Int J Theor Phys (2015) 54:100–105
DOI 10.1007/s10773-014-2205-7

Quantum Secure Direct Communication Achieved by Using Multi-Entanglement

Wenlin Li · Junbo Chen · Xiaolong Wang · Chong Li

Received: 14 January 2014 / Accepted: 22 May 2014 / Published online: 1 July 2014

Abstract A quantum secure direct communication (QSDC) scheme is proposed based on multi-body entangled system in this paper. The mathematical description of the QSDC scheme is given firstly and the process of direct communication is investigated. The communication scheme based on multi-body entangled system and the general method of information coding are further completed. Finally, a communication scheme using four-body systems is introduced as example.

Keywords QSDC · Multi-body entangled system · Information coding · Mathematical description

1 Introduction

Quantum communication is one of the important components of quantum information. The basic idea is that classical or quantum information can be transmitted through a quantum channel. Quantum communication exhibits better security and higher capability which can't be replaced by the classic communication because quantum mechanics takes on some unique natures, for examples, quantum coherence, quantum non-cloning, etc. Therefore, quantum communication has many potential applications in the military, secure communication, signal transmission and other fields [1–6].

In all quantum communication schemes reported previously, the quantum secure direct communication (QSDC) is an ideal scheme and has attracted comprehensive attention quickly. Its advantages are the quantum key does not need to appoint in advance and the quantum entanglement is used to achieve secure bidirectional communication. Since Beige et al. proposed QSDC ideas [7], Boström et al., Deng et al. have designed a ping-pong

W. Li · J. Chen · X. Wang · C. Li (✉)
School of Physics and Optoelectronic Engineering, Dalian University of Technology,
Dalian 116024, China
e-mail: lichong@dlut.edu.cn

protocol and a two-step protocol, respectively [8, 9]. The safety is discussed and a specific operation scheme for quantum direct communication processes is proposed. After that, Cao et al. extended information carrier of the schemes from the Bell state of two-body to w state of three-body [10]. Deng et al. discussed further QSDC security [11]. Recently, Lin et al. designed the QSDC scheme based on χ-type entangled states [12] and Yu et al. investigated the QSDC scheme based on non-orthogonal state [13]. These fruitful works establish a solid foundation for the theoretical and application research of QSDC.

So far, the investigations about QSDC schemes are mainly two-body or three-body entangled system, which has exposed limitations in the direct communication. Not only less information is transferred in a single communication and all particles are intercepted easily by attacker owing to the constitution with limited number particles, but also the difficulty of physical realization is increased because of the influence of physical implementation in which communication scheme is confined on two-body or three-body particles. In recent years, Barreior et al. researched photonic superdense coding by using pairs of photons entangled in their spin and orbital angular momentum, and achieved a dense-coding experiment with a large channel capacity [14]. Subsequently, a experimental demonstration of a hyper-entangled Schröinger cat state have also been reproted [15]. These achievements make it valuable to discuss a high-dimensional quantum communication process. In view of the above reasons, the QSDC scheme based on multi-body entangled system to complete the direct communication is proposed in this paper. Firstly, we give the mathematical description of the QSDC scheme and analyze the process of direct communication based on multi-body entangled system. At the same time, we design a general method of information coding. The communication model based on four-body systems is taken as an example to validate the effectiveness of the scheme proposed in our work. The results show that the scheme is of universal and convenient because the specific communication scheme can be designed expediently according to the required number of particles in practical physics system.

This paper is organized as follows. In Section 2 the general design method of QSDC based on multi-body particle system and the corresponding mathematical description are given. In Section 3 the QSDC communication process based on *2m* entangled system is investigated, and QSDC scheme using four-body entangled system to complete the direct communication is taken as an example. Finally we conclude our results in Section 4.

2 The Basic Processes of QSDC and the Mathematical Description

2.1 The Basic Processes of QSDC

The QDCS scheme based on two-body two-level system has been investigated repeatedly since the concept of quantum direct communication has been proposed. Here, we give a universal process of realizing quantum direct communication scheme base on the existing ones.

