Quantum steganography with a large payload based on dense coding and entanglement swapping of Greenberger–Horne–Zeilinger states*

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 22 November 2012; revised manuscript received 27 December 2012)

A quantum steganography protocol with a large payload is proposed based on the dense coding and the entanglement swapping of the Greenberger–Horne–Zeilinger (GHZ) states. Its super quantum channel is formed by building up a hidden channel within the original quantum secure direct communication (QSDC) scheme. Based on the original QSDC, secret messages are transmitted by integrating the dense coding and the entanglement swapping of the GHZ states. The capacity of the super quantum channel achieves six bits per round covert communication, much higher than the previous quantum steganography protocols. Its imperceptibility is good, since the information and the secret messages can be regarded to be random or pseudo-random. Moreover, its security is proved to be reliable.

Keywords: quantum steganography, quantum secure direct communication, dense coding, entanglement swapping

PACS: 03.67.Dd, 03.67.Hk **DOI:** 10.1088/1674-1056/22/5/050309

1. Introduction

Quantum secure communication can transmit secret messages with unconditional security by using the law of quantum mechanics, and can be classified into quantum key distribution (QKD),[1–4] quantum secure direct communication (QSDC),[5–14] quantum secret sharing (QSS),[15–18] and so on. The goal of QKD is to establish a shared secret key between two remote authorized users. In 1984, Bennett and Brassard[1] proposed the famous BB84 protocol, which is the first QKD protocol. Afterward, a lot of QKD schemes have been put forward.[2–4] The QSDC allows secret messages to be transmitted directly without creating a key to encrypt them in advance. The main protocols proposed are summarized as follows. In 2002, Beige *et al.*[5] put forward the first QSDC protocol. In the same year, Bostrom and Felbinger[6] suggested the famous ping–pong protocol. In 2003, Deng *et al.*[7] presented a two-step QSDC based on the Bell states. In 2004, Cai and Li[8] introduced two additional unitary operations to improve the capacity of the ping–pong protocol.[6] In 2005, Wang *et al.*[9] put forward a multi-step QSDC using the multi-particle Greenberger–Horne–Zeilinger (GHZ) state, and Gao *et al.*[10] put forward a simultaneous QSDC between the central party and other M parties. In 2008, Sun *et al.*[11] proposed a new multiparty simultaneous QSDC based on GHZ states and dense coding; Chen *et al.*[12] proposed a novel controlled QSDC protocol with quantum encryption using a partially entangled GHZ state; Chen *et al.*[13] proposed a novel three-party controlled QSDC protocol based on the W state. In 2012, Huang *et al.*[14] proposed two robust channel-encrypting QSDC protocols over different collective-noise channels. As the quantum counterpart of the classical secret sharing, the QSS allows that neither individual agent is able to obtain the secret messages sent by the dealer unless they cooperate. In 1999, Hillery *et al.*[15] put forward the first QSS protocol with the GHZ state. In 2003, Guo *et al.*[16] presented a QSS protocol only using product states. In 2012, Chen *et al.*[17] put forward an improved multiparty QSS based on the GHZ state to resist attacks from both outside attackers and inside participants. In 2013, Chen *et al.*[18] put forward a three-party QSS protocol via the entangled GHZ state using a single-particle quantum state to encode the information.

Classical steganography inserts secret messages into an innocent cover object to hide the existence of secret messages. In recent years, the concept of quantum steganography has been put forward, which extends the concept of the classical steganography into the quantum scenario. Different from traditional quantum secure communication, quantum steganography always builds up another hidden channel within the normal quantum channel to transmit secret messages. That is, quantum steganography uses the hidden channel to hide the secret messages into the normal quantum channel. In 2002, Gea-Banacloche[19] used the quantum error-correcting code to encode quantum data and hid secret messages as errors. In 2004, Worley[20] suggested a fuzzy quantum watermarking protocol with the relative frequency of error from observing qubits. In 2007, based on the BB84 QKD scheme,[1]

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

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

© 2013 Chinese Physical Society and IOP Publishing Ltd

Martin[21] presented a novel quantum steganography protocol. In 2010, based on Guo *et al.*'s QSS scheme,[16] Liao *et al.*[22] proposed a novel multi-party quantum steganography protocol. In 2010, based on an improved ping–pong scheme (IBF),[8] Qu *et al.*[23] suggested a novel quantum steganography scheme with a large payload. However, the capacity of the quantum channels in Refs. [19]– [22] is only one bit or one qubit per round covert communication, which is apparent too small for efficient covert communication. Although the capacity in Ref. [23] has been increased to four bits, it is still not large enough.

