Vol 14 No 9, September 2005
1009-1963/2005/14(09)/1821-04

Chinese Physics

© 2005 Chin. Phys. Soc.
and IOP Publishing Ltd

Scheme for implementing quantum secret sharing via cavity QED*

Chen Zhi-Hua(陈志华)[a)†] and Lin Xiu-Min(林秀敏)[a)b)‡]

[a)] *School of Physics and Optoelectronics Technology, Fujian Normal University, Fuzhou 350007, China*

[b)] *Key Laboratory of Quantum Information, University of Science and Technology of China, Heifei 230026, China*

(Received 14 May 2004; revised manuscript received 7 April 2005)

An experimentally feasible scheme for implementing quantum secret sharing via cavity quantum electrodynamics (QED) is proposed. The scheme requires the large detuning of the cavity field from the atomic transition, the cavity is only virtually excited, thus the requirement on the quality factor of the cavity is greatly loosened.

Keywords: quantum secret sharing, cavity QED
PACC: 4250

1. Introduction

Quantum secret sharing (QSS), plays a key role in protecting secret quantum information. The simplest scheme of QSS is that the sender Alice sends a secret message to two receivers Bob and Charlie so that none of the receivers can recover the message on his own. Using QSS we can create joint checking accounts containing quantum money,[1] share hard-to-create ancilla states,[2] and perform a secure distributed quantum computation. Owing to its numerous practical applications, many schemes have been presented to realize QSS.[3−5]

Entanglement plays a major role in quantum information processing including QSS. Cavity quantum electrodynamics (QED) is one of the ideal systems for preparing entangled states. Reference [6] proposed an efficient scheme to prepare two-atom maximally entangled states by means of two Rydberg atoms interacting with a nonresonant cavity, this scheme has been experimentally implemented.[7] It can be used to realize teleportation,[6] dense coding,[8] quantum cloning,[9] and the preparing of multiparticle entanglement.[10,11] In this paper, we propose a scheme for implementing QSS based on the cavity QED model.

2. Quantum secret sharing

Now we briefly review the protocol of QSS presented in Ref.[3]. Suppose Alice, Bob and Charlie initially share a Greenberger–Horne–Zeilinger (GHZ) state

$$|\psi\rangle_{124} = \frac{1}{\sqrt{2}}(|e_1 g_2 g_4\rangle - |g_1 e_2 e_4\rangle), \tag{1}$$

where $|e\rangle_j$ and $|g\rangle_j$ (j=1, 2, 3, 4, 5) are two states of the jth Rydberg atoms respectively. Alice now wants to send a message encoded in the 5th qubit

$$|\varphi\rangle_5 = \alpha|g_5\rangle + \beta|e_5\rangle \tag{2}$$

to Bob and Charlie in such a way that any one can recover the quantum information but not without the assistance of the remaining, where $|\alpha|^2+|\beta|^2 = 1$. The state of the four-particle system can be written as

$$\begin{aligned} |\Psi\rangle_{5124} =& \frac{1}{2}[|\Phi^+\rangle_{51}(\alpha|gg\rangle_{24} - \beta|ee\rangle_{24}) \\ &+ |\Phi^-\rangle_{51}(\alpha|gg\rangle_{24} + \beta|ee\rangle_{24}) \\ &+ |\Psi^+\rangle_{51}(\beta|gg\rangle_{24} - \alpha|ee\rangle_{24}) \\ &+ |\Psi^-\rangle_{51}(-\beta|gg\rangle_{24} - \alpha|ee\rangle_{24})], \end{aligned} \tag{3}$$

where

$$\begin{aligned} |\Phi^\pm\rangle_{51} &= \frac{1}{\sqrt{2}}(|ge\rangle_{51} \pm |eg\rangle_{51}), \\ |\Psi^\pm\rangle_{51} &= \frac{1}{\sqrt{2}}(|gg\rangle_{51} \pm |ee\rangle_{51}). \end{aligned} \tag{4}$$

*Project supported by the Fujian Provincial Natural Science Foundation (Grant No A0410016).