Assume that S is a complete set of orthogonal basis vectors in n dimensional Hilbert space. $U = U_A \otimes U_B$ is conversion operator set and the operator in U can change every state in S to another, i.e.

$$S = \{|\psi_1\rangle, |\psi_2\rangle, \cdots, |\psi_n\rangle\}, \langle\psi_i|\psi_j\rangle = \delta_{ij} \tag{1}$$

$$U_A = \left\{U_A^1, U_A^2, \cdots, U_A^n\right\}, U_B = \left\{U_B^1, U_B^2, \cdots, U_B^n\right\}, \quad U^i U^{i\dagger} = I \tag{2}$$

The basic process of quantum direct communication can be formed by the following steps:

a. Alice and Bob, who want to communicate, engage a same arbitrary state $|\Psi_k\rangle$ chosen from the set S before communication, take it as the initial state and share a EPR-pair which on this state. At the same time, they encode for each operation in U_A and U_B.
b. In communication, Alice and Bob do the local operations for their particles respectively using the operation corresponding with their information transferred.
c. Alice sends all the particles owned by herself to Bob. Then Bob measures all the particles in the basis S and announces the measurement results.

This moment, Alice and Bob have known respectively the information as follows: the selected initial state, the measurement results of final state and the operations done by themselves. Therefore, they can figure out operations in the opposite side based on the decode formula and seize information each other. It should be noted that the scheme would return to the common QSDC scheme based on two-body system if taking $S = \{\left|\phi^+\right\rangle, \left|\phi^-\right\rangle, \left|\varphi^+\right\rangle, \left|\varphi^+\right\rangle$ and $U_A = U_B = \{\sigma_0, \sigma_x, i\sigma_y, \sigma_z\}$.

2.2 The Mathematical Description of QSDC Scheme

A simple representation method will be given for two-body quantum state [16–18].

Suppose vector

$$\mathbf{e} = (|0\rangle, |1\rangle, \cdots, |n\rangle) \tag{3}$$

$$\tilde{\mathbf{e}}^{\mathbf{T}} = (\langle 0|, \langle 1|, \cdots, \langle n|)^{\mathbf{T}} \tag{4}$$

And for a given two-body state $|\psi_k\rangle_{AB}$, it can be expressed as

$$|\psi_k\rangle_{AB} = \mathbf{e}T_k\tilde{\mathbf{e}}^{\mathbf{T}} \tag{5}$$

here, T_k is a coefficient matrix which is used to represent the quantum state $|\psi_k\rangle_{AB}$.

Then, two particles are operated by U_A^i and U_B^j, respectively.

$$U_A^i \otimes U_B^j \, |\psi_k\rangle_{AB} \tag{6}$$

also be written as

$$U_A^i T_k U_B^{jT} \tag{7}$$

Thus, the quantum direct communication process described above can be thought of as the mathematical process as follow:

$$\begin{aligned} &\forall\, |\Psi_k\rangle_{AB} \in S, \\ &\forall U_A^i \otimes U_B^j \in U_A \otimes U_B, \\ &\exists\, |\Psi_m\rangle_{AB} \in S, \\ &|\Psi_m\rangle_{AB} = U_A^i \otimes U_B^j |\Psi_k\rangle_{AB} \end{aligned} \tag{8}$$

According to the forms of (5)–(7), (8) can be expressed as

$$T_m = U_A^i T_k U_B^{jT} \tag{9}$$

so, the decode formula based on (9) can be derived as

$$U_A^i = T_m \left(U_B^{jT}\right)^{-1} (T_k)^{-1} \tag{10}$$

$$U_B^{jT} = (T_k)^{-1} \left(U_A^i\right)^{-1} T_m \tag{11}$$

3 The QSDC Based on Multi-Body Particles

It is unnecessary to consider the dimension of the set S in the quantum direct communication process above-mentioned, so the scheme can be extended to any numbers of particles so long as an apposite set of complete orthogonal basis vectors S and a set of conversion operators U which corresponds with S are found. The key of designing a QSDC scheme was reduced to find a complete orthogonal basis set S and the corresponding set of conversion operators U. In this section, a QSDC scheme based on a four-body two-level system is proposed, and on this basis, the general design method of a QSDC scheme based on multi-body particles is discussed.

