Письма в ЭЧАЯ. 2011. Т. 8, № 5(168). С. 767–771

MULTIQUBIT TELEPORTATION ALGORITHM AND TELEPORTATION MANAGER

I. V. Blinova, I. Yu. Popov[1]

St. Petersburg State University of Information Technologies, Mechanics and Optics, St. Petersburg, Russia

A variant of teleportation algorithm is suggested. It is based on using multiqubit states. Particularly, it allows the teleportation manager to create a proper entangled state between A and B and, consequently, to control the result of the teleportation between A and B. The problem of quantum secret sharing is considered in the framework of the suggested approach.

Предложен вариант телепортационного алгоритма. Он основан на использовании многокубитовых состояний. В частности, он позволяет телепортационному менеджеру создавать надлежащее перепутанное состояние между A и B и, следовательно, контролировать результат телепортации между A и B. В рамках предлагаемого подхода рассмотрена квантовая проблема распределения секретного ключа.

PACS: 03.67.Hk; 03.67.Lx

INTRODUCTION

Rapid development of nanoelectronics stimulates the investigation of quantum algorithms. At present, some algorithms are created (e.g., Shor factorization, Grover database search [1], etc.). Teleportation suggested by Bennett and Brassard [2] is one of the most important algorithms. There are some versions of main teleportation scheme: one-bit teleportation, dense coding, entanglement swapping (see, e.g., [3, 4]). For teleportation over three-qubit states, we recall the Hillery–Buzek–Berthiaume [5] protocol, which is the splitting and reconstruction of quantum information over the Greenberger–Horne–Zeilinger (GHZ) state by local quantum operations and classical communication (LOCC). The protocol can be modified into a teleportation protocol over a general three-qubit state in the compound system 123, as presented in [6, 7]. The modified protocol is described as follows: Let i, j, and k be distinct in 1, 2, 3. (i) Make a one-qubit orthogonal measurement on the system i. (ii) Prepare an arbitrary one-qubit state, and then make a two-qubit orthogonal measurement on the one qubit and the system j. (iii) On the system k, apply a proper unitary operation depending on the three-bit classical information of the two above measurement outcomes.

In the present paper we suggest new variants of the teleportation protocol over N-qubit states. Particularly, for $N = 3$, we assume that three persons (A, B, M) are involved in the

[1]E-mail: popov@mail.ifmo.ru

scheme. M is a manager who wants to make a teleporting of a qubit $|D\rangle = \alpha|0\rangle + \beta|1\rangle$ (with unknown α, β) to A or B, using one quantum channel (one entangled state). Moreover, we want that M would choose the recipient (A or B) only at the final stage of the algorithm. It is the first version of our protocol. The second version is related with another possibility given by our scheme. Namely, it allows M to control the result of the teleportation of a qubit from A to B by creation of proper entangled state of A and B. This state is used for conventional two-qubit teleportation of a qubit from A to B (note that A and B do not know the type of this entangled state and, consequently, cannot predict the result of the teleportation, the manager predetermines the result).

A version of quantum secret sharing based on the generalization of the suggested teleportation scheme for many-qubit case is described. A problem of a creation of classical secret key in the framework of our approach is also discussed.

1. ALGORITHM

Initially there are $|\mathrm{GHZ}\rangle$ state (Greenberger–Horne–Zeilinger): $|\mathrm{GHZ}\rangle = 2^{-1/2}(|000\rangle + |111\rangle$ of qubits A, B, M. We assume that A and B can do two-qubit operations. As for M, he can do operation with qubits M and D. All persons are connected by classical communication channel.

