A novel quantum information hiding protocol based on entanglement swapping of high-level Bell states*

Xu Shu-Jiang(徐淑奖)[a)b)†], Chen Xiu-Bo(陈秀波)[b)c)],
Wang Lian-Hai(王连海)[a)], Niu Xin-Xin(钮心忻)[b)], and Yang Yi-Xian(杨义先)[b)]

[a)] *Shandong Provincial Key Laboratory of Computer Networks, Shandong Computer Science Center (National Supercomputer Center in Jinan), Jinan* 250014, *China*

[b)] *Information Security Center, State Key Laboratory of Networking and Switching Technology, Beijing University of Posts and Telecommunications, Beijing* 100876, *China*

[c)] *State Key Laboratory of Information Security, Institute of Information Engineering, Chinese Academy of Sciences, Beijing* 100093, *China*

(Received 6 August 2014; revised manuscript received 26 December 2014; published online 27 March 2015)

Using entanglement swapping of high-level Bell states, we first derive a covert layer between the secret message and the possible output results of the entanglement swapping between any two generalized Bell states, and then propose a novel high-efficiency quantum information hiding protocol based on the covert layer. In the proposed scheme, a covert channel can be built up under the cover of a high-level quantum secure direct communication (QSDC) channel for securely transmitting secret messages without consuming any auxiliary quantum state or any extra communication resource. It is shown that this protocol not only has a high embedding efficiency but also achieves a good imperceptibility as well as a high security.

Keywords: quantum information hiding, quantum covert channel, entanglement swapping, high-level Bell states

PACS: 03.67.Dd, 03.67.–a, 03.65.–w, 03.67.Hk **DOI:** 10.1088/1674-1056/24/5/050306

1. Introduction

For realizing secure communication utilizing quantum mechanical systems, many researchers have made great efforts to investigate quantum cryptographic protocols in the past few years. A well-known example are the quantum key distribution (QKD) protocols that provide a novel way for two legitimate parties to establish an unconditionally secure shared key. Since the first QKD, namely, the BB84 protocol,[1] was proposed by Bennett and Brassard in 1984, research on QKD has made rapid progress[2,3] in the last 30 years. Following the proposal of QKD and the proof of its unconditional security, researchers have tried to achieve other cryptographic tasks with quantum mechanical effects, such as quantum secure direct communication (QSDC),[4–6] quantum secret sharing (QSS),[7,8] quantum information hiding, and so on.

Information hiding is the art and science of hiding messages within another innocuous looking medium and transmitting the resulting data over a communication channel so that the secret message is not readable apart from the sender and the intended recipient. As an alternative method for privacy and security, information hiding has been widely employed in the covert exchange of information[9] and copyright protection.[10] The idea of combining the classical information hiding and the quantum secure communication has formed a new research area, named quantum information hiding. Just like the quantum steganography protocol,[11–13] the quantum covert channel protocol is one of the important subdisciplines of the quantum information hiding protocol. The quantum covert channel (QCC)[14–20] can be defined as a quantum communication channel that transfers some kind of information using a method originally not intended to transfer this kind of information. The idea of building a quantum covert channel for sending secret messages is a contribution to the field of quantum information hiding, which was first proposed by Qu *et al.*[14,15] using entanglement swapping of quantum states. Respectively based on the entanglement swapping of GHZ states and the entanglement swapping between one GHZ state and one Bell state in cavity quantum electrodynamics, Ye and Jiang[16,17] proposed two quantum covert channel protocols in 2013. However, the protocols in Refs. [14]–[17] have the defect of consuming auxiliary quantum states. In 2012, Fatahi and Naseri[18] proposed a quantum information hiding protocol without consuming any auxiliary quantum state. The protocols in Refs. [14] and [18] are both based on the entanglement swapping of Bell states, while the capacity of the former is 4/3 of the latter. Xu *et al.*[19,20] presented the concept of

*Project supported by the National Natural Science Foundation of China (Grant Nos. 61303199, 61272514, 61170272, 61121061, and 61411146001), the Shandong Provincial Natural Science Foundation of China (Grant Nos. ZR2013FM025, ZR2013FQ001, and ZR2014FM003), the Shandong Provincial Outstanding Research Award Fund for Young Scientists of China (Grant Nos. BS2013DX010 and BS2014DX007), the Program for New Century Excellent Talents in Universities, China (Grant No. NCET-13-0681), the National Development Foundation for Cryptological Research, China (Grant No. MMJJ201401012), the Fok Ying Tong Education Foundation, China (Grant No. 131067), and the Shandong Academy of Sciences Youth Fund Project, China (Grant No. 2013QN007).

†Corresponding author. E-mail: xsj3917@163.com

© 2015 Chinese Physical Society and IOP Publishing Ltd

QCC and formally introduced the covert channel into quantum information. They also analyzed why a covert channel can be established within any QSDC channel.[20]

It is pointed out that the QCC protocol has the advantages of large capacity and high security.[14,15] The capacity of the QCC protocols in Refs. [14]–[17] can be $2/3$ of that of the QSDC channel used in them. While the capacity of most quantum steganography protocols is small, in which only a one-bit (qubit) secret message is transmitted in each round of covert communication. Due to the excellent imperceptibility, the QCC is imperceptible except for the participants of the communication. So the QCC protocol is at least as secure as the given quantum communication channel. Note that the covert channel is distinct from steganography in three aspects. Firstly, the carrier of steganography is another object, while the carrier of the covert channel is a communication (cryptography) protocol. Secondly, the steganography cannot be performed in some high secure operation systems, while the covert channel can tunnel through secure operating systems with special control measures. Thirdly, after embedding the secret messages, the carrier of a steganography protocol is usually slightly modified, while the carrier of the covert channel has no perceptible change.

