CMC, vol.56, no.1, pp.47-59, 2018

A Novel Quantum Stegonagraphy Based on Brown States

Zhiguo Qu[1, *], Tiancheng Zhu[2], Jinwei Wang[1] and Xiaojun Wang[3]

Abstract: In this paper, a novel quantum steganography protocol based on Brown entangled states is proposed. The new protocol adopts the CNOT operation to achieve the transmission of secret information by the best use of the characteristics of entangled states. Comparing with the previous quantum steganography algorithms, the new protocol focuses on its anti-noise capability for the phase-flip noise, which proved its good security resisting on quantum noise. Furthermore, the covert communication of secret information in the quantum secure direct communication channel would not affect the normal information transmission process due to the new protocol's good imperceptibility. If the number of Brown states transmitted in carrier protocol is many enough, the imperceptibility of the secret channel can be further enhanced. In aspect of capacity, the new protocol can further expand its capacity by combining with other quantum steganography protocols. Due to that the proposed protocol does not require the participation of the classic channel when it implements the transmission of secret information, any additional information leakage will not be caused for the new algorithm with good security. The detailed theoretical analysis proves that the new protocol can own good performance on imperceptibility, capacity and security.

Keywords: Quantum steganography, quantum secure direct communication, entanglement, anti-noise robustness.

1 Introduction

With the development of network technology [Qu, Keeney, Robitzsch et al. (2016)], information security [Liu, Wang, Yuan et al. (2016)] becomes more and more important, especially to information hiding. Quantum steganography as a quantum version of steganography, is one of quantum information security techniques by transmitting classical or quantum information through public quantum channels. At present, quantum key distribution (QKD), quantum key agreement (QKA) [Liu, Xu, Yang et al. (2018)], quantum secure direct communication (QSDC) and quantum secret sharing (QSS) are four regular quantum information security techniques. Comparing with other quantum quantum information security techniques, quantum secure direct communication mainly

[1] Jiangsu Engineering Center of Network Monitoring, Nanjing University of Information Science and Technology, Nanjing 210044, P. R. China.

[2] School of Computers & Software, Nanjing University of Information Science and Technology, Nanjing 210044, P. R. China.

[3] School of Electronic Engineering, Dublin City University, Dublin, Ireland.

[*] Corresponding Author: Zhiguo Qu. Email: qzghhh@126.com.

CMC. doi:10.3970/cmc.2018.02215

protects transmitted information by preventing from various eavesdropping attacks. By comparison, quantum steganography builds up the hidden channel for covert communication based on various open quantum secure communication channels, which can achieve high level security for secret information transmitted. Quantum steganography has three important parameters, imperceptibility, capacity and security. In detail, imperceptibility means that the hidden channel cannot be detected or is hardly detected to prevent supervisors or attackers from eavesdropping or attacking it. Capacity denotes maximum quantity of secret messages transmitted per round of covert communication. And security refers to that the protocol can prevent most of the possible quantum attacks or eavesdropping on secret information, even if the hidden channel has been exposed. Among them, imperceptibility is one of the most important performance parameters for quantum steganography.

In general, quantum steganography can be divided into two categories. One is called as Quantum Multi-secret Sharing (QMS) [Chattopadhyay and Sarkar (2007); DiVincenzo (2002); Eggeling and Werner (2002); Gottesman (2000); Guo and Guo (2003); Hayden, Leung and Smith (2005); Hillery, Buzek and Berthiaume (1999); Terhal, Divincenzo and Leung (2001)] which can be generalized to hide the classical information bits in multipartite quantum states for sharing secret information. Participants in this type of steganography can extract embedded secret information through local operations and classic channel. And the other category is called as Quantum Data Hiding (QDH) [Martin (2007); Matthews, Wehner and Winter (2009)] which builds up the hidden channel within the public quantum channel to transmit secret information. Comparing with QMS, QDH is more close to the classical steganography and can more effectively transmit classical secret information. In recent years, quantum steganography has been extensively investigated and achieved a series of achievements. In early stage, many quantum steganography achievements are immature, such as Natori [Natori (2006); Qu, Chen, Zhong et al. (2010); Qu, Chen, Zhong et al. (2011)] by using super-dense coding and [Geabanacloche (2002)] by using quantum error-correcting codes. Although these protocols can transmit secret information securely between parties indeed, these achievements did not clearly describe how to embed secret information into the carrier. In 2007, Martin [Martin (2007)] presented a novel quantum steganography protocol. It was believed as the first quantum steganography protocol to establish one hidden channel within public quantum channel with concrete quantum embedding method. In 2009, Banacloche [Banacloche (2009)] adopted Quantum Error Correcting Code (QECC) to hide secret messages as errors in arbitrary quantum data files. The protocol was mainly based on the BB84 protocol. It analyzed imperceptibility and security in detail, and accurately calculated the capacity of its hidden channel. In 2010, Qu et al. [Qu, Chen, Zhong et al. (2010)] proposed a novel quantum steganographic protocol with large payload. The protocol using entanglement swapping of Bell states for steganography is based on the improved ping-pong protocol. In 2011, Qu et al. [Qu, Chen, Zhong et al. (2011)] using the entanglement of the χ -state with the similar method was proposed with larger capacity and security. In 2015, quantum steganography using prior entanglement was proposed in Mihara [Mihara (2015)]. This protocol embeds the secret information into the carrier information through CNOT operation by using entanglement between the particles. However, due to that its carrier in this protocol is unavailable for both parties and its hidden channel was not built on any public quantum channels, it was with obvious drawback of lacking of imperceptibility considerations.