†E-mail: chenzhihua77@hotmail.com
‡E-mail: xmlin@mail.ustc.edu.cn

After performing a Bell measurement on her two qubits 1 and 5, Alice informs Bob to measure his atom 2 in the x direction, where $|\pm x\rangle = \frac{1}{\sqrt{2}}(|g\rangle \pm |e\rangle)$. Then Alice tells Charlie the result of her measurement so that he can obtain amplitude information about her qubit 5.[3] However, at this stage Charlie can not recover the whole message exactly. He can obtain the phase information about Alice's qubit 5 if and only if he gains a bit of classical information from Bob. Finally, Charlie can reconstruct Alice's qubit 5 by performing certain local operations as follows:

$$|\Phi^+\rangle_{51}|-x\rangle_2, |\Phi^-\rangle_{51}|+x\rangle_2 \to I, \tag{5a}$$

$$|\Phi^+\rangle_{51}|+x\rangle_2, |\Phi^-\rangle_{51}|-x\rangle_2 \to \sigma_z, \tag{5b}$$

$$|\Psi^+\rangle_{51}|-x\rangle_2, |\Psi^-\rangle_{51}|+x\rangle_2 \to \sigma_x, \tag{5c}$$

$$|\Psi^+\rangle_{51}|+x\rangle_2, |\Psi^-\rangle_{51}|-x\rangle_2 \to \sigma_x\sigma_z, \tag{5d}$$

where I is the identity operator, σ_x and σ_z are Pauli operators. Namely, the state of atom 4 collapses to the state depicted in Eq.(2) after Charlie performing one of the above operations. As the discussion above, we see that Charlie can not recover the qubit in its exact form without Bob's information, and it is impossible for both Bob and Charlie to get hold of the desired state as it is forbidden by the no-cloning theorem.[12]

3. Interaction of the atoms with the field

Consider that two identical Rydberg atoms simultaneously interact with a single-mode cavity field of high quality factor. The relevant atomic levels and transitions are shown in Fig.1, where the states $|e\rangle$, $|g\rangle$, and $|f\rangle$ represent the three circular levels of the Rydberg atom with principal quantum numbers 51, 50 and 49 respectively. In the rotating-wave approximation, the interaction Hamiltonian of the system in the interaction picture is (assuming $\hbar = 1$)[6]

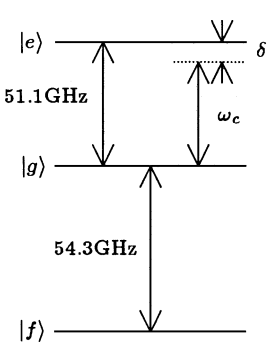


Fig.1. Rydberg atom interacts with a single-mode cavity field.

$$H_{\rm I} = \eta \sum_{j=1,2} (\mathrm{e}^{-\mathrm{i}\delta t} a^+ s_j^- + \mathrm{e}^{\mathrm{i}\delta t} a s_j^+), \tag{6}$$

where $s_j^- = |g_j\rangle\langle e_j|$ and $s_j^+ = |e_j\rangle\langle g_j|$ are the atomic transition operators, a^+ and a are the creation and annihilation operators for the cavity field respectively, and η is the atom-cavity coupling strength. As δ (where δ denotes the detuning between the cavity field mode and the $|e\rangle \leftrightarrow |g\rangle$ transition) satisfies $\delta \ll (\omega_g - \omega_f) - (\omega_e - \omega_g)$=3.2GHz, the state $|f\rangle$ will not be affected during the atom-cavity interaction. In the large detuning case of $\delta \gg \eta$, no energy exchange between the atoms and the cavity will happen. Assume that the cavity field is initially in the vacuum state, the Hamiltonian reduces to[6]

$$H_{\rm I} = \lambda \Big[\sum_{j=1,2} |e_j\rangle\langle e_j| + s_1^+ s_2^- + s_1^- s_2^+ \Big], \tag{7}$$

where $\lambda = \frac{\eta^2}{\delta}$. Then the state evolution of the system is given by

