Int J Theor Phys (2011) 50:2799–2804
DOI 10.1007/s10773-011-0778-y

Quantum Information Splitting of an Arbitrary Multi-qubit GHZ-type State by Using a Four-qubit Cluster State

Yi-you Nie · Yuan-hua Li · Cui-ping Jin · Jun-chang Liu · Ming-huang Sang

Received: 23 January 2011 / Accepted: 23 March 2011 / Published online: 8 April 2011

Abstract A new application of the four-qubit cluster state is investigated for quantum information splitting (QIS) of an arbitrary N-qubit GHZ-type state among three parties. We demonstrate that a four-qubit cluster state can be used to realize the deterministic QIS of an arbitrary N-qubit GHZ-type state by introducing $N-1$ ancillary qubits and performing $N-1$ controlled-NOT operations. The presented protocols considered here are secure against certain eavesdropping attacks.

Keywords Quantum information · Cluster state · Quantum information splitting · Arbitrary N-qubit GHZ-type state · Controlled-NOT operation

1 Introduction

For classical information a shared key can be established between one party and two or more others, all of whom should work together to read the message. In the case of quantum information, the sender teleported a qubit in a way that the qubit can be recovered if and only if two or more parties at the receiving end agree to collaborate. Quantum secret sharing is an important branch of quantum information processing, it is the generalization of classical secret sharing into quantum scenario. After Hillery et al. [1] demonstrated that the GHZ states can be used for quantum information splitting (QIS), several QIS protocols have been devised with the help of multi-particle entangled states, such as Bell states [2], W states [3], a genuine five-qubit [4, 5] and six-qubit [6] entangled states.

In 2001, Briegel and Raussendorf [7] introduced a class of n-qubit entangled states, i.e., the cluster states. It is known that the n-qubit ($n > 3$) cluster state is maximally connected

Y.-y. Nie (✉) · Y.-h. Li · C.-p. Jin · J.-c. Liu · M.-h. Sang
Department of Physics, Jiangxi Normal University, Nanchang 330022, China
e-mail: nieyiyou@163.com

Y.-y. Nie
e-mail: nieyiyou@jxnu.edu.cn

Y.-y. Nie
Key Laboratory of Optoelectronic & Telecommunication of Jiangxi Province, Nanchang 330022, China

with the better persistency than the GHZ-type state [8]. Also cluster states are robust against decoherence [9]. And it has been shown that a four-qubit cluster state can be used for quantum error correction [10], as well as quantum computation [11, 12]. In Ref. [13], it was demonstrated that a four-qubit cluster state may be useful in QIS of an arbitrary single qubit state and an entangled two-qubit state. So far, the preparation of the cluster states have attracted much attention [14, 15] and a lot of applications of cluster states have been investigated [16–21]. This gives us motivation to study the new application of the four-qubit cluster state for QIS protocol.

In this paper, we describe a scheme to realize QIS of an arbitrary N-qubit GHZ-type state by using a four-qubit cluster state among three parties. Firstly, the sender can transfer all the information of an arbitrary N-qubit GHZ-type state into a qubit, and then performs a Bell-state measurement (BSM) on her rest qubits. Then Charlie, one of the two agents, needs to make a two-qubit measurement on his own qubits. Finally Bob, the other one (say the receiver), can obtain the original N-qubit GHZ-type state by introducing $N-1$ ancillary qubits and performing $N-1$ controlled-NOT operations. In our scheme, we first consider how to realize the QIS of an arbitrary three-qubit GHZ-type state by the scheme proposed here, then we provide a generalization to the case of QIS of N-qubit GHZ-type state.