For most of the current achievements, it usually is assumed that secret information will be transmitted in the ideal noiseless channel. However, in the reality, the public quantum channel is unavoidably noisy, so that most of the current protocols become invalid. In order to resolve this terrible issue, this paper proposes a novel quantum steganography protocol based on QSDC by using Brown states. As with Mihara [Mihara (2015)], the new protocol also adopts prior entanglement to embed or extract secret information through CNOT operations, by making the hidden channel independent of the other carrier channels. As a result, the new protocol has a strong anti-noise robustness and can effectively protect the secret information from many typical quantum noises, especially to the phase-flip noise. With the anti-noise robustness, the new protocol can accurately transmit secret information in quantum noisy channel. Moreover, due to the hidden channel is randomly selected and built, the probability that the attacker detects the hidden channel can be arbitrarily reduced by increasing the transmission scale of the carrier. Therefore, the hidden channel of the new protocol can be considered as very difficult or even impossible to be detected for attackers or eavesdroppers. From the perspective of capacity, there is a great potential for expansion to the new protocol's capacity by combining it with other powerful quantum secure communication protocols. In addition, since the hidden channel of the new protocol will be built up within public quantum carrier protocols with great security, the new protocol's security can be better guaranteed as natural inheritance.

The rest of this paper is organized as follows. In Section 2, we will introduce the operations and preparations of the new protocol as the preliminary knowledge. In Section 3, the specific steps of the new proposed protocol are presented in detail. The anti-noise robustness, imperceptibility, capacity and security of the new protocol will be analyzed in Section 4. The conclusions are given in Section 5.

2 Preliminaries

In this section, the related notations, quantum states and the main operations' definitions are given. And the fundamental methods of embedding and extracting secret information by CNOT operations are also presented in detail as follows.

Firstly, the carrier information $|c_0>$ used in the protocol is the Brown state. And its specific form is shown in the Eq. (1), where the subscripts represent the different qubits.

$$\begin{aligned}|\psi_5>=&\frac{1}{2\sqrt{2}}[|001>(|01>-|10>)+|010>(|00>-|11>)\\&+|100>(|01>+|10>)+|111>(|00>-|11>)]_{12345}\end{aligned} \tag{1}$$

The Brown state $|\psi_5>$ can also be written in the following form.

$$|\psi_5>=\frac{1}{2}(|G_{010}>|00>-|G_{111}>|01>+|G_{001}>|10>-|G_{100}>|11>)_{12534} \tag{2}$$

Here, $|G_{ijk}>$ is one of the three particle GHZ states, and its specific form is given as follow.

$$|G_{ijk}>=\frac{1}{\sqrt{2}}(|0>|j>|k>+(-1)^i|1>|j\oplus 1>|k\oplus 1>) \tag{3}$$

Here, i, j, k={0,1} and $\oplus$ means the modulo-2 addition operation. If the Pauli operations are performed on the qubits 1, 2 and 5 of the Brown state, as shown in the Eq. (2), the state will turn to be

$$\sigma_1^{2S_0}\sigma_2^{2S_1+S_2}\sigma_5^{2S_3+S_4}|\psi_5>=\frac{1}{2}[(-1)^{S_1}|G_{S_0\oplus S_1\oplus S_3,S_2\oplus 1,S4}>|00>+(-1)^{S_1\oplus S_3}|G_{S_0\oplus S_1\oplus S_3\oplus 1,S_2\oplus 1,S_4\oplus 1}>$$

$$|01>+(-1)^{S_3}|G_{S_0\oplus S_1\oplus S_3,S_2,S_4\oplus 1}>|10>-|G_{S_0\oplus S_1\oplus S_3\oplus 1,S_2,S_4}>|11>]_{12534} \tag{4}$$