In this paper, we further study the QCC protocol based on the entanglement swapping of quantum states. Without consuming any auxiliary quantum state or extra quantum communication resource, a new QCC protocol is proposed based on a high-level QSDC protocol. We first employ the entanglement swapping to build up a covert layer between the secret message and the possible output results of entanglement swapping between any two generalized Bell states. A covert channel can then be built up within a given QSDC channel for securely transmitting secret messages. Here the given QSDC channel utilizes the superdense coding rule to encode information, and the covert channel uses the covert layer to encode secret messages. The generalized Bell states, which are encoded to carry the information dits in the given QSDC channel, are taken as the output states of the entanglement swapping for the covert layer. The two parties of the communication do not need to perform any quantum operation on the covert channel, all they need to do in the covert channel is classical computing. Therefore, the sender/receiver can encode/decode the secret message without consuming any auxiliary quantum state or any extra communication except the QSDC in the secret message encoding/decoding process. Because the eavesdropping check technique with decoy photon is adopted, the new protocol can effectively prevent the intercept–resend attack, the measurement–resend attack, and the ancilla attack. Furthermore, due to the use of Bell states in the high-level Hilbert space, the proposed scheme has some important advantages, such as generality and high resource capacity. In other words, this protocol achieves a high communication efficiency and a high security.

The rest of this paper is organized as follows. The covert layer based on the entanglement swapping of d-level Bell states is briefly introduced in Section 2. Section 3 draws a QCC protocol on the basis of the covert layer. The performance of the protocol including capacity, imperceptibility, and security is analyzed in Section 4. Two possible variations of the proposed protocol are suggested to enhance its performance in Section 5. Finally, Section 6 concludes this paper.

2. The covert layer based on the entanglement swapping of high-level Bell states

2.1. The generalized high-level Bell states

Consider a generalization of the familiar Bell states for qudits which were introduced in Refs. [21] and [22]. These d^2 maximally entangled Bell states form an orthonormal basis for the two-qudit space. The generalized d-level two-qudit Bell state has the form

$$|\phi(m,n)\rangle = \frac{1}{\sqrt{d}} \sum_{j=0}^{d-1} \xi^{mj} |j,[j+n]\rangle, \tag{1}$$

where $\xi = \mathrm{e}^{\frac{2\pi \mathrm{i}}{d}}$, $m,n \in \{0,1,\ldots,d-1\}$, and [ ] means the modulo-d operation. When $d=2$, these states can be reduced to the Bell states, which are usually denoted as $|\Phi^{\pm}\rangle = (|00\rangle \pm |11\rangle)/\sqrt{2}$ and $|\Psi^{\pm}\rangle = (|01\rangle \pm |10\rangle)/\sqrt{2}$. Analogous to the Pauli operators for qubits, the generalized Pauli operators for the d-level quantum states are defined as

$$U(m,n) = \frac{1}{\sqrt{d}} \sum_{j=0}^{d-1} \xi^{mj} |j\rangle\langle[j+n]|. \tag{2}$$

When $d=2$, these local unitary operators $U(0,0)$, $U(0,1)$, $U(1,0)$, and $U(1,1)$ reduce to the four Pauli operators I, σ_X, σ_Z, and $\mathrm{i}\sigma_Y$, respectively. Based on the idea of superdense coding, the information can be encoded by applying the encoding unitary operation $U(m,n)$ to one particle of a generalized Bell state.

Suppose that the first particle of a d-level Bell state belongs to Alice and the second to Bob. Only by performing the local unitary operation shown in Eq. (2) on her particle, Alice can transform the given d-level Bell state into another one.[23] The relationship between the initial and the final d-level Bell states is described as

$$U(n,m)|\phi(r,s)\rangle = |\phi([r+n],[s+m])\rangle. \tag{3}$$

2.2. The covert layer based on the entanglement swapping of high-level Bell states

In the proposed protocol, the two parties of the communication will establish a covert channel inside a given QSDC channel to send secret messages. Here the given QSDC channel employs the dense coding method to encode information.

In this subsection, we propose a covert layer to encode secret messages for the covert channel. The tensor product of two generalized Bell states that are encoded to carry the information in the given QSDC channel is taken as the output of the entanglement swapping for the covert layer. Encoding the output of the entanglement swapping between two generalized Bell states into a 4-bit secret message is shown as follows.

Suppose that $|\phi(u_1,u_2)\rangle_{12}$ and $|\phi(v_1,v_2)\rangle_{34}$ are shared by two distant parties, Alice and Bob. Here, Alice has particles 1, 4 and Bob has particles 2, 3. Let us review the entanglement swapping of two generalized Bell states[24–26]

$$\begin{aligned}&|\phi(u_1,u_2)\rangle_{12}|\phi(v_1,v_2)\rangle_{34}\\ &=\frac{1}{d}\sum_{k,l=0}^{d-1}\xi^{kl}|\phi([u_1+k],[v_2+l])\rangle_{14}|\phi([v_1-k],[u_2-l])\rangle_{32},\end{aligned}\quad(4)$$

where the initial states of particles 1, 2 and 3, 4 are $|\phi(u_1,u_2)\rangle$ and $|\phi(v_1,v_2)\rangle$, respectively. Then after performing the generalized Bell measurement on the pair of particles 1 and 4, the input states collapse into one of the states $|\phi([u_1+k],[v_2+l])\rangle_{14}|\phi([v_1-k],[u_2-l])\rangle_{32}$, $(k,l=0,1,\ldots,d-1)$ with equal probability $1/d^2$.

