Int J Theor Phys (2010) 49: 1775–1780
DOI 10.1007/s10773-010-0358-6

Three-Party Quantum Secure Sharing Using a Four-Particle Cluster State and Driven Cavity QED

C.-J. Shan · J.-B. Liu · T. Chen · W.-W. Cheng · T.-K. Liu · Y.-X. Huang · H. Li

Received: 18 February 2010 / Accepted: 13 April 2010 / Published online: 22 April 2010

Abstract We propose a scheme for implementing three-party quantum secure sharing via a four-particle cluster state in driven cavity QED. In our protocol, each of the two receivers can read out the sender's secret communication message only if they choose to cooperate with each other. The protocol does not require the joint Bell-state measurement needed in the previous schemes and can considerably reduce the realization difficulty in experiment. Moreover, the cavity is only virtually excited and thus is insensitive to the cavity decay and the thermal field. The probability of success in our scheme can reach 1.0.

Keywords Quantum secret sharing · Four-particle cluster state · Driven cavity QED

1 Introduction

Quantum secret sharing (QSS), an important branch of quantum communication, is the generalization of classical secret sharing into a quantum scenario. The basic idea of secret sharing in a simple case is that Alice wants to send a secret message to two distant parties, Bob and Charlie. If and only if when they cooperate, can they get complete information about the message. Meanwhile, if one of them is dishonest, the honest players may keep the dishonest one from doing any damage. An original QSS scheme [1] was proposed by Hillery, Buzek, and Berthiaume in 1999 through using three-particle or four-particle entangled Greenberger-Horne-Zeilinger (GHZ) states for distributing a private key among some agents and sharing classical information. Since then, many QSS protocols [2–11] have been proposed in both theoretical and experimental aspects. Li et al. proposed a multiparty quantum secret sharing (MQSS) protocol using a multi-particle GHZ-basis measurement. Zhang et al. proposed a MQSS protocol based on entanglement swapping by using three Einstein-Podolsky-Rosen (EPR) pairs and a Bell measurement. The above schemes, the entangled states as quantum channel are EPR pairs, GHZ class states, or W class states. Tripartite entangled states can be classified into two inequivalent classes, the Greenberger-Horne-Zeilinger (GHZ) class

C.-J. Shan (✉) · J.-B. Liu · T. Chen · W.-W. Cheng · T.-K. Liu · Y.-X. Huang · H. Li
College of Physics and Electronic Science, Hubei Normal University, Huangshi 435002, China
e-mail: shanchuanjia@yahoo.com.cn

and the W class. While, the four-particle entangled state was divided to different families of states under stochastic local operations and classical communication (SLOCC). Recently, Briegel and Raussendorf introduced an interesting type of multi-qubit entangled states, i.e., the so-called cluster states [12]. This kind of states have high persistence of entanglement, and can be regarded as an entanglement resource for the GHZ states but are more immune to decoherence than them. The cluster states have extensive applications in quantum physics. Many theoretical schemes of generating cluster states have been proposed in different types of physical systems, such as linear optical systems [13], cavity QED [14], and other kinds of systems [15]. Experimentally, Mandel et al. [16] prepare the cluster state of neutral atom in optical lattice. Walther et al. [17] have generated four-photon cluster states and demonstrated the feasibility of the one-way quantum computation.

On the other hand, the microwave cavity QED, with Rydberg atoms crossing superconducting cavities, provides an almost ideal system for the realization of quantum information processing. Cavity quantum electrodynamics (QED) technique has been proven to be a promising candidate for the physical realization of quantum information processing. The cavity usually acts as memory in quantum information processing, thus the decoherence of the cavity field becomes one of the main obstacles for the implementation of quantum information in cavity QED. Zheng and Guo proposed a novel scheme [18], which greatly prolongs the efficient decoherence time of the cavity. Osnaghi et al. [19] had experimentally implemented the scheme using two Rydberg atoms crossing a nonresonant cavity. Zou et al. [20] proposed a scheme for QDC with theory of QSS in the cavity QED.

