Large payload quantum steganography based on cavity quantum electrodynamics*

Ye Tian-Yu(叶天语)† and Jiang Li-Zhen(蒋丽珍)

College of Information & Electronic Engineering, Zhejiang Gongshang University, Hangzhou 310018, *China*

(Received 7 August 2012; revised manuscript received 20 October 2012)

A large payload quantum steganography protocol based on cavity quantum electrodynamics (QED) is presented in this paper, which effectively uses the evolutionary law of atoms in cavity QED. The protocol builds up a hidden channel to transmit secret messages using entanglement swapping between one GHZ state and one Bell state in cavity QED together with the Hadamard operation. The quantum steganography protocol is insensitive to cavity decay and the thermal field. The capacity, imperceptibility and security against eavesdropping are analyzed in detail in the protocol. It turns out that the protocol not only has good imperceptibility but also possesses good security against eavesdropping. In addition, its capacity for a hidden channel achieves five bits, larger than most of the previous quantum steganography protocols.

Keywords: quantum steganography, hidden capacity, entanglement swapping, Hadamard operation, cavity QED

PACS: 03.67.Dd, 03.65.Hk **DOI:** 10.1088/1674-1056/22/4/040305

1. Introduction

Steganography is a technique that hides a secret message into innocent-looking cover data to make stego data almost the same as cover data. In essence, steganography hides the existence of a secret message to escape from the suspicion of an eavesdropper. Cryptography is the art of scrambling a secret message. In essence, cryptography hides the content of a secret message. However, a secret message scrambled by cryptography is so unreadable that it easily arouses the suspicion of an eavesdropper.

Quantum secure communication has been one of the most ingenious applications of quantum mechanics, which can achieve unconditional security. It mainly includes quantum key distribution (QKD),[1,2] quantum secure direct communication (QSDC),[3–9] quantum secret sharing (QSS),[10–14] and so on. The aim of QKD is to establish an unconditionally secure key between two remote legitimate parties through the transmission of a quantum signal. In 1984, Bennett and Brassard[1] proposed the first QKD protocol (BB84 protocol) using a single particle. In 2002, Long and Liu[2] proposed an efficient two-step QKD protocol. QSDC's object is to transmit a secret message directly between two remote legitimate parties via a quantum channel without establishing a key in advance. In 2002, Beige *et al.*[3] proposed the first QSDC protocol. Then, Bostrom and Felbinger[4] proposed the famous Ping–Pong protocol (BF protocol) in 2002. In 2004, Cai and Li[5] proposed an improved Ping–Pong protocol (IBF) to double the capacity of the Ping–Pong protocol by introducing two additional unitary operations. In 2008, Chen *et al.*[6] proposed a novel controlled QSDC protocol with quantum encryption using a partially entangled GHZ state. In 2008, Chen *et al.*[7] proposed a novel three-party controlled QSDC protocol based on the W state. In 2011, Gu *et al.*[8] proposed a two-step QSDC protocol with hyperentanglement in both the spatial-mode and the polarization degrees of freedom of photon pairs. In 2012, Huang *et al.*[9] proposed two robust channel-encrypting QSDC protocols over different collective-noise channels. QSS is the generalization of classical secret sharing to a quantum scenario, where only when all parties cooperate together can they obtain the secret message sent by the initial sender through the transmission of the quantum signal. In 1999, Hillery *et al.*[10] proposed the first QSS protocol based on the Greenberger–Horne–Zeilinger (GHZ) state. In 2003, Guo G P and Guo G C[11] proposed a QSS protocol only using product states. In 2010, Yang *et al.*[12] put forward a novel three-party QSS protocol of secure direct communication based on χ-type entangled states. In 2012, Zhu *et al.*[13] made an improvement on the QSS protocol in Ref. [12] to prevent Bob from legally obtaining secret messages without being detected. In 2012, Chen *et al.*[14] put forward a three-party QSS protocol via the entangled GHZ state using the single-particle quantum state to encode the information. In recent years, based on the efforts of researchers, quantum secure communication, including QKD, QSDC, QSS, and so on, has been greatly developed.

In the meanwhile, quantum data hiding (QDH)[15,16] was also presented, which is derived from the QSS. The feature of QDH is that some parties are unable to extract a secret message

*Project supported by the National Natural Science Foundation of China (Grant No. 60972071) and the Natural Science Foundation of Zhejiang Province, China (Grant Nos. LQ12F02012 and Y6100421).

†Corresponding author. E-mail: flystu008@yahoo.com.cn

© 2013 Chinese Physical Society and IOP Publishing Ltd

only by using local operations together with classical communication. Quantum steganography,[17–22] which has been regarded as a new branch of quantum secure communication in recent years, is the generalization of classical steganography to a quantum scenario. It always builds up a hidden channel within a normal quantum channel to transmit a secret message, and can be used in covert communication and quantum identity authentication and so on. In 2002, Gea-Banacloche[17] encoded the arbitrary quantum data using a quantum error-correcting code (QECC) and hid a secret message as errors. In 2004, Worley III[18] presented a fuzzy quantum watermarking scheme based on the relative frequency of error in observing qubits in a dissimilar basis from the one where they were written. In 2007, Martin[19] presented a quantum steganography protocol based on the BB84 protocol.[1] In 2010, Liao *et al.*[20] proposed a multi-party quantum steganography protocol based on Guo *et al.*'s QSS protocol.[11] In 2010, Qu *et al.*[21] presented a new quantum steganography protocol with a large payload based on the improved Ping–Pong protocol (IBF).[5] In 2011, Qu *et al.*[22] presented a new quantum steganography protocol with a large payload based on the entanglement swapping of χ-type entangled states.

However, most of the above quantum steganography protocols[17–21] have the drawback of small hidden capacity. The hidden capacity of Ref. [17] is only one bit or one qubit. The hidden capacity in each of Refs. [18]–[20] is also only one bit. We think that the capacity of the hidden channel in each of Refs. [17]–[20] is too small to perform an efficient covert communication. Although the capacity of the hidden channel in Ref. [21] can achieve four bits per round covert communication, we still think that it should be further improved.

In this paper, we aim to enhance the capacity of the hidden channel, since it is a key point for an efficient quantum steganography protocol. A large payload quantum steganography protocol based on cavity quantum electrodynamics (QED) is proposed in the paper, which effectively uses the evolutionary law of atoms in cavity QED. The protocol builds up a hidden channel to transmit secret messages using entanglement swapping between one GHZ state and one Bell state in cavity QED together with the Hadamard operation. The capacity of the hidden channel achieves five bits, larger than those in Refs. [17]–[21].