Here, S_i ϵ {0,1} and σ^i represents the Pauli operation.

$$\sigma^0=I=|0><0|+|1><1|\ ,\ \sigma^1=X=|0><1|+|1><0|$$

$$\sigma^2=Z=|0><0|-|1><1|,\ \sigma^3=-XZ=|0><1|-|1><0| \tag{5}$$

All of these states as shown in the Eq. (4) can construct a mutually orthogonal basis $FMB=\{\sigma_1^{2S_0}\sigma_2^{2S_1+S_2}\sigma_5^{2S_3+S_4}|\psi_5>|s_i=0,1\}$, which satisfies the condition $S_0\oplus S_1\oplus S_2\oplus S_3\oplus S_4=0$.

If one makes a measurement on the qubits 3 and 4 under the basis $BM_1=\{|0+>,|0->,|1+>,|1->\||\pm>=\frac{1}{\sqrt{2}}(|0>\pm|1>)\}$, the state will collapse and the other particles will end up in a corresponding three-qubit entangled state. The state $|\psi_5>$ can be rewritten as

$$|\psi_5>=\frac{1}{2}(|\Phi_0^->|0+>+|\Phi_0^+>|0->+|\Phi_1^->|1+>+|\Phi_1^+>|1->)_{12534} \tag{6}$$

Here, $|\Phi_0^\pm>=\frac{1}{\sqrt{2}}(G_{010}\pm G_{111}),|\Phi_1^\pm>=\frac{1}{\sqrt{2}}(G_{001}\pm G_{100})$. These four states and the other states $|\Phi_2^\pm>=\frac{1}{\sqrt{2}}(G_{000}\pm G_{101}),|\Phi_3^\pm>=\frac{1}{\sqrt{2}}(G_{011}\pm G_{110})$ can form an orthonormal basis AM_1 within the three-qubit Hilbert space. It can be seen that there are four possible results: $|\Phi_0^->|0+>$, $|\Phi_0^+>|0->$, $|\Phi_1^->|1+>$ and $|\Phi_1^+>|1->$. Furthermore, these results appear with the equal probability of 1/4. On the other hand, we also can rewrite the state $|\psi_5>$ as

$$|\psi_5>=\frac{1}{2}(|\Psi_0^+>|+0>-|\Psi_0^->|-0>-|\Psi_1^+>|+1>+|\Psi_1^->|-1>)_{12534} \tag{7}$$

Here, $|\Psi_0^\pm>=\frac{1}{\sqrt{2}}(G_{001}\pm G_{010}),|\Psi_1^\pm>=\frac{1}{\sqrt{2}}(G_{100}\pm G_{111})$. Hence, there exists the similar correlation between the results, if the qubits (1, 2, 5) and (3, 4) are measured on the basis $AM_2=\{|\Psi_0^\pm>,|\Psi_1^\pm>,|\Psi_2^\pm>=\frac{1}{\sqrt{2}}(|G_{000}>\pm|G_{011}>),|\Psi_3^\pm>=\frac{1}{\sqrt{2}}(|G_{101}>\pm|G_{110}>)\}$ and $BM_2=\{|+0>,|-0>,|+1>,|-1>\}$, respectively.

Let $|c_0>=|\varphi_0>+|\varphi_1>$, and $|\varphi_b>$ means its last bit is b. For example, if $|c_0>=|\psi_5>$, then $|\varphi_0>=\frac{1}{2}(|G_{010}>|00>+|G_{001}>|10>)_{12534}$, and $|\varphi_1>=-\frac{1}{2}(|G_{111}>|01>+|G_{100}>|11>)_{12534}$. It is worth to be noted here that if the particle 5 and the particle 4 are bit-flipped and the particle 5 are phase-flipped at the same time, $|\varphi_0>$ and $|\varphi_1>$ can be converted to each other.

