Int J Theor Phys (2010) 49: 334–342
DOI 10.1007/s10773-009-0206-8

Controlled Quantum Secure Direct Communication with Local Separate Measurements in Cavity QED

Chuan-Jia Shan · Ji-Bing Liu · Tao Chen · Tang-Kun Liu · Yan-Xia Huang · Hong Li

Received: 3 October 2009 / Accepted: 24 November 2009 / Published online: 2 December 2009

Abstract In this paper, we proposed an experimentally feasible new scheme for controlled quantum secure direct communication in cavity quantum electrodynamics without apparent joint Bell-state measurement. According to the results measured by the sender and the controller, the receiver can obtain different secret messages in a deterministic way using GHZ state as the quantum channel with unit successful probability if controller cooperates with it. In the communication processes, with the assistance of a strong classical driving field, the interactions between atoms and a single-mode nonresonant cavity substitute the generalized joint Bell-basis measurements. So this scheme only need separate measurements. In addition, the scheme is insensitive to the cavity decay and the thermal field. The discussion of the scheme indicates that it is simple and realizable with present technology.

Keywords Controlled quantum secure direct communication · Separate measurements · Cavity QED

1 Introduction

Quantum key distribution (QKD) is one of many important branches in quantum cryptography and has promising applications in quantum information processing. The main aim of QKD is to provide a secure way for creating a secret key between distant legitimate parties, Alice and Bob, over a long distance, in the presence of an eavesdropper, Eve, who interferes with the signals. Since Bennett and Brassard [1] proposed the standard BB84 protocol, QKD has attracted a widespread attention and progressed quickly on both theoretical and experimental aspects [2–5]. Recently, a novel quantum secure direct communication (QSDC) protocol has been presented and actively pursued by some groups [6–38]. Different from QKD, QSDC is the direct communication of secret messages without first establishing a key to encrypt them. In one kind of QSDC protocols, it is necessary to send the qubits carrying secret

C.-J. Shan (✉) · J.-B. Liu · T. Chen · T.-K. Liu · Y.-X. Huang · H. Li
College of Physics and Electronic Science, Hubei Normal University, Huangshi 435002, China
e-mail: shanchuanjia1122@yahoo.com.cn

message in the public channel. Therefore a potential eavesdropper can interfere the transmitting qubits. In order to prevent the qubits from being transmitted in the public channel, based on entanglement swapping and Bell basis measurement, many protocols on quantum secure direct communication have been put forward using EPR pairs or GHZ states. Since it is not necessary to transmit the secret message in the public channel, information is secure as long as the quantum channel is perfect. Controlled quantum communication scheme was first presented by Karlsson and Bourennane [39], which achieves the task that the secret can not be transmitted between the sender and receiver if the controller does not cooperate. The role of the controllers is that they have the right to decide whether and when the task should be processed. Controlled communication is useful in networked quantum information processing and cryptographic conferences, and therefore, a great number of works about it have been proposed [40–47]. The basic idea of a controlled QSDC scheme is to let the secret messages be recovered by a remote receiver only when he cooperates with the controllers. It is similar to another branch of quantum communication, quantum state sharing (QSTS) [48–54], whose task is to let several receivers share an unknown secret message with cooperations. Essentially one receiver can reconstruct the originally unknown state with the help of others. In principle, almost all the QSTS schemes can be used for controlled QSDC with or without a little modification, and vice versa. Moreover, most of the QSDC schemes require Bell-basis measurement (BM) or GHZ-basis measurement (GHZM). However, the realization of the BM or GHZM is still difficult in experiments. To overcome this difficulty, a great number of quantum communication protocols have been proposed by using cavity QED technology [55–62].

In this paper, we propose a experimentally feasible new protocol for controlled quantum secure direct communication in cavity QED. Compared with the previous schemes, our protocols have the following distinct advantages: (1) The scheme utilizes entangled atoms as the quantum channel. QED technique has also been implemented on the first experimental realization of the atomic qubits in ion-trap system by Riebe et al. [63] and Barrett et al. [64]. It is more applicable in the real world. (2) In this paper, no qubits carrying the secret messages are transmitted between two communicators, so the scheme is completely secure if perfect quantum channels are used. (3) In the former studies, the interaction between atoms and cavity is a resonant one, but the atomic spontaneous emission and cavity decay are the main sources of decoherence. The cavity decay and the thermal field will affect the scheme strongly. In our scheme, the cavity is only virtually excited and thus the efficient decoherence time of the cavity is greatly prolonged. (4) However, in experiments, the realization of the joint Bell state measurement is still difficult in quantum direct communication: although the joint operation has been realized, the operations needed are very complex. The scheme in this paper overcomes the difficulty of the Bell state measurement, as what is necessary is not the joint measurement to identify Bell states but a separate measurement in the cavity QED. (5) More importantly, the communication between two sides depends on the agreement of the third side, so the legitimate user can receive different secret messages in a direct way by using Greenberger-Horne-Zeilinger state only if controller cooperates with it. The probability of the success in our scheme is 1.0. Due to these advantages, our scheme is easier to implement experimentally and may open promising prospects for quantum information manipulation.