2. The encoding scheme

As two-atom maximally entangled states, Bell states form a complete orthogonal basis for four-dimensional Hilbert space. Four Bell states are $|\phi^{\pm}\rangle = (1/\sqrt{2})(|gg\rangle \pm |ee\rangle)$ and $|\psi^{\pm}\rangle = (1/\sqrt{2})(|ge\rangle \pm |eg\rangle)$. As three-atom maximally entangled states, GHZ states form a complete orthogonal basis for eight-dimensional Hilbert space. Eight GHZ states are $|S^{\pm}\rangle = (1/\sqrt{2})(|gee\rangle \pm |egg\rangle)$, $|P^{\pm}\rangle = (1/\sqrt{2})(|ggg\rangle \pm |eee\rangle)$, $|Q^{\pm}\rangle = (1/\sqrt{2})(|gge\rangle \pm |eeg\rangle)$, and $|R^{\pm}\rangle = (1/\sqrt{2})(|geg\rangle \pm |ege\rangle)$.

Assume that the atoms A, B, and C are in one of the four GHZ states including $|S^{\pm}\rangle_{ABC} = (1/\sqrt{2})(|gee\rangle \pm |egg\rangle)$ and $|P^{\pm}\rangle_{ABC} = (1/\sqrt{2})(|ggg\rangle \pm |eee\rangle)$, while the atoms D, E are in one of the above four Bell states. Atoms A and D belong to Alice, and Atoms B, C, and E belong to Bob. Alice aims to covertly send secret messages to Bob by quantum channel. $U_0 = I = |g\rangle\langle g| + |e\rangle\langle e|$, $U_1 = \sigma_X = |g\rangle\langle e| + |e\rangle\langle g|$, $U_2 = \mathrm{i}\sigma_Y = |g\rangle\langle e| - |e\rangle\langle g|$, and $U_3 = \sigma_Z = |g\rangle\langle g| - |e\rangle\langle e|$ are four unitary operations. Each unitary operation represents two-bit information as indicated in the following formula:

$$U_0 \to 00, \quad U_1 \to 01, \quad U_2 \to 10, \quad U_3 \to 11. \tag{1}$$

It is apparent that after one of the four unitary operations is performed, the above four Bell states can be transformed into each other. It is also straightforward for the above four GHZ states.

Without loss of generality, assume that the initial state of the atoms A, B, and C is $|S^{-}\rangle_{ABC}$ and the initial state of the atoms D and E is $|\psi^{-}\rangle_{DE}$. Two identical single-mode cavities are considered here. The atoms A and D are sent to Bob by Alice through the quantum channel at first. Afterwards, atoms A and D are simultaneously sent into one single-mode cavity by Bob. Driven by a classical field, atoms A and D simultaneously interact with the single-mode cavity. Then, atoms B and E are simultaneously sent into the other single-mode cavity by Bob. Driven by a classical field, atoms B and E interact with the other single-mode cavity. Under the rotating-wave approximation, the interactive Hamiltonian between the single-mode cavity and the atoms can be expressed as[23–25]

$$\begin{aligned} H \;=\; & \omega_0 S_z + \omega_a a^{\dagger} a + \sum_{j=1}^{2} [g(a^{\dagger} S_j^{-} + a S_j^{\dagger}) \\ & + \Omega(S_j^{\dagger} \mathrm{e}^{-\mathrm{i}wt} + S_j^{-} \mathrm{e}^{\mathrm{i}wt})], \end{aligned} \tag{2}$$

where $S_z = (1/2)\sum_{j=1}^{2}(|e_j\rangle\langle e_j| - |g_j\rangle\langle g_j|)$, $S_j^{-} = |g_j\rangle\langle e_j|$, $S_j^{\dagger} = |e_j\rangle\langle g_j|$, $\langle g_j|$ and $|e_j\rangle$ being the ground and excited states of the j-th atom, and g the atom–cavity coupling strength; a and $a^{\dagger}$ are the annihilation and creation operators for the cavity mode; ω_0, ω_a, ω, and Ω are the atomic transition frequency, the cavity frequency, the classical field frequency, and the Rabi frequency, respectively. Assume that $\omega_0 = \omega$. Accordingly, the evolution operator of the system in the interaction picture can be expressed as[23–25]

$$U(t) = \mathrm{e}^{-\mathrm{i}H_0 t} \mathrm{e}^{-\mathrm{i}H_{\mathrm{e}} t}, \tag{3}$$

where $H_0 = \Omega \sum_{j=1}^{2}(S_j^{\dagger} + S_j^{-})$ and H_{e} is the effective Hamiltonian. Considering the large detuning case $\delta \gg g$ (δ is the detuning between ω_0 and ω_a) and the strong driving regime $\Omega \gg \delta, g$, there is no energy exchange between the atomic

system and the cavity. As a result, the effects of cavity decay and thermal field are eliminated. Then, in the interaction picture, the effective interaction Hamiltonian H_e can be described by[23–25]

$$H_e = (\lambda/2)\Big[\sum_{j=1}^{2}(|e_j\rangle\langle e_j| + |g_j\rangle\langle g_j|) + \sum_{i,j=1,i\neq j}^{2}(S_i^{\dagger}S_j^{-} + S_i^{\dagger}S_j^{\dagger} + \text{H.C.})\Big], \quad (4)$$

where $\lambda = g^2/2\delta$. Rabi frequency and the interaction time are consistently chosen by Bob to satisfy $\Omega t = \pi$ and $\lambda t = \pi/4$ in both evolutionary cases. After the Hadamard operation ($H = (1/\sqrt{2})[(|g\rangle + |e\rangle)\langle g| + (|g\rangle - |e\rangle)\langle e|]$) is performed on the atom C, the total system finally evolves into

$$\begin{aligned}
&|S^-\rangle_{ABC}\otimes|\psi^-\rangle_{DE}\\
&= (\sqrt{2}/4)[(-\mathrm{i}|gg\rangle_{AD}|gg\rangle_{BE} + \mathrm{i}|eg\rangle_{AD}|eg\rangle_{BE}\\
&\quad + \mathrm{i}|ge\rangle_{AD}|ge\rangle_{BE} - \mathrm{i}|ee\rangle_{AD}|ee\rangle_{BE})|g\rangle_C + (-|gg\rangle_{AD}|ee\rangle_{BE}\\
&\quad - |eg\rangle_{AD}|ge\rangle_{BE} + |ge\rangle_{AD}|eg\rangle_{BE} + |ee\rangle_{AD}|gg\rangle_{BE})|e\rangle_C]. \quad (5)
\end{aligned}$$