If the result of the entanglement swapping between two states $|\phi(u_1,u_2)\rangle_{12}$ and $|\phi(v_1,v_2)\rangle_{34}$ is $|\phi(u_3,u_4)\rangle_{14}$ and $|\phi(v_3,v_4)\rangle_{32}$,

$$|\phi(u_1,u_2)\rangle_{12}|\phi(v_1,v_2)\rangle_{34}=|\phi(u_3,u_4)\rangle_{14}|\phi(v_3,v_4)\rangle_{32}.\quad(5)$$

according to Eqs. (4) and (5), we can find

$$[u_1+v_1]\equiv[u_3+v_3],\quad[u_2+v_2]\equiv[u_4+v_4].\quad(6)$$

Based on the property of the modulo-d addition, $[u_3+v_3]$, $[u_4+v_4]\in\{0,1,\ldots,d-1\}$. To embed the secret message under the cover of normally transferred information, we establish a covert layer between the secure message and the output results of the entanglement swapping of any two generalized Bell states, as follows:

$$s=s_1s_2=[u_3+v_3+a_1][u_4+v_4+a_2],\quad(7)$$

where a_1,a_2 are two constants and $a_1,a_2\in\{0,1,\ldots,d-1\}$. In fact, s divides the output results of the entanglement swapping of any two generalized Bell states into d^2 classes. On the basis of Eq. (4), there are d^2 possible output results of the entanglement swapping between any two generalized Bell states, i.e., each class of the output result of any two generalized Bell states has d^2 different elements. In addition, both u_3 and u_4 will go through the entire integer from 0 to $d-1$ based on Eq. (4). For example, when $d=3$, the possible output results of $|\phi(0,0)\rangle_{12}|\phi(0,0)\rangle_{34}$ are

$$\begin{aligned}&|\phi(0,0)\rangle_{14}|\phi(0,0)\rangle_{32},\quad|\phi(0,1)\rangle_{14}|\phi(0,2)\rangle_{32},\\ &|\phi(0,2)\rangle_{14}|\phi(0,1)\rangle_{32},\quad|\phi(1,0)\rangle_{14}|\phi(2,0)\rangle_{32},\\ &|\phi(1,1)\rangle_{14}|\phi(2,2)\rangle_{32},\quad|\phi(1,2)\rangle_{14}|\phi(2,1)\rangle_{32},\\ &|\phi(2,0)\rangle_{14}|\phi(1,0)\rangle_{32},\quad|\phi(2,1)\rangle_{14}|\phi(1,2)\rangle_{32},\\ &|\phi(2,2)\rangle_{14}|\phi(1,1)\rangle_{32}.\end{aligned}\quad(8)$$

They are all encoded to a_1a_2 according to Eq. (7). To improve the embedding capacity, the d^2 different elements in each class can be further encoded into d^2 different secret message substrings as follows:

$$\begin{aligned}s&=s_1s_2s_3s_4\\ &=[u_3+v_3+a_1][u_4+v_4+a_2][u_3+a_3][u_4+a_4],\end{aligned}\quad(9)$$

where a_i is constant and $a_i\in\{0,1,\ldots,d-1\}$ $(i=1,2,3,4)$. By this means, the covert layer for embedding secret messages based on the entanglement swapping of any two generalized Bell states can be obtained. For instance, the nine different results in the above example (Eq. (12)) can be respectively encoded to 1111, 1112, 1110, 1121, 1122, 1120, 1101, 1102, and 1100 when $d=3$ and $a_i=1$ $(i=1,2,3,4)$. It is worth noting that the covert layer is more general than that used in Refs. [14] and [18] even $d=2$, because the four constants a_i $(i=1,2,3,4)$ are adopted in this layer. Compared with the layer used in Refs. [14] and [18], this covert layer has a lower computational complexity, since the complicated computation of entanglement swapping is no longer needed.

Suppose that $|\phi(u_3,u_4)\rangle$ and $|\phi(v_3,v_4)\rangle$ are used to encode the information $m_1m_2m_3m_4$ in the given QSDC channel and the initial states of the QSDC channel are $|\phi(r,t)\rangle$, according to Eq. (3) and the superdense encoding rule, we can obtain

$$\begin{aligned}&m_1=[u_3-r],\quad m_2=[u_4-t],\\ &m_3=[v_3-r],\quad m_4=[v_4-t].\end{aligned}\quad(10)$$

Based on Eqs. (9) and (10), the relationship between the generalized Pauli transformations $U(m_1,m_2)$, $U(m_3,m_4)$ and the secret messages $s_1s_2s_3s_4$ can be obtained as

$$\begin{aligned}&s_1=[m_1+m_3+2r+a_1],\quad s_2=[m_2+m_4+2t+a_2],\\ &s_3=[m_1+r+a_3],\quad s_4=[m_2+t+a_4].\end{aligned}\quad(11)$$

Equation (9) or (11) is the covert layer for secret message encoding.

3. Quantum covert channel protocol based on the entanglement swapping of high-level Bell states

Using the covert layer proposed in the above section, a novel protocol for bilayer covert communication is presented in this section. As shown in Fig. 1, the proposed QCC protocol has two communication channels, one is the given QSDC channel which is used to send normal information with the superdense encoding rule, the other is the covert channel which

is established inside the given QSDC channel. Due to the universality and the secrecy of the unitary transformation used in the given QSDC channel,[20] the secret messages can be sent via the proposed QCC, which is imperceptible except for the two participants of the given QSDC channel. The details of the protocol are illustrated as follows.

