Int J Theor Phys (2014) 53:2282–2287
DOI 10.1007/s10773-014-2028-6

Bidirectional Quantum Secure Communication Based on One-Dimensional Four-Particle Cluster States

Gan Gao

Received: 10 August 2013 / Accepted: 23 January 2014 / Published online: 31 January 2014

Abstract Using one-dimensional four-particle cluster states, we propose a bidirectional quantum secure communication protocol, in which the information leakage does not exist. In order to judge whether two sequences composed of cluster states are transmitted safely, two batches of decoy particles are used. Moreover, we show that this protocol is secure against eavesdropping.

Keywords Bidirectional quantum secure communication · One-dimensional four-particle cluster state · Information leakage

1 Introduction

As we all know, it is impossible to implement physically secure communication between distant parties only by the transmission of classical signals. However, quantum mechanical properties of physical systems can achieve such a task. In 1984, Bennett and Brassard borrowed the properties to put forward the first quantum key distribution (QKD) protocol, which is customarily called BB84 protocol [1]. Subsequently, a variety of QKD protocols [2–7] were proposed. It can be seen that, in the QKD, what is distributed between two parties is only secret keys and the two parties make use of the distributed keys to encode and decode secret messages. Recently, a new concept in quantum cryptography, that is, quantum secure direct communication (QSDC) [8] was proposed. It is different from the QKD and can directly communicate secret messages without establishing secret keys to encrypt them in advance. In some sense, the QSDC may cost less time than the QKD during the transmission of secret messages. Thus far, all kinds of QSDC protocols [9–21] have been put forward. In the QSDC, we can see that one party will directly send his (her) secret messages to the other. That is to say, one is the sender of secret messages, and the other is the receiver. Clearly, secret messages are transmitted by a single-direction way. In 2004, Nguyen put forward an

G. Gao (✉)
Department of Electrical Engineering, Tongling University, Tongling 244000, China
e-mail: gaogan0556@163.com

interesting communication protocol in which secret messages may be transmitted by a bidirectional way, that is, the so-called bidirectional quantum secure communication (BQSC) (also called quantum dialogue) [22]. In the BQSC, we see that both of the two communication parties are not only the senders of messages, but also the receivers. Unfortunately, there is an information-leakage shortcoming in Nguyen's BQSC protocol, which has been pointed out by Gao et al. [23]. In order to overcome the shortcoming, Shi et al. used single photons to propose a BQSC protocol [24], and we also proposed two BQSC protocols [25] by swapping the entanglement of Bell states in 2010. In addition, there are other BQSC protocols based on triple particle W states [26], four-qubit DF states [27], five-qubit entangled states [28], which the shortcoming does not exist in. In this paper, by using one-dimensional four-particle cluster states, we will propose a BQSC protocol without information leakage. By the way, since Briegel and Raussendorf reported the cluster states [29] in 2001, the studies [30–34] on it are always gone on. Before describing our BQSC protocol, we first define sixteen one-dimensional four-particle cluster states as follows:

$$\left|C_4^{00}\right\rangle_{abcd} = \frac{1}{2}\left(|+\rangle|0\rangle|-\rangle|0\rangle - |+\rangle|0\rangle|+\rangle|1\rangle - |-\rangle|1\rangle|+\rangle|0\rangle + |-\rangle|1\rangle|-\rangle|1\rangle\right)_{abcd}$$

Here, $|+\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)$, $|-\rangle = \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)$. The other fifteen cluster states can be obtained by the following way:

$$\left|C_4^{ij}\right\rangle_{abcd} = \sigma_a^i \sigma_c^j \left|C_4^{00}\right\rangle_{abcd} \quad (i, j = 0, 1, 2, 3) \tag{1}$$