Extending $|\psi^-\rangle_{DE}$ to other three Bell states $|\psi^+\rangle_{DE}$, $|\phi^-\rangle_{DE}$, and $|\phi^+\rangle_{DE}$, if the evolving conditions and processes are the same as the above, the total system will respectively evolve into

$$\begin{aligned}
&|S^-\rangle_{ABC}\otimes|\psi^+\rangle_{DE}\\
&= (\sqrt{2}/4)[(-|ee\rangle_{AD}|gg\rangle_{BE} - |eg\rangle_{AD}|ge\rangle_{BE}\\
&\quad + |ge\rangle_{AD}|eg\rangle_{BE} + |gg\rangle_{AD}|ee\rangle_{BE})|g\rangle_C + (\mathrm{i}|gg\rangle_{AD}|gg\rangle_{BE}\\
&\quad + \mathrm{i}|eg\rangle_{AD}|eg\rangle_{BE} + \mathrm{i}|ge\rangle_{AD}|ge\rangle_{BE} + \mathrm{i}|ee\rangle_{AD}|ee\rangle_{BE})|e\rangle_C], \quad (6)\\
&|S^-\rangle_{ABC}\otimes|\phi^-\rangle_{DE}\\
&= (\sqrt{2}/4)[(-\mathrm{i}|gg\rangle_{AD}|ge\rangle_{BE} + \mathrm{i}|eg\rangle_{AD}|ee\rangle_{BE}\\
&\quad + \mathrm{i}|ge\rangle_{AD}|gg\rangle_{BE} - \mathrm{i}|ee\rangle_{AD}|eg\rangle_{BE})|g\rangle_C + (-|gg\rangle_{AD}|eg\rangle_{BE}\\
&\quad - |eg\rangle_{AD}|gg\rangle_{BE} + |ge\rangle_{AD}|ee\rangle_{BE} + |ee\rangle_{AD}|ge\rangle_{BE})|e\rangle_C], \quad (7)\\
&|S^-\rangle_{ABC}\otimes|\phi^+\rangle_{DE}\\
&= (\sqrt{2}/4)[(-|eg\rangle_{AD}|gg\rangle_{BE} + |ge\rangle_{AD}|ee\rangle_{BE}\\
&\quad - |ee\rangle_{AD}|ge\rangle_{BE} + |gg\rangle_{AD}|eg\rangle_{BE})|g\rangle_C + (\mathrm{i}|ge\rangle_{AD}|gg\rangle_{BE}\\
&\quad + \mathrm{i}|eg\rangle_{AD}|ee\rangle_{BE} + \mathrm{i}|ee\rangle_{AD}|eg\rangle_{BE} + \mathrm{i}|gg\rangle_{AD}|ge\rangle_{BE})|e\rangle_C]. \quad (8)
\end{aligned}$$

According to formulas (5)–(8), after the evolution of the total system, each result of atoms A and D, atoms B and E, and atom C does correspond only to one initial state among the above four known initial states. Four collections composed of different results of atoms A and D, atoms B and E, and atom C after evolution can be coded as

$$\begin{aligned}
&\{|gg\rangle_{AD}|gg\rangle_{BE}|g\rangle_C, |eg\rangle_{AD}|eg\rangle_{BE}|g\rangle_C, |ge\rangle_{AD}|ge\rangle_{BE}|g\rangle_C,\\
&|ee\rangle_{AD}|ee\rangle_{BE}|g\rangle_C, |gg\rangle_{AD}|ee\rangle_{BE}|e\rangle_C, |eg\rangle_{AD}|ge\rangle_{BE}|e\rangle_C,\\
&|ge\rangle_{AD}|eg\rangle_{BE}|e\rangle_C, |ee\rangle_{AD}|gg\rangle_{BE}|e\rangle_C\} \to 00, \quad (9)\\
&\{|ee\rangle_{AD}|gg\rangle_{BE}|g\rangle_C, |eg\rangle_{AD}|ge\rangle_{BE}|g\rangle_C, |ge\rangle_{AD}|eg\rangle_{BE}|g\rangle_C,\\
&|gg\rangle_{AD}|ee\rangle_{BE}|g\rangle_C, |gg\rangle_{AD}|gg\rangle_{BE}|e\rangle_C, |eg\rangle_{AD}|eg\rangle_{BE}|e\rangle_C,\\
&|ge\rangle_{AD}|ge\rangle_{BE}|e\rangle_C, |ee\rangle_{AD}|ee\rangle_{BE}|e\rangle_C\} \to 11, \quad (10)\\
&\{|gg\rangle_{AD}|ge\rangle_{BE}|g\rangle_C, |eg\rangle_{AD}|ee\rangle_{BE}|g\rangle_C, |ge\rangle_{AD}|gg\rangle_{BE}|g\rangle_C,\\
&|ee\rangle_{AD}|eg\rangle_{BE}|g\rangle_C, |gg\rangle_{AD}|eg\rangle_{BE}|e\rangle_C, |eg\rangle_{AD}|gg\rangle_{BE}|e\rangle_C,\\
&|ge\rangle_{AD}|ee\rangle_{BE}|e\rangle_C, |ee\rangle_{AD}|ge\rangle_{BE}|e\rangle_C\} \to 01. \quad (11)\\
&\{|eg\rangle_{AD}|gg\rangle_{BE}|g\rangle_C, |ge\rangle_{AD}|ee\rangle_{BE}|g\rangle_C, |ee\rangle_{AD}|ge\rangle_{BE}|g\rangle_C,\\
&|gg\rangle_{AD}|eg\rangle_{BE}|g\rangle_C, |ge\rangle_{AD}|gg\rangle_{BE}|e\rangle_C, |eg\rangle_{AD}|ee\rangle_{BE}|e\rangle_C,\\
&|ee\rangle_{AD}|eg\rangle_{BE}|e\rangle_C, |gg\rangle_{AD}|ge\rangle_{BE}|e\rangle_C\} \to 10. \quad (12)
\end{aligned}$$

Further extending $|S^-\rangle_{ABC}$ to other three GHZ states $|S^+\rangle_{ABC}$, $|P^+\rangle_{ABC}$, and $|P^-\rangle_{ABC}$, all the result collections composed of different results of atoms A and D, atoms B and E, and atom C after evolution from different initial states of atoms A, B, and C and atoms D and E are listed in Table 1 (i). Take the initial state of atoms A, B, and C to be $|P^+\rangle_{ABC}^{10}$ and the initial state of atoms D and E to be $|\phi^+\rangle_{DE}^{10}$ for example. The superscripts in both $|P^+\rangle_{ABC}^{10}$ and $|\phi^+\rangle_{DE}^{10}$ denote that performing U_2 on the first atom can transform $|S^-\rangle_{ABC}$ to $|P^+\rangle_{ABC}$ and $|\psi^-\rangle_{DE}$ to $|\phi^+\rangle_{DE}$ respectively, while 11 denotes that the result collection composed of the results of atoms A and D, atoms B and E, and atom C after evolution from $|P^+\rangle_{ABC}$ and $|\phi^+\rangle_{DE}$ corresponds to formula (10).