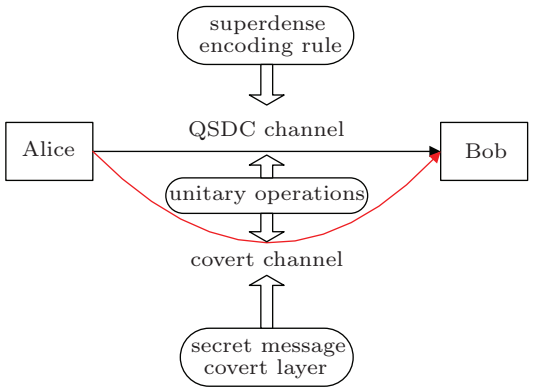


Fig. 1. (color online) The proposed quantum covert channel protocol.

Step 1. Preparation of the initial generalized Bell states

(i) Before performing the protocol, the two parties of the protocol agree that the QSDC channel utilizes the superdense encoding rule, i.e., each of the d^2 unitary operations represents $2\log_2 d$ bit (2 dits) of the classical information based on a given rule, $U(m,n) \mapsto mn$ $(m,n = 0,1,\ldots,d-1)$.

(ii) The intended receiver, Bob, prepares N pairs of entangled particles in the generalized Bell state $S = \{|\phi(0,0)\rangle^n\}$, $n = 1,2,\ldots,N$. Bob takes the first particles from each of the generalized Bell states to build up the traveling sequence $T = [P_1^1, P_1^2, \ldots, P_1^N]$. The remaining partner particles form the home sequence $H = [P_2^1, P_2^2, \ldots, P_2^N]$. Here P_j^i indicates the j-th particle of the i-th generalized Bell state in sequence S.

(iii) Alice and Bob agree on the value of a_i $(i = 1,2,3,4)$ for the covert layer of the covert communication. For convenience, we choose $a_1 = a_2 = a_3 = a_4 = 1$ in this paper.

Step 2. Eavesdropping check for Bob to Alice channel

To prevent the eavesdropper from stealing the information, the decoy photon technique, which is employed in many protocols,[27,28] is used for the eavesdropping check. The eavesdropping check processes are omitted here. If there is no eavesdropping, then they can continue to the next step, otherwise they abort the quantum communication.

Step 3. Information encoding and secret message hiding

(i) **Information encoding** According to the information sequence m_1m_2, m_3m_4, …, $m_{2N-1}m_{2N}$, Alice performs unitary operations $U(m_1,m_2)$, …, $U(m_{2N-1},m_{2N})$ on particles of sequence T to encode information, and then the sequence T is changed into another sequence $T' = [P_{1'}^1, P_{1'}^2, \ldots, P_{1'}^N]$.

(ii) **Secret message encoding** Suppose that Alice wants to send the secret message $s_1s_2s_3s_4$ $(s_i \in \{0,1,\ldots,d-1\})$ over a covert channel under the cover of the QSDC channel. Alice should choose two proper adjacent particles $P_{1'}^m$, $P_{1'}^{m+1}$ from sequence T' which are employed to transfer the information dits $n_1n_2n_3n_4$ in (i). The tensor product of the two encoded generalized Bell states, $|\phi(n_1,n_2)\rangle^m \otimes |\phi(n_3,n_4)\rangle^{m+1}$, is taken as the output of the entanglement swapping for the covert layer. According to Eq. (11), the sequences $n_1n_2n_3n_4$ and $s_1s_2s_3s_4$ must satisfy

$$\begin{aligned} &n_1 = [s_3 - a_3], \quad n_2 = [s_4 - a_4], \\ &n_3 = [s_1 - s_3 + a_3 - a_1], \quad n_4 = [s_2 - s_4 + a_4 - a_2]. \end{aligned} \tag{12}$$

Alice can send the hidden position information m for each pairs of the chosen particles by the QSDC channel.

Step 4. Eavesdropping check for Alice to Bob channel

The eavesdropping check is performed with the decoy photon technique. If the security of the channel is ensured, then they continue to the next step, otherwise they abort the quantum communication.

Step 5. Information decoding

Through sequence H, which retains at home for Bob, keeps intact, for consistently describing with Step 3(i), Bob adopts H' to represent the original H of his own after the second eavesdropping check, i.e., $H' = H = [P_{2'}^1, P_{2'}^2, \ldots, P_{2'}^N]$, $P_{2'}^i = P_2^i$. Bob can decode the information and the hiding data as follows.

(i) **Normal information decoding** Bob performs generalized Bell measurements on each pair of particles in $(P_{1'}^1, P_{2'}^1)$, $(P_{1'}^2, P_{2'}^2)$, …, $(P_{1'}^N, P_{2'}^N)$. According to his measurement results, he can decode the information that is sent through the QSDC channel.

(ii) **The hidden secret message decoding** After receiving the hidden position information m, Bob first decodes the information dits $n_1n_2n_3n_4$ which is carried by the pair of particles $P_{1'}^m$ and $P_{1'}^{m+1}$, and then the secret messages can be gained via the covert layer as follows:

$$\begin{aligned} &s_3 = [n_1 + a_3], \quad s_4 = [n_2 + a_4], \\ &s_1 = [n_1 + n_3 + a_1], \quad s_2 = [n_2 + n_4 + a_2]. \end{aligned} \tag{13}$$

To further illustrate the proposed protocol, let us consider a simple case with 3-level Bell states. Alice sends the information sequence 01 02 11 10 00 11 21 00 20 22 02 01 ⋯ over the QSDC channel, while her purpose is to send secret messages 1112 and 2001 to Bob over the covert channel. Their operation is carried out as follows.