Here, $\sigma^{i(j)}$ belongs to one of four Pauli operators: $\sigma^0 = I = |0\rangle\langle 0| + |1\rangle\langle 1|$, $\sigma^1 = \sigma_x = |0\rangle\langle 1| + |1\rangle\langle 0|$, $\sigma^2 = \sigma_z = |0\rangle\langle 0| - |1\rangle\langle 1|$, $\sigma^3 = \sigma_y = |0\rangle\langle 1| - |1\rangle\langle 0|$, and the local operations $\sigma_a^i \otimes \sigma_c^j$ are performed on the subsystem of particles a and c. The other fifteen states are spread as follows:

$$\left|C_4^{01}\right\rangle_{abcd} = \frac{1}{2}\left(-|+\rangle|0\rangle|-\rangle|0\rangle - |+\rangle|0\rangle|+\rangle|1\rangle - |-\rangle|1\rangle|+\rangle|0\rangle - |-\rangle|1\rangle|-\rangle|1\rangle\right)_{abcd}$$

$$\left|C_4^{02}\right\rangle_{abcd} = \frac{1}{2}\left(|+\rangle|0\rangle|+\rangle|0\rangle - |+\rangle|0\rangle|-\rangle|1\rangle - |-\rangle|1\rangle|-\rangle|0\rangle + |-\rangle|1\rangle|+\rangle|1\rangle\right)_{abcd}$$

$$\left|C_4^{03}\right\rangle_{abcd} = \frac{1}{2}\left(|+\rangle|0\rangle|+\rangle|0\rangle + |+\rangle|0\rangle|-\rangle|1\rangle + |-\rangle|1\rangle|-\rangle|0\rangle + |-\rangle|1\rangle|+\rangle|1\rangle\right)_{abcd}$$

$$\left|C_4^{10}\right\rangle_{abcd} = \frac{1}{2}\left(|+\rangle|0\rangle|-\rangle|0\rangle - |+\rangle|0\rangle|+\rangle|1\rangle + |-\rangle|1\rangle|+\rangle|0\rangle - |-\rangle|1\rangle|-\rangle|1\rangle\right)_{abcd}$$

$$\left|C_4^{20}\right\rangle_{abcd} = \frac{1}{2}\left(|-\rangle|0\rangle|-\rangle|0\rangle - |-\rangle|0\rangle|+\rangle|1\rangle - |+\rangle|1\rangle|+\rangle|0\rangle + |+\rangle|1\rangle|-\rangle|1\rangle\right)_{abcd}$$

$$\left|C_4^{30}\right\rangle_{abcd} = \frac{1}{2}\left(-|-\rangle|0\rangle|-\rangle|0\rangle + |-\rangle|0\rangle|+\rangle|1\rangle - |+\rangle|1\rangle|+\rangle|0\rangle + |+\rangle|1\rangle|-\rangle|1\rangle\right)_{abcd}$$

$$\left|C_4^{11}\right\rangle_{abcd} = \frac{1}{2}\left(-|+\rangle|0\rangle|-\rangle|0\rangle - |+\rangle|0\rangle|+\rangle|1\rangle + |-\rangle|1\rangle|+\rangle|0\rangle + |-\rangle|1\rangle|-\rangle|1\rangle\right)_{abcd}$$

$$\left|C_4^{12}\right\rangle_{abcd} = \frac{1}{2}\left(|+\rangle|0\rangle|+\rangle|0\rangle - |+\rangle|0\rangle|-\rangle|1\rangle + |-\rangle|1\rangle|-\rangle|0\rangle - |-\rangle|1\rangle|+\rangle|1\rangle\right)_{abcd}$$

$$\left|C_4^{13}\right\rangle_{abcd} = \frac{1}{2}\left(|+\rangle|0\rangle|+\rangle|0\rangle + |+\rangle|0\rangle|-\rangle|1\rangle - |-\rangle|1\rangle|-\rangle|0\rangle - |-\rangle|1\rangle|+\rangle|1\rangle\right)_{abcd}$$

$$\left|C_4^{21}\right\rangle_{abcd} = \frac{1}{2}\left(-|-\rangle|0\rangle|-\rangle|0\rangle - |-\rangle|0\rangle|+\rangle|1\rangle - |+\rangle|1\rangle|+\rangle|0\rangle - |+\rangle|1\rangle|-\rangle|1\rangle\right)_{abcd}$$

$$\left|C_4^{22}\right\rangle_{abcd} = \frac{1}{2}\left(|-\rangle|0\rangle|+\rangle|0\rangle - |-\rangle|0\rangle|-\rangle|1\rangle - |+\rangle|1\rangle|-\rangle|0\rangle + |+\rangle|1\rangle|+\rangle|1\rangle\right)_{abcd}$$