In addition, if atoms A, B, and C are in one of the four GHZ states including $|Q^{\pm}\rangle = (1/\sqrt{2})(|gge\rangle \pm |eeg\rangle)$ and $|R^{\pm}\rangle = (1/\sqrt{2})(|geg\rangle \pm |ege\rangle)$, and atoms D and E are still in one of the four Bell states, all the result collections composed of different results of atoms A and D, atoms B and E, and atom C after evolution from different initial states of the atoms A, B, and C, and the atoms D and E will be shown in Table 1 (ii).

Table 1. The result collections composed of different results of atoms A and D, the B and E, and atom C after evolution from different initial states of the atoms A, B, and C, and the atoms D and E (The superscript denotes the codes of U_j, $j = 0, 1, 2, 3$).

(i)

	$\|\psi^+\rangle_{DE}^{11}$	$\|\psi^-\rangle_{DE}^{00}$	$\|\phi^+\rangle_{DE}^{10}$	$\|\phi^-\rangle_{DE}^{01}$
$\|S^+\rangle_{ABC}^{11}$	00	11	01	10
$\|S^-\rangle_{ABC}^{00}$	11	00	10	01
$\|P^+\rangle_{ABC}^{10}$	10	01	11	00
$\|P^-\rangle_{ABC}^{01}$	01	10	00	11

(ii)

	$\|\psi^+\rangle_{DE}^{11}$	$\|\psi^-\rangle_{DE}^{00}$	$\|\phi^+\rangle_{DE}^{10}$	$\|\phi^-\rangle_{DE}^{01}$
$\|Q^+\rangle_{ABC}^{11}$	10	01	11	00
$\|Q^-\rangle_{ABC}^{00}$	01	10	00	11
$\|R^+\rangle_{ABC}^{10}$	00	11	01	10
$\|R^-\rangle_{ABC}^{01}$	11	00	10	01

3. Quantum steganography protocol

The goal of our quantum steganography protocol is to covertly transmit secret messages from Alice to Bob by build-

ing up a hidden channel within a normal quantum channel. The secret messages are grouped by three bits. Our quantum steganography protocol is illustrated in detail as follows.

Step 1 Preparation mode

A large number of $|\psi^-\rangle_{DE}$ are prepared by Bob as the initial states of atoms D and E. If the first bit from each group of secret messages is 1, a large number of $|S^-\rangle_{ABC}$ will be prepared by Bob as the initial states of atoms A, B, and C; otherwise, a large number of $|Q^-\rangle_{ABC}$ will be prepared by Bob as the initial states of the atoms A, B, and C. Let G_A, G_B, G_C, G_D, and G_E represent the atom groups of A, B, C, D, and E, respectively. Hence, $G_A = [A_1, A_2, \ldots, A_n]$, $G_B = [B_1, B_2, \ldots, B_n]$, $G_C = [C_1, C_2, \ldots, C_n]$, $G_D = [D_1, D_2, \ldots, D_n]$, and $G_E = [E_1, E_2, \ldots, E_n]$. Bob transmits atom D in G_D to Alice through a quantum channel at first, and they perform eavesdropping checking together. Afterwards, Bob transmits atom A in G_A to Alice through a quantum channel, and they perform eavesdropping checking together. Consequently, if there is no eavesdropping, Alice holds G_A and G_D, and Bob holds G_B, G_C, and G_E.

Step 2 Control mode

Substep 2a Eavesdropping checking for the transmission of the atom D in G_D.

(2a1) Alice selects a large enough subgroup from G_D, randomly measures atom D_i under the Z-basis $\{|g\rangle, |e\rangle\}$ or X-basis $\{|+\rangle, |-\rangle\}$, where $|+\rangle = 1/\sqrt{2}(|g\rangle + |e\rangle)$ and $|-\rangle = 1/\sqrt{2}(|g\rangle - |e\rangle)$, and publishes her measurement basis and corresponding measurement result to Bob through the classical channel;

(2a2) Bob measures E_i from the corresponding subgroup of G_E under the same basis;

(2a3) By comparing Alice's measurement result, Bob knows if there is eavesdropping. If the channel is safe, their measurement results are highly correlated. For example, when Alice and Bob perform a Z-basis, Bob's measurement result should be $|g\rangle$ ($|e\rangle$) if Alice obtains the measurement result $|e\rangle(|g\rangle)$. Then, if Bob confirms that there is an eavesdropping, they abort the communication; otherwise, they enter into Substep (2b);

Substep 2b Eavesdropping checking for the transmission of the atom A in G_A.

(2b1) Alice selects a large enough subgroup from G_A, randomly measures atom A_i under the Z-basis or X-basis, and publishes her measurement basis and corresponding measurement result to Bob through the classical channel;

(2b2) Bob measures B_i from the corresponding subgroup of G_B and C_i from the corresponding subgroup of G_C under the same basis;

(2b3) By comparing Alice's measurement result, Bob can know if there is eavesdropping. If the channel is safe, their measurement results are highly correlated. Then, if Bob confirms that there is eavesdropping, they abort the communication; otherwise, they enter into information transmission mode.

Step 3 Information transmission mode

Substep 3a According to the bits sequence of information, the unitary operations are performed by Alice on the atoms in G_A and G_D, respectively (Note that after performed unitary operations, G_A and G_D turn into G'_A and G'_D, respectively. Although no unitary operations have been performed on the atoms in G_B, G_C, and G_E, for consistence, G'_B, G'_C, and G'_E are still used to represent the original G_B, G_C, and G_E, respectively. Accordingly, G'_B is the same as G_B, G'_C is the same as G_C, and G'_E is the same as G_E);

Substep 3b Two atoms A'_m, A'_{m+1} are chosen by Alice from G'_A according to the final two bits from each group of secret messages, and the secret messages hiding mode follows;

Substep 3c G'_A and G'_D are sent back to Bob by Alice through a quantum channel;

Substep 3d After G'_A and the value of m are obtained, a GHZ-basis measurement is performed by Bob on $A'_m B'_m C'_m$ to recover the information they carried and the first bit from each group of secret messages.