2 Model

We consider two identical two-level atoms simultaneously interacting with a single-mode cavity field and driven by a classical field. In the rotating-wave approximation, the Hamil-

tonian is

$$H = \omega_0 S_z + \omega_a a^+ a + \sum_{j=1}^{2}[g(a^+ S_j^- + a S_j^+) + \Omega(S_j^+ e^{-i\omega t} + S_j^- e^{i\omega t})], \tag{1}$$

where $S_z = \frac{1}{2}\sum_{j=1,2}|e_j\rangle\langle e_j| - |g_j\rangle\langle g_j|$, $S_j^+ = |e_j\rangle\langle g_j|$, $S_j^- = |g_j\rangle\langle e_j|$, and $|e_j\rangle$, $|g_j\rangle$ are the excited and ground state of the jth atom, respectively. a^+, a are the creation and annihilation operators for the cavity mode, g is the atom-cavity coupling strength, Ω is the Rabi frequency, ω_0 is the atomic transition frequency, ω_a is the cavity frequency, and ω is the frequency of the classical field.

Suppose $\omega_0 = \omega$, in the interaction picture, the evolution operator of the system is given by

$$U(t) = \exp(-iH_0 t)\exp(-iH_e t), \tag{2}$$

where $H_0 = \Omega\sum_{j=1,2}(S_j^+ + S_j^-)$, H_e is the effective Hamiltonian. In the strong driving regime $\Omega \gg \delta$, g (δ is the detuning between the atomic transition frequency ω_0 and cavity frequency ω_a) and in the case $\delta \gg g$, there is no energy exchange between the atomic system and the cavity thus the scheme is insensitive to both cavity decay and the thermal field. Then in the interaction picture, the effective interaction Hamiltonian reads [65]

$$H_e = \frac{\lambda}{2}\left[\sum_{j=1}^{2}(|e\rangle_{jj}\langle e| + |g\rangle_{jj}\langle g|) + \sum_{i,j=1,i\neq j}^{2}(S_i^+ S_j^- + S_i^+ S_j^+ + H.C.)\right], \tag{3}$$

where $\lambda = g^2/2\delta$.

If two atoms are sent into the cavity described above simultaneously and interact with it, at the same time the atoms are driven by a classical field. The state of the two atoms will undergo the following evolution:

$$\begin{aligned}
|ee\rangle_{jk} \longrightarrow\ & e^{-i\lambda t}[\cos\lambda t(\cos\Omega t|e\rangle_j - i\sin\Omega t|g\rangle_j) \times (\cos\Omega t|e\rangle_k - i\sin\Omega t|g\rangle_k) \\
& - i\sin\lambda t(\cos\Omega t|g\rangle_j - i\sin\Omega t|e\rangle_j) \times (\cos\Omega t|g\rangle_k - i\sin\Omega t|e\rangle_k)], \qquad (4) \\
|eg\rangle_{jk} \longrightarrow\ & e^{-i\lambda t}[\cos\lambda t(\cos\Omega t|e\rangle_j - i\sin\Omega t|g\rangle_j) \times (\cos\Omega t|g\rangle_k - i\sin\Omega t|e\rangle_k) \\
& - i\sin\lambda t(\cos\Omega t|g\rangle_j - i\sin\Omega t|e\rangle_j) \times (\cos\Omega t|e\rangle_k - i\sin\Omega t|g\rangle_k)], \qquad (5) \\
|ge\rangle_{jk} \longrightarrow\ & e^{-i\lambda t}[\cos\lambda t(\cos\Omega t|g\rangle_j - i\sin\Omega t|e\rangle_j) \times (\cos\Omega t|e\rangle_k - i\sin\Omega t|g\rangle_k) \\
& - i\sin\lambda t(\cos\Omega t|e\rangle_j - i\sin\Omega t|g\rangle_j) \times (\cos\Omega t|g\rangle_k - i\sin\Omega t|e\rangle_k)], \qquad (6) \\
|gg\rangle_{jk} \longrightarrow\ & e^{-i\lambda t}[\cos\lambda t(\cos\Omega t|g\rangle_j - i\sin\Omega t|e\rangle_j) \times (\cos\Omega t|g\rangle_k - i\sin\Omega t|e\rangle_k) \\
& - i\sin\lambda t(\cos\Omega t|e\rangle_j - i\sin\Omega t|g\rangle_j) \times (\cos\Omega t|e\rangle_k - i\sin\Omega t|g\rangle_k)]. \qquad (7)
\end{aligned}$$