Secret messages encoding According to Eq. (12), Alice should choose the information sequences 0102 and 2022 to hide the secret messages 1112 and 2001, respectively. Since the initial states shared by Alice and Bob are all in $|\phi(0,0)\rangle$

and $T = [P_1^1, P_1^2, \ldots, P_1^{12}, \ldots]$, $H = [P_2^1, P_2^2, \ldots, P_2^{12}, \ldots]$, for sending the given information, Alice needs to perform a sequence of unitary operations $U(0,1), U(0,2), U(1,1), U(1,0), U(0,0), U(1,1), U(2,1), U(0,0), U(2,0), U(2,2), U(0,2), U(0,1), \ldots$ on particles $P_1^1, P_1^2, \ldots, P_1^{12}, \ldots$ according to Eq. (3), and then sends the encoded sequence T' with some decoy photons to Bob. After the encoding operation, the quantum states are changed into $|\phi(0,1)\rangle$, $|\phi(0,2)\rangle$, …, $|\phi(0,1)\rangle$, ….

Secret messages decoding If the security of the channel is confirmed by eavesdropping check, then Bob can perform generalized Bell measurements on each pair of particles in T' and H', and then the information that Alice sends to Bob can be decoded. On the basis of the two hiding position information and the corresponding information sequences 0102 and 2022, which he has received through the QSDC channel, Bob can obtain the secret messages 1112 and 2001 by Eq. (13).

4. Performance analysis

To illustrate the performance of the proposed QCC protocol, the feasibility analysis of the protocol, including capacity analysis, imperceptibility analysis, and security analysis, is given in this section.

4.1. Capacity analysis

The capacity, or embedding payload, indicates the maximum quantity of secret messages that can be transmitted in each round of covert communication. In this protocol, the d-level Bell state instead of the 2-level Bell state is used, each generalized Bell state can be employed to encode a $2\log_2 d$ bits (2 dits) secret message by the covert layer, so the capacity is largely extended. Note that the quantum or classical cost is taken into account in some quantum communication protocols.[29,30] However, the evaluation index, capacity does not take the quantum cost into account. So the index cannot show the efficiency of the covert communication. To describes how many secret messages can be embedded by consuming a one-bit quantum state in a quantum information hiding scheme, reference [19] introduced a new evaluation index, which is called the embedding efficiency,

$$E_{\mathrm{E}} = \frac{C}{ND\log_2 d}, \tag{14}$$

where C is the embedding payload of each round of covert communication, N and d indicate that there are N d-level quantum states consumed in a round of covert communication excluding the quantum states used for eavesdropping check, and D refers to the dimension of the quantum state. If the evaluation index illustrated in Eq. (14) is employed to compute the transmission efficiency (E_{T}) of a QSDC scheme, then we can obtain $E_{\mathrm{T}} = 1$ for a QSDC protocol based on superdense coding, for example, the transmission efficiencies of the QSDC schemes in Refs. [4]–[6] are 1.

According to Section 3, a covert channel can be built up within the given QSDC channel without consuming any auxiliary quantum state. By transferring two particles $P_{1'}^m$ and $P_{1'}^{m+1}$ that carry $4\log_2 d$ bits of information over the QSDC channel, Alice can send a $4\log_2 d$-bit secret message through the covert channel. Bob can decode the information by performing generalized Bell basis measurements on the two pairs of particles $(P_{1'}^m, P_{2'}^m)$ and $(P_{1'}^{m+1}, P_{2'}^{m+1})$. At the same time, he can recover the embedded secret message based on the covert layer. In fact, the role that particles P_1^m and P_1^{m+1} play is information transmission over the QSDC channel, all the participants only need to perform classical computation in the covert channel. Since there are no auxiliary particles consumed except those in the QSDC process, the embedding payload of the proposed protocol is at least $2N\log_2 d$ bits for each round of covert communication by consuming N generalized Bell states which are used for the QSDC process. As a result, the capacity of the covert channel is the same as that of the given QSDC scheme in Ref. [6], which achieves a higher resource capacity. To further enhance the embedding capacity, each of the middle 2-dit information substrings can be used again to encode secret messages. For example, given the contiguous carrier sequences 01, 02, 11, and 10 for $d = 3$, we can use 0102, 0211, and 1110 to respectively embed secret messages 1112, 2110, and 0222, in which the middle two carrier substrings 02 and 11 are used twice. In this way, a $4(N-1)\log_2 d$-bit secret message can be sent in a round of covert communication by transmitting $2N\log_2 d$ bits of information over the QSDC channel, i.e., $C = 4(N-1)\log_2 d$. Because an auxiliary quantum state is consumed for each entanglement swapping of two quantum states in the two protocols in Refs. [14] and [15], the above secret message embedding method cannot be adopted in them.

According to Step 3, each of the position information, m, corresponds a $4\log_2 d$-bit secret message, we can draw the following conclusion.

Theorem 1 The maximum embedding efficiency of the proposed QCC protocol does not exceed 2.