Step 4 Secret messages hiding mode

Substep 4a According to the final two bits from each group of secret messages, two atoms A'_m and A'_{m+1} are chosen by Alice from G'_A, where the subscript m represents the position of the atom A'_m in G'_A. The value of m must satisfy the consistent condition, which means that the GHZ initial state formed by $A'_m B'_m C'_m$ and the Bell initial state formed by $D'_m E'_m$ must be consistent with the final two bits from each group of secret messages, which is shown in Table 1 (An appropriate m can be determined by Alice in advance before sending m to Bob by implementing QSDC or one-time pad through a classical channel.[21,22]);

Substep 4b By performing the same unitary operation on A_{m+1} in advance, $A'_{m+1} B'_{m+1} C'_{m+1}$ can copy the information carried by $A'_m B'_m C'_m$. Consequently, $A'_{m+1} B'_{m+1} C'_{m+1}$ does not normally transmit information but acts as an auxiliary GHZ state to help hide secret messages.

Step 5 The atoms A'_{m+1} and D'_m are simultaneously sent into one single-mode cavity by Bob. Driven by a classical field, the atoms A'_{m+1} and D'_m simultaneously interact with the single-mode cavity. The Rabi frequency and the interaction time are chosen by Bob to satisfy $\Omega t = \pi$ and $\lambda t = \pi/4$.

Step 6 The atoms B'_{m+1} and E'_m are simultaneously sent into the other single-mode cavity by Bob. Driven by a classical field, the atoms B'_{m+1} and E'_m simultaneously interact with the other single-mode cavity. The Rabi frequency and the interaction time are chosen by Bob to satisfy $\Omega t = \pi$ and $\lambda t = \pi/4$.

Step 7 Secret messages decoding mode

Substep 7a The Hadamard operation is performed on the atom C'_{m+1} by Bob;

Substep 7b After flying out the single-mode cavity, the states of the atoms A'_{m+1} and D'_m are detected by Bob under the Z-basis, respectively;

Substep 7c After flying out the other single-mode cavity, the states of the atoms B'_{m+1} and E'_m are detected by Bob under the Z-basis, respectively;

Substep 7d The state of the atom C'_{m+1} is detected by Bob under the Z-basis;

Substep 7e Based on the detection results of the atoms A'_{m+1} and D'_m, the atoms B'_{m+1} and E'_m, and the atom C'_{m+1}, the final two bits from each group of secret messages can be decoded by Bob, according to formulas (9)–(12). Then, according to the state of $A'_mB'_mC'_m$, the first bit from each group of secret messages can be decoded by Bob. Finally, with the final two bits from each group of secret messages together with the state of $A'_mB'_mC'_m$, the information carried by $D'_mE'_m$ can also be recovered by Bob, according to Table 1.

We use an example to explain our quantum steganography protocol. Assuming that a group of secret messages Alice wants to send to Bob is **111**, and the information sequence $\cdots$ $\mathbf{11}_{00}\cdots\mathbf{00}_{11}\cdots$ $\mathbf{10}_{10}\cdots\mathbf{01}_{01}\cdots$ is generated by Alice (The information is divided by four bits, since two U_j's denote four-bit information). In Step 1, a large number of $|\psi^-\rangle_{DE}$ are prepared as the initial states of the atoms D and E, and a large number of $|S^-\rangle_{ABC}$ are prepared as the initial states of the atoms A, B, and C, since the first bit from this group of secret messages is **1**. In Step 3, the unitary operations are performed by Alice on G_A and G_D, respectively, according to the information sequence. Assume that the group numbers of $\mathbf{11}_{00}$, $\mathbf{00}_{11}$, $\mathbf{10}_{10}$, and $\mathbf{01}_{01}$ in the information sequence are Nos. 3, 7, 11, and 16, respectively. In Step 4, Alice can make m =3, 7, 11 or 16 to satisfy the consistency in Table 1 (i). If m =3, $A'_3B'_3C'_3$ will be $|S^+\rangle$ and $D'_3E'_3$ will be $|\psi^-\rangle$. Accordingly, the group of secret messages **111** is transmitted after entanglement swapping between $A'_4B'_4C'_4$ and $D'_3E'_3$ in cavity QED together with Hadamard operation. The group of secret messages **111** can also be transmitted in the same way, if m =7, 11 or 16. $A'_4B'_4C'_4$ cannot be used to transmit the information like other normal GHZ states, and acts as an auxiliary GHZ state to help hide secret messages. In Step 7, the Hadamard operation is performed by Bob on the atom C'_4. Afterward, the states of atoms A'_4 and D'_3, the states of atoms B'_4 and E'_3, and the state of atom C'_4 are detected by Bob under the Z-basis, respectively. According to formulas (9)–(12), it can be decoded by Bob that the final two bits from this group of secret messages are **11**. Then, according to the state of $A'_3B'_3C'_3$, it can be decoded by Bob that the first bit from this group of secret messages is **1**. Finally, through the final two bits from this group of secret messages together with the state of $A'_3B'_3C'_3$, according to Table 1 (i), it can be easily judged by Bob that the information carried by $D'_3E'_3$ is **00**.

4. Analysis

4.1. Capacity and quantum resource used

In the above quantum steganography protocol, each three-bit secret message is transmitted by entanglement swapping between one GHZ state of $A'_{m+1}B'_{m+1}C'_{m+1}$ and one Bell state of $D'_mE'_m$ in cavity QED together with the Hadamard operation ($A'_{m+1}B'_{m+1}C'_{m+1}$ copies the information carried by $A'_mB'_mC'_m$ and acts as an auxiliary GHZ state to help hide secret messages). It is apparent that each three-bit secret message can be transmitted by four different kinds of initial states. For example, according to Table 1 (i), **111** can be transmitted by four different kinds of initial states $\{|S^+\rangle^{11}_{ABC},|\psi^-\rangle^{00}_{DE}\}$, $\{|S^-\rangle^{00}_{ABC},|\psi^+\rangle^{11}_{DE}\}$, $\{|P^+\rangle^{10}_{ABC},|\phi^+\rangle^{10}_{DE}\}$, and $\{|P^-\rangle^{01}_{ABC},|\phi^-\rangle^{01}_{DE}\}$. After coding these four different kinds of initial states by the following formula:

$$1100\rightarrow 00,\ 0011\rightarrow 01,\ 1010\rightarrow 10,\ 0101\rightarrow 11, \quad (13)$$

the capacity of the hidden channel in the above quantum steganography protocol can be increased to five bits. Consequently, the capacity of the hidden channel is five times that of Refs. [17]– [20], respectively, and 1.25 times that of Ref. [21]. However, the capacity of Ref. [22], which achieves eight bits, is 1.6 times that of our quantum steganography protocol. It can be concluded that our quantum steganography protocol has advantages over most of those previous quantum steganography protocols in the capacity of the hidden channel.