3 Controlled Quantum Secure Direct Communication Protocol

In this section, we assume the quantum channel is a maximally three-atom GHZ entangled state and a maximally two-atom entangled state, i.e. $|\psi^-\rangle_{125} = \frac{1}{\sqrt{2}}(|g\rangle|e\rangle|e\rangle - i|e\rangle|g\rangle|g\rangle)$, $|\psi^-\rangle_{34} = \frac{1}{\sqrt{2}}(|g\rangle|e\rangle - i|e\rangle|g\rangle)$. Here the atoms 1, 3 belong to the sender Alice, atoms 2, 4 belong to the receiver Bob, and atom 5 the controlling atom belongs to Charlie. In our

scheme, we will encode information using the following four local unitary operators. It is easily verified that, the four Bell states can be transformed into each other by some unitary operations, which can be performed locally with nonlocal effects. For examples: Let U_{00}, U_{01}, U_{10}, U_{11} be in turn the unitary operations $\left(\begin{smallmatrix}1&0\\0&1\end{smallmatrix}\right)$, $\left(\begin{smallmatrix}1&0\\0&-1\end{smallmatrix}\right)$, $\left(\begin{smallmatrix}0&1\\1&0\end{smallmatrix}\right)$, $\left(\begin{smallmatrix}0&-1\\1&0\end{smallmatrix}\right)$ respectively, then $|\psi_{34}^{-}\rangle$ will be in turn transformed into $|\psi_{34}^{-}\rangle$, $|\psi_{34}^{+}\rangle$, $|\phi_{34}^{-}\rangle$, $|\phi_{34}^{+}\rangle$ after the unitary operations U_{00}, U_{01}, U_{10}, U_{11} on anyone atom of the pair, respectively. Assume that each of the above four unitary operations corresponds to a two-bit encoding respectively, i.e., U_{00} to '00', U_{01} to '01', U_{10} to '10' and U_{11} to '11'. Then, taking advantage of quantum entanglement and the assumption of the two-bit codings, a controlled quantum secure direct communication protocol is proposed. It can be verified that the state of the total system will evolve into the following state:

$$\begin{aligned}|\psi^{-}\rangle_{125}\otimes|\psi^{-}\rangle_{34}=\frac{1}{4}[&(|gg\rangle_{13}-i|ee\rangle_{13})(|ee\rangle_{24}-i|gg\rangle_{24})|e\rangle_5\\&-i(|eg\rangle_{13}-i|ge\rangle_{13})(|ge\rangle_{24}-i|eg\rangle_{24})|g\rangle_5\\&-i(|ge\rangle_{13}-i|eg\rangle_{13})(|eg\rangle_{24}-i|ge\rangle_{24})|e\rangle_5\\&-(|ee\rangle_{13}-i|gg\rangle_{13})(|gg\rangle_{24}-i|ee\rangle_{24})|g\rangle_5],\end{aligned}\tag{8}$$

by selecting the interaction time which satisfies $\lambda t=\frac{\pi}{4}$ and making the Rabi frequency which satisfies $\Omega t=\pi$. From (8) we observe that atoms 2 and 4 collapse into a separate state if one detects the state of atoms 1 and 3 after they fly out of the cavity. However, for a known initial state, after the interaction, the detection results of atoms 1 and 3 are not correlated to the state of the atoms 2 and 4. For example, if Alice measures the result of atoms 1 and 3 in $|ee\rangle_{13}$, the state of the atoms 2 and 4 will collapse into $|ee\rangle_{24}$ or $|gg\rangle_{24}$ even if Charlie informs Alice and Bob of his measurement results via classical communication. That is to say, the controlled quantum secure direct communication protocol failed. In the above description $|\psi\rangle_{12}\otimes|\psi\rangle_{34}$ is chosen as the initial state of the total system. In fact, similar results can also be achieved provided that other choices of the initial states are given and the condition of evolving process is same as the case presented above. We can hold the following equations if we change the initial state of atoms 3 and 4.

$$\begin{aligned}|\psi^{-}\rangle_{125}\otimes|\psi^{+}\rangle_{34}=\frac{1}{4}[&(|gg\rangle_{13}-i|ee\rangle_{13})(|ee\rangle_{24}-i|gg\rangle_{24})|e\rangle_5\\&-i(|eg\rangle_{13}-i|ge\rangle_{13})(|ge\rangle_{24}-i|eg\rangle_{24})|g\rangle_5\\&+i(|ge\rangle_{13}-i|eg\rangle_{13})(|eg\rangle_{24}-i|ge\rangle_{24})|e\rangle_5\\&+(|ee\rangle_{13}-i|gg\rangle_{13})(|gg\rangle_{24}-i|ee\rangle_{24})|g\rangle_5],\end{aligned}\tag{9}$$