$$\left|C_4^{23}\right\rangle_{abcd} = \frac{1}{2}\left(|-\rangle|0\rangle|+\rangle|0\rangle + |-\rangle|0\rangle|-\rangle|1\rangle + |+\rangle|1\rangle|-\rangle|0\rangle + |+\rangle|1\rangle|+\rangle|1\rangle\right)_{abcd}$$

$$\left|C_4^{31}\right\rangle_{abcd} = \frac{1}{2}\left(|-\rangle|0\rangle|-\rangle|0\rangle + |-\rangle|0\rangle|+\rangle|1\rangle - |+\rangle|1\rangle|+\rangle|0\rangle - |+\rangle|1\rangle|-\rangle|1\rangle\right)_{abcd}$$

$$\left|C_4^{32}\right\rangle_{abcd} = \frac{1}{2}\left(-|-\rangle|0\rangle|+\rangle|0\rangle + |-\rangle|0\rangle|-\rangle|1\rangle - |+\rangle|1\rangle|-\rangle|0\rangle + |+\rangle|1\rangle|+\rangle|1\rangle\right)_{abcd}$$

$$\left|C_4^{33}\right\rangle_{abcd} = \frac{1}{2}\left(-|-\rangle|0\rangle|+\rangle|0\rangle - |-\rangle|0\rangle|-\rangle|1\rangle + |+\rangle|1\rangle|-\rangle|0\rangle + |+\rangle|1\rangle|+\rangle|1\rangle\right)_{abcd}$$

2 Bidirectional Quantum Secure Communication Protocol

In our BQSC protocol, two legitimate communication parties are Alice and Bob, respectively, and they exchange the secret messages at the same time. Our BQSC protocol can be realized with the following five steps.

(1) Alice prepares two same sequences (1P sequence and 2P sequence) which are composed of one-dimensional four-particle cluster states. For clarity, we denote each sequence with $[P_1^a, P_1^b, P_1^c, P_1^d, P_2^a, P_2^b, P_2^c, P_2^d, \ldots, P_n^a, P_n^b, P_n^c, P_n^d]$. Here, the a, b, c and d represent four particles in one cluster state and the subscripts $1, 2, 3, \ldots$ and n indicate the orders of cluster states in a sequence, and what each cluster state is secret and known by Alice. In addition, she prepares two batches of decoy particles [29–31] (saying j particles and k particles), and each decoy particle is randomly in one of the four states $(|0\rangle, |1\rangle, |+\rangle, |-\rangle)$. Alice inserts the j particles into the 1P sequence and sends the 1P sequence including the j particles to Bob.

(2) After Bob receives the 1P sequence, they check whether it is attacked. First, Alice tells him the positions of j particles in the sequence and the state of each j particle. Next, Bob uses a correct basis ($\{|0\rangle, |1\rangle\}$ or $\{|+\rangle, |-\rangle\}$) to measure each j particle. According to Alice's announcing information, Bob can analyze the error rate of the 1P sequence transmission. If the error rate goes beyond the threshold, the process is aborted. Otherwise, the process goes on. Bob gets rid of the j particles, and uses cluster basis to measure each four particles in the 1P sequence in order. In result, he obtains all the information of cluster states in the 1P sequence.

(3) Alice encodes her secret messages by performing $\sigma_a^i \sigma_c^j$ operations on each cluster state in the 2P sequence. In advance, they agree that $\sigma^i \sigma^j$ corresponds to a four-bit classical message, for example, $\sigma^0\sigma^0 \to 0000$, $\sigma^0\sigma^1 \to 0001$, $\sigma^0\sigma^2 \to 0010, \ldots, \sigma^3\sigma^3 \to 1111$. Next, Alice inserts the k particles into the 2P sequence and sends the 2P sequence including the k particles to Bob.

(4) After Bob receives the 2P sequence, they check whether it is transmitted safely. First, Alice tells Bob the position of each k particle in the sequence and the state of each k particle. Then, Bob measures each k particle with a correct measuring basis. By comparing his measuring outcomes with Alice's announcing states, Bob can judge whether the 2P sequence is eavesdropped. Obviously, its security check is the same as that of the 1P sequence. Next, Bob gets rid of k particles, and encodes his secret messages by performing $\sigma_a^i \sigma_c^j$ operations on each cluster state in the 2P sequence.