Based on the above analysis, for improving quantum channel's capacity, we propose a novel quantum steganography protocol with a large payload based on the dense coding and the entanglement swapping of the GHZ states. Its super quantum channel is formed by building up the hidden channel within the original QSDC. Based on the original QSDC, secret messages are transmitted by integrating the dense coding and the entanglement swapping of the GHZ states. It can transmit six bits per round covert communication, six times of that in Refs. [19]– [22] and one and half times of that in Ref. [23]. Since the information and secret messages can be regarded to be random or pseudo-random, its imperceptibility is good. Moreover, its security is proved to be reliable.

2. Coding scheme

The dense coding of the GHZ states is briefly introduced first. The dense coding of the GHZ states, proposed by Lee *et al.*,[24] is the generalization of the dense coding scheme of Bennett and Wiesner.[25] The GHZ states are three-particle maximally entangled states, and form a complete orthogonal basis of 8-dimensional Hilbert space. The eight independent GHZ states are

$$
\begin{aligned}
&|\Psi_1\rangle = \frac{1}{\sqrt{2}}(|000\rangle + |111\rangle), \quad |\Psi_2\rangle = \frac{1}{\sqrt{2}}(|000\rangle - |111\rangle),\\
&|\Psi_3\rangle = \frac{1}{\sqrt{2}}(|100\rangle + |011\rangle), \quad |\Psi_4\rangle = \frac{1}{\sqrt{2}}(|100\rangle - |011\rangle),\\
&|\Psi_5\rangle = \frac{1}{\sqrt{2}}(|010\rangle + |101\rangle), \quad |\Psi_6\rangle = \frac{1}{\sqrt{2}}(|010\rangle - |101\rangle),\\
&|\Psi_7\rangle = \frac{1}{\sqrt{2}}(|110\rangle + |001\rangle), \quad |\Psi_8\rangle = \frac{1}{\sqrt{2}}(|110\rangle - |001\rangle). \qquad (1)
\end{aligned}
$$

By performing single-particle unitary operations on any two of the three particles, one GHZ state can be transformed into another GHZ state, where four single-particle unitary operations are

$$
\begin{aligned}
&I = |0\rangle\langle 0| + |1\rangle\langle 1|, \quad \sigma_z = |0\rangle\langle 0| - |1\rangle\langle 1|,\\
&\sigma_x = |0\rangle\langle 1| + |1\rangle\langle 0|, \quad \mathrm{i}\sigma_y = |0\rangle\langle 1| - |1\rangle\langle 0|. \qquad (2)
\end{aligned}
$$

Without loss of generality, $|\Psi_1\rangle$ is assumed as the initial state. Accordingly, $|\Psi_1\rangle$ can be transformed into $|\Psi_k\rangle$ $(k = 1, 2, \ldots, 8)$ by performing U_k on its first and second particles, namely,

$$
U_k|\Psi_1\rangle = |\Psi_k\rangle, \quad (k = 1, 2, \ldots, 8), \qquad (3)
$$

where

$$
\begin{aligned}
&U_1 = \sigma_z \otimes \sigma_z, \quad U_2 = I \otimes \sigma_z, \quad U_3 = \mathrm{i}\sigma_y \otimes \sigma_z,\\
&U_4 = \sigma_x \otimes \sigma_z, \quad U_5 = I \otimes \sigma_x, \quad U_6 = \sigma_z \otimes \sigma_x,\\
&U_7 = \sigma_x \otimes \sigma_x, \quad U_8 = \mathrm{i}\sigma_y \otimes \sigma_x. \qquad (4)
\end{aligned}
$$

Let each U_k correspond to three bits information, namely,

$$
\begin{aligned}
&U_1 \to 000, \ U_2 \to 001, \ U_3 \to 010, \ U_4 \to 011,\\
&U_5 \to 100, \ U_6 \to 101, \ U_7 \to 110, \ U_8 \to 111. \qquad (5)
\end{aligned}
$$

Based on the above description, after the dense coding of the GHZ states, one GHZ state can transmit three bits information.