$$\begin{aligned}|\psi^{-}\rangle_{125}\otimes|\phi^{-}\rangle_{34}=\frac{1}{4}[&(|ge\rangle_{13}-i|eg\rangle_{13})(|ee\rangle_{24}-i|gg\rangle_{24})|e\rangle_5\\&-i(|ee\rangle_{13}-i|gg\rangle_{13})(|ge\rangle_{24}-i|eg\rangle_{24})|g\rangle_5\\&-i(|gg\rangle_{13}-i|ee\rangle_{13})(|eg\rangle_{24}-i|ge\rangle_{24})|e\rangle_5\\&-(|eg\rangle_{13}-i|ge\rangle_{13})(|gg\rangle_{24}-i|ee\rangle_{24})|g\rangle_5],\end{aligned}\tag{10}$$

$$\begin{aligned}|\psi^{-}\rangle_{125}\otimes|\phi^{+}\rangle_{34}=\frac{1}{4}[&(|ge\rangle_{13}-i|eg\rangle_{13})(|ee\rangle_{24}-i|gg\rangle_{24})|e\rangle_5\\&-i(|ee\rangle_{13}-i|gg\rangle_{13})(|ge\rangle_{24}-i|eg\rangle_{24})|g\rangle_5\end{aligned}$$

$$+ i(|gg\rangle_{13} - i|ee\rangle_{13})(|eg\rangle_{24} - i|ge\rangle_{24})|e\rangle_5$$
$$+ (|eg\rangle_{13} - i|ge\rangle_{13})(|gg\rangle_{24} - i|ee\rangle_{24})|g\rangle_5]. \quad (11)$$

From (8)–(11) one can see that different results by the detection of atoms 1, 3 and 2, 4 do not correspond to different initial states for the above four known initial states. For examples, when $|ee\rangle_{13}$ and $|ee\rangle_{24}$ are obtained, the initial state may be $|\psi^-\rangle_{12} \otimes |\psi^+\rangle_{34}$ or $|\psi^-\rangle_{12} \otimes |\psi^-\rangle_{34}$; while if $|eg\rangle_{13}$ and $|ee\rangle_{24}$ are obtained, the initial state may be $|\psi^-\rangle_{12} \otimes |\phi^+\rangle_{34}$ or $|\psi^-\rangle_{12} \otimes |\phi^-\rangle_{34}$; and so on.
If Charlie would like to help Bob with the communication, he should perform the Hadamard operation in the following forms on atom 5 in the basis $|g\rangle$, $|e\rangle$.

$$H|g\rangle = \frac{1}{\sqrt{2}}(|g\rangle + |e\rangle),\ H|e\rangle = \frac{1}{\sqrt{2}}(|g\rangle - |e\rangle), \quad (12)$$

the evolution of the total system in (8)–(11) is presented as follows

$$|\psi^-\rangle_{125} \otimes |\psi^-\rangle_{34} = \frac{\sqrt{2}}{4}[(-|ee\rangle_{13}|gg\rangle_{24} - |eg\rangle_{13}|eg\rangle_{24} - |ge\rangle_{13}|ge\rangle_{24}$$
$$+ |gg\rangle_{13}|ee\rangle_{24})|g\rangle_5] + i(|ee\rangle_{13}|ee\rangle_{24} - |eg\rangle_{13}|ge\rangle_{24}$$
$$+ |ge\rangle_{13}|eg\rangle_{24} + |gg\rangle_{13}|gg\rangle_{24})|e\rangle_5], \quad (13)$$
$$|\psi^-\rangle_{125} \otimes |\psi^+\rangle_{34} = \frac{1}{2}[(-i|ee\rangle_{13}|ee\rangle_{24} - i|eg\rangle_{13}|ge\rangle_{24} + i|ge\rangle_{13}|eg\rangle_{24}$$
$$- i|gg\rangle_{13}|gg\rangle_{24}])|g\rangle_5] + (|ee\rangle_{13}|gg\rangle_{24} - |eg\rangle_{13}|eg\rangle_{24}$$
$$- |ge\rangle_{13}|ge\rangle_{24} - |gg\rangle_{13}|ee\rangle_{24})|e\rangle_5], \quad (14)$$
$$|\psi^-\rangle_{125} \otimes |\phi^-\rangle_{34} = \frac{1}{2}[(-|ee\rangle_{13}|eg\rangle_{24} - |eg\rangle_{13}|gg\rangle_{24} + |ge\rangle_{13}|ee\rangle_{24}$$
$$- |gg\rangle_{13}|ge\rangle_{24})|g\rangle_5 + i(-|ee\rangle_{13}|ge\rangle_{24} - |eg\rangle_{13}|ee\rangle_{24}$$
$$- |ge\rangle_{13}|gg\rangle_{24} + |gg\rangle_{13}|eg\rangle_{24})|e\rangle_5], \quad (15)$$
$$|\psi^-\rangle_{125} \otimes |\phi^+\rangle_{34} = \frac{1}{2}[i(-|eg\rangle_{13}|ee\rangle_{24} - |ge\rangle_{13}|gg\rangle_{24} + |gg\rangle_{13}|eg\rangle_{24}$$
$$- |ee\rangle_{13}|ge\rangle_{24})|g\rangle_5 + (-|ge\rangle_{13}|ee\rangle_{24} + |eg\rangle_{13}|gg\rangle_{24}$$
$$- |gg\rangle_{13}|ge\rangle_{24} - |ee\rangle_{13}|eg\rangle_{24})|e\rangle_5]. \quad (16)$$