Then, let describe how to prepare the initial state in detail. Firstly, it is assumed that Alice is the sender of secret information, while Bob is the receiver. And they share an entanglement state beforehand, that is given as follow.

$$\frac{1}{\sqrt{2}}(|0>_A|0>_B+|1>_A|1>_B) \tag{8}$$

Here, the subscript indicates the holder of the particle. If Alice wants to send a bit of secret information $|b>$ to Bob, Alice will prepare a $|\psi_5>$ state as the carrier information $|c_0>$ firstly, and then Alice obtains the following state. Here, in order to facilitate understanding, we number all the particles, while Alice holds the particles 0-5 and particle 7, and Alice holds the particle 6.

$$|b>_0|c_0>_{12534}\frac{1}{\sqrt{2}}(|0>_6|0>_7+|1>_6|1>_7) \tag{9}$$

Next, Alice applies the CNOT operation, while the particle 4 is the control qubit and the particle 7 is the target qubit. Then, the state will turn to be

$$\frac{1}{\sqrt{2}}|b>_0(|0>_7(|\varphi_0>_{12534}|0>_6+|\varphi_1>_{12534}|1>_6)$$
$$+|1>_7(|\varphi_0>_{12534}|1>_6+|\varphi_1>_{12534}|0>_6)) \tag{10}$$

Here, let put Alice's entangled qubit (the particle 7) as the first position to simplify the representation. After Alice applies the CNOT operation, the particle 7 becomes the control qubit and the particle 0 is the target qubit. Then, the state will turn to be

$$\frac{1}{\sqrt{2}}(|b>_0|0>_7(|\varphi_0>_{12534}|0>_6+|\varphi_1>_{12534}|1>_6)$$
$$+|\bar{b}>_0|1>_7(|\varphi_0>_{12534}|1>_6+|\varphi_1>_{12534}|0>_6)) \tag{11}$$

Finally, Alice applies the CNOT operation, while the particle 0 is the control qubit and the particles 4, 5 and 7 are the target qubits. And then, she also applies the QCPG operation, while the particle 0 is the control qubit and the particles 5 is the target qubit, and the state becomes

$$\frac{1}{\sqrt{2}}(|0>+|1>)_7\,|b>_0(|\varphi_b>_{12534}|0>_6+|\varphi_{\bar{b}}>_{12534}|1>_6) \tag{12}$$

After removing the particles 0 and 7, the rest exactly is the initial state that will be used in this protocol, shown as the Eq. (13).

$$|\varphi_b>_{12534}|0>_6+|\varphi_{\bar{b}}>_{12534}|1>_6 \tag{13}$$

Following the steps given above, Alice also can implement the embedding process of secret information. If Bob wants to extract secret information, he only needs to apply the CNOT operation again, while the particle 4 is the control qubit and the particle 6 is the target qubit. Then, the state will turn to be

$$(|\varphi_b>+|\varphi_{\bar{b}}>)_{12534}\,|b>_6=|c_0>_{12534}|b>_6 \tag{14}$$

As shown in the Eq. (14), Bob can receive the secret information particle $|b>$ and then extract secret information that Alice wants to send to him, by using projection measurement of $\{|0\rangle, |1\rangle\}$ basis on the particle $|b>$.

3 The proposed quantum steganography protocol

The carrier protocol [Lin, Gao and Liu (2011)] used in the new protocol is a protocol of quantum secure direct communication [Cai (2003); Wójcik (2003); Bennett and Wiesner (1992); Wang, Deng, Li et al. (2005)]. This protocol is required to transmit two quantum sequences for communicating secret information. So that, the hidden channel can be built up within the carrier protocol. In this case, the hidden channel's security can be perfectly guaranteed by virtue of the carrier protocol's great security.

Now, let describe the proposed quantum steganography protocol in detail.

Step (1) To guarantee the security of the secret message, Alice (the sender) and Bob (the receiver) firstly agree on a one-way hash function $h:\{0,1\}^k \rightarrow \{0,1\}^l$. According to her secret information m, Alice constructs a sent message s, which consists of the secret information and an authentication message $\mathrm{h}(\mathrm{m})$, i.e. $\mathrm{s}=\mathrm{m}+\mathrm{h}(\mathrm{m})$.

Step (2) Next, Alice prepares the initial state shown in the Eq. (12) by following the process in Section 2.

Step (3) Then, Alice prepares n (n is large enough) $|\psi_5>$. After that, Alice mixes the first five qubits of the initial state into all the quantum states that will be used in the carrier protocol and records the position m of these five qubits, which is denoted as $|\psi_5>_m$. As a follow, Alice divides all the states into five particle sequences. Every particle sequence is denoted as $C_i=[P_i^1,P_i^2,\ldots,P_i^n]$. Here, P_i represents the *i*-th particle of the Brown state, and the superscript represents the position of the corresponding Brown state in the particle sequence. At last, Alice sends the particle sequence C_3 and C_4 to Bob.

Step (4) After Bob receives C_3 and C_4, Alice randomly determines to enter the control mode or secret information transmission mode. If Alice determines to enter the control mode, she will select a part of particles from C_1, C_2 and C_5 for reliable eavesdropping detection.