2 QIS of an Arbitrary Three-qubit GHZ-type State

Our scheme can be described as follows. Suppose there are three legitimate parties, say, Alice, Bob and Charlie. Alice is the sender of quantum information. Bob and Charlie are two agents. Suppose Alice has an arbitrary three-qubit GHZ-type state, which can be described as follows

$$|\psi\rangle_{123} = \alpha|000\rangle_{123} + \beta|111\rangle_{123}, \tag{1}$$

where $|\alpha|^2 + |\beta|^2 = 1$. Alice, Bob and Charlie share a four-qubit cluster state

$$|C\rangle_{ABCD} = \frac{1}{2}(|0000\rangle + |0101\rangle + |1010\rangle - |1111\rangle)_{ABCD}, \tag{2}$$

the qubits 1, 2, 3 and A belong to Alice, qubit B and D belong to Charlie, and qubit C belongs to Bob, respectively. Here, we assume that Alice wants to transmit the state $|\psi\rangle_{123}$ to Bob who is assigned to reconstruct the original state with the help of Charlie.

The state of the whole system is

$$|\Psi\rangle_{123ABCD} = |\psi\rangle_{123} \otimes |C\rangle_{ABCD}. \tag{3}$$

In order to achieve the QIS of an arbitrary three-qubit GHZ-type state simply, Alice firstly transfer all the information of a three-qubit GHZ-type state $(\alpha|000\rangle + \beta|111\rangle)_{123}$ into qubit 1, its state is $(\alpha|0\rangle + \beta|1\rangle)_1$. And it can be generated in the following way.

To gain $(\alpha|0\rangle + \beta|1\rangle)_1$ from the state $(\alpha|000\rangle + \beta|111\rangle)_{123}$, Alice needs to carry out two controlled-NOT operations on the three qubits with qubit 1 as controlled qubit and each of two qubits 2, 3 as target qubits. The specific steps are illustrated by the quantum circuit showed in Fig. 1. Let us follow the state $|\psi\rangle_{123} = (\alpha|000\rangle + \beta|111\rangle)_{123}$ in the circuit to see clearly the process of generating $(\alpha|0\rangle + \beta|1\rangle)_1$. The input state of circuit is $|\psi\rangle_{123}$, after sending the three qubits through two controlled-NOT gates, the state of all the three qubits becomes

$$|\psi'\rangle_{123} = (\alpha|0\rangle + \beta|1\rangle)_1 \otimes |00\rangle_{23}. \tag{4}$$

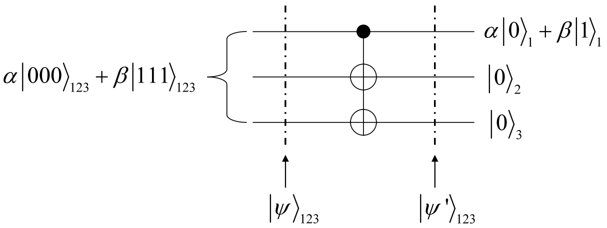
$\alpha|000\rangle_{123}+\beta|111\rangle_{123}$
$\alpha|0\rangle_1+\beta|1\rangle_1$
$|0\rangle_2$
$|0\rangle_3$
$|\psi\rangle_{123}$
$|\psi'\rangle_{123}$

Fig. 1 Quantum circuit for generating $\alpha|0\rangle_1+\beta|1\rangle_1$

Table 1 The outcome of the measurement performed by Alice and the state obtained by Bob and Charlie, where the normalization factors have been omitted for convenience

Alice's result	State obtained by Bob and Charlie
$\|\Phi^+\rangle_{1A}$	$\|\phi^1\rangle_{BCD}=(\alpha(\|000\rangle+\|101\rangle)+\beta(\|010\rangle-\|111\rangle))_{BCD}$
$\|\Phi^-\rangle_{1A}$	$\|\phi^2\rangle_{BCD}=(\alpha(\|000\rangle+\|101\rangle)-\beta(\|010\rangle-\|111\rangle))_{BCD}$
$\|\Psi^+\rangle_{1A}$	$\|\phi^3\rangle_{BCD}=(\alpha(\|010\rangle-\|111\rangle)+\beta(\|000\rangle+\|101\rangle))_{BCD}$
$\|\Psi^-\rangle_{1A}$	$\|\phi^4\rangle_{BCD}=(\alpha(\|010\rangle-\|111\rangle)-\beta(\|000\rangle+\|101\rangle))_{BCD}$

Now, we note that all the information of the state $(\alpha|000\rangle+\beta|111\rangle)_{123}$ have been transferred into the state $(\alpha|0\rangle+\beta|1\rangle)_1$.