Assume that four-body particles with the following state are used to communicate directly:

$$|\psi_0\rangle_{1234} = \frac{1}{2}[|00\rangle_{13}|00\rangle_{24} + |01\rangle_{13}|01\rangle_{24} + |10\rangle_{13}|10\rangle_{24} + |11\rangle_{13}|11\rangle_{24}] \tag{12}$$

If let $|00\rangle \to |0\rangle$, $|01\rangle \to |1\rangle$, $|10\rangle \to |2\rangle$ and $|11\rangle \to |3\rangle$, The state describing four-body can be rewritten as a "two-body like" state, i.e.

$$|\psi_0\rangle = \frac{1}{2}[|0\rangle|0\rangle + |1\rangle|1\rangle + |2\rangle|2\rangle + |3\rangle|3\rangle] \tag{13}$$

Therefore, a set of complete orthogonal vectors basis S can be written as:

$$\begin{aligned}
S = \\
\Big\{ &|\psi_0\rangle = \tfrac{1}{2}[|0\rangle\,|0\rangle + |1\rangle\,|1\rangle + |2\rangle\,|2\rangle + |3\rangle\,|3\rangle],\ |\psi_1\rangle = \tfrac{1}{2}[|0\rangle\,|0\rangle + |1\rangle\,|1\rangle - |2\rangle\,|2\rangle - |3\rangle\,|3\rangle], \\
&|\psi_2\rangle = \tfrac{1}{2}[|0\rangle\,|0\rangle - |1\rangle\,|1\rangle - |2\rangle\,|2\rangle + |3\rangle\,|3\rangle],\ |\psi_3\rangle = \tfrac{1}{2}[|0\rangle\,|0\rangle - |1\rangle\,|1\rangle + |2\rangle\,|2\rangle - |3\rangle\,|3\rangle], \\
&|\psi_4\rangle = \tfrac{1}{2}[|0\rangle\,|3\rangle + |1\rangle\,|2\rangle + |2\rangle\,|1\rangle + |3\rangle\,|0\rangle],\ |\psi_5\rangle = \tfrac{1}{2}[|0\rangle\,|3\rangle + |1\rangle\,|2\rangle - |2\rangle\,|1\rangle - |3\rangle\,|0\rangle], \\
&|\psi_6\rangle = \tfrac{1}{2}[|0\rangle\,|3\rangle - |1\rangle\,|2\rangle - |2\rangle\,|1\rangle + |3\rangle\,|0\rangle],\ |\psi_7\rangle = \tfrac{1}{2}[|0\rangle\,|3\rangle - |1\rangle\,|2\rangle + |2\rangle\,|1\rangle - |3\rangle\,|0\rangle], \\
&|\psi_8\rangle = \tfrac{1}{2}[|0\rangle\,|1\rangle + |1\rangle\,|0\rangle + |2\rangle\,|3\rangle + |3\rangle\,|2\rangle],\ |\psi_9\rangle = \tfrac{1}{2}[|0\rangle\,|1\rangle + |1\rangle\,|0\rangle - |2\rangle\,|3\rangle - |3\rangle\,|2\rangle], \\
&|\psi_{10}\rangle = \tfrac{1}{2}[|0\rangle\,|1\rangle - |1\rangle\,|0\rangle - |2\rangle\,|3\rangle + |3\rangle\,|2\rangle],\ |\psi_{11}\rangle = \tfrac{1}{2}[|0\rangle\,|1\rangle - |1\rangle\,|0\rangle + |2\rangle\,|3\rangle - |3\rangle\,|2\rangle], \\
&|\psi_{12}\rangle = \tfrac{1}{2}[|0\rangle\,|2\rangle + |1\rangle\,|3\rangle + |2\rangle\,|0\rangle + |3\rangle\,|1\rangle],\ |\psi_{13}\rangle = \tfrac{1}{2}[|0\rangle\,|2\rangle + |1\rangle\,|3\rangle - |2\rangle\,|0\rangle - |3\rangle\,|1\rangle], \\
&|\psi_{14}\rangle = \tfrac{1}{2}[|0\rangle\,|2\rangle - |1\rangle\,|3\rangle - |2\rangle\,|0\rangle + |3\rangle\,|1\rangle],\ |\psi_{15}\rangle = \tfrac{1}{2}[|0\rangle\,|2\rangle - |1\rangle\,|3\rangle + |2\rangle\,|0\rangle - |3\rangle\,|1\rangle], \Big\}
\end{aligned} \tag{14}$$

It is known from above discussion that once an apposite U corresponding S can be found, the design of the scheme can be completed. Here, a convenient method of finding the set U is given.