Proof Assume that the position information and the embedded secret messages are transmitted using the same round of QSDC and $d^{2(n-1)} < N \leq d^{2n}$, where N and d are the same as those used in Eq. (14) and n is a positive integer. The total position information that can be sent in a round of QSDC does not exceed N. Because each pair of the generalized Bell states can carry a $4\log_2 d$-bit secret message, we can obtain

$$C \leq 4N\log_2 d. \tag{15}$$

By Eq. (14), the upper bound of the embedding efficiency is

$$E_{\mathrm{E}} \leq 2. \tag{16}$$

If the position information is transmitted by two or more rounds of QSDC so as to send more position information, and one of these rounds is used to transmit the embedded secret message, then C can be larger, but $E_{\rm E}$ is not changed according to Eq. (14).

Since each of the hidden positions is different from the others and the source capacity of the QSDC channel is limited, the total position information which is sent by the QSDC is $\lfloor N/n \rfloor$, thus

$$C = 4\left\lfloor \frac{N}{n} \right\rfloor \log_2 d. \tag{17}$$

By Eq. (14), we have

$$E_{\rm E} = \frac{2}{N}\left\lfloor \frac{N}{n} \right\rfloor, \tag{18}$$

where $\lfloor x \rfloor$ rounds the element of x to the nearest integer less than or equal to x. Obviously, equation (18) satisfies Theorem 1. Following this, we give Theorem 2.

Theorem 2 The maximum $E_{\rm E}$ of the proposed QCC protocol based on QSDC is $\frac{2}{N}\lfloor \frac{N}{n} \rfloor$, where $d^{2(n-1)} < N \leq d^{2n}$, N and d indicate that there are N d-level quantum states consumed in a round of covert communication excluding the particles used for eavesdropping check, and n is a positive integer.

Obviously, $E_{\rm E}$ may achieve the maximum possible value 2, which is almost twice that of the QSDC's transmission efficiency when $N \leq d^2$ (i.e., $n = 1$). Moreover, the larger n is, the smaller $E_{\rm E}$ can be achieved. According to Eq. (18), $E_{\rm E} = 1$ when $n = 2$ and N is an even number, which is the same as the $E_{\rm T}$ of the QSDC protocol.[16] As we know, a QSDC scheme which combines the superdense encoding method achieves a high efficiency. So we advise $N = d^4$ (d is an even number) or $N = d^4 - 1$ (d is an odd number) to achieve a high efficiency for the proposed scheme.

To show that our protocol can achieve the maximum embedding efficiency, two simple examples are given below. Note that we count from the 0th (00 or 0000) hidden position in the two examples.

(i) Suppose that $d = 3, n = 1, N = 9$, and Alice sends the information sequences 01, 12, 10, 02, 21, 00, 11, 20, and 12 to Bob over the QSDC channel, each of the nine information sequences denotes a hidden position. According to the secret message encoding method, the 1st (01), 5th (12), 3rd (10), 2nd (02), 7th (21), 0th (00), 4th (11), 6th (20), and 5th (12) information sequences 1210, 0011, 0221, 1002, 2012, 0112, 2100, 1120, and 0011 can be respectively employed to encode the secret messages sequences 0020, 2211, 0110, 2021, 1001, 2112, 0202, 1222, and 2211. We can obtain the capacity $C = 36\log_2 3$ bits and the embedding efficiency $E_{\rm E} = 2$. Thus, the maximum embedding efficiency in Eq. (18) can be achieved when $n = 1$.

(ii) When $n = 2$, $d = 3$, and $N = 12$, the decimal form of 22 is $8 < 3^2$, so Alice should use a 4-dit information sequence to describe a position information. Suppose that Alice sends the 12 information sequences 00, 10, 00, 20, 01, 01, 00, 22, 00, 12, 00, and 01 to Bob over the QSDC channel, each of the substrings 0010, 0020, 0101, 0022, 0012, and 0001 denotes a position information. Alice can use the 3rd (0010), 6th (0020), 10th (0101), 8th (0022), 5th (0012), and 1st (0001) information substrings 2001, 0022, 0001, 0012, 0100, and 1000 to respectively hide the secret messages sequences 0201, 0011, 1211, 2011, 1212, and 2121. So the capacity and the embedding efficiency are $C = 24\log_2 3$ bits and $E_{\rm E} = 1 = 2/n$, respectively. Thus, the maximum embedding efficiency in Eq. (18) can be achieved when $n > 1$.

Since most of the previous quantum information hiding protocols can embed 1 bit (qbit) in each round of covert communication, their embedding efficiency is smaller than 1. The comparison of capacity and embedding efficiency for five quantum information hiding protocols[12–15,18] and our protocol is shown in Table 1. Obviously, the proposed scheme achieves a high embedding efficiency. The two protocols proposed by Qu *et al.*[14,15] have the same embedding efficiency, and our maximum embedding efficiency is three times of that of Qu's.

Table 1. Comparison of capacity and embedding efficiency for some protocols.

Protocol	Mogos[12]	Liao[13]	Qu10[14]	Qu11[15]	Fatahi[18]	Our protocol
Maximum capacity/bits	1	1	$4N/3$	$8N/3$	N	$4N\log_2 d$
Maximum embedding efficiency	$1/3$	$1/2N$	$2/3$	$2/3$	$1/2$	2

4.2. Imperceptibility analysis

An information hiding scheme is accomplished through embedding a message in another innocuous looking object so as to keep the existence of the hidden data secret. The invisibility is the primary and foremost requirement of an information hiding algorithm because the strength of the information hiding scheme depends on its ability of not being (or hardly being) detected. According to the quantum uncertainty theorem and the no-cloning theorem, the imperceptibility of a quantum information hiding scheme has some natural advantages compared with a classical one. In fact, the protocol including the above Steps 1–5(i) excluding Steps 1(iii) and 3(ii) is just a QSDC protocol. The imperceptibility of the proposed QCC scheme mainly lies in the invisibility of the covert channel.