Now we only need to consider the state of qubits $1, A, B, C, D$ which is

$$|\Psi'\rangle_{1ABCD}=(\alpha|0\rangle+\beta|1\rangle)_1\otimes|C\rangle_{ABCD}. \tag{5}$$

Then Alice performs a BSM on her qubit pair $(1, A)$. The outcome of the measurement performed by Alice and the entangled state obtained by Bob and Charlie are shown in Table 1, where $|\Phi^{\pm}\rangle_{1A}=\frac{1}{\sqrt{2}}(00\pm 11)_{1A}$ and $|\Psi^{\pm}\rangle_{1A}=\frac{1}{\sqrt{2}}(01\pm 10)_{1A}$.

Then Alice sends her measured result to Charlie and Bob via a classical channel, Charlie then makes a measurement in the basis of $\{|00\rangle_{BD}, |11\rangle_{BD}\}$ and informs Bob of his measured result. Having known the outcomes of both their measurements, Bob can obtain an arbitrary single-qubit state. For instance, had the Bob-Charlie system evolved into the first state shown in table 1 and if the outcome of Charlie's measurement is $|00\rangle_{BD}$, then Bob's state collapses into the following state

$$|\varphi\rangle_C=\alpha|0\rangle_C+\beta|1\rangle_C. \tag{6}$$

In order to obtain the original three-qubit GHZ-type state, Bob introduces two ancillary qubits a_1 and a_2 in the initial state $|00\rangle_{a_1a_2}$, and then carries out two controlled-NOT operations on his three qubits with qubit C as controlled qubit and each of two ancillary qubits as target qubit. The specific steps are illustrated by the quantum circuit showed in Fig. 2.

Let us follow the states $|\varphi\rangle_C$ and $|00\rangle_{a_1a_2}$ in the circuit to see clearly the process of generating $|\psi\rangle_{Ca_1a_2}=\alpha|000\rangle_{Ca_1a_2}+\beta|111\rangle_{Ca_1a_2}$. The input state of circuit is

$$|\Phi\rangle_{Ca_1a_2}=(\alpha|0\rangle_C+\beta|1\rangle_C)\otimes|00\rangle_{a_1a_2}=\alpha|000\rangle_{Ca_1a_2}+\beta|100\rangle_{Ca_1a_2}, \tag{7}$$

after sending the three qubits through two controlled-NOT gates with qubit C as controlled qubit and each of two ancillary qubits as target qubit, the state of all the three qubits becomes

$$|\psi\rangle_{Ca_1a_2}=\alpha|000\rangle_{Ca_1a_2}+\beta|111\rangle_{Ca_1a_2}, \tag{8}$$

this is the state that Alice wants to send to Bob.

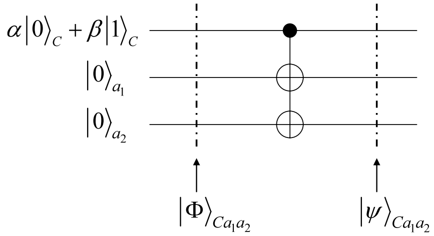

Fig. 2 Quantum circuit for generating $|\psi\rangle_{Ca_1a_2}$

Now we discuss the security problem of this scheme against certain eavesdropping attacks. We assume that an eavesdropper (say Eve) has managed to entangle an ancilla qubit to a qubit possessed by Charlie, so that she can measure the ancilla qubit to gain information about the unknown qubit state. Suppose, all the three participants are unaware of this attack of Eve, then after Alice transfers all the information into a qubit and performs a BSM measurement, the combined state of Charlie, Bob and Eve collapses into a four-qubit entangled state. However, after Charlie makes a two-qubit measurement, the Bob-Eve system collapses into a product state, leaving Eve with no information about the unknown qubit. To see this scenario more explicitly, assume the ancilla entangled to the qubit B of the entangled channel possessed by Charlie to be $|0\rangle_E$. If Alice gets the result $|\Phi^+\rangle_{1A}$, then the combined state of Charlie, Bob and Eve would be,