$$|g_1 f_2\rangle \to |g_1 f_2\rangle, \tag{8a}$$

$$|g_1 g_2\rangle \to |g_1 g_2\rangle, \tag{8b}$$

$$|e_1 f_2\rangle \to e^{-\mathrm{i}\lambda t}|e_1 f_2\rangle, \tag{8c}$$

$$|e_1 g_2\rangle \to \mathrm{e}^{-\mathrm{i}\lambda t}[\cos(\lambda t)|e_1 g_2\rangle - \mathrm{i}\sin(\lambda t)|g_1 e_2\rangle]. \tag{8d}$$

Suppose that two atoms are initially in the state $|e_1 g_2\rangle$, we can obtain the maximally entangled two-atom state by choosing $\lambda t = \frac{\pi}{4}$, i.e.

$$|\psi\rangle \to \frac{1}{\sqrt{2}}(|e_1 g_2\rangle - \mathrm{i}|g_1 e_2\rangle), \tag{9}$$

where we have discarded the common phase factor.

In our scheme, the single qubit unitary operation is implemented by the resonant interaction of atoms with a classical field. If the classical field is resonant with the $|m\rangle \leftrightarrow |n\rangle$ $(m, n = e, g, f; m \neq n)$ transition of the jth atom, the evolution operator of the atomic state can be easily shown under the bases $\{|m\rangle, |n\rangle\}$ as follows:[8]

$$U_{mn}^j(\theta, \varphi) = \begin{pmatrix} \cos\theta & -\mathrm{i}\mathrm{e}^{-\mathrm{i}\varphi}\sin\theta \\ -\mathrm{i}\mathrm{e}^{\mathrm{i}\varphi}\sin\theta & \cos\theta \end{pmatrix}, \tag{10}$$

where $\theta = \Omega_{mn}|\alpha|t$, $\alpha = |\alpha|\mathrm{e}^{\mathrm{i}\varphi}$ is the complex amplitude of the classical field, Ω_{mn} is the atom-field coupling constant, and the state $|k\rangle$ $(k = e, g, f; k \neq m, n)$ takes no effect during this stage.

4. Realization of quantum secret sharing

Now we describe in detail how to realize QSS using this cavity QED model. The procedure can be divided into four steps (depicted in Fig.2).

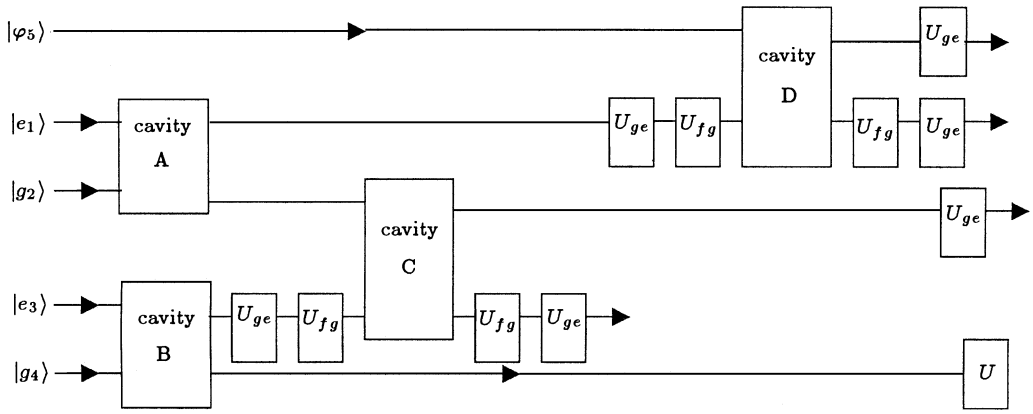


Fig.2. Schematic setup to implement quantum secret sharing. U denotes one of the four unitary operations $\{I, \sigma_x, \sigma_z, \sigma_x\sigma_z\}$.