If the eavesdropper, Eve, attempts to detect the covert channel between Alice and Bob, she can either observe the abnormity caused by the covert communication directly or observe the abnormity of particles from Alice to Bob by performing measurements on the intercepted particles. For the former, it is completely impossible to find out the abnormity, since the proposed QCC protocol that does not consume any auxiliary quantum state seems the same as a QSDC scheme. That is to say, there is no abnormity between the proposed protocol and the QSDC protocol, so Eve has no chance to discover the covert channel. For the latter, Eve can adopt the intercept–resend attack or the auxiliary particle attack. No matter what kind of attack she adopts, it is inevitable to introduce errors that would be detected by Alice and Bob. As a result, Eve fails to find the abnormity of particles from Alice to Bob by the intercept–resend attack or the auxiliary particle attack. Even if she can successfully escape the eavesdropping check via the auxiliary particle attack, Eve can only obtain the measurement result of P_1^i in sequence T on condition that she chooses the correct measurement basis. Since it is impossible to speculate the whole generalized Bell state $|\phi(m,n)\rangle$ only by P_1^i without knowing P_2^i, Eve does not know the information carried by P_1^i in QSDC. Due to the difficulty of getting the hidden position information m, that is guaranteed by the security of the QSDC protocol, Eve is incapable of getting the right position information of the hiding data from the QSDC channel. Consequently, the imperceptibility of the proposed protocol can be guaranteed.

4.3. Security analysis

The security of an information hiding protocol means that the protocol can prevent the secret messages from being attacked or eavesdropped by most of the possible quantum attacks. The QSDC protocol used in this paper seems the same as that in Ref. [5] except the eavesdropping check. From the point view of cryptography, these two QSDC schemes which can be regarded as the same have the same security. Because of the excellent imperceptibility of the proposed protocol, the existence of the covert channel established within the given QSDC channel is imperceptible, while the existence of the QSDC channel is perceptible. From this point of view, the proposed QCC scheme is at least as secure as the QSDC.[5] Even if some information of the given QSDC channel is revealed, the eavesdropper cannot read out the secret messages without knowing the secret key a_i.

Due to the remarkable effects of the eavesdropping check technique with decoy photon, which are shown in many quantum communication protocols,[27,28] any eavesdropper hidden in the quantum channel will be detected, and the proposed protocol can resist all serious attacks brought forward in recent years including the man-in-the-middle attack, the intercept–resend attack, and the auxiliary particle attack. By two rounds of eavesdropping check, the eavesdropper Eve can neither pretend to be Alice nor pretend to be Bob. As a result, Eve can obtain neither the carrier sequence nor the embedded sequence, thus all the classical steganalysis methods shown in Ref. [31] are ineffective. Moreover, since a high-level QSDC protocol provides better security than that obtained with 2-level Bell states,[5] the security of this protocol based on the d-level Bell states is higher than that in Ref. [14] and [18] which is based on the 2-level Bell states. Therefore, the proposed protocol has a high security.

As illustrated in Ref. [5], the QSDC scheme can be used in a noisy channel with the help of quantum privacy amplification by quantum purification and quantum error correction, so the proposed QCC protocol can also be used in a noisy channel in the same way.

5. Two variations to the QCC protocol

To strengthen the performance of the proposed QCC protocol, two possible variations are presented in this section.

5.1. The first variation

In the secret message encoding process given in Section 3, Alice can choose two proper adjacent or non-adjacent particles $P_{1'}^{m_1}, P_{1'}^{m_2}$ from T' which correspond to two generalized Bell states $|\phi(n_1,n_2)\rangle^{m_1}$ and $|\phi(n_3,n_4)\rangle^{m_2}$ ($n_i \in \{0,1,\ldots,d-1\}$, $i=1,2,3,4$), and take the tensor product $|\phi(n_1,n_2)\rangle^{m_1} \otimes |\phi(n_3,n_4)\rangle^{m_2}$ as the output of the entanglement swapping for the covert layer. Here the carrier sequence $n_1n_2n_3n_4$ and the secret message $s_1s_2s_3s_4$ must satisfy Eq. (12) based on the covert layer. Although the quantity of the position information is increased, the confusion for an eavesdropper will also increase. So it is more difficult for the eavesdropper to get the particles' position. As a result, the imperceptibility and security of the proposed protocol are strengthened. However, the maximum embedding efficiency will be decreased because more position information needs to be sent over the given QSDC channel.

Now, let us visit again the example shown at the end of Section 3, where the information sequence is 01 02 11 10 00 11 21 00 20 22 02 01 and the secret message is 1112. In order to send the secret message 1112, Alice can choose $m_1=0$, $m_2=1$; $m_1=0$, $m_2=10$; $m_1=11$, $m_2=1$; or $m_1=11$, $m_2=10$. So there are four choices for Alice in the variation scheme, while there is only one choice in the original protocol. Therefore, the imperceptibility and the security are strengthened significantly. Nevertheless, the position information that needs to be transmitted is twice that of the original protocol for each $4\log_2 d$-bit secret message. According to Eq. (14), the maximum possible embedding efficiency of this variation will be half of that of the original protocol.