$$|\Xi\rangle_{BCDE}=\frac{1}{\sqrt{2}}(\alpha(|0000\rangle+|1011\rangle)+\beta(|0100\rangle-|1111\rangle))_{BCDE}.$$

Suppose that Charlie obtains the $|00\rangle_{BD}$, then the Bob-Eve system collapses into a product state, $|\Omega\rangle_{CE}=(\alpha|0\rangle+\beta|1\rangle)_C|0\rangle_E$. It is evident that Eve's state is unaltered leaving no chance for her to gain any information about the unknown qubit state, so this protocol is secure.

3 QIS of an Arbitrary N-qubit GHZ-type State

The previous protocol can be generalized to QIS an arbitrary N-qubit GHZ-type state. We here assume that Bob reconstruct the original state. We suppose that Alice has an arbitrary N-qubit GHZ-type state

$$|\psi\rangle_{12\cdots N}=\alpha|00\cdots 0\rangle_{12\cdots N}+\beta|11\cdots 1\rangle_{12\cdots N}. \tag{9}$$

Alice, Bob and Charlie share a four-qubit cluster state in the expression of (2). The qubit B and D belong to Charlie, and qubit C belongs to Bob. The state of the whole system is

$$|\Psi\rangle_{12\cdots N_{ABCD}}=|\psi\rangle_{12\cdots N}\otimes|C\rangle_{ABCD}. \tag{10}$$

In order to achieve the QIS of an arbitrary N-qubit GHZ-type state simply, Alice firstly transfer all the information of an arbitrary N-qubit GHZ-type state $|\psi\rangle_{12\cdots N}$ into qubit 1, its state is $(\alpha|0\rangle+\beta|1\rangle)_1$. And it can be generated in the following way.

To gain $(\alpha|0\rangle+\beta|1\rangle)_1$ from the state $|\psi\rangle_{12\cdots N}$, Alice needs to carry out $N-1$ controlled-NOT operations on the N qubits with qubit 1 as controlled qubit and each of $N-1$ qubits $2,3,\ldots,N$ as target qubits. The specific steps are illustrated by the quantum circuit showed in Fig. 3. Let us follow the state $|\psi\rangle_{12\cdots N}$ in the circuit to see clearly the process of generating

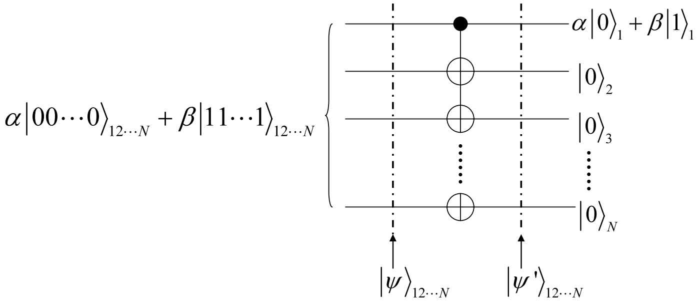
$\alpha|00\cdots0\rangle_{12\cdots N}+\beta|11\cdots1\rangle_{12\cdots N}$
$\alpha|0\rangle_1+\beta|1\rangle_1$
$|0\rangle_2$
$|0\rangle_3$
$|0\rangle_N$
$|\psi\rangle_{12\cdots N}$
$|\psi'\rangle_{12\cdots N}$

Fig. 3 Quantum circuit for generating $\alpha|0\rangle_1+\beta|1\rangle_1$

$(\alpha|0\rangle+\beta|1\rangle)_1$. The input state of circuit is $|\psi\rangle_{12\cdots N}$, after sending the N qubits through $N-1$ controlled-NOT gates, the state of all the N qubits becomes

$$|\psi'\rangle_{12\cdots N}=(\alpha|0\rangle+\beta|1\rangle)_1\otimes|00\cdots0\rangle_{23\cdots N}. \tag{11}$$

Now, we note that all the information of the state $|\psi\rangle_{12\cdots N}$ have been transferred into the state $(\alpha|0\rangle+\beta|1\rangle)_1$.