In this paper, we propose a protocol for three-party quantum secure sharing by using a four-particle cluster state and driven cavity QED. Compared with the previous schemes, our protocol has the following notable advantage: The scheme utilizes a four-particle cluster state as the quantum channel. In our scheme, the cavity is only virtually excited and thus the efficient decoherence time of the cavity is greatly prolonged. Alice does operation on her particle with one of unitary operators. Because there are four choices, they justly represent two-bits classical information. The secret messages are imposed on the particle. The transmitted particles do not carry any useful secret messages, the sender encodes the secret message and transmits it to the receiver by using the separate measurement, which ensures the security of our protocol. Instead of performing unitary operations to recover Alice's secret message, the receivers measure the particles and recover Alice's secret message according to the correlation between the measurement results. The scheme in the paper overcame the difficulty of Bell state measurement, not the joint Bell-state measurement but the separate measurement is necessary in the cavity QED. Due to these advantages our scheme may open promising prospects for quantum-information manipulation.

2 The Model

Here, we consider the interaction of a single mode in a cavity of high quality factor with two identical two-level atoms. At the same time, the two atoms are driven by a classical field. The interaction between atoms and the cavity can be described as follows:

$$H = \omega_0 \sum_{j=1}^{2} (S_j^z) + \omega_a a^\dagger a + \sum_{j=1}^{2} [g(a^\dagger S_j^- + a S_j^+) + \Omega(S_j^+ e^{-i\omega_d t} + S_j^- e^{i\omega_d t})], \qquad (1)$$

where ω_0, ω_a and ω_d are atomic transition frequency, cavity frequency and the frequency of driving field, respectively, $a^\dagger$ and a are creation and annihilation operators for the cavity

mode, g is the coupling constant between atoms and cavity, $S_j^+ = |e\rangle_j\langle g|$, $S_j^- = |g\rangle_j\langle e|$, $S_j^z = \frac{1}{2}(|e\rangle_j\langle e| - |g\rangle_j\langle g|)$ are atomic operators, and Ω is the Rabi frequency of the classical field. We consider the case $\omega_0 = \omega_d$. In the interaction picture, the evolution operator of the system is

$$U(t) = e^{-iH_0t}e^{-iH_et}, \tag{2}$$

where $H_0 = \sum_{j=1}^{2}\Omega(S_j^- + S_j^+)$, H_e is the effective Hamiltonian. In the large detuning $\delta \gg \frac{1}{2}g$ and strong driving field $2\Omega \gg \delta, g$ limit, the effective Hamiltonian for this interaction can be described as follows [21]:

$$H_e = \lambda\left[\sum_{j=1}^{2}\frac{1}{2}(|e\rangle_j\langle e| + |g\rangle_j\langle g|) + \sum_{j,k=1,j\neq k}^{2}(S_j^+S_k^+ + S_j^+S_k^-) + H.c\right], \tag{3}$$

where $\lambda = g^2/2\delta$, δ is the detuning between ω_0 and ω_a. From (3), we know that H_e is independent of creation and annihilation operators of the cavity mode and is only related with atomic operators. So the effects of cavity decay and thermal field are all eliminated.

When two atoms enter into the cavity, after interaction time t, the state of the two atoms will undergo the following evolution:

$$\begin{aligned}|ee\rangle_{jk} \longrightarrow\ & e^{-i\lambda t}[\cos\lambda t(\cos\Omega t|e\rangle_j - i\sin\Omega t|g\rangle_j)\times(\cos\Omega t|e\rangle_k - i\sin\Omega t|g\rangle_k)\\ & - i\sin\lambda t(\cos\Omega t|g\rangle_j - i\sin\Omega t|e\rangle_j)\times(\cos\Omega t|g\rangle_k - i\sin\Omega t|e\rangle_k)],\end{aligned} \tag{4}$$

$$\begin{aligned}|eg\rangle_{jk} \longrightarrow\ & e^{-i\lambda t}[\cos\lambda t(\cos\Omega t|e\rangle_j - i\sin\Omega t|g\rangle_j)\times(\cos\Omega t|g\rangle_k - i\sin\Omega t|e\rangle_k)\\ & - i\sin\lambda t(\cos\Omega t|g\rangle_j - i\sin\Omega t|e\rangle_j)\times(\cos\Omega t|e\rangle_k - i\sin\Omega t|g\rangle_k)],\end{aligned} \tag{5}$$