From (13)–(16) we can see that, different results by the detection of atoms 1, 3 and 2, 4 do correspond to different initial states for the above four known initial states under the permission of the controller. If Charlie allows the communications between the two users, he performs measurements on his qubit in the state $|g\rangle_5$, for the unitary operations U_{00}, if atoms 1 and 3 are detected in the sate $|ee\rangle_{13}$ ($|eg\rangle_{13}$, $|ge\rangle_{13}$, $|gg\rangle_{13}$), atoms 2 and 4 will collapse affirmatively into $|gg\rangle_{24}$ ($|eg\rangle_{24}$, $|ge\rangle_{24}$, $|ee\rangle_{24}$) with probability $\frac{1}{4}$, thus the total success probability of detection results is equal to 1. Meanwhile, if Alice and Charlie publish their operation information, accordingly, Bob can deduce the initial state of atoms 1, 2, 3, 4, alternatively, he can extract the messages. This means that for a known initial state, after the interaction, the detection results of atoms 1 and 3 are correlated to the state of the atoms 2 and 4.

Let us turn to depict our communication protocol. To begin with, we assumed Alice and Bob have shared a large enough number of two-atom and three-atom maximally entangled state, all in the same state $|\psi^-\rangle_{abc}$ with atom a at Alice's site, b at Bob's hand and c at Charlie's hand, which can be achieved during the free time of communication. Suppose in a certain communication run, Alice wants to send a two-bit classical messages (m, n), with $(m, n) \in \{0, 1\}$ to Bob. Then the procedure can be implemented as follows.

(S1) Alice selects a two-atom and three-atom maximally entangled state, say, $|\psi^-\rangle_{125}$ and $|\psi^-\rangle_{34}$, as the quantum channels, with atoms 1, 3 at Alice's hand, Bob possesses 2, 4 and Charlie has atom 5. For two bits of messages (m, n), Alice encodes the messages on one of her two atoms 1 and 3 by performing a local unitary operation $U_{m,n}$, respectively. Then Alice sends these two atoms 1 and 3 into a single-mode cavity and interact with it simultaneously, at the same time the system are driven by a classical field. The evolution operator of the system is given in (4)–(7). By selecting interaction time which satisfies $\lambda t = \pi/4$ and making the Rabi frequency which satisfies $\Omega t = \pi$, the evolution of the total system is presented in (8)–(11). After the atoms 1 and 3 fly out the cavity, Alice detects the states of them, respectively. Alice informs Bob of the conclusion of her operations and the detection results of atoms 1 and 3.

(S2) After receiving Alice's information, Bob sends atoms 2 and 4 into a cavity and interact with it simultaneously, at the same time two atoms are driven by a classical field. The system evolution is described by (4)–(7). Bob chooses the interaction time and Rabi frequency appropriately such that $\lambda t = \pi/4$, $\Omega t = \pi$, the evolution of the total states is given in (8)–(11). Then Bob detects the states of atoms 2 and 4 respectively.

(S3) Firstly, Bob gets nothing without the help of controller Charlie, as there will be no perfect quantum channel between Alice and Bob. As a consequence, Bob cannot extract Alice's secret messages solely, and the controlled quantum secure direct communication protocol failed. Suppose that the administrative personnel of server, Charlie, wishes to control the correspondence between users. This means that if and only if attaining his permissibility, one can correspond with another. Moreover, the users can make their communication secret to Charlie and not altered during transmission. If Charlie would like to help Alice and Bob to communicate, he first performs a Hadamard operation on his atom. After the above operations, then he measures the atom and informs Alice and Bob of his measurement results via classical communication. The procedure goes. Based on Alice's public announcement and his own detection results, Bob can conclude the operation performed by Alice. Alternatively, he can extract the two-bit messages Alice sends to him (see Table 1).

For example, if Alice wants to send two bits messages (i, j) to Bob. Firstly, Alice performs an operation U_{ij} on atoms 1 or 3 randomly. After the evolution of the atoms and the cavity, we assume Alice's detection results on atoms 1 and 3 is $|ee\rangle_{1,3}$. Now Alice informs Bob of the result of the measurement by the classical channels, after Charlie receives the information, Charlie performs a Hadamard operation on his atom. If his detection results on atoms 5 is $|e\rangle_5$, in the following, through the evolution process of atoms 2, 4 with the cavity, Bob will obtain the state $|eg\rangle_{2,4}$. Accordingly, Bob can deduce the initial state of atoms 1, 2, 3, 4, 5 is $|\psi^-\rangle_{1,2,5} \otimes |\phi^+\rangle_{3,4}$, alternatively, he can extract the messages (1, 1).