(5) After his encoding, Bob makes a cluster state measurement on each four particles in the 2P sequence in order, and publishes his measurement outcomes. According to Bob's

publishing measurement outcomes, Alice is able to deduce his secret messages. Meanwhile, Bob is also able to deduce Alice's. For example, let us assume that the cluster state prepared by Alice is $|C_4^{00}\rangle_{abcd}$, and her and Bob's performing secret operations are $\sigma^2\sigma^3$ and $\sigma^0\sigma^0$, respectively. The $|C_4^{00}\rangle_{abcd}$ evolves as follows:

$$\left|C_4^{00}\right\rangle_{abcd} \quad \Rightarrow \quad \sigma_a^2\sigma_c^3\left|C_4^{00}\right\rangle_{abcd} = \left|C_4^{23}\right\rangle_{abcd} \quad \Rightarrow \quad \sigma_a^0\sigma_c^0\left|C_4^{23}\right\rangle_{abcd} = \left|C_4^{23}\right\rangle_{abcd} \tag{2}$$

The last result $|C_4^{23}\rangle_{abcd}$ is measured and published by Bob. Obviously, according to three known messages: $|C_4^{00}\rangle_{abcd}$, $\sigma^2\sigma^3$ and $|C_4^{23}\rangle_{abcd}$, Alice can deduce that Bob's secret operation is $\sigma^0\sigma^0$. Since Bob has obtained the information of cluster states in the 1P sequence and the 1P sequence and the 2P sequence are entirely identical, the $|C_4^{00}\rangle_{abcd}$ prepared by Alice is also known by Bob. Therefore, according to three messages: $|C_4^{00}\rangle_{abcd}$, $\sigma^0\sigma^0$ and $|C_4^{23}\rangle_{abcd}$, Bob can also deduce that Alice's operation is $\sigma^2\sigma^3$. So Alice and Bob can simultaneously transmit the secret messages each other.

So far, we have successfully established this BQSC protocol using one-dimensional four-particle cluster states. In this protocol, there are two same processes of security check, which are finished by employing decoy particles. Later on, we will give the reason why the two processes can prevent eavesdropper from eavesdropping. Next, let us calculate the efficiency of this BQSC protocol. Here, we employ Cabello's definition of the efficiency [35]: $\eta = \frac{b_s}{q_t+b_t}$; η denotes the efficiency, b_s is the expected secret bits received, q_t and b_t are the qubit used and the classical bits exchanged between Alice and Bob, respectively. Obviously, in the case that the wasting quantum and classical bits in the checking eavesdropping aren't taken count of, b_s equals to 8 bits in our protocol, and q_t and b_t equal to 8 and 4 bits, respectively. So the efficiency of our protocol η equals to 66.7 %.

3 Security of Our BQSC Protocol

In the ahead Introduction, we have claimed that the information leakage doesn't exist also in our BQSC protocol. Next, let us analyze why not to exist. In Step (5), we see that Bob only publishes one cluster state measurement outcome, that is, the $|C_4^{23}\rangle_{abcd}$ in the given example. And the $|C_4^{00}\rangle_{abcd}$ is only known by Alice and Bob, and is not published. In other words, the $|C_4^{00}\rangle_{abcd}$ is entirely secret for a outsider. In addition, we still see that the operation combination of Alice and Bob may be arbitrary. So there are 16×16 operation combinations. Provided that 16×16 combinations have equal probability, the channel contains $-\sum p_i \log p_i = -(16 \times 16) \times \frac{1}{16\times 16} \log \frac{1}{16\times 16} = 8$ bits secret messages. On the beam, the quantity of the exchanged messages between Alice and Bob is 8 bits also. Clearly, the information leakage doesn't exist in our BQSC protocol.

As we all know, that the information leakage happens doesn't require the eavesdropper's positive attack. So we can't help asking that, when eavesdropper's positive attack occurs, our BQSC protocol is still secure? In what follows, we will reply this.