5.2. The second variation

A more generalized bipartite d-level entangled pure state instead of the generalized Bell state is suggested for the second variation of the proposed QCC protocol. Recently, Wu *et al.*[32] presented a generalized ping–pong QSDC protocol based on the generalized bipartite d-level entangled pure states and figured out the decoding formula for their QSDC. To extend the original protocol to a more generalized form, we can modify the original protocol with the d-level entangled pure states.

6. Conclusion

Based on the entanglement swapping of d-level Bell states, a covert layer between the output results of the entanglement swapping of any two d-level Bell states and the secret message is established. Under the control of the covert layer, a covert channel can be built up within the QSDC channel to transfer secret messages without consuming any auxiliary quantum state or extra communication resource except the QSDC. Compared with the quantum covert channel protocols in Refs. [14]–[17], this quantum covert channel protocol has three remarkable features. Firstly, this protocol has a low computation complexity. Because high-level Bell states, high-level unitary transformations, and the entanglement swapping between two high-level Bell states all have general term formulas, the complex computation of entanglement swapping is no longer needed. Secondly, this protocol has a high embedding efficiency because it consumes no auxiliary quantum state. Thirdly, this protocol has a large capacity since the high-level quantum states instead of the 2-level quantum states are employed. Furthermore, the performance analysis shows that the proposed protocol has a good imperceptibility and a high security.

The proposed QCC scheme is aimed to perform covert communication with high security. It can be used to covertly transfer secret documents for the government and the military. From a practical point of view, we can transfer any 8 bits (1 byte) secret message, which is an ASCII code and widely used in classical information coding, using 4-level Bell states. Similarly, a decimal (octal or hexadecimal) encoded secret message can quickly be sent using 10-level (8-level or 16-level) Bell states. As mentioned in Refs. [14] and [15], the QCC protocol can be employed to achieve another two purposes: identity authentication and distributed transmission of both common information and secret messages which have different security requirements.

References

[1] Bennett C H and Brassard G 1984 *Proc. IEEE Int. Conf. on Computers, Systems, and Signal Processing*, 12–19 December, 1984, Bangalore, India, p. 175
[2] Ekert A K 1991 *Phys. Rev. Lett.* **67** 661
[3] Li F Y 2014 *Chin. Phys. Lett.* **31** 070302
[4] Deng F G and Long G L 2004 *Phys. Rev. A* **69** 052319
[5] Wang C, Deng F G, Li Y S, Liu X S and Long G L 2005 *Phys. Rev. A* **71** 044305
[6] Lin S, Wen Q Y, Gao F and Zhu F C 2008 *Phys. Rev. A* **78** 064304
[7] Cleve R, Gottesman D and Lo H K 1999 *Phys. Rev. Lett.* **83** 648
[8] Chen X B, Niu X X, Zhou X J and Yang Y X 2013 *Quantum Inf. Process* **12** 365
[9] Bailey K and Curran K 2006 *Multimedia Tools and Applications* **30** 55
[10] Lin E T and Eskicioglu A M 2005 *Proceedings of the IEEE, Special Issue on Advances in Video Coding and Delivery* **93** 171
[11] Shaw B A and Brun T A 2011 *Phys. Rev. A* **83** 022310
[12] Mogos G 2008 *International Symposium on Computer Science and Its Applications*, 13–15 October, 2008, Hobart, Australia, p. 187
[13] Liao X, Wen Q Y, Sun Y and Zhang J 2010 *The Journal of Systems and Software* **83** 1801
[14] Qu Z G, Chen X B, Niu X X and Yang Y X 2010 *Opt. Commun.* **283** 4782
[15] Qu Z G, Chen X B, Niu X X and Yang Y X 2011 *Opt. Commun.* **284** 2075
[16] Ye T Y and Jiang L Z 2013 *Chin. Phys. B* **22** 050309
[17] Ye T Y and Jiang L Z 2013 *Chin. Phys. B* **22** 040305
[18] Fatahi N and Naseri M 2012 *Int. J. Theor. Phys* **51** 2094
[19] Xu S J, Chen X B, Niu X X and Yang Y X 2013 *Sci. Chin. Phys.* **56** 1745
[20] Xu S J, Chen X B, Niu X X and Yang Y X 2013 *Commun. Theor. Phys.* **59** 547
[21] Cerf N J 2000 *Phys. Rev. Lett.* **84** 4497
[22] Cerf N J 2000 *J. Mod. Opt.* **47** 187
[23] Zukowski M, Zeilinger A, Horne M A and Ekert A K 1993 *Phys. Rev. Lett.* **71** 4287
[24] Karimipour V and Bahraminasab B 2000 *Phys. Rev. A* **65** 042320
[25] Bose S, Vedral V and Knight P L 1998 *Phys. Rev. A* **57** 822
[26] Hardy L and Song D D 2000 *Phys. Rev. A* **62** 052315
[27] Chen X B, Wen Q Y, Guo F Z, Sun Y, Xu G and Zhu F C 2008 *Int. J. Quantum Inform.* **6** 899
[28] Chen X B, Wang T Y, Du J Z, Wen Q Y and Zhu F C 2008 *Int. J. Quantum Inform.* **6** 543
[29] Dai H Y, Chen P X, Liang L M and Li C Z 2006 *Phys. Lett. A* **355** 285
[30] Dai H Y, Zhang M and Kuang L E 2008 *Commun. Theor. Phys.* **50** 73
[31] Ashok J, Raju Y, Munisankara S and Srinivas K 2010 *Int. J. Eng. Sci. Technol.* **2** 5985
[32] Wu Y H, Zhai W D, Cao W Z and Li C 2011 *Int. J. Theor. Phys.* **50** 325