Table 1 Corresponding relations among the unitary operations (i.e., the encoding bits), the initial states, and Alice's, Bob's and Charlie's detection results

Alice	Charlie	Bob	Encoding	Alice	Charlie	Bob	Encoding
$\|ee\rangle_{13}$	$\|e\rangle_5$	$\|ee\rangle_{24}$	U_{00}	$\|ee\rangle_{13}$	$\|g\rangle_5$	$\|ee\rangle_{24}$	U_{01}
$\|eg\rangle_{13}$	$\|e\rangle_5$	$\|ee\rangle_{24}$	U_{10}	$\|eg\rangle_{13}$	$\|g\rangle_5$	$\|ee\rangle_{24}$	U_{11}
$\|ge\rangle_{13}$	$\|e\rangle_5$	$\|ee\rangle_{24}$	U_{11}	$\|ge\rangle_{13}$	$\|g\rangle_5$	$\|ee\rangle_{24}$	U_{10}
$\|gg\rangle_{13}$	$\|e\rangle_5$	$\|ee\rangle_{24}$	U_{01}	$\|gg\rangle_{13}$	$\|g\rangle_5$	$\|ee\rangle_{24}$	U_{00}
$\|ee\rangle_{13}$	$\|e\rangle_5$	$\|eg\rangle_{24}$	U_{11}	$\|ee\rangle_{13}$	$\|g\rangle_5$	$\|eg\rangle_{24}$	U_{10}
$\|eg\rangle_{13}$	$\|e\rangle_5$	$\|eg\rangle_{24}$	U_{01}	$\|eg\rangle_{13}$	$\|g\rangle_5$	$\|eg\rangle_{24}$	U_{00}
$\|ge\rangle_{13}$	$\|e\rangle_5$	$\|eg\rangle_{24}$	U_{00}	$\|ge\rangle_{13}$	$\|g\rangle_5$	$\|eg\rangle_{24}$	U_{01}
$\|gg\rangle_{13}$	$\|e\rangle_5$	$\|eg\rangle_{24}$	U_{10}	$\|gg\rangle_{13}$	$\|g\rangle_5$	$\|eg\rangle_{24}$	U_{11}
$\|ee\rangle_{13}$	$\|e\rangle_5$	$\|ge\rangle_{24}$	U_{10}	$\|ee\rangle_{13}$	$\|g\rangle_5$	$\|ge\rangle_{24}$	U_{11}
$\|eg\rangle_{13}$	$\|e\rangle_5$	$\|ge\rangle_{24}$	U_{00}	$\|eg\rangle_{13}$	$\|g\rangle_5$	$\|ge\rangle_{24}$	U_{01}
$\|ge\rangle_{13}$	$\|e\rangle_5$	$\|ge\rangle_{24}$	U_{01}	$\|ge\rangle_{13}$	$\|g\rangle_5$	$\|ge\rangle_{24}$	U_{00}
$\|gg\rangle_{13}$	$\|e\rangle_5$	$\|ge\rangle_{24}$	U_{11}	$\|gg\rangle_{13}$	$\|g\rangle_5$	$\|ge\rangle_{24}$	U_{10}
$\|ee\rangle_{13}$	$\|e\rangle_5$	$\|gg\rangle_{24}$	U_{01}	$\|ee\rangle_{13}$	$\|g\rangle_5$	$\|gg\rangle_{24}$	U_{00}
$\|eg\rangle_{13}$	$\|e\rangle_5$	$\|gg\rangle_{24}$	U_{11}	$\|eg\rangle_{13}$	$\|g\rangle_5$	$\|gg\rangle_{24}$	U_{10}
$\|ge\rangle_{13}$	$\|e\rangle_5$	$\|gg\rangle_{24}$	U_{10}	$\|ge\rangle_{13}$	$\|g\rangle_5$	$\|gg\rangle_{24}$	U_{11}
$\|gg\rangle_{13}$	$\|e\rangle_5$	$\|gg\rangle_{24}$	U_{00}	$\|gg\rangle_{13}$	$\|g\rangle_5$	$\|gg\rangle_{24}$	U_{01}