All the states in S can be predigested firstly into the format given in Section 2.2 and a coefficient matrix set T will be obtained. Afterward, the matrix in T is transformed to the unitary matrix $T' \in S$.

$$
\begin{aligned}
S = &\left\{ \begin{pmatrix} 1&0&0&0\\0&1&0&0\\0&0&1&0\\0&0&0&1 \end{pmatrix}, \begin{pmatrix} 1&0&0&0\\0&1&0&0\\0&0&-1&0\\0&0&0&-1 \end{pmatrix}, \begin{pmatrix} 1&0&0&0\\0&-1&0&0\\0&0&-1&0\\0&0&0&1 \end{pmatrix}, \begin{pmatrix} 1&0&0&0\\0&-1&0&0\\0&0&1&0\\0&0&0&-1 \end{pmatrix} \right.\\
&, \begin{pmatrix} 0&0&0&1\\0&0&1&0\\0&1&0&0\\1&0&0&0 \end{pmatrix}, \begin{pmatrix} 0&0&0&1\\0&0&1&0\\0&-1&0&0\\-1&0&0&0 \end{pmatrix}, \begin{pmatrix} 0&0&0&1\\0&0&-1&0\\0&-1&0&0\\1&0&0&0 \end{pmatrix}, \begin{pmatrix} 0&0&0&1\\0&0&-1&0\\0&1&0&0\\-1&0&0&0 \end{pmatrix}\\
&, \begin{pmatrix} 0&1&0&0\\1&0&0&0\\0&0&0&1\\0&0&1&0 \end{pmatrix}, \begin{pmatrix} 0&1&0&0\\1&0&0&0\\0&0&0&-1\\0&0&-1&0 \end{pmatrix}, \begin{pmatrix} 0&1&0&0\\-1&0&0&0\\0&0&0&-1\\0&0&1&0 \end{pmatrix}, \begin{pmatrix} 0&1&0&0\\-1&0&0&0\\0&0&0&1\\0&0&-1&0 \end{pmatrix}\\
&\left., \begin{pmatrix} 0&0&1&0\\0&0&0&1\\1&0&0&0\\0&1&0&0 \end{pmatrix}, \begin{pmatrix} 0&0&1&0\\0&0&0&1\\-1&0&0&0\\0&-1&0&0 \end{pmatrix}, \begin{pmatrix} 0&0&1&0\\0&0&0&-1\\-1&0&0&0\\0&1&0&0 \end{pmatrix}, \begin{pmatrix} 0&0&1&0\\0&0&0&-1\\1&0&0&0\\0&-1&0&0 \end{pmatrix} \right\}
\end{aligned}
\tag{15}
$$

The operation set U can be expressed after rewriting the T':

$$
\begin{aligned}
U = \{&\sigma_0 \otimes \sigma_0, \sigma_z \otimes \sigma_0, \sigma_z \otimes \sigma_z, \sigma_0 \otimes \sigma_z, \sigma_x \otimes \sigma_x, i\sigma_y \otimes \sigma_x, i\sigma_y \otimes i\sigma_y, \sigma_x \otimes i\sigma_y,\\
&\sigma_0 \otimes \sigma_x, \sigma_z \otimes \sigma_x, \sigma_z \otimes i\sigma_y, \sigma_0 \otimes i\sigma_y, \sigma_x \otimes \sigma_0, i\sigma_y \otimes \sigma_0, i\sigma_y \otimes \sigma_z, \sigma_x \otimes \sigma_z\}
\end{aligned}
\tag{16}
$$

where $\sigma_i \otimes \sigma_j$ means that σ_i is used to act on the first particle and σ_j to act on the second particle.

The QSDC can be performed while Alice and Bob encode and operate by using the operators in (16), respectively.

At this point, a QSDC scheme based on $2m$-body 2-level particles ($m \in N$) can be summarized as following:

a. Alice and Bob, who want to communicate, rewrite the $2m$-body state as a "two-body like" state and find the set S of complete orthogonal vectors.
b. Alice and Bob get the coefficient matrix T corresponding with each state in S and transform them to the unitary matrix. In the process, the operation operator set U can be found and the information can be encoded into each conversion operator.
c. Alice and Bob prepare the particles held by themselves on the engaged initial state and each person holds m particles.
d. In communication, Alice and Bob do the local operations for their particles respectively using the operation corresponding with their information transferred.
e. Alice sends all the particles she owned to Bob. Then, Bob measures all the particles in the basis S and announces.
f. Based on the measurement results and added operation, Alice and Bob can figure out respective information by the decoding formula (10) and (11).