The algorithm is as follows. The initial state can be represented in the following form:

$$
\begin{aligned}
|ABMD\rangle &= |\mathrm{GHZ}\rangle \otimes (\alpha|0\rangle + \beta|1\rangle) = \\
&= (|\Phi^+_{MD}\rangle \otimes (\alpha|0_A 0_B\rangle + \beta|1_A 1_B\rangle) + |\Phi^-_{MD}\rangle \otimes (\alpha|0_A 0_B\rangle - \beta|1_A 1_B\rangle) + \\
&\quad + |\Psi^+_{MD}\rangle \otimes (\beta|0_A 0_B\rangle + \alpha|1_A 1_B\rangle) + |\Psi^-_{MD}\rangle \otimes (\beta|0_A 0_B\rangle - \alpha|1_A 1_B\rangle),
\end{aligned}
$$

where $|\Phi^\pm_{MD}\rangle, |\Psi^\pm_{MD}\rangle$ is the Bell basis:

$$
|\Phi^\pm_{MD}\rangle = 2^{-1/2}(|0_M 0_D\rangle \pm |1_M 1_D\rangle), |\Psi^\pm_{MD}\rangle = 2^{-1/2}(|0_M 1_D\rangle \pm |1_M 0_D\rangle).
$$

Then, M makes a measurement in the Bell basis. There are four possible results. M informs (by classical channel) A and B about the two-qubit operation G they should do. After that the teleportation is finished. As for the mentioned operations, they are as follows. Consider the situation when M decided to create the proper qubit for A.

If the measurement result is $|\Phi^+_{MD}\rangle$, then the corresponding operation G is CNOT. For the result $|\Phi^-_{MD}\rangle$: $g_{11} = g_{22} = g_{43} = 1$. $g_{34} = -1$ (we list nonzero terms). For the result $|\Psi^+_{MD}\rangle$: $g_{14} = g_{22} = g_{31} = g_{43} = 1$. For the result $|\Psi^-_{MD}\rangle$: $g_{31} = g_{22} = g_{43} = 1$. $g_{14} = -1$. One can see that in such a way the teleportation of qubit D from M to A is made. For the case of teleportation from M to B an evident change in final two-qubit operation should be made. Thus, the sender determines who is the recipient of the qubit at the final stage only.

The suggested scheme can easily be modified to obtain a proper entangled state (determined by the manager) of qubits A and B. It allows the manager to control the result of the teleportation of a qubit $|F\rangle$ from A to B. It is well known that one can use different entangled states to make a teleportation. The most frequently used are $|\mathrm{CAT}\rangle = 2^{1/2}(|00\rangle + |11\rangle)$ and $|\mathrm{EPR}\rangle = 2^{1/2}(|01\rangle + |10\rangle)$ states. The type of unitary one-qubit operator used by B

to complete the teleportation depends on the type of the entangled state in question. For instance, let A and B be able to use two above-mentioned entangled states, and they believe that they have $|\mathrm{CAT}\rangle$ state and make the corresponding operations. However, the type of the entangled state is predetermined by the manager who can change the state in accordance with the scheme described above. In this situation the result of the teleportation would be another, and it is the manager who knows the result. Moreover, he can control this result by choosing the entangled state of A and B. Let us consider the example in more detail. Let the manager (M) be able to replace $|\mathrm{CAT}\rangle$ by $|\mathrm{EPR}\rangle$ or not change the state. In the second case B gets the qubit $|F\rangle$. But if the manager makes a replacement, the result is another. Namely, in accordance with the conventional teleportation procedure after the measurement of two-qubit state $|AF\rangle$ in Bell basis M gets one of four results (the first column) and informs B about the proper one-qubit operator (the second column), B applies the operator and obtains the following result (the third column):

$$\begin{array}{lrr} \Phi^+ & I & \mathrm{NOT}|F\rangle \\ \Phi^- & \sigma_3 & -\mathrm{NOT}|F\rangle \\ \Psi^+ & \sigma_1 & \mathrm{NOT}|F\rangle \\ \Psi^- & -i\sigma_2 & \mathrm{NOT}|F\rangle \end{array},$$

where $\sigma_j, j = 1, 2, 3$ is the corresponding Pauli matrix. One can see that B really gets $\mathrm{NOT}|F\rangle$. Note that A and B do not know the result of the teleportation. The manager only knows what is the result: $\mathrm{NOT}|F\rangle$ or $|F\rangle$.