Step (5) Control mode: Alice firstly selects a part of particles from C_1, C_2 and C_5, then she measures the particle 1, 2 and 5 under the basis AM_1 or AM_2, and publishes her measurement basis and corresponding measurement results through the classical channel. After getting Alice's results, Bob measures his corresponding particles 3 and 4 from C_3 and C_4 under the basis BM_1 or BM_2 and compares his results with that of Alice to detect eavesdropping. If Alice finds out that the eavesdropping exists, she will abort the communication. Otherwise, their communication will enter the secret information transmission mode or the normal information transmission mode.

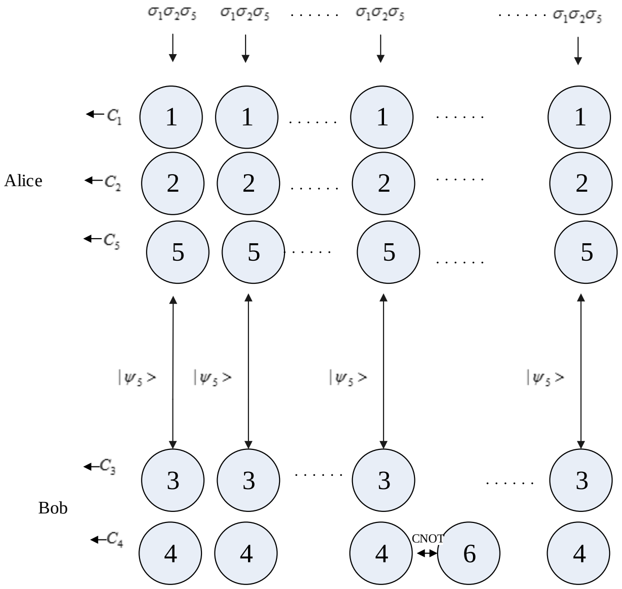
$\sigma_1\sigma_2\sigma_5$
$\sigma_1\sigma_2\sigma_5$
......
$\sigma_1\sigma_2\sigma_5$
......
$\sigma_1\sigma_2\sigma_5$
Alice
C_1
C_2
C_5
1
2
5
$|\psi_5>$
Bob
C_3
C_4
3
4
CNOT
6

Figure 1: The secret information transmission process

Step (6) Secret information transmission mode: Bob finds out the qubit P_4^{m} (Alice sents m to Bob by implementing QKD or one-time pad through classical channel in advance), and then he applies the CNOT operation on the state, while P_4^{m} is the control qubit and P_6^{m} is the target qubit, as shown in the Fig. 1. After that, the state is shown as the Eq. (13), where P_6^{m} becomes $|b>$ by removing the entanglement with the carrier state $|c_0>$. Here, $|b>$ is the carrier particle of secret information received by Alice. It is worth noting that, all these operations do not change the carrier state $|c_0>$, and the carrier state $|c_0>$ has no difference with other Brown states after the secret message transmission. As a result, we still can use $|c_0>$ to transmit normal information.

Step (7) Normal information transmission mode: According to the bit sequence s, Alice performs the corresponding unitary operations on C_1, C_2 and C_5. Supposing that the sent message s is $"s_0 s_1 s_2 s_3"(s_i \in \{0,1\})$, Alice performs operations σ^{2S_0}, $\sigma^{2S_1+S_2}$ and $\sigma^{2S_3+(S_0 \oplus S_1 \oplus S_2 \oplus S_3)}$ on the qubits 1, 2, and 5, respectively. The process in this mode is also shown as the Fig. 1. Then, Alice transmits these particles to Bob. After receiving these encoding particles, Bob measures the entangled pairs in the basis FMB and decodes the received message $\mathrm{s}' = \mathrm{m}' + \mathrm{h}(\mathrm{m})'$. Only when $\mathrm{h}(\mathrm{m}') = \mathrm{h}(\mathrm{m})'$, Bob can sure that he has received the whole secret message $\mathrm{m} = \mathrm{m}'$. Otherwise, he thinks that the secret message is tampered with during the transmission and discards the received message.

4 The performance analysis

4.1 Anti-noise robustness

Unlike most of the previous quantum steganography protocols, the new protocol has a good security resisting on quantum noises. By virtue of this capability, the new protocol can still transmit secret information accurately in quantum noisy channel. The quantum channel in reality is always noisy, so the security resisting on quantum noise is very important for quantum steganography. It can effectively prevent the secret information from affected or destroyed by quantum noise. Due to its own characteristics of the new protocol, it can be immune to the phase-flip noise. In this case, even though in the quantum channels of these noises, the new protocol can still accurately transmit secret information.