Step 1 The preparation of a GHZ state[13] Atom 1 (3) and 2 (4) initially prepared in the $|e_1\rangle$ ($|e_3\rangle$) and $|g_2\rangle$ ($|g_4\rangle$) respectively, are simultaneously sent into cavity A (B) with same velocity but at different positions. After the interaction time $t_1 = t_2 = \dfrac{\pi}{4\lambda}$, both atoms leave the cavity A (B) and are prepared in the state described by Eq.(9). Subsequently, the operations $U^3_{fg}\left(\dfrac{\pi}{2},\dfrac{\pi}{2}\right)U^3_{ge}\left(\dfrac{\pi}{4},\dfrac{\pi}{2}\right)$ are performed, then both atoms 3 and 2 are sent into cavity C. After the interaction $t_3 = \dfrac{\pi}{\lambda}$, both atoms leave the cavity C and the operations $U^3_{ge}\left(\dfrac{\pi}{4},\dfrac{\pi}{2}\right)U^3_{fg}\left(\dfrac{\pi}{2},\dfrac{\pi}{2}\right)$ are performed. By measuring the state of atom 3, we can prepare a GHZ state. If the state of atom 3 is $|e_3\rangle$, the state of atoms 1, 2 and 4 will collapse to the state described by Eq.(1); if the state of atom 3 is $|g_3\rangle$, the state of atoms 1, 2 and 4 will collapse to $|\psi'\rangle_{124} = \dfrac{1}{\sqrt{2}}(|e_1g_2e_4\rangle + |g_1e_2g_4\rangle)$, which can be transformed into the state of Eq.(1) after performing the local operation $\sigma_z\sigma_x$ on atom 4. Without loss of generality, we assume that the state of atom 3 is $|e_3\rangle$, therefore, the atoms 1, 2 and 4, which belong to Alice, Bob and Charlie respectively, is in the state of Eq.(1).

Step 2 Alice performs a Bell measurement on her two qubits Alice performs the operations $U^1_{fg}\left(\dfrac{\pi}{2},\dfrac{\pi}{2}\right)U^1_{ge}\left(\dfrac{\pi}{4},\dfrac{\pi}{2}\right)$, then simultaneously sends atoms 1 and 5, which is in the state described in Eq.(2), into the cavity D for interacting $t_4 = \dfrac{\pi}{\lambda}$. After leaving the cavity for the two atoms, Alice performs the operations $U^5_{ge}\left(\dfrac{\pi}{4},\dfrac{\pi}{2}\right)U^1_{ge}\left(\dfrac{\pi}{4},\dfrac{\pi}{2}\right)U^1_{fg}\left(\dfrac{\pi}{2},\dfrac{\pi}{2}\right)$ and measures the states of atom 1 and 5 respectively. Thus the evolution of the Bell states (shown in Eq.(4)) is given by

$$|\Phi^+\rangle_{51} \to |ee\rangle_{51}, \tag{11a}$$
$$|\Phi^-\rangle_{51} \to |ge\rangle_{51}, \tag{11b}$$
$$|\Psi^+\rangle_{51} \to -|eg\rangle_{51}, \tag{11c}$$
$$|\Psi^+\rangle_{51} \to -|gg\rangle_{51}. \tag{11d}$$

Step 3 Bob makes his measurement Bob performs $U^2_{ge}\left(\dfrac{\pi}{4},\dfrac{\pi}{2}\right)$ operation, then he measures the state of the atom 2. There are two possible results $|e_2\rangle$ or $|g_2\rangle$, where $|e_2\rangle$ ($|g_2\rangle$) corresponds to the state $|+x\rangle_2$ ($|-x\rangle_2$) of Eq.(5) respectively.