Since all the quantum steganography protocols in Refs. [21] and [22] and our protocol use entanglement swapping to build up a hidden channel, we make a comparison in the quantum resource used among them. Without considering the preparation mode and the control mode, in order to transmit a five-bit secret message and four-bit information successfully, our protocol needs to communicate three qubits (i.e., A'_m, D'_m, and A'_{m+1}) from Alice to Bob, and use five qubits (i.e., a GHZ state of $A'_mB'_mC'_m$ and a Bell state of $D'_mE'_m$) as a normal quantum resource together with consuming three qubits (i.e., a GHZ state of $A'_{m+1}B'_{m+1}C'_{m+1}$) as the auxiliary quantum resource in total. Moreover, five Z-basis measurements (i.e., measurements on A'_{m+1}, D'_m, B'_{m+1}, E'_m, and C'_{m+1}), and a GHZ-basis measurement (i.e., measurements on $A'_mB'_mC'_m$) are performed in total. In Ref. [21], without considering the preparation mode and the control mode, in order to transmit a four-bit secret message and four-bit information successfully, it needs to communicate three qubits (i.e., A'_{m-1}, A'_m, and A'_{m+1}) from Alice to Bob, and use four qubits (i.e., a Bell state of $A'_{m-1}B'_{m-1}$ and a Bell state of $A'_mB'_m$) as a normal quantum resource together with consuming two qubits (i.e., a Bell

state of $A'_{m+1}B'_{m+1}$) as an auxiliary quantum resource in total. Moreover, three Bell-basis measurements (i.e., measurements on $A'_mA'_{m+1}$, $B'_mB'_{m+1}$, and $A'_{m-1}B'_{m-1}$) are performed in total. In Ref. [22], without considering the preparation mode and the control mode, in order to transmit an eight-bit secret message and eight-bit information successfully, it needs to communicate six qubits (i.e., P_1^{m-1}, P_3^{m-1}, P_1^m, P_3^m, P_1^{m+1}, and P_3^{m+1}) from Alice to Bob, and use eight qubits (i.e., a χ-type state of $|\chi^{ij}\rangle_{3214}^{m-1}$ and a χ-type state of $|\chi^{pq}\rangle_{3'2'1'4'}^{m}$) as a normal quantum resource together with consuming four qubits (i.e., a χ-type state of $|\chi^{ij}\rangle_{3214}^{m+1}$) as an auxiliary quantum resource in total. Moreover, two CMB-basis measurements (i.e., measurements on particle groups $[P_3^m, P_1^{m+1}, P_2^m, P_4^{m+1}]$ and $[P_3^{m+1}, P_1^m, P_2^{m+1}, P_4^m]$) and one FMB-basis measurement (i.e., measurement on $|\chi^{ij}\rangle_{3214}^{m-1}$) are performed in total. It can be concluded that the capacity of Ref. [22] is larger than that of our protocol and that of Ref. [21] at the cost of more quantum resource being used.

4.2. Imperceptibility

In our quantum steganography protocol, the choice of m is not arbitrary for Alice, since the value of m must satisfy the consistent condition with respect to $A'_mB'_mC'_m$, $D'_mE'_m$ and the final two bits from each group of secret messages. Consequently, the imperceptibility mainly depends on the difficulty of knowing m by Eve. As pointed out in Refs. [21] and [22], choosing m can still be treated as arbitrary behavior for Eve, since both information and secret message can be regarded as being random or pseudo-random. If information or secret message is not distributed randomly in advance, pseudo-random sequence encryption can be adopted to make its distribution randomized.

For example, if a group of secret messages Alice wants to send to Bob is **111**, in order to choose m, Alice needs to find out all the group numbers of "$\mathbf{11}_{00}$", "$\mathbf{00}_{11}$", "$\mathbf{10}_{10}$", "$\mathbf{01}_{01}$" in the information sequence. Accordingly, the states of $A'_mB'_mC'_m$ and $D'_mE'_m$ will be "$|S^+\rangle|\psi^-\rangle$", "$|S^-\rangle|\psi^+\rangle$", "$|P^+\rangle|\phi^+\rangle$", and "$|P^-\rangle|\phi^-\rangle$", respectively. If the information is distributed evenly, the probability for each of "$\mathbf{11}_{00}$", "$\mathbf{00}_{11}$", "$\mathbf{10}_{10}$", and "$\mathbf{01}_{01}$" will be $1/16$. Consequently, their total probability is $1/4$. It is straightforward if a group of secret messages is **100**, or **101**, or **110**. Therefore, the probability distributions of information and secret messages will make m's uncertainty best, according to Shannon's information theory, as pointed out in Refs. [21] and [22]. Consequently, choosing m can be regarded as being random for Eve. This means that the imperceptibility of our quantum steganography protocol is good.

4.3. Security

The security of our quantum steganography protocol is based on the security for the transmission of G_D and G_A from Bob to Alice.