As described above, assuming that the secret information b=0, the initial state before transmission of the secret protocol is as follows.

$$|\varphi_b>_{12534}|0>_6 + |\varphi_{\bar{b}}>_{12534}|1>_6$$

$$= \frac{1}{2}(|G_{010}>|00> + |G_{001}>|10>)_{12534}|0>_6 - \frac{1}{2}(|G_{111}>|01> + |G_{100}>|11>)_{12534}|1>_6 \quad (15)$$

If there is no noise in the channel, the above state will keep intact. In this case, Bob can receive secret information by performing a simple CNOT operation. Otherwise, if there is the phase-flip noise in the channel, the state which Bob's received will changed. If particle 3 and 4 are both affected by noise and phase flip occurs, the phase flip will be cancelled, the system will not change, and the secret information will not change, either. If the particle 3 or 4 is affected by quantum noise, the system state is given as follow.

$$|\varphi_b>_{12534}|0>_6 + |\varphi_{\bar{b}}>_{12534}|1>_6$$

$$= \frac{1}{2}(|G_{010}>|00> - |G_{001}>|10>)_{12534}|0>_6 - \frac{1}{2}(|G_{111}>|01> - |G_{100}>|11>)_{12534}|1>_6 \quad (16)$$

If the secret information is extracted in the changed state (as shown in the Eq. (16)), Bob can still receive the secret information b correctly after applying CNOT operation by adopting the same method. It can be seen that the new protocol is completely immune to phase-flip noises. In addition, both the amplitude-damping noise and the depolarized noise are superimposed with components of the bit-flip noise and the phase-flip noise. In other words, the amplitude-damping noise and the depolarized noise can be regarded as the combination of the bit-flip noise and the phase-flip noise in different proportional components, and the components of the phase-flip noise will be immune to the proposed protocol. Therefore, the new protocol also has good security resisting on the bit-flip, depolarization and amplitude-damping noises respectively.

In summary, the new protocol can be completely immune to the phase-flip noise. Moreover, since the effect of various noises will cancel each other partially, the security of secret information can be further better than that of the theoretical analysis. From this point of view, the new protocol has good security resisting on quantum noise.

4.2 Imperceptibility

Quantum steganography protects the security of secret information mainly by hiding quantum channel of secret information transmission. As a result, it is easy to know that imperceptibility is the most significant performance parameter for quantum steganography. Fortunately, comparing to the classical steganography, the imperceptibility of quantum steganography has more innate advantages, due to the quantum uncertainty theorem and no-cloning theorem. If the attacker Eve tries to detect the hidden quantum channel between Alice and Bob, there are two optional approaches for him. One is to observe abnormity caused by covert communication, the other is to initiatively discover abnormity caused by covert communication by performing measurement on intercepted particles. Since embedding secret information will not change the state of the carrier information in the new protocol, so there is no chance to detect the hidden channel for Eve by adopting the first option. For the second option, Eve does have a certain probability of getting some useful information about secret information. However, because it is impossible to know the position value of m, or the right particles' location, or even correct measurement basis in advance, Eve can only get random measurement outcomes on intercepted particles for him. From the theorem of quantum uncertainty, it is easy to know these measurement outcomes could not produce the so-called abnormity, which can be used to find out the hidden channel. In addition, according to the theorem of quantum non-cloning, if Eve carried out measurement on more transmitted particles, his actions will definitely disturb the normal quantum communication, and consequently will be detected by Alice and Bob, followed by the process to abort communication. As mentioned above, it is almost impossible for Eve to find the hidden channel by random measurement. In fact, the only available way that Eve can discover the hidden channel, is to obtain the correct position value m and perform the correct measurement on the right particles in the proper basis. So the critical step of detecting hidden channel for Eve is to obtain m.

Then, let us further consider the possibility of obtaining m for Eve. According to the detailed steps of the new protocol, the value of m has nothing to do with the information sequence, and there is no need to satisfy any conditions, m is completely random for Alice to choose. Moreover, m can be sent to Bob by implementing QKD or one time one pad through in classical channel, which have been proved to be absolutely safety. In addition, according to Shannon's information theory, random probability distributions of the information will make m's uncertainty best, which means it is extremely difficult for Eve to obtain m. So that, the imperceptibility of our protocol can be further enhanced. In term of this conclusion, it is very reasonable to randomize the information m by presetting it as a random sequence or by adopting a pseudo-random sequence encryption method to generate it. As a result, the only way to obtain m for Eve is to randomly guess with the possibility of 1/n, since it is nearly impossible to obtain the information sent by Alice to Bob in advance.

Moreover, unlike most of the QKD protocols and some QSDC protocols, there is no need of extra information's transmission through a classical channel during information transmission for the new protocol. Therefore, the new protocol's imperceptibility can be better guaranteed.