4 Conclusion

The process of the direct communication using multi-body entangled system is presented in this paper and its mathematical description is given on the basis of the existing QSDC scheme of two-body system. A four-body system is taken further as an example to research the QSDC scheme based on multi-body particles and the general design method of QSDC scheme based on $2m$-body system is concluded. This work provides the theoretical basis for realizing QSDC scheme and the communication scheme required can be designed conveniently according to the number of particles in practical physical system because the method proposed in our work exhibits universality.

Acknowledgments This work was supported by the National Nature Science Foundation of China (under Grant No.11105021 and No.11175033), the Fundamental Research Funds for the Central Universities (DUT13LK05) and Training Program of Innovation and Entrepreneurship for Undergraduates of DUT (Grant No. 201210141204).

References

1. Liu, Y., Ju, L., Liang, X.L., Tang, S.B., Shen Tu, G.L., Zhou, L., Peng, C.Z., Chen, K., Chen, T.Y., Chen, Z.B., Pan, J.W.: Experimental demonstration of counterfactual quantum communication. Phys. Rev. Lett. **109**(3), 030501–5 (2012)
2. Wang, Z.M., Wu, L.A.: Central symmetry in two-dimensional lattices and quantum information transmission. Phys. Rev. A **87**(6), 064301–4 (2013)
3. Muschik, C.A., Hammerer, K., Polzik, E.S., Cirac, I.J.: Quantum teleportation of dynamics and effective interactions between remote systems. Phys. Rev. Lett. **111**(2), 020501–5 (2013)
4. Cardillo, A., Galve, F., Zueco, D., Gómez-Gardeñes, J.: Information sharing in quantum complex networks. Phys. Rev. A **87**(5), 052312–7 (2013)
5. Xia, Y., Yang, K.Y.: Joint remote preparation of a general three-qubit state via non-maximally GHZ states. Int. J. Theor. Phys. **51**(5), 1647–1654 (2012)
6. Xia, Y., Song, H.S.: Controlled quantum secure direct communication using a non-symmetric quantum channel with quantum superdense coding. Phys. Lett. A **364**(2), 117–122 (2007)
7. Beige, A., Englert, B.G., Kurtsiefer, C., Weinfurter, H.: Secure communication with single-photon two-qubit states. J. Phys. A: Math. Gen. **35**(28), 407–413 (2002)
8. Boström, K., Felbinger, T.: Deterministic secure direct communication using entanglement. Phys. Rev. Lett. **89**(18), 187902–4 (2002)
9. Deng, F.G., Long, G.L., Liu, X.S.: Two-step quantum direct communication protocol using the Einstein-Podolsky-Rosen pair block. Phys. Rev. A **68**(4), 042317–6 (2003)
10. Cao, H.J., Song, H.S.: Quantum secure direct communication with W state. Chin. Phys. Lett. **23**(2), 290–292 (2006)
11. Deng, F.G., Li, X.H., Li, C.Y., Zhou, P., Zhou, H.Y.: Eavesdropping on the 'ping-pong' quantum communication protocol freely in a noise channel. Chin. Phys. **16**(2), 277–281 (2007)
12. Lin, S., Wen, Q.Y., Gao, F., Zhu, F.C.: Quantum secure direct communication with χ-type entangled states. Phys. Rev. A **78**(6), 064304–4
13. Yu, C.H., Guo, G.D., Lin, S.: Quantum secure direct communication with authentication using two nonorthogonal states. Int. J. Theor. Phys. **52**(6), 1937–1945 (2013)
14. Barreiro, J.T., Wei, T.C., Kwiat, P.G.: Beating the channel capacity limit for linear photonic superdense coding. Nat. Phys. **4**(4), 282–286 (2008)
15. Gao, W.B., Lu, C.Y., Yao, X.C., Xu, P., Gühne, O., Goebel, A., Chen, Y.A., Peng, C.Z., Chen, Z.B., Pan, J.W.: Experimental demonstration of a hyper-entangled ten-qubit Schröinger cat state. Nat. Phys. **6**(5), 331–335 (2010)
16. Li, C., Song, H.S., Luo, Y.X.: Criterion for general quantum teleportation. Phys. Lett. A **29**(3–4), 121–125 (2002)
17. Li, C., Song, H.S., Zhou, L.: Alternative notation for quantum information theory. Int. J. Theor. Phys. **46**(7), 1815–1822 (2007)
18. Wang, Z., Tian, L.J., Cao, W.Z.: Conditions for bipartite general Bell states. Int. J. Quantum. Inf. **8**(7), 1213–1217 (2010)