If initially A and B plan to use $|\mathrm{EPR}\rangle$ state and the manager can replace (or does not replace) it by $|\mathrm{CAT}\rangle$, the result is absolutely analogous. Namely, in the case of replacement, the above table has the following form:

$$\begin{array}{lrr} \Phi^+ & \sigma_1 & \mathrm{NOT}|F\rangle \\ \Phi^- & i\sigma_2 & -\mathrm{NOT}|F\rangle \\ \Psi^+ & I & \mathrm{NOT}|F\rangle \\ \Psi^- & \sigma_3 & \mathrm{NOT}|F\rangle \end{array}.$$

2. $2n + 1$-QUBIT CASE

It is not difficult to generalize the suggested algorithm to $2n + 1$-qubit case. Namely, the starting point is the following entangled state of qubits $A_1, B_1, A_2, B_2, \ldots, A_n, B_n, M$:

$$|A_1, B_1, \ldots, A_n, B_n, M\rangle = |(2n+1)\mathrm{CAT}\rangle = (|00\ldots0\rangle + |11\ldots1\rangle)/\sqrt{2}.$$

Using the procedure described above, one can obtain the corresponding entangled state between qubits $A_i, B_i, i = 1, 2, \ldots n$. Namely, let $i = 1$ (for simplicity). The starting state is

$$(|A_1, B_1, \ldots, A_n, B_n, M\rangle \otimes (\alpha\,|00\rangle + \beta\,|11\rangle), (|\alpha|^2 + |\beta|^2 = 1).$$

The manager M makes a measurement in the basis $|\Phi^{\pm}_{MDF}\rangle, |\Psi^{\pm}_{MDF}\rangle$:

$$|\Phi^{\pm}_{MDF}\rangle = 2^{-1/2}(|0_M 0_D 0_F\rangle \pm |1_M 1_D 1_F\rangle), \quad |\Psi^{\pm}_{MDF}\rangle = 2^{-1/2}(|0_M 1_D 1_F\rangle \pm |1_M 0_D 0_F\rangle).$$

If the result is Φ^+_{MDF}, then one has the state $(\alpha, 0 \dots 0, \beta)^T$ ($16(n-1)-$vector). To obtain the proper state of A_1B_1, $\alpha\,|0_{A_1}0_{B_1}\rangle + \beta\,|1_{A_1}1_{B_1}\rangle) \otimes \beta\,|10\dots0\rangle)$, it is necessary to multiply the vector by $16(n-1) \times 16(n-1)$ matrix G_{Φ^+} with the following elements: $g_{ii} = 1, i \neq 12n-11, 16(n-1), g_{12n-11,12n-11} = g_{16(n-1),16(n-1)} = 0, g_{12n-11,16(n-1)} = g_{16(n-1),12n-11} = 1$, $g_{ij} = 0$ in other cases.

If the measurement shows another result, the matrix changes. We write down below the list of the results of the manager measurements, the corresponding state vector and the proper matrix G.

For Φ^-_{MDF} one has the state vector $(\alpha, 0 \dots 0, -\beta)^T$ and the matrix G_{Φ^-} with the following elements: $g_{ii} = 1, i \neq 12n-11, 16(n-1), g_{12n-11,12n-11} = g_{16(n-1),16(n-1)} = 0, g_{12n-11,16(n-1)} = -1, g_{16(n-1),12n-11} = 1$, $g_{ij} = 0$ in other cases.

For Ψ^+_{MDF} one has the state vector $(\beta, 0 \dots 0, \alpha)^T$ and the matrix G_{Ψ^+} with the following elements: $g_{ii} = 1, i \neq 1, 12n-11, 16(n-1), g_{12n-11,12n-11} = g_{1,1} = g_{16(n-1),16(n-1)} = 0, g_{12n-11,1} = g_{1,16(n-1)} = g_{16(n-1),12n-11} = 1$, $g_{ij} = 0$ in other cases.

For Ψ^-_{MDF} one has the state vector $(\beta, 0 \dots 0, -\alpha)^T$ and the matrix G_{Ψ^-} with the following elements: $g_{ii} = 1, i \neq 1, 12n-11, 16(n-1), g_{12n-11,12n-11} = g_{1,1} = g_{16(n-1),16(n-1)} = 0, g_{12n-11,1} = 1, g_{1,16(n-1)} = -1, g_{16(n-1),12n-11} = 1$, $g_{ij} = 0$ in other cases.