The results of entanglement swapping between $|\Psi_1\rangle$ and arbitrary one of the eight GHZ states are shown as follows:

$$
\begin{aligned}
&|\Psi_1\rangle_{A_1B_1C_1} \otimes |\Psi_1\rangle_{A_2B_2C_2}\\
&= \left(\frac{1}{\sqrt{2}}\right)^3 \big(|\Phi^+\rangle_{A_1A_2}|\Phi^+\rangle_{B_1B_2}|\Phi^+\rangle_{C_1C_2}\\
&+ |\Phi^+\rangle_{A_1A_2}|\Phi^-\rangle_{B_1B_2}|\Phi^-\rangle_{C_1C_2}\\
&+ |\Phi^-\rangle_{A_1A_2}|\Phi^+\rangle_{B_1B_2}|\Phi^-\rangle_{C_1C_2}\\
&+ |\Phi^-\rangle_{A_1A_2}|\Phi^-\rangle_{B_1B_2}|\Phi^+\rangle_{C_1C_2}\\
&+ |\Psi^+\rangle_{A_1A_2}|\Psi^+\rangle_{B_1B_2}|\Psi^+\rangle_{C_1C_2}\\
&+ |\Psi^+\rangle_{A_1A_2}|\Psi^-\rangle_{B_1B_2}|\Psi^-\rangle_{C_1C_2}\\
&+ |\Psi^-\rangle_{A_1A_2}|\Psi^+\rangle_{B_1B_2}|\Psi^-\rangle_{C_1C_2}\\
&+ |\Psi^-\rangle_{A_1A_2}|\Psi^-\rangle_{B_1B_2}|\Psi^+\rangle_{C_1C_2}\big), \qquad (6)\\
&|\Psi_1\rangle_{A_1B_1C_1} \otimes |\Psi_2\rangle_{A_2B_2C_2}\\
&= \left(\frac{1}{\sqrt{2}}\right)^3 \big(|\Phi^+\rangle_{A_1A_2}|\Phi^+\rangle_{B_1B_2}|\Phi^-\rangle_{C_1C_2}\\
&+ |\Phi^+\rangle_{A_1A_2}|\Phi^-\rangle_{B_1B_2}|\Phi^+\rangle_{C_1C_2}\\
&+ |\Phi^-\rangle_{A_1A_2}|\Phi^+\rangle_{B_1B_2}|\Phi^+\rangle_{C_1C_2}\\
&+ |\Phi^-\rangle_{A_1A_2}|\Phi^-\rangle_{B_1B_2}|\Phi^-\rangle_{C_1C_2}\\
&- |\Psi^+\rangle_{A_1A_2}|\Psi^+\rangle_{B_1B_2}|\Psi^-\rangle_{C_1C_2}\\
&- |\Psi^+\rangle_{A_1A_2}|\Psi^-\rangle_{B_1B_2}|\Psi^+\rangle_{C_1C_2}\\
&- |\Psi^-\rangle_{A_1A_2}|\Psi^+\rangle_{B_1B_2}|\Psi^+\rangle_{C_1C_2}\\
&- |\Psi^-\rangle_{A_1A_2}|\Psi^-\rangle_{B_1B_2}|\Psi^-\rangle_{C_1C_2}\big), \qquad (7)\\
&|\Psi_1\rangle_{A_1B_1C_1} \otimes |\Psi_3\rangle_{A_2B_2C_2}\\
&= \left(\frac{1}{\sqrt{2}}\right)^3 \big(|\Psi^+\rangle_{A_1A_2}|\Phi^+\rangle_{B_1B_2}|\Phi^+\rangle_{C_1C_2}\\
&+ |\Psi^+\rangle_{A_1A_2}|\Phi^-\rangle_{B_1B_2}|\Phi^-\rangle_{C_1C_2}\\
&+ |\Psi^-\rangle_{A_1A_2}|\Phi^+\rangle_{B_1B_2}|\Phi^-\rangle_{C_1C_2}\\
&+ |\Psi^-\rangle_{A_1A_2}|\Phi^-\rangle_{B_1B_2}|\Phi^+\rangle_{C_1C_2}\\
&+ |\Phi^+\rangle_{A_1A_2}|\Psi^+\rangle_{B_1B_2}|\Psi^+\rangle_{C_1C_2}\\
&+ |\Phi^+\rangle_{A_1A_2}|\Psi^-\rangle_{B_1B_2}|\Psi^-\rangle_{C_1C_2}\\
&+ |\Phi^-\rangle_{A_1A_2}|\Psi^+\rangle_{B_1B_2}|\Psi^-\rangle_{C_1C_2}
\end{aligned}
$$

$$+\left|\Phi^{-}\right\rangle_{A_1A_2}\left|\Psi^{-}\right\rangle_{B_1B_2}\left|\Psi^{+}\right\rangle_{C_1C_2}\big), \tag{8}$$