Then Alice performs a BSM on her qubit pair $(1, A)$. The outcome of the measurement performed by Alice and the entangled state obtained by Bob and Charlie are shown in Table 1. and then she informs Charlie and Bob of her measured result. Charlie then makes a measurement in the basis of $\{|00\rangle_{BD}, |11\rangle_{BD}\}$ and communicates the result of her measurement to Bob. Having known the outcomes of both their measurements, Bob can apply an appropriate unitary transformation to obtain an arbitrary single-qubit state $\alpha|0\rangle_C+\beta|1\rangle_C$.

In order to obtain the original N-qubit GHZ-type state, Bob introduces $N-1$ ancillary qubits $a_1, a_2, \ldots, a_{N-1}$ in the initial state $|00\cdots0\rangle_{a_1a_2\cdots a_{N-1}}$, and then carries out $N-1$ controlled-NOT operations on his N qubits with qubit C as controlled qubit and each of $N-1$ ancillary qubits as target qubit. The specific steps are illustrated by the quantum circuit showed in Fig. 4.

Let us follow the states $\alpha|0\rangle_C+\beta|1\rangle_C$ and $|00\cdots0\rangle_{a_1a_2\cdots a_{N-1}}$ in the circuit to see clearly the process of generating $|\psi\rangle_{Ca_1a_2\cdots a_{N-1}}=\alpha|00\cdots0\rangle_{Ca_1a_2\cdots a_{N-1}}+\beta|11\cdots1\rangle_{Ca_1a_2\cdots a_{N-1}}$. The input state of circuit is

$$\begin{aligned}|\Phi'\rangle_{Ca_1a_2\cdots a_{N-1}}&=(\alpha|0\rangle_C+\beta|1\rangle_C)\otimes|00\cdots0\rangle_{a_1a_2\cdots a_{N-1}}\\&=\alpha|000\cdots0\rangle_{Ca_1a_2\cdots a_{N-1}}+\beta|100\cdots0\rangle_{Ca_1a_2\cdots a_{N-1}}\end{aligned} \tag{12}$$

after sending the N qubits through $N-1$ controlled-NOT gates with qubit C as controlled qubit and each of $N-1$ ancillary qubits as target qubit, the state of all the N qubits becomes

$$|\psi\rangle_{Ca_1a_2\cdots a_{N-1}}=\alpha|00\cdots0\rangle_{Ca_1a_2\cdots a_{N-1}}+\beta|11\cdots1\rangle_{Ca_1a_2\cdots a_{N-1}}, \tag{13}$$

this is the state that Alice wants to send to Bob.

The security of this protocol against certain eavesdropping attacks can be demonstrated by using the same proof method proposed in Sect. 2, so this protocol can be made to be secure.

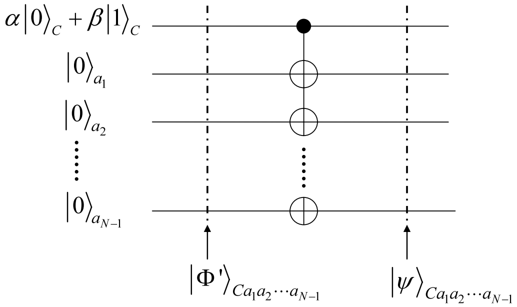
$\alpha|0\rangle_C+\beta|1\rangle_C$
$|0\rangle_{a_1}$
$|0\rangle_{a_2}$
$|0\rangle_{a_{N-1}}$
$|\Phi'\rangle_{Ca_1a_2\cdots a_{N-1}}$
$|\psi\rangle_{Ca_1a_2\cdots a_{N-1}}$