We now analyze the security for the transmission of the atom D in G_D from Bob to Alice at first. According to the Stinespring dilation theorem, the eavesdropping of Eve can be realized by a unitary operation $\hat{E}$ on a larger Hilbert space, $|x,E\rangle \equiv |x\rangle|E\rangle$. Then, the state of the composite system constructed by Bob, Alice, and Eve is

$$|\psi\rangle = \sum_{a,b\in\{g,e\}} |\varepsilon\rangle|a\rangle|b\rangle, \tag{14}$$

where $|\varepsilon\rangle$ denotes Eve's probe state, $|a\rangle$ and $|b\rangle$ are single-atom states of Alice and Bob in each Bell state, respectively. The condition on the states of Eve's probe is

$$\sum_{a,b\in\{g,e\}} \langle\varepsilon|\varepsilon\rangle = 1. \tag{15}$$

Eve can only eavesdrop G_D before the first checking, and Eve's effect on the system will be

$$\hat{E}|g,E\rangle = \hat{E}|g\rangle|E\rangle = \alpha_1|g\rangle|\varepsilon_{00}\rangle + \beta_1|e\rangle|\varepsilon_{01}\rangle, \tag{16}$$

$$\hat{E}|e,E\rangle = \hat{E}|e\rangle|E\rangle = \beta'_1|g\rangle|\varepsilon_{10}\rangle + \alpha'_1|e\rangle|\varepsilon_{11}\rangle. \tag{17}$$

Then, the whole system will be

$$\begin{aligned}|\psi\rangle \;=\; & \frac{1}{\sqrt{2}}[(\alpha_1|g\rangle|\varepsilon_{00}\rangle + \beta_1|e\rangle|\varepsilon_{01}\rangle)|e\rangle \\ & -(\beta'_1|g\rangle|\varepsilon_{10}\rangle + \alpha'_1|e\rangle|\varepsilon_{11}\rangle)|g\rangle],\end{aligned} \tag{18}$$

where ε_{00}, ε_{01}, ε_{10}, and ε_{11} are Eve's states, respectively. Moreover, Eve's probe operator can be expressed as

$$\hat{E} = \begin{pmatrix} \alpha_1 & \beta'_1 \\ \beta_1 & \alpha'_1 \end{pmatrix}. \tag{19}$$

Since $\hat{E}$ is a unitary operator, the complex numbers α_1, β_1, α'_1, and β'_1 should satisfy

$$E\hat{E}^\dagger = 1. \tag{20}$$

Consequently, we can obtain the following relationship

$$|\alpha_1|^2 = |\alpha'_1|^2, \quad |\beta_1|^2 = |\beta'_1|^2. \tag{21}$$

Then, the error rate introduced by Eve's eavesdropping on G_D will be

$$\tau_1 = |\beta_1|^2 = |\beta'_1|^2 = 1 - |\alpha_1|^2 = 1 - |\alpha'_1|^2. \tag{22}$$

Therefore, Eve's eavesdropping on G_D will inevitably introduce an error rate, and be discovered by Alice and Bob.

Without loss of generality, we take the measurement-resend attack on G_D for example to further explain the error rate introduced by Eve's eavesdropping. Eve intercepts the atom D in G_D, randomly measures it in the Z-basis or X-basis, and resends his measurement result to Alice. In the first case, Eve performs a Z-basis measurement. The state of the whole system will collapse to $|g\rangle_D|e\rangle_E$ or $|e\rangle_D|g\rangle_E$ each with probability $1/2$. Take the state $|g\rangle_D|e\rangle_E$ for example. Accordingly, Eve resends $|g\rangle_D$ to Alice. Then, if Alice performs a

Z-basis measurement to check eavesdropping, no error will be introduced by Eve. If Alice performs an X-basis measurement, the state collapses to $|+\rangle_D|+\rangle_E$, $|+\rangle_D|-\rangle_E$, $|-\rangle_D|+\rangle_E$ or $|-\rangle_D|-\rangle_E$ each with probability $1/4$. As a result, the error rate introduced by Eve will be 50%. Therefore, the total error rate in this case is 25%. In the second case, Eve performs an X-basis measurement. The state of the whole system will collapse to $|+\rangle_D|-\rangle_E$ or $|-\rangle_D|+\rangle_E$ each with probability $1/2$. Take the state $|+\rangle_D|-\rangle_E$ for example. Accordingly, Eve resends $|+\rangle_D$ to Alice. Then, if Alice performs a Z-basis measurement to check eavesdropping, the state collapses to $|g\rangle_D|g\rangle_E$, $|g\rangle_D|e\rangle_E$, $|e\rangle_D|g\rangle_E$ or $|e\rangle_D|e\rangle_E$ each with probability $1/4$. As a result, the error rate introduced by Eve will be 50%. If Alice performs an X-basis measurement, no error will be introduced by Eve. Therefore, the total error rate in this case is 25%. Therefore, the random Z-basis or X-basis measurement guarantees that Eve's measurement-resend attack on G_D, can be found out by an eavesdropping check.

The security for the transmission of G_A from Bob to Alice can be analyzed in a similar way as mentioned above. After Eve eavesdrops G_A before the second checking, the whole system will be

$$\begin{aligned}|S\rangle \;&= \frac{1}{\sqrt{2}}[(\alpha_2|g\rangle|\varepsilon_{00}\rangle+\beta_2|e\rangle|\varepsilon_{01}\rangle)|ee\rangle\\ &\quad-(\beta_2'|g\rangle|\varepsilon_{10}\rangle+\alpha_2'|e\rangle|\varepsilon_{11}\rangle)|gg\rangle]\end{aligned}\tag{23}$$

or

$$\begin{aligned}|Q\rangle \;&= \frac{1}{\sqrt{2}}[(\alpha_2|g\rangle|\varepsilon_{00}\rangle+\beta_2|e\rangle|\varepsilon_{01}\rangle)|ge\rangle\\ &\quad-(\beta_2'|g\rangle|\varepsilon_{10}\rangle+\alpha_2'|e\rangle|\varepsilon_{11}\rangle)|eg\rangle].\end{aligned}\tag{24}$$

Finally, by deducing in the same way as mentioned above, we can know that the error rate introduced by Eve's eavesdropping on G_A will be

$$\tau_2=|\beta_2|^2=|\beta_2'|^2=1-|\alpha_2|^2=1-|\alpha_2'|^2.\tag{25}$$

It can also be concluded that Eve's eavesdropping on G_A will inevitably introduce an error rate, and be discovered by Alice and Bob.