$$\begin{aligned}&\left|\Psi_1\right\rangle_{A_1B_1C_1}\otimes\left|\Psi_4\right\rangle_{A_2B_2C_2}\\ =&\left(\frac{1}{\sqrt{2}}\right)^3\big(\left|\Psi^{+}\right\rangle_{A_1A_2}\left|\Phi^{+}\right\rangle_{B_1B_2}\left|\Phi^{-}\right\rangle_{C_1C_2}\\ &+\left|\Psi^{+}\right\rangle_{A_1A_2}\left|\Phi^{-}\right\rangle_{B_1B_2}\left|\Phi^{+}\right\rangle_{C_1C_2}\\ &+\left|\Psi^{-}\right\rangle_{A_1A_2}\left|\Phi^{+}\right\rangle_{B_1B_2}\left|\Phi^{+}\right\rangle_{C_1C_2}\\ &+\left|\Psi^{-}\right\rangle_{A_1A_2}\left|\Phi^{-}\right\rangle_{B_1B_2}\left|\Phi^{-}\right\rangle_{C_1C_2}\\ &-\left|\Phi^{+}\right\rangle_{A_2A_2}\left|\Psi^{+}\right\rangle_{B_1B_2}\left|\Psi^{-}\right\rangle_{C_1C_2}\\ &-\left|\Phi^{+}\right\rangle_{A_1A_2}\left|\Psi^{-}\right\rangle_{B_1B_2}\left|\Psi^{+}\right\rangle_{C_1C_2}\\ &-\left|\Phi^{-}\right\rangle_{A_1A_2}\left|\Psi^{+}\right\rangle_{B_1B_2}\left|\Psi^{+}\right\rangle_{C_1C_2}\\ &-\left|\Phi^{-}\right\rangle_{A_1A_2}\left|\Psi^{-}\right\rangle_{B_1B_2}\left|\Psi^{-}\right\rangle_{C_1C_2}\big),\end{aligned} \tag{9}$$

$$\begin{aligned}&\left|\Psi_1\right\rangle_{A_1B_1C_1}\otimes\left|\Psi_5\right\rangle_{A_2B_2C_2}\\ =&\left(\frac{1}{\sqrt{2}}\right)^3\big(\left|\Phi^{+}\right\rangle_{A_1A_2}\left|\Psi^{+}\right\rangle_{B_1B_2}\left|\Phi^{+}\right\rangle_{C_1C_2}\\ &+\left|\Phi^{+}\right\rangle_{A_1A_2}\left|\Psi^{-}\right\rangle_{B_1B_2}\left|\Phi^{-}\right\rangle_{C_1C_2}\\ &+\left|\Phi^{-}\right\rangle_{A_1A_2}\left|\Psi^{+}\right\rangle_{B_1B_2}\left|\Phi^{-}\right\rangle_{C_1C_2}\\ &+\left|\Phi^{-}\right\rangle_{A_1A_2}\left|\Psi^{-}\right\rangle_{B_1B_2}\left|\Phi^{+}\right\rangle_{C_1C_2}\\ &+\left|\Psi^{+}\right\rangle_{A_1A_2}\left|\Phi^{+}\right\rangle_{B_1B_2}\left|\Psi^{+}\right\rangle_{C_1C_2}\\ &+\left|\Psi^{+}\right\rangle_{A_1A_2}\left|\Phi^{-}\right\rangle_{B_1B_2}\left|\Psi^{-}\right\rangle_{C_1C_2}\\ &+\left|\Psi^{-}\right\rangle_{A_1A_2}\left|\Phi^{+}\right\rangle_{B_1B_2}\left|\Psi^{-}\right\rangle_{C_1C_2}\\ &+\left|\Psi^{-}\right\rangle_{A_1A_2}\left|\Phi^{-}\right\rangle_{B_1B_2}\left|\Psi^{+}\right\rangle_{C_1C_2}\big),\end{aligned} \tag{10}$$