Fig. 4 Quantum circuit for generating $|\psi\rangle_{Ca_1a_2\cdots a_{N-1}}$

4 Conclusion

In this paper, we have demonstrated that a four-qubit cluster state can be used to realize the deterministic QIS of an arbitrary N-qubit GHZ-type state by introducing $N-1$ ancillary qubits and performing $N-1$ controlled-NOT operations. Our scheme considered here are secure against certain eavesdropping attacks. In our scheme, one only needs a BSM and the two qubit measurements, which can be fulfilled in the experiment. Therefore such a scheme is experimentally accessible. We hope that our scheme will soon be realized in the experiment.

Acknowledgements This work is supported by the National Natural Science Foundation of China (Grant No. 60807014), the Natural Science Foundation of Jiangxi Province, China (Grant No. 2009GZW0005), the Research Foundation of state key laboratory of advanced optical communication systems and networks, and the Research Foundation of the Education Department of Jiangxi Province (Grant No. GJJ09153).

References

1. Hillery, M., Bužek, V., Berthiaume, A.: Phys. Rev. A **59**, 1829 (1999)
2. Deng, F.G., Li, X.H., Li, C.Y., Zhou, P., Zhou, H.Y.: Phys. Rev. A **72**, 044301 (2005)
3. Zheng, S.B.: Phys. Rev. A **74**, 054303 (2006)
4. Muralidharan, S., Panigrahi, P.K.: Phys. Rev. A **77**, 032321 (2008)
5. Hou, K., Li, Y.B., Shi, S.H.: Opt. Commun. **283**, 1961 (2010)
6. Li, Y.H., Liu, J.C., Nie, Y.Y.: Int. J. Theor. Phys. **49**, 2592 (2010)
7. Briegel, H.J., Raussendorf, R.: Phys. Rev. Lett. **86**, 910 (2001)
8. Dong, P., Xue, Z.Y., Yang, M., Cao, Z.L.: Phys. Rev. A **73**, 033818 (2006)
9. Hein, M., Dür, W., Briegel, H.J.: Phys. Rev. A **71**, 032350 (2005)
10. Schlingemann, D., Werner, R.F.: Phys. Rev. A **65**, 012308 (2001)
11. Raussendorf, R., Briegel, H.J.: Phys. Rev. Lett. **86**, 5188 (2001)
12. Walther, P., Resch, K.J., Rudolph, T., Schenck, E., Weinfurter, H., Vedral, V., Aspelmeyer, M., Zeilinger, A.: Nature **434**, 169 (2005)
13. Muralidharan, S., Panigrahi, P.K.: Phys. Rev. A **78**, 062333 (2008)
14. Zhan, Z.M.: Commun. Theor. Phys. **48**, 83 (2007)
15. Wang, X.W., Cao, S., Xia, L.X.: Commun. Theor. Phys. **49**, 1217 (2008)
16. Zhang, B.B., Liu, Y.: Int. J. Theor. Phys. **48**, 2644 (2009)
17. Nie, Y.Y., Hong, Z.H., Huang, Y.B., Yi, X.J., Li, S.S.: Int. J. Theor. Phys. **48**, 1485 (2009)
18. Muralidharan, S., Jain, S., Panigrahi, P.K.: arXiv:0904.0563v2 (2009)
19. Liu, J.C., Li, Y.H., Nie, Y.Y.: Int. J. Theor. Phys. **49**, 1976 (2010)
20. Wang, X.W., Yang, G.J.: Commun. Theor. Phys. **52**, 588 (2009)
21. Wang, X.W., Shan, Y.G., Xia, L.X., Lu, M.W.: Phys. Lett. A **364**, 7 (2007)