Without loss of generality, we take the measurement-resend attack on G_A for example to further explain the error rate introduced by Eve's eavesdropping. Assume that $|S^-\rangle_{ABC}$ is prepared by Bob as the initial states of the atoms A, B, and C. Eve intercepts the atom A in G_A, randomly measures it in the Z-basis or X-basis, and resends his measurement result to Alice. In the first case, Eve performs a Z-basis measurement. The state of the whole system will collapse to $|g\rangle_A|e\rangle_B|e\rangle_C$ or $|e\rangle_A|g\rangle_B|g\rangle_C$ each with a probability of $1/2$. Take the state $|g\rangle_A|e\rangle_B|e\rangle_C$ for example. Accordingly, Eve resends $|g\rangle_A$ to Alice. Then, if Alice performs a Z-basis measurement to check eavesdropping, no error will be introduced by Eve. If Alice performs an X-basis measurement, the state collapses to $|+\rangle_A|+\rangle_B|+\rangle_C$, $|+\rangle_A|+\rangle_B|-\rangle_C$, $|+\rangle_A|-\rangle_B|+\rangle_C$, $|+\rangle_A|-\rangle_B|-\rangle_C$, $|-\rangle_A|+\rangle_B|+\rangle_C$, $|-\rangle_A|+\rangle_B|-\rangle_C$, $|-\rangle_A|-\rangle_B|+\rangle_C$ or $|-\rangle_A|-\rangle_B|-\rangle_C$ each with probability $1/8$. As a result, the error rate introduced by Eve will be 50%. Therefore, the total error rate in this case is 25%. In the second case, Eve performs an X-basis. The state of the whole system will collapse to $|+\rangle_A|+\rangle_B|-\rangle_C$, $|+\rangle_A|-\rangle_B|+\rangle_C$, $|-\rangle_A|+\rangle_B|+\rangle_C$ or $|-\rangle_A|-\rangle_B|-\rangle_C$ each with probability $1/4$. Take the state $|+\rangle_A|+\rangle_B|-\rangle_C$ for example. Accordingly, Eve resends $|+\rangle_A$ to Alice. Then, if Alice performs a Z-basis measurement to check eavesdropping, the state collapses to $|g\rangle_A|g\rangle_B|g\rangle_C$, $|g\rangle_A|g\rangle_B|e\rangle_C$, $|g\rangle_A|e\rangle_B|g\rangle_C$, $|g\rangle_A|e\rangle_B|e\rangle_C$, $|e\rangle_A|g\rangle_B|g\rangle_C$, $|e\rangle_A|g\rangle_B|e\rangle_C$, $|e\rangle_A|e\rangle_B|g\rangle_C$ or $|e\rangle_A|e\rangle_B|e\rangle_C$ each with a probability of $1/8$. As a result, the error rate introduced by Eve will be 75%. If Alice performs an X-basis measurement, no error will be introduced by Eve. Therefore, the total error rate in this case is 37.5%. Therefore, the random Z-basis or X-basis measurement guarantees that Eve's measurement-resend attack on G_A can be found out by an eavesdropping check. If $|Q^-\rangle_{ABC}$ is prepared by Bob as the initial states of the atoms A, B, and C, the same conclusion can be drawn with respect to Eve's measurement-resend attack on G_A.

Further consider the influence caused by the leakage of m. Assume that Eve obtains not only m but also D_m' and A_{m+1}' through some advanced eavesdropping attacks (It is possible for Eve to eavesdrop D_m' and A_{m+1}', since atom D and atom A are travelling). However, Eve still cannot obtain secret messages, because Eve does not know that a Hadamard operation has been performed on atom C_{m+1}' by Bob. Moreover, even if Eve knows about the Hadamard operation, according to formulas (9)–(12), only knowing D_m' and A_{m+1}' is not enough to decode secret messages.

5. Conclusion

In this paper, we present a large payload quantum steganography protocol based on cavity QED, which effectively uses the evolution law of atom in cavity QED. The protocol builds up a hidden channel to transmit secret messages using entanglement swapping between one GHZ state and one Bell state in cavity QED together with the Hadamard operation. It is insensitive to cavity decay and the thermal field. Its imperceptibility and security can be guaranteed. Furthermore, the capacity of the hidden channel achieves five bits, larger than those for most of those previous quantum steganography protocols.

References

[1] Bennett C H and Brassard G 1984 *Proc. IEEE Int. Conf. Computers, Systems and Signal Processin*g, December 9–12, 1984, Bangalore, India (New York: IEEE) p. 175

[2] Long G L and Liu X S 2002 *Phys. Rev. A* **65** 032302
[3] Beige A, Englert B G, Kurtsiefer C and Weinfurter H 2002 *Acta Phys. Pol. A* **101** 357
[4] Bostrom K and Felbinger T 2002 *Phys. Rev. Lett.* **89** 187902
[5] Cai Q Y and Li B W 2004 *Phys. Rev. A* **69** 054301
[6] Chen X B, Wang T Y, Du J Z, Wen Q Y and Zhu F C 2008 *Int. J. Quantum Inf.* **6** 543
[7] Chen X B, Wen Q Y, Guo F Z, Sun Y, Xu G and Zhu F C 2008 *Int. J. Quantum Inf.* **6** 899
[8] Gu B, Huang Y G, Fang X and Zhang C Y 2011 *Chin. Phys. B* **20** 100309
[9] Huang W, Wen Q Y, Jia H Y, Qin S J and Gao F 2012 *Chin. Phys. B* **21** 100308
[10] Hillery M, Buzek V and Berthiaume A 1999 *Phys. Rev. A* **59** 1829
[11] Guo G P and Guo G C 2003 *Phys. Lett. A* **310** 247
[12] Yang Y G, Gao W F and Wen Q Y 2010 *Chin. Phys. B* **19** 050306
[13] Zhu Z C, Zhang Y Q and Fu A M 2012 *Chin. Phys. B* **21** 010307
[14] Chen X B, Niu X X, Zhou X J and Yang Y X 2013 *Quantum Inf. Process.* **12** 365
[15] Terhal B M, DiVincenzo D P and Leung D W 2001 *Phys. Rev. Lett.* **86** 5807
[16] Eggeling T and Werner R F 2002 *Phys. Rev. Lett.* **89** 097905
[17] Gea-Banacloche J 2002 *J. Math. Phys.* **43** 4531
[18] Worley III G G 2004 arXiv: ph/0401041v2
[19] Martin K 2007 *IH2007, LNCS* **4567** 32
[20] Liao X, Wen Q Y, Sun Y and Zhang J 2010 *J. Syst. Software* **83** 1801
[21] Qu Z G, Chen X B, Zhou X J, Niu X X and Yang Y X 2010 *Opt. Commun.* **283** 4782
[22] Qu Z G, Chen X B, Luo M X, Niu X X and Yang Y X 2011 *Opt. Commun.* **284** 2075
[23] Shan C J, Liu J B, Chen T, Liu T K, Huang Y X and Li H 2010 *Int. J. Theor. Phys.* **49** 334
[24] Zheng S B 2003 *Phys. Rev. A* **68** 035801
[25] Zheng S B and Guo G C 2000 *Phys. Rev. Lett.* **85** 2392