$$\begin{aligned}|ge\rangle_{jk} \longrightarrow\ & e^{-i\lambda t}[\cos\lambda t(\cos\Omega t|g\rangle_j - i\sin\Omega t|e\rangle_j)\times(\cos\Omega t|e\rangle_k - i\sin\Omega t|g\rangle_k)\\ & - i\sin\lambda t(\cos\Omega t|e\rangle_j - i\sin\Omega t|g\rangle_j)\times(\cos\Omega t|g\rangle_k - i\sin\Omega t|e\rangle_k)],\end{aligned} \tag{6}$$

$$\begin{aligned}|gg\rangle_{jk} \longrightarrow\ & e^{-i\lambda t}[\cos\lambda t(\cos\Omega t|g\rangle_j - i\sin\Omega t|e\rangle_j)\times(\cos\Omega t|g\rangle_k - i\sin\Omega t|e\rangle_k)\\ & - i\sin\lambda t(\cos\Omega t|e\rangle_j - i\sin\Omega t|g\rangle_j)\times(\cos\Omega t|e\rangle_k - i\sin\Omega t|g\rangle_k)].\end{aligned} \tag{7}$$

Assume the state of the two atoms is initially in $|e\rangle|g\rangle$, we can choose $\lambda t = \frac{1}{4}\pi$, $\Omega t = \pi$ by modulating the driving field appropriately, the state of the two atoms will become $\frac{1}{\sqrt{2}}(|e\rangle|g\rangle - i|g\rangle|e\rangle)$. The quantum channel which shared by Alice and Bob is a one-dimensional maximally four-particle cluster state (Atoms 3, 4, 5, 6) $|\phi\rangle_{3456} = \frac{1}{2}(|gggg\rangle_{3456} + |eegg\rangle_{3456} + |ggee\rangle_{3456} - |eeee\rangle_{3456})$. The initial state of the whole system is given by

$$|\psi\rangle = \frac{1}{\sqrt{2}}(|e\rangle_1|g\rangle_2 - i|g\rangle_1|e\rangle_2)\otimes\frac{1}{2}(|gggg\rangle_{3456} + |eegg\rangle_{3456} + |ggee\rangle_{3456} - |eeee\rangle_{3456}) \tag{8}$$

Let us suppose Alice owns atoms 1 and 3, Bob owns atoms 2 and 5, and Charlie owns atoms 4 and 6. In order to encode two bits of classical information, Alice performs one of the four local operations $(I, \sigma^x, i\sigma^y, \sigma^z)$ on her atom 1. This operation will transform state in (8) into

$$|\psi_1\rangle = \frac{1}{\sqrt{2}}(|e\rangle_1|g\rangle_2 - i|g\rangle_1|e\rangle_2) \otimes \frac{1}{2}(|gggg\rangle_{3456} + |eegg\rangle_{3456} + |ggee\rangle_{3456} - |eeee\rangle_{3456}) \tag{9}$$

$$|\psi_2\rangle = \frac{1}{\sqrt{2}}(|g\rangle_1|g\rangle_2 - i|e\rangle_1|e\rangle_2) \otimes \frac{1}{2}(|gggg\rangle_{3456} + |eegg\rangle_{3456} + |ggee\rangle_{3456} - |eeee\rangle_{3456}) \tag{10}$$

$$|\psi_3\rangle = \frac{1}{\sqrt{2}}(|g\rangle_1|g\rangle_2 + i|e\rangle_1|e\rangle_2) \otimes \frac{1}{2}(|gggg\rangle_{3456} + |eegg\rangle_{3456} + |ggee\rangle_{3456} - |eeee\rangle_{3456}) \tag{11}$$

$$|\psi_4\rangle = \frac{1}{\sqrt{2}}(|e\rangle_1|g\rangle_2 + i|g\rangle_1|e\rangle_2) \otimes \frac{1}{2}(|gggg\rangle_{3456} + |eegg\rangle_{3456} + |ggee\rangle_{3456} - |eeee\rangle_{3456}) \tag{12}$$

Assume that each of the above four unitary operations corresponds to a two-bit encoding respectively, the information is encoded into atom 1. Next, we will introduce the scheme for Quantum secret sharing.