Step 4 Charlie recovers Alice's qubit Based on the results of the measurement by Alice and Bob, Charlie decides to perform one of the four U operations $\{I, \sigma_x, \sigma_z, \sigma_x\sigma_z\}$ (see Eq.(5)), which can be implemented as follows:

$$U^4_{ge}(0,0) \to I, \tag{12a}$$
$$U^4_{fg}(\pi,0)U^4_{ge}\left(\frac{\pi}{2},\frac{\pi}{2}\right) \to \sigma_x, \tag{12b}$$
$$U^4_{fg}(\pi,0)U^4_{ge}(\pi,0) \to \sigma_z, \tag{12c}$$
$$U^4_{ge}\left(\frac{\pi}{2},\frac{\pi}{2}\right) \to \sigma_x\sigma_z. \tag{12d}$$

After that, Charlie's qubit collapses to the state $|\varphi\rangle_4 = \alpha|g_4\rangle + \beta|e_4\rangle$. Thus the procedure of QSS is completed.

5. Discussion and conclusion

The key of the scheme is that both atoms should be simultaneously sent through the cavity, otherwise there will be some deviation. Neglecting the cavity decay and the atomic radiative transmission, we make a rough estimation. Assume that atom 1 (3) enters the cavity A (B) $0.1t_1$ ($0.1t_2$) sooner than atom 2 (4), atom 2 (5) enters the cavity C (D) $0.1t_3$ ($0.1t_4$) sooner

than atom 3 (1), the results of the measurements in step 2 and 3 are $|ge\rangle_{51}$ and $|e\rangle_2$ respectively, Charlie should consequently perform I operation on atom 4 in order to reconstruct Alice's qubit. In this case we get the fidelity $F = |\langle\psi|\psi_a\rangle|^2 \approx 0.98$ with the choice $\alpha = \beta = \frac{1}{\sqrt{2}}$, where $|\psi\rangle$ and $|\psi_a\rangle$ are the final states of atom 4 when the atoms are sent through the cavities at the same time and at the different time respectively.

The radiative time of the Rydberg atoms is about $T_r = 3 \times 10^{-2}$s, the efficient decay time of the cavity is about $T_c = 1 \times 10^{-3}$s, the coupling constant is $\eta = 2\pi \times 25$kHz.[14] With the choice $\delta = 10\eta$, the interaction time in cavities are $t_1 = t_2 = \frac{\pi\delta}{4\eta^2} = 5 \times 10^{-5}$s and $t_3 = t_4 = \frac{\pi\delta}{\eta^2} = 2 \times 10^{-4}$s respectively, which are much shorter than T_c. Suppose the length of the cavity is 2.75cm, the distance between cavities C and A (D) is 5.5cm, the velocity of the atoms leaving the cavities is of the order 550m/s, thus the total time performing the scheme is 10^{-3}s, which is much shorter than T_r.

In summary, we have proposed a high-fidelity scheme for QSS. The distinct advantage of our scheme is that the cavity decay can be effectively suppressed as the cavities are only virtually excited and based on the current experimental technology[7] the scheme is possible to be realized.

References

[1] Wiesner S 1983 *IGACT News* **15** 78

[2] Gottesman D and Chuarg I 1999 *Nature* (London) **402** 390

[3] Hillery M, Buzek V and Berthiaume A 1999 *Phys. Rev.* A **59** 1829

[4] Gottesman D 2000 *Phys. Rev.* A **61** 042311

[5] Cleve R, Gottesman D and Lo H K 1999 *Phys. Rev. Lett.* **83** 648

[6] Zheng S B and Guo G C 2000 *Phys. Rev. Lett.* **85** 2392

[7] Osnaghi S *et al* 2001 *Phys. Rev. Lett.* **87** 037902

[8] Lin X M, Zhou Z W, Xue P, Gu Y J and Guo G C 2003 *Phys. Lett.* A **313** 351

[9] Zou X B, Pahlke K and Mathis W 2003 *Phys. Rev.* A **67** 024304

[10] Guo G P, Li C F, Li J and Guo G C 2002 *Phys. Rev.* A **65** 042102

[11] Zhang J and Ye L 2004 *Chin. Phys.* **13** 1438

[12] Wootters W K and Zurek W H 1982 *Nature* **299** 802

[13] Bose S, Vedral V and Knight P L 1998 *Phys. Rev.* A **57** 822

[14] Raimond J M, Brune M and Haroche S 2001 *Rev. Mod. Phys.* **73** 565