Based on the above analysis, it is proved that the new protocol has good imperceptibility. The attacker almost impossible to find the hidden channel.

4.3 Capacity

Capacity characterizes maximum quantity of secret information transmitted per round of covert communication. It means that the larger the capacity is, the more secret information can be transmitted. According to the new protocol, it is easy to know there is one bit secret information transmitted in per round of covert communication, which means the capacity of the new protocol is equal to one, as the same as most of the previous quantum steganography protocols. However, since the location of the hidden channel in the covert information is completely random and independent of the normal information transmission, the number of the hidden channel can be appropriately increased per round. As a result, the capacity of the new protocol can be increased correspondingly.

Because the hidden channel is built up by applying CNOT operation and it is independent of the states used by the carrier protocol, this protocol has a strong scalability and can be combined with many other QSDC protocols. If it combined with a large-capacity steganography protocol, the capacity of the combined protocol will be larger than the large-capacity protocol. In addition, since the transmission of the secret information does not change the entanglement state of the carrier protocol, the entanglement exchange and super-dense coding can be used to extend the covert channel and transmit more secret information. The specific operation is similar to Qu et al. [Qu, Chen, Luo et al. (2011)]. After the expansion, the capacity of the protocol will increase further.

In short, the capacity of the new protocol is the same as most of the previous quantum steganography protocol, but it is available to expand its capacity without affecting the transmission of secret information by extending to more powerful quantum steganography or QSDC protocols using Brown state. It must be noted that there is always a reciprocal balance between capacity and imperceptibility. Therefore, the choice to expand an appropriate capacity requires a comprehensive consideration to imperceptibility.

4.4 Security

Security means that the protocol can effectively resist on most of eavesdropping attacks or various quantum noises' effect, so that the secret information can be transmitted securely. Therefore, security is also a very important performance parameter to quantum steganography. In this section, the security resisting on quantum noises has been analyzed and proved in detail. As for the security resisting on eavesdropping attacks, due to the new protocol is based on the QSDC protocol [Lin, Gao and Liu (2011)], the hidden channel built up within it can be effectively proved by its good security, which had been analyzed in detail in Lin et al. [Lin, Gao and Liu (2011)].

From the point of view of eavesdroppers, there is still no chance or nearly impossible to obtain secret information for them. It is because secret information is only embedded in the hidden channel, and there are only two particles as the travel particles during the covert communication. Even if eavesdroppers enable to intercept and obtains these travel particles, since only a part of particles of Brown state in their hand is not available to achieve the whole information of this Brown state, so they could not obtain secret information yet. Moreover, because the secret information mainly depends on the last two particles of the initial state, even if eavesdroppers measure the travel particles, they also could not interfere the transmission of secret information, so secret information still can be transmitted securely.

Overall, the security of the new protocol is proved to be excellent.

5 Conclusion

In this paper, a novel anti-noise quantum steganography protocol based on Brown states is proposed. It embeds and extracts secret information by applying CNOT operation. The obvious advantage of the new protocol is its good security resisting on quantum noises comparing with the previous achievements. By virtue of the cover of carrier protocol, the new protocol has a good imperceptibility. In addition, the transmission scale of the carrier protocol can be arbitrarily increased, so that the imperceptibility of the new protocol can be further enhanced. As for security, due to the carrier protocol owns the high level security as the QSDC protocol, so the new protocol can effectively deal with various eavesdropping attacks, as the same as the carrier protocol. In aspect of capacity, the new protocol can further expand its capacity by combining with other powerful quantum secure communication protocols. Furthermore, the independence of the hidden channel in the new protocol makes it own good scalability and practicability, either.

However, since a certain number of particles are needed during the preparation of the initial state, as well as some auxiliary particles during the processes of embedding and extracting secret information, so the consumption of the new protocol is a little bit higher. In order to make up for this defect, how to reduce the consumption without performance degradation for the protocol will be the next step of our research in the future.

Acknowledgement: This work was supported by the National Natural Science Foundation of China (No. 61373131, 61303039, 61232016, 61501247), the Six Talent Peaks Project of Jiangsu Province (Grant No. 2015-XXRJ-013), Natural Science Foundation of Jiangsu Province (Grant No. BK20171458), the Natural Science Foundation of the Higher Education Institutions of Jiangsu Province (China under Grant No. 16KJB520030), Sichuan Youth Science and Technique Foundation (No. 2017JQ0048), NUIST Research Foundation for Talented Scholars (2015r014), PAPD and CICAEET funds.