3 The Scheme for Quantum Secret Sharing

In order to realize the quantum secret sharing, Alice, Bob and Charlie send her atoms into the above cavities respectively. Choosing the interaction time $\lambda t = \frac{1}{4}\pi$, $\Omega t = \pi$ by modulating the driving field appropriately, the quantum state of the atoms in (9–12) will evolve into

$$\begin{aligned}|\psi_1\rangle = \frac{1}{4}(&|eg\rangle_{13}|ge\rangle_{25}|ge\rangle_{46} - |ge\rangle_{13}|eg\rangle_{25}|ge\rangle_{46} - |eg\rangle_{13}|eg\rangle_{25}|eg\rangle_{46} - |ge\rangle_{13}|ge\rangle_{25}|eg\rangle_{46}\\ &+ |ee\rangle_{13}|gg\rangle_{25}|eg\rangle_{46} - |gg\rangle_{13}|ee\rangle_{25}|eg\rangle_{46} - |ee\rangle_{13}|ee\rangle_{25}|ge\rangle_{46} - |gg\rangle_{13}|gg\rangle_{25}|ge\rangle_{46}\\ &+ i(-|ge\rangle_{13}|gg\rangle_{25}|gg\rangle_{46} - |eg\rangle_{13}|ee\rangle_{25}|gg\rangle_{46} + |ge\rangle_{13}|ee\rangle_{25}|ee\rangle_{46}\\ &- |eg\rangle_{13}|gg\rangle_{25}|ee\rangle_{46} + |gg\rangle_{13}|ge\rangle_{25}|ee\rangle_{46} - |gg\rangle_{13}|eg\rangle_{25}|gg\rangle_{46}\\ &+ |ee\rangle_{13}|ge\rangle_{25}|gg\rangle_{46} + |ee\rangle_{13}|eg\rangle_{25}|ee\rangle_{46}))\end{aligned} \tag{13}$$

$$\begin{aligned}|\psi_2\rangle = \frac{1}{4}(&|gg\rangle_{13}|ge\rangle_{25}|ge\rangle_{46} - |ee\rangle_{13}|eg\rangle_{25}|ge\rangle_{46} - |gg\rangle_{13}|eg\rangle_{25}|eg\rangle_{46} - |ee\rangle_{13}|ge\rangle_{25}|eg\rangle_{46}\\ &+ |ge\rangle_{13}|gg\rangle_{25}|eg\rangle_{46} - |eg\rangle_{13}|ee\rangle_{25}|eg\rangle_{46} - |ge\rangle_{13}|ee\rangle_{25}|ge\rangle_{46} - |eg\rangle_{13}|gg\rangle_{25}|ge\rangle_{46}\\ &+ i(-|ee\rangle_{13}|gg\rangle_{25}|gg\rangle_{46} - |gg\rangle_{13}|ee\rangle_{25}|gg\rangle_{46} + |ee\rangle_{13}|ee\rangle_{25}|ee\rangle_{46}\\ &- |gg\rangle_{13}|gg\rangle_{25}|ee\rangle_{46} + |eg\rangle_{13}|ge\rangle_{25}|ee\rangle_{46} - |eg\rangle_{13}|eg\rangle_{25}|gg\rangle_{46}\\ &+ |ge\rangle_{13}|ge\rangle_{25}|gg\rangle_{46} + |ge\rangle_{13}|eg\rangle_{25}|ee\rangle_{46}))\end{aligned} \tag{14}$$

$$\begin{aligned}|\psi_3\rangle = \frac{1}{4}(&|gg\rangle_{13}|gg\rangle_{25}|gg\rangle_{46} - |ee\rangle_{13}|ee\rangle_{25}|gg\rangle_{46} - |gg\rangle_{13}|ee\rangle_{25}|ee\rangle_{46} - |ee\rangle_{13}|gg\rangle_{25}|ee\rangle_{46}\\ &- |ge\rangle_{13}|ge\rangle_{25}|ee\rangle_{46} - |eg\rangle_{13}|eg\rangle_{25}|ee\rangle_{46} + |ge\rangle_{13}|eg\rangle_{25}|gg\rangle_{46} + |eg\rangle_{13}|ge\rangle_{25}|gg\rangle_{46}\\ &+ i(-|gg\rangle_{13}|ge\rangle_{25}|eg\rangle_{46} - |ee\rangle_{13}|ge\rangle_{25}|ge\rangle_{46} - |ge\rangle_{13}|gg\rangle_{25}|ge\rangle_{46}\\ &- |eg\rangle_{13}|gg\rangle_{25}|eg\rangle_{46} + |ee\rangle_{13}|eg\rangle_{25}|eg\rangle_{46} - |gg\rangle_{13}|eg\rangle_{25}|ge\rangle_{46} + |eg\rangle_{13}|ee\rangle_{25}|ge\rangle_{46}\\ &- |ge\rangle_{13}|ee\rangle_{25}|eg\rangle_{46}))\end{aligned} \tag{15}$$