4 Conclusions and Discussions

In the present protocol, we propose a experimentally feasible new protocol for controlled quantum secure direct communication in cavity QED using the property of local separate measurements instead of joint Bell-state measurement. If the sender (Alice) wants to transmit messages to the receiver (Bob), Charlie must take a Hadamard operation on each of his atom, measure it, and tell the results to Bob and Alice. When GHZ entangled state is successfully shared, no qubit has to be exchanged in a quantum channel. If no eavesdropping is found in the checking procedure, the secret messages can be transmitted successfully. Because there is not a transmission of the qubit that carries the secret messages between Alice and Bob in a public channel, it is completely secure for controlled secure direct communication if a perfect quantum channel is used. After insuring the security of the quantum channels, if Charlie would like to help Alice and Bob to communicate, Alice and Bob can communicate secret messages directly under the control of the third side Charlie. Only with the help of controller Charlie, the sender and the receiver can implement secure direct communication successfully. This protocol can also be generalized to a multi-party control system in which N parties share a large number of N-particle GHZ entangled states. The multi-party controlled secure direct communication can also succeed, anyone of the multi-partners can send messages to any receiver secretly with the help of controllers by using a local operation and a public channel. Since the message transferred only by using local operations and public channels after entanglement was successfully distributed, this protocol can protect the communication against the destroying-travel-qubit-type attack. Finally, to discuss the feasibility of our procedure, 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 [66]. Then we get that the interaction time of atom and cavity is on the order of 10^{-4} s. Then the total time for the whole system

is much shorter than T_r and T_c. Two-atom maximally entangled state can be readily prepared by atom-cavity field interaction and has been experimentally realized [67]. Hence, the present scheme might be realizable based on cavity QED.

Acknowledgements We thank Professor Guang-Can Guo for helpful suggestions. This work is supported by the National Natural Science Foundation of China under Grant No. 10904033, Educational Commission of Hubei Province under Grant No. D20092204 and the Postgraduate Programme of Hubei Normal University under Grant No. 2007D20.

References

1. Bennett, C.H., Brassard, G.: In: Proceedings of IEEE International Conference on Computer, Systems and Signal Processing, Bangalore, India, pp. 175. IEEE, New York (1984)
2. Xue, P., Li, C.F., Guo, G.C.: Phys. Rev. A **65**, 022317 (2002)
3. Hwang, W.Y.: Phys. Rev. Lett. **91**, 057901 (2003)
4. Wang, X.B.: Phys. Rev. Lett. **92**, 077902 (2004)
5. Li, X.H., Deng, F.G., Zhou, H.Y.: Phys. Rev. A **78**, 022321 (2008)
6. Nguyen, B.A.: Phys. Lett. A **328**, 6 (2004)
7. Man, Z.X., Zhang, Z.J., Li, Y.: Chin. Phys. Lett. **22**, 18 (2005)
8. Lucamarini, M., Mancini, S.: Phys. Rev. Lett. **94**, 140501 (2005)
9. Deng, F.G., Long, G.L.: Phys. Rev. A **69**, 052319 (2004)
10. Deng, F.G., Long, G.L., Liu, X.S.: Phys. Rev. A **68**, 042317 (2003)
11. Wang, J., Zhang, Q., Tang, C.J.: Phys. Lett. A **358**, 256 (2006)
12. Jin, X.R., Zhang, Y.Q., Zhang, S., Hong, S.K., Yeon, K.H., Um, C.I.: Phys. Lett. A **354**, 67 (2006)
13. Man, Z.X., Zhang, Z.J., Li, Y.: Chin. Phys. Lett. **22**, 22 (2005)
14. Wojcik, A.: Phys. Rev. Lett. **90**, 157901 (2003)
15. Zhang, Z.J., Man, Z.X., Li, Y.: Phys. Lett. A **333**, 46 (2004)
16. Zhu, A.D., Xia, Y., Fan, Q.B., Zhang, S.: Phys. Rev. A **73**, 022338 (2006)
17. Xia, Y., Fu, C.B., Zhang, S., Hong, S.K., Yeon, K.H., Um, C.I.: J. Korean Phys. Soc. **48**, 24 (2006)
18. Wang, C., Deng, F.G., Li, Y.S., Liu, X.S., Long, G.L.: Phys. Rev. A **71**, 044305 (2005)
19. Li, X.H., Deng, F.G., Zhou, H.Y.: Phys. Rev. A **74**, 054302 (2006)
20. Deng, F.G., Li, X.H., Li, C.Y., Zhou, P., Zhou, H.Y.: Phys. Lett. A **359**(5), 359 (2006)
21. Deng, F.G., Long, G.L., Zhou, H.Y.: Phys. Lett. A **340**, 43 (2005)
22. Deng, F.G., Li, X.H., Li, C.Y., Zhou, P., Zhou, H.Y.: Phys. Lett. A **354**, 190 (2006)
23. Lin, S., Wen, Q.Y., Gao, F., Zhu, F.C.: Phys. Rev. A **79**, 054303 (2009)
24. Lin, S., Wen, Q.Y., Gao, F., Zhu, F.C.: Phys. Rev. A **78**, 064304 (2008)
25. Wang, C., Li, Y.S., Long, G.L.: Commun. Theor. Phys. (Beijing) **46**, 440 (2006)
26. Xia, Y., Song, H.S.: Phys. Lett. A **364**, 117 (2007)
27. Zhang, L.L., Zhan, Y.B., Zhang, Q.Y.: Int. J. Theor. Phys. **48**, 2971 (2009)
28. Xia, Y., Song, J., Nie, J., Song, H.S.: Commun. Theor. Phys. (Beijing) **48**, 841 (2007)
29. Zhang, Z.J., Liu, J., Wang, D., Shi, S.: Phys. Rev. A **75**, 026301 (2007)
30. Liu, J., Liu, Y.M., Cao, H.J., Shi, S.H., Zhang, Z.J.: Chin. Phys. Lett. **23**, 2652 (2006)
31. Zhang, Z.J.: Phys. Lett. A **342**, 60 (2005)
32. Zhang, Z.J., Li, Y., Man, Z.X.: Phys. Lett. A **341**, 385 (2005)
33. Wang, C., Deng, F.G., Long, G.Lu.: Opt. Commun. **253**, 15 (2005)
34. Han, Y.J., Zhang, Y.S., Guo, G.C.: Phys. Lett. A **295**, 61 (2002)
35. Shi, B., Tomita, A.: Phys. Lett. A **296**, 161 (2002)
36. Cao, H.J., Chen, J., Song, H.S.: Commun. Theor. Phys. (Beijing) **45**, 271 (2006)
37. Xiu, X.M., Dong, L., Gao, Y.J., Chi, F.: Opt. Commun. **282**, 2457 (2009)
38. Dong, L., Xiu, X.M., Gao, Y.J., Chi, F.: Opt. Commun. **282**, 1688 (2009)
39. Karlsson, A., Bourennane, M.: Phys. Rev. A **58**, 4394 (1998)
40. Xiu, X.M., Dong, L., Gao, Y.J., Chi, F.: Opt. Commun. **282**, 333 (2009)
41. Wang, J., Zhang, Q., Tang, C.J.: Opt. Commun. **266**, 732 (2006)
42. Yang, C.P., Chu, S., Han, S.: Phys. Rev. A **70**, 022329 (2004)
43. Yang, C.P., Han, S.: Phys. Lett. A **343**, 267 (2005)
44. Man, Z.X., Xia, Y.J., An, N.B.: Phys. Rev. A **75**, 052306 (2007)
45. Li, X.H., Zhou, P., Li, C.Y., Zhou, H.Y., Deng, F.G.: J. Phys., At. Mol. Opt. Phys. **39**, 1975 (2006)
46. SaiToh, A., Rahimi, R., Nakahara, M.: Phys. Rev. A **79**, 062313 (2009)