We see that, in our BQSC protocol, two same sequences composed of one-dimensional four-particle cluster states are transmitted from Alice to Bob and the methods that check whether they are transmitted safely are same, and both depend on the inserting and measuring decoy particles. That is, after Bob receives each sequence, Alice publishes the states of decoy particles and Bob measures every decoy particle with the proper basis, and then he can decide the error rate of each sequence transmission by comparing his measurement outcomes with Alice's announcing states. This kind of method is very valid to stand against the following common attacks. (i) *The intercept-resend attack* When the 1P sequence is

traveling from Alice to Bob, the eavesdropper intercepts it and sends a fake sequence in which each particle is in one of the four states ($|0\rangle$, $|1\rangle$, $|+\rangle$, $|-\rangle$) to Bob. Her purpose is to plan to eavesdrop the information of cluster states in the 1P sequence. Since the intercepted 1P sequence contains the j particles, the eavesdropper must get rid of them firstly. Obviously, this is easily done. As soon as Alice publishes the positions of the j particles, the eavesdropper can. However, when Bob measures the j particles in order to check the security, the eavesdropper's intercepting action will be detected. This is because the particles Bob really measures are not the j particles, but from the eavesdropper's fake sequence. We know it is impossible that the states of the measured particles and the states of the j particles are entirely identical. Thus, this kind of attack has to introduce a big error rate. (ii) *The entangle-measure attack* The eavesdropper intercepts the 1P sequence while it is traveling between Alice and Bob. Then she performs a general operation on the particle in the 1P sequence and the auxiliary particle that she prepares in advance. By observing the auxiliary particle, the eavesdropper tries to obtain some useful messages. In what follows, we will analyze whether this kind of attack can be detected. We see that the 1P sequence contains the j particles, and since each j particle is randomly prepared in one of the four states by Alice, its state is $\rho = \frac{1}{2}(|0\rangle\langle 0| + |1\rangle\langle 1|)$ for the eavesdropper. Suppose that the eavesdropper's auxiliary particle is prepared in $|\varepsilon\rangle$ and her general operation is U_e. When the eavesdropper performs U_e on the j particle and the auxiliary particle, we will see:

$$U_e|0\rangle|\varepsilon\rangle = \alpha_0|0\rangle|\varepsilon_{00}\rangle + \beta_0|1\rangle|\varepsilon_{01}\rangle$$
$$U_e|1\rangle|\varepsilon\rangle = \alpha_1|0\rangle|\varepsilon_{00}\rangle + \beta_1|1\rangle|\varepsilon_{01}\rangle$$

Where, $|\varepsilon_{00}\rangle$, $|\varepsilon_{01}\rangle$, $|\varepsilon_{10}\rangle$, $|\varepsilon_{11}\rangle$ are the eavesdropper's states. Because U_e is the general operation, the complex number α_0, α_1, β_0, β_1 satisfy $|\alpha_0|^2 + |\beta_0|^2 = |\alpha_1|^2 + |\beta_1|^2 = 1$. The error rate introduced by the eavesdropper is $\epsilon = |\beta_0|^2 = |\alpha_1|^2 = 1 - |\beta_1|^2 = 1 - |\alpha_0|^2$. Clearly, this kind of attack will also be detected.

4 Conclusion

In summary, by using one-dimensional four-particle cluster states, decoy particles [36–38] and the special "two-step" transmission [2], we have successfully proposed a BQSC protocol. The highlights of this protocol are as follows: (i) It is the first time that the quantum channels of BQSC are composed of the cluster states, (ii) This protocol needn't cost the expensive quantum entanglement source in checking eavesdropping, (iii) The information leakage does not exist in this protocol. Compared with the listed protocols [24–28], the biggest difference is that we use one-dimensional four-particle cluster states as quantum channels of BQSC. In addition, in the efficiency, this protocol is equal with the listed protocols [24, 25]. Finally, we explain why the "two-step" transmission in this protocol is special. This is because it differs from the original "two-step" transmission [2], where the two transmitted sequences have the entangled correlation. However, the two ones in this protocol have not.

Acknowledgements This work is supported by the National Natural Science Foundation of China under grant No. 11205115 and by Anhui Provincial Natural Science Foundation under grant No. 1308085QA20.