$$
\begin{aligned}
|\psi_4\rangle = \frac{1}{4}(&|eg\rangle_{13}|gg\rangle_{25}|gg\rangle_{46} - |ge\rangle_{13}|ee\rangle_{25}|gg\rangle_{46} - |eg\rangle_{13}|ee\rangle_{25}|ee\rangle_{46} - |ee\rangle_{13}|gg\rangle_{25}|ee\rangle_{46} \\
&- |ee\rangle_{13}|ee\rangle_{25}|ee\rangle_{46} - |gg\rangle_{13}|eg\rangle_{25}|ee\rangle_{46} + |ee\rangle_{13}|eg\rangle_{25}|gg\rangle_{46} + |gg\rangle_{13}|ge\rangle_{25}|gg\rangle_{46} \\
&+ i(-|eg\rangle_{13}|ge\rangle_{25}|eg\rangle_{46} - |ge\rangle_{13}|ge\rangle_{25}|ge\rangle_{46} - |ee\rangle_{13}|gg\rangle_{25}|ge\rangle_{46} \\
&- |gg\rangle_{13}|gg\rangle_{25}|eg\rangle_{46} + |ge\rangle_{13}|eg\rangle_{25}|eg\rangle_{46} - |eg\rangle_{13}|eg\rangle_{25}|ge\rangle_{46} \\
&+ |gg\rangle_{13}|ee\rangle_{25}|ge\rangle_{46} - |ee\rangle_{13}|ee\rangle_{25}|eg\rangle_{46}))) \qquad (16)
\end{aligned}
$$

Obviously, there is an explicit correspondence between Alice's operation and the measurement results of the two receivers, which means that if they cooperate, both of them can get the information. But if they do not cooperate, neither of the two users can obtain the information by local operation in a deterministic manner.

Now let us describe the quantum secret sharing scheme in detail as follows.

(1) By using cavity QED, a four-particle cluster state is prepared as the quantum channel, with the atoms 1, 3 at Alice's hand, atoms 2, 5 at Bob's, and atoms 4, 6 at Charlie's. After Alice confirms that Bob and Charlie receive their atoms, she performs one of the four local operations $(I, \sigma^x, i\sigma^y, \sigma^z)$ on her atom 1. Alice, Bob and Charlie agree on the four local operations representing two bits of messages 00, 01, 10 and 11, respectively. The encoding of two bits information is completed.

(2) We consider two identical two-level atoms interacting a single mode and driven by a classical field. Alice, Bob and Charlie simultaneously send her atoms into her own cavity, and then make a separate measurement on their atoms with the choice $\lambda t = \frac{1}{4}\pi$, $\Omega t = \pi$ by modulating the driving field appropriately. The separate state of the two atoms may evolve into a maximally two-atom entangled state. The joint Bell-state measurement in the previous scheme is not needed in the current protocol, i.e. the joint Bell-state measurement has been converted into the separated measurement on the atoms in cavity QED.

(3) If Alice is sure that it is secure, she publicly announces the measurement results to Bob and Charlie. In (13–16), there is an explicit correspondence between Alice's operation and the measurement results of the two receivers, both of them can read the secret message according to his measurement outcomes and the classical information from Alice if they cooperate. But if they do not cooperate, neither of the two users could obtain the information by local operation in a deterministic manner. Alternatively, either of them can extract the two-bit messages Alice sends to him. If Bob and Charlie agree to collaborate, they can read out Alice's secret messages. We can see that when atoms 1, 3 and atoms 2, 5 and atoms 4, 6 enter into the cavity, because every atom has two levels, 64 kinds of different separate states can be derived. Every local operation corresponds with 16 kinds of different separate states. As an example, if Alice announces his own detection result ($|eg\rangle_{13}$), at this time, although Charlie obtains the measurement results, he cannot recover Alice's secret message without Bob's cooperation because Charlie does not know which operation Bob has performed on each particle. Bob announces his own measurement result ($|gg\rangle_{25}$) in public, Charlie can receive one of the four local operations (σ^z) based on his own measurement result ($|gg\rangle_{46}$).