47. Shan, C.-J., Liu, J.-B., Liu, T.-K., Huang, Y.-X., Li, H.: Int. J. Theor. Phys. **48**, 1516 (2009)
48. Wang, T.Y., Wen, Q.Y., Chen, X.B., Guo, F.Z., Zhu, F.C.: Opt. Commun. **281**, 6130 (2008)
49. Chen, X.B., Zhu, F.C.: Opt. Commun. **282**, 3647 (2009)
50. Zhang, Z.J., Gao, G., Wang, X., Han, L.F., Shi, S.H.: Opt. Commun. **269**, 418 (2007)
51. Han, L.F., Liu, Y.M., Liu, J., Zhang, Z.J.: Opt. Commun. **281**, 2690 (2008)
52. Zhang, Z.J., Li, Y., Man, Z.X.: Phys. Rev. A **71**, 044301 (2005)
53. Markham, D., Sanders, B.C.: Phys. Rev. A **78**, 042309 (2008)
54. Deng, F.G., Li, X.H., Li, C.Y., Zhou, P., Zhou, H.Y.: Eur. Phys. J. D **39**, 459 (2006)
55. Xue, Z.Y., Yi, Y.M., Cao, Z.L.: Physica A **374**, 119 (2007)
56. Xue, Z.Y., Yang, M., Yi, Y.M., Cao, Z.L.: Opt. Commun. **258**, 315 (2006)
57. Cao, Z.L., Zhang, L.H., Yang, M.: Phys. Rev. A **73**, 014303 (2006)
58. Dong, P., Xue, Z.Y., Yang, M., Cao, Z.L.: Phys. Rev. A **73**, 033818 (2006)
59. Yang, M., Song, W., Cao, Z.L.: Phys. Rev. A **71**, 034312 (2005)
60. Zheng, S.B., Guo, G.C.: Phys. Rev. A **73**, 032329 (2006)
61. Zheng, S.B.: Phys. Rev. A **77**, 044303 (2008)
62. Zheng, S.B.: Phys. Rev. A **69**, 055801 (2004)
63. Riebe, M., et al.: Nature **429**, 734 (2004)
64. Barrett, M.D., et al.: Nature **429**, 737 (2004)
65. Zheng, S.B., Guo, G.C.: Phys. Rev. Lett. **85**, 2392 (2000)
66. Brune, M., Hagley, E., Dreyer, J., Maitre, X., Maali, A., Wunderlich, C., Raimond, J.M., Haroche, S.: Phys. Rev. Lett. **77**, 4887 (1996)
67. Osnaghi, S., et al.: Phys. Rev. Lett. **87**, 037902 (2001)