The manager informs A_1, B_1 about the type of matrix G by classical channel. They apply the matrix to the vector and obtain the proper entangled state.

Simple modification of the procedure allows us to obtain proper entangled state of qubits A_i, B_i for each i. No-cloning theorem does not allow us to make a teleportation of unknown two-qubit state (i.e., for arbitrary α, β) to all pairs A_i, B_i simultaneously. But if we deal with a known basic vector (e.g., CAT or EPR), it is possible, and it is the manager who predetermines the recipients and the types of the entangled states. In this situation the procedure of choosing of matrix G for obtaining the proper state is conventional. We choose new orthogonal basis, which contains our vector as an element. Then, one constructs unitary matrix which transforms the initial basic vector to the proper one (tensor product of proper two-qubit states for each pair). Transformation to the original basis gives us the unitary matrix we need.

Of course, the participants can determine what pair (A_i, B_i) has received the entangled state for the next teleportation, but they do not know what state is needed (CAT or EPR). As for the eavesdropper, he cannot determine even the recipients.

This scheme can be used for quantum secret sharing. Namely, let a secret be shared between some quantum states (in our case — $B_1, \dots, B_n$). Authorized set of states is such a set that someone holding all of these shares can exactly reconstruct the original secret [8]. Note that unauthorized set is such that someone holding just these shares can acquire no information at all about the secret quantum state (i.e., the density matrix of an unauthorized set is the same for all encoded states). For a generic state split up into a number of shares, most sets will be neither authorized nor unauthorized (only for perfect quantum sharing scheme each set is either authorized or unauthorized one). Using the suggested scheme, the manager can create the proper two-qubit states in selected pairs A_i, B_i. Then, A_i makes a teleportation of standard initial state to B_i, and B_i receives the proper state if he was among manager selected recipients (or another state otherwise); i.e., the manager predetermines the results of these teleportations. In such a way the manager creates the authorized set of states (among $B_1, \dots, B_n$). The manager is the only person who knows the authorized set.

As a variant, this scheme is a way of creating a classical secret sequence. It is interesting that although A_i and B_i create this sequence, they do not know the result. Moreover, the classical secret key (sequence) is coded by the entangled states of A_i, B_i (i.e., the information is well protected due to no-cloning theorem) and appears as a classical key at the last stage only (after the last teleportation).

Acknowledgements. The work is supported by the Russian Foundation for Basic Research and by project 2.1.1/4215 of the program «Development of the Potential of High School of Russia 2009–2010».

REFERENCES

1. *Grover L. K.* Quantum Computers Can Search Arbitrarily Large Databases by a Single Query // Phys. Rev. Lett. 1997. V. 79. P. 4709–4712.
2. *Bennett C. H. et al.* Teleporting an Unknown Quantum State via Dual Classical and Einstein–Podolsky–Rosen Channels // Phys. Rev. Lett. 1993. V. 70. P. 1895–1899.
3. *Plenio M. B., Vedral V.* Teleportation, Entanglement and Thermodynamics in the Quantum World // Contemp. Phys. 1998. V. 39, No. 6. P. 431–446.
4. *Gottesman D., Chuang I. L.* Demonstrating the Viability of Universal Quantum Computation Using Teleportation and Single-Qubit Operations // Nature. 1999. V. 402. P. 390–392.
5. *Hillery M., Buzek V., Berthiaume A.* Quantum Secret Sharing // Phys. Rev. A. 1999. V. 59, No. 3. P. 1829–1834.
6. *Lee S., Joo J., Kim J.* Entanglement of Three-Qubit Pure States in Terms of Teleportation Capability // Phys. Rev. A. 2005. V. 72. P. 024302–024305.
7. *Lee S., Joo J., Kim J.* Teleportation Capability, Distillability, and Nonlocality on Three-Qubit States // Phys. Rev. A. 2007. V. 76. P. 012311–012314.
8. *Gottesman D.* Theory of Quantum Secret Sharing // Phys. Rev. A. 2000. V. 61. P. 042311–042318.