References

Bennett, C. H.; Wiesner, S. J. (1992): Communication via one- and two-particle operators on Einstein-Podolsky-Rosen states. *Physical Review Letters*, vol. 69, no. 20, pp. 2881-2884.

Banacloche, J. G. (2009): Quantum error correcting code. *Physical Review Letters*, vol. 29, no. 1, pp. 813.

Cai, Q. Y. (2003): The Ping-Pong protocol can be attacked without eavesdropping. *Physical Review Letters*, vol. 91, no. 10.

Chattopadhyay, I.; Sarkar, D. (2007): Local indistinguishability and possibility of hiding cbits in activable bound entangled states. *Physics Letters A*, vol. 365, no. 4, pp. 273-277.

DiVincenzo, D. P.; Leung, D. W.; Terhal, B. M. (2002): Quantum data hiding. *IEEE Transactions on Information Theory*, vol. 48, no. 3, pp. 580-598.

Eggeling, T.; Werner, R. F. (2002): Hiding classical data in multipartite quantum states. *Physical Review Letters*, vol. 89, no. 9, pp. 7905.

Geabanacloche, J. (2002): Hiding messages in quantum data. *Journal of Mathematical Physics*, vol. 43, no. 9, pp. 4531-4536.

Gottesman, D. (2000): Theory of quantum secret sharing. *Physical Review A*, vol. 61, no. 4, pp. 2311.

Guo, G. C.; Guo, G. P. (2003): Quantum data hiding with spontaneous parameter down-conversion. *Physical Review A*, vol. 68, no. 4, pp. 4303.

Hayden, P.; Leung, D.; Smith, G. (2005): Multiparty data hiding of quantum information. *Physical Review A*, vol. 71, no. 6, pp. 2339.

Hillery, M.; Buzek, V.; Berthiaume, A. (2017): Quantum secret sharing. *Physical Review A*, vol. 59, no. 3, pp. 1829.

Lin, S.; Gao, F.; Liu, X. F. (2011): Quantum secure direct communication with five-qubit entangled state. *Chinese Physics Letters*, vol. 28, no. 3.

Liu, W. J.; Wang, H. B.; Yuan, G. L.; Xu, Y.; Chen, Z. Y. et al. (2016): Multiparty quantum sealed-bid auction using single photons as message carrier. *Quantum Information Processing*, vol. 15, no. 2, pp. 869-879.

Liu, W. J.; Xu, Y.; Yang, C. N.; Gao, P. P.; Yu, W. B. (2018): An efficient and secure arbitrary n-party quantum key agreement protocol using bell states. *International Journal of Theoretical Physics*, vol. 57, no. 1, pp. 195-207.

Martin, K. (2007): Steganographic communication with quantum information. *International Conference on Information Hiding*, vol. 4567, pp. 32-49.

Matthews, W.; Wehner, S.; Winter, A. (2009): Distinguishability of quantum states under restricted families of measurements with an application to quantum data hiding. *Communications in Mathematical Physics*, vol. 291, no. 3, pp. 813-843.

Mihara, T. (2015): Quantum steganography using prior entanglement. *Physics Letters A*, vol. 379, no. 12, pp. 952-955.

Natori, S. (2006): Quantum computation and information. *Topics in Applied Physics*, vol.

102, pp. 235.

Qu, Z. G.; Chen, X. B.; Zhong, X. J.; Niu, X. X.; Yang, Y. X. (2010): Novel quantum steganography with large payload. *Optics Communications*, vol. 283, no. 23, pp. 4782-4786.

Qu, Z. G.; Chen, X. B.; Zhong, X. J.; Niu, X. X.; Yang, Y. X. (2011): Quantum steganography with large payload based on entanglement swapping of χ-type entangled states. *Optics Communications*, vol. 284, no. 7, pp. 2075-2082.

Qu, Z. G.; Keeney, J.; Robitzsch, S.; Zaman, F.; Wang, X. (2016): Multilevel pattern mining architecture for automatic network monitoring in heterogeneous wireless communication networks. *China Communications*, vol. 13, no. 7, pp. 108-116.

Terhal, B. M.; Divincenzo, D. P.; Leung, D. W. (2000): Hiding bits in bell states. *Physical Review Letters*, vol. 86, no. 25, pp. 5807-5810.

Wang, C.; Deng, F. G.; Li, Y. S.; Long, G. L. (2005): Quantum secure direct communication with high-dimension quantum super-dense coding. *Physical Review A*, vol. 71, no. 4.

Wójcik, A. (2003): Eavesdropping on the “ping-pong” quantum communication protocol. *Physical Review Letters*, vol. 90, no. 15.