reverse process of the state evolution.

Let us analyze 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 he wants to throw off all the agents' control. If so, the strategy Bob can adopt is to get each agent's control parameter via eavesdropping attacks. Because for each entangled photon pair only one photon qubit travels in the quantum channel and Bob cannot get access to another photon qubit stored in Alice's or agent's lab at all, as same as those quantum communication scheme using entangled qubits.[14−26] Bob cannot know the secret key at all. Hence the acquirement of control parameter for each agent can be securely realized according to our method.

It is necessary for us to compare our present method with the recent method.[11] From the description above, one can see the following facts. (i) Bell states are sufficient for use in the present method. However, in Yang *et al.*'s method,[12] the complicated initial entangled states are needed to be prepared (cf., Eqs. (2), (21), and (29) in Ref. [12]). Hence, the present method greatly reduces the preparation difficulty of initial states; (ii) In our method only the Bell states are needed to be identified by Alice no matter 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 that in the present method the difficulty of Alice's identification on her entangled states is reduced; (iii) To our knowledge, so far preparation of five-photon entangled states has been achieved in experiment,[27] 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 more demanding. 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; (iv) Local operations (i.e., the Hadamard operations in Ref. [12]) on Alice's qubit and on the agents' qubits are not needed in the present method at all.

To summarize, in this paper, by using quantum entanglement swapping we have proposed a new method of teleporting multi-qubit quantum information from one place to another via the control of many agents in a network. Compared to Yang *et al.*'s recent method,[12] the present method works in a much easier way. Our method owns 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; and it does not need Hadamard operations.

References

[1] C.H. Bennett, G. Brassard, C. Crepeau, R. Jozsa, A. Peres, and W.K. Wotters, Phys. Rev. Lett. **70** (1993) 1895.

[2] A. Karlsson and M. Bourennane, Phys. Rev. A **58** (1998) 4394.

[3] M. Hillery, V. Buzk, and A. Berthiaume, Phys. Rev. A **59** (1999) 1829.

[4] A. Shamir, Commun. ACM **22** (1979) 612.

[5] R. Cleve, D. Gottesman, and H.K. Lo, Phys. Rev. Lett. **83** (1999) 648.

[6] S. Bandyopadhyay, Phys. Rev. A **62** (2000) 012308.

[7] L.Y. Hsu, Phys. Rev. A **68** (2003) 022306.

[8] Y.M. Li, K.S. Zhang, and K.C. Peng, Phys. Lett. A **324** (2004) 420.

[9] A.M. Lance, T. Symul, W.P. Bowen, B.C. Sanders, and P.K. Lam, Phys. Rev. Lett. **92** (2004) 177903.

[10] Z.J. Zhang, Y. Li, and Z.X. Man, Phys. Rev. A **71** (2005) 044301.

[11] Z.J. Zhang, J. Yang, Z.X. Man, and Y. Li, Eur. Phys. J. D **33** (2005) 133.

[12] Chui-Ping Yang, Shi-I Chu, and Si-Yuan Han, Phys. Rev. A **70** (2004) 022329.

[13] T. Gao, Commun. Theor. Phys. (Beijing, China) **42** (2004) 223.

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

[15] G.P. Guo, C.F. Li, B.S. Shi, J. Li, and G.C. Guo, Phys. Rev. A **64** (2001) 042301.

[16] Y.M. Li, K.S. Zhang, and K.C. Peng, Phys. Lett. A **324** (2004) 420.

[17] Z.J. Zhang, Z.X. Man, and Y. Li, Int. J. Quantum Information **2** (2004) 521.

[18] Z.J. Zhang, Z.X. Man, and Y. Li, Phys. Lett. A **333** (2004) 46.

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

[20] Daegene Song, Phys. Rev. A **69** (2004) 034301.

[21] Kim Bostrom and Timo Felbinger, Phys. Rev. Lett. **89** (2002) 187902.

[22] Z.X. Man, Z.J. Zhang, and Y. Li, Chin. Phys. Lett. **22** (2005) 18.

[23] Z.X. Man, Z.J. Zhang, and Y. Li, Chin. Phys. Lett. **22** (2005) 22.

[24] L. Xiao, G.L. Long, F.G. Deng, and J.W. Pan, Phys. Rev. A **69** (2004) 052307.

[25] G.L. Long and X.S. Liu, Phys. Rev. A **65** (2002) 032302.

[26] F.G. Deng and G.L. Long, Phys. Rev. A **68** (2003) 042315.

[27] Z. Zhao, Y.A. Chen, A.N. Zhang, T. Yang, H.J. Briegel, and J.W. Pan, Nature (London) **430** (2004) 54.