Finally, it is necessary to give a brief discussion on the experimental matters. We consider the typical experimental values of the parameters for Rydberg atoms with principal quantum numbers 49, 50, 51, the radiative time is about $T_r = 3 \times 10^{-2}$ s, and the coupling constant is $g = 2\pi \times 24$ kHz. For a normal cavity, the decay time can reach $T_c = 1.0 \times 10^{-3}$ s. The atoms can be selected according to their velocities by optical pumping, which account for the control of interaction time between the atoms and the cavities. Then we get that the interaction time of atom and cavity is on the order of 10^{-4} s. Hence the total time for the

whole system is much shorter than T_r and T_c. Since the cavity is only virtually excited, the decoherence arising from the cavity decay is suppressed.

4 Summary

We have proposed a simple scheme to realize three-party quantum secret sharing. Two atoms exist in single-mode cavity and are driven by a classical field. By detecting the states of atoms, they can get complete information about the message if they cooperate each other. The feature in this paper consists in the fact that the difficult Bell state measurements on the atoms are not needed and the scheme is insensitive to the cavity decay and the thermal field. Meanwhile the success probability is equal to 1. Generating cluster states have been proposed in different types of physical systems, thus this scheme is realizable by current available technology. The important features of our scheme can also be demonstrated in ion trap system. This may open a new perspective for the applications of cluster states in quantum information processing.

Acknowledgements This work is supported by the National Natural Science Foundation of China under Grant No. 10904033, Natural Science Foundation of Hubei Province Grant No. 2009CDA145, Educational Commission of Hubei Province under Grant No. D20092204 and the Postgraduate Programme of Hubei Normal University under Grant No. 2007D20.

References

1. Hillery, M., Buzek, V., Berthiaume, A.: Phys. Rev. A **59**, 1829 (1999)
2. Cleve, R., Gottesman, D., Lo, H.-K.: Phys. Rev. Lett. **83**, 648 (1999)
3. Karlsson, A., Koashi, M., Imoto, N.: Phys. Rev. A **59**, 162 (1999)
4. Li, N.Y., Zhang, K.S., Peng, K.C.: Phys. Lett. A **324**, 420 (2004)
5. Xiao, L., Long, G.L., Deng, F.G., Pan, J.W.: Phys. Rev. A **69**, 052307 (2004)
6. Zhang, Z.J., Li, Y., Man, Z.X.: Phys. Rev. A **71**, 044301 (2005)
7. Deng, F.G., et al.: Phys. Rev. A **72**, 044302 (2005)
8. Tittel, W., Zbinden, H., Gisin, N.: Phys. Rev. A **63**, 042301 (2001)
9. Lance, A.M., Symul, T., Bowen, W.P., Sanders, B.C., Lam, P.K.: Phys. Rev. Lett. **92**, 177903 (2004)
10. Chen, Y.A., Zhang, A.N., Zhao, Z., et al.: Phys. Rev. Lett. **95**, 200502 (2005)
11. Lu, H., Guo, G.C.: Phys. Lett. A **276**, 209 (2000)
12. Briegel, H.J., Raussendorf, R.: Phys. Rev. Lett. **86**, 910 (2001)
13. Nielsen, M.A.: Phys. Rev. Lett. **93**, 040503 (2004)
14. Wang, X.W., Yang, G.J.: Opt. Commun. **281**, 5282 (2008)
15. Cho, J., Lee, H.W.: Phys. Rev. Lett. **95**, 160501 (2005)
16. Mandel, O., Greiner, M., Widera, A., Rom, T.: Nature **425**, 937 (2003)
17. Walther, P., Resch, K.J., et al.: Nature **434**, 169 (2005)
18. Zheng, S.B., Guo, G.C.: Phys. Rev. Lett. **85**, 2392 (2000)
19. Osnaghi, S., Bertet, P., Auffeves, A., et al.: Phys. Rev. Lett. **87**, 037902 (2001)
20. Zou, C.-L., Xue, Z.Y., Cao, Z.L.: Commun. Theor. Phys. **49**, 365 (2008)
21. Zheng, S.B.: Phys. Rev. A **68**, 035801 (2003)