References

1. Bennett, C.H., Brassard, G.: In: Proceedings of the IEEE International Conference on Computers, Systems and Signal Processings, Bangalore, India, p. 175. IEEE, New York (1984)
2. Long, G.L., Liu, X.S.: Phys. Rev. A **65**, 032302 (2002)
3. Wen, K., Long, G.L.: Phys. Rev. A **72**, 022336 (2005)
4. Gao, G.: Opt. Commun. **281**, 876 (2008)
5. Gao, G.: Commun. Theor. Phys. **51**, 820 (2009)
6. Gao, G.: Phys. Scr. **81**, 065005 (2010)
7. Gao, G.: Int. J. Theor. Phys. **49**, 1870 (2010)
8. Beige, A., Englert, B.G., Kurtsiefer, Ch., Weinfurter, H.: Acta Phys. Pol. A **101**, 357 (2002)
9. Boström, K., Felbinger, T.: Phys. Rev. Lett. **89**, 187902 (2002)
10. Deng, F.G., Long, G.L., Liu, X.S.: Phys. Rev. A **68**, 042317 (2003)
11. Deng, F.G., Long, G.L.: Phys. Rev. A **69**, 052319 (2004)
12. Yan, F.L., Zhang, X.: Eur. Phys. J. B **41**, 75 (2004)
13. Cai, Q.Y., Li, B.W.: Chin. Phys. Lett. **21**, 601 (2004)
14. Xia, Y., Song, H.S.: Phys. Lett. A **364**, 117 (2007)
15. Lucamarini, M., Mancini, S.: Phys. Rev. Lett. **94**, 140501 (2005)
16. Man, Z.X., Zhang, Z.J., Li, Y.: Chin. Phys. Lett. **22**, 22 (2005)
17. Zhu, A.D., Xia, Y., Fan, Q.B., Zhang, S.: Phys. Rev. A **73**, 022338 (2006)
18. Li, X.H., Deng, F.G., Zhou, H.Y.: Phys. Rev. A **74**, 054302 (2006)
19. Wang, C., Deng, F.G., Li, Y.S., Liu, X.S., Long, G.L.: Phys. Rev. A **71**, 044305 (2005)
20. Han, L.F., Chen, Y.M., Yuan, H.: Commun. Theor. Phys. **51**, 648 (2009)
21. Shi, J., Gong, Y.X., Xu, P., Zhu, S.N., Zhan, Y.B.: Commun. Theor. Phys. **56**, 831 (2011)
22. Nguyen, B.A.: Phys. Lett. A **328**, 6 (2004)
23. Gao, F., Guo, F.C., Wen, Q.Y., Zhu, F.C.: Sci. China, Ser. G, Phys. Mech. Astron. **51**, 559 (2008)
24. Shi, G.F., Xi, X.Q., Hu, M.L., Yue, R.H.: Opt. Commun. **283**, 1984 (2010)
25. Gao, G.: Opt. Commun. **283**, 2288 (2010)
26. Yang, C., Hwang, T.: Quantum Inf. Process. **12**, 2131 (2013)
27. Li, Y., Li, X., Sang, M., Nie, Y., Wang, Z.: Quantum Inf. Process. **12**, 3835 (2013)
28. Zhou, N., Wu, G., Gong, L., Liu, S.: Int. J. Theor. Phys. **52**, 3204 (2013)
29. Briegel, H.J., Raussendorf, R.: Phys. Rev. Lett. **86**, 910 (2001)
30. Yuan, H., Liu, Y.M., Zhang, Z.J.: Phys. Lett. A **372**, 5938 (2008)
31. Han, L.F., Yuan, H.: Int. J. Quantum Inf. **06**, 1093 (2008)
32. Han, L.F., Yuan, H.: Int. J. Quantum Inf. **09**, 539 (2011)
33. Han, L.F., Xu, H.F.: Int. J. Theor. Phys. **51**, 2540 (2012)
34. Han, L.F., Yuan, H.: Indian J. Phys. **87**, 777 (2013)
35. Cabello, A.: Phys. Rev. Lett. **85**, 5635 (2000)
36. Li, C.Y., Zhou, H.Y., Wang, Y., Deng, F.G.: Chin. Phys. Lett. **22**, 1049 (2005)
37. Hwang, W.Y.: Phys. Rev. Lett. **91**, 057901 (2003)
38. Wang, X.B.: Phys. Rev. A **72**, 012322 (2005)