$$\begin{aligned}&\left|\Psi_1\right\rangle_{A_1B_1C_1}\otimes\left|\Psi_6\right\rangle_{A_2B_2C_2}\\ =&\left(\frac{1}{\sqrt{2}}\right)^3\big(\left|\Phi^{+}\right\rangle_{A_1A_2}\left|\Psi^{+}\right\rangle_{B_1B_2}\left|\Phi^{-}\right\rangle_{C_1C_2}\\ &+\left|\Phi^{+}\right\rangle_{A_1A_2}\left|\Psi^{-}\right\rangle_{B_1B_2}\left|\Phi^{+}\right\rangle_{C_1C_2}\\ &+\left|\Phi^{-}\right\rangle_{A_1A_2}\left|\Psi^{+}\right\rangle_{B_1B_2}\left|\Phi^{+}\right\rangle_{C_1C_2}\\ &+\left|\Phi^{-}\right\rangle_{A_1A_2}\left|\Psi^{-}\right\rangle_{B_1B_2}\left|\Phi^{-}\right\rangle_{C_1C_2}\\ &-\left|\Psi^{+}\right\rangle_{A_1A_2}\left|\Phi^{+}\right\rangle_{B_1B_2}\left|\Psi^{-}\right\rangle_{C_1C_2}\\ &-\left|\Psi^{+}\right\rangle_{A_1A_2}\left|\Phi^{-}\right\rangle_{B_1B_2}\left|\Psi^{+}\right\rangle_{C_1C_2}\\ &-\left|\Psi^{-}\right\rangle_{A_1A_2}\left|\Phi^{+}\right\rangle_{B_1B_2}\left|\Psi^{+}\right\rangle_{C_1C_2}\\ &-\left|\Psi^{-}\right\rangle_{A_1A_2}\left|\Phi^{-}\right\rangle_{B_1B_2}\left|\Psi^{-}\right\rangle_{C_1C_2}\big),\end{aligned} \tag{11}$$

$$\begin{aligned}&\left|\Psi_1\right\rangle_{A_1B_1C_1}\otimes\left|\Psi_7\right\rangle_{A_2B_2C_2}\\ =&\left(\frac{1}{\sqrt{2}}\right)^3\big(\left|\Psi^{+}\right\rangle_{A_1A_2}\left|\Psi^{+}\right\rangle_{B_1B_2}\left|\Phi^{+}\right\rangle_{C_1C_2}\\ &+\left|\Psi^{+}\right\rangle_{A_1A_2}\left|\Psi^{-}\right\rangle_{B_1B_2}\left|\Phi^{-}\right\rangle_{C_1C_2}\\ &+\left|\Psi^{-}\right\rangle_{A_1A_2}\left|\Psi^{+}\right\rangle_{B_1B_2}\left|\Phi^{-}\right\rangle_{C_1C_2}\\ &+\left|\Psi^{-}\right\rangle_{A_1A_2}\left|\Psi^{-}\right\rangle_{B_1B_2}\left|\Phi^{+}\right\rangle_{C_1C_2}\\ &+\left|\Phi^{+}\right\rangle_{A_1A_2}\left|\Phi^{+}\right\rangle_{B_1B_2}\left|\Psi^{+}\right\rangle_{C_1C_2}\\ &+\left|\Phi^{+}\right\rangle_{A_1A_2}\left|\Phi^{-}\right\rangle_{B_1B_2}\left|\Psi^{-}\right\rangle_{C_1C_2}\\ &+\left|\Phi^{-}\right\rangle_{A_1A_2}\left|\Phi^{+}\right\rangle_{B_1B_2}\left|\Psi^{-}\right\rangle_{C_1C_2}\\ &+\left|\Phi^{-}\right\rangle_{A_1A_2}\left|\Phi^{-}\right\rangle_{B_1B_2}\left|\Psi^{+}\right\rangle_{C_1C_2}\big),\end{aligned} \tag{12}$$

$$\begin{aligned}&\left|\Psi_1\right\rangle_{A_1B_1C_1}\otimes\left|\Psi_8\right\rangle_{A_2B_2C_2}\\ =&\left(\frac{1}{\sqrt{2}}\right)^3\big(\left|\Psi^{+}\right\rangle_{A_1A_2}\left|\Psi^{+}\right\rangle_{B_1B_2}\left|\Phi^{-}\right\rangle_{C_1C_2}\\ &+\left|\Psi^{+}\right\rangle_{A_1A_2}\left|\Psi^{-}\right\rangle_{B_1B_2}\left|\Phi^{+}\right\rangle_{C_1C_2}\\ &+\left|\Psi^{-}\right\rangle_{A_1A_2}\left|\Psi^{+}\right\rangle_{B_1B_2}\left|\Phi^{+}\right\rangle_{C_1C_2}\\ &+\left|\Psi^{-}\right\rangle_{A_1A_2}\left|\Psi^{-}\right\rangle_{B_1B_2}\left|\Phi^{-}\right\rangle_{C_1C_2}\\ &-\left|\Phi^{+}\right\rangle_{A_1A_2}\left|\Phi^{+}\right\rangle_{B_1B_2}\left|\Psi^{-}\right\rangle_{C_1C_2}\\ &-\left|\Phi^{+}\right\rangle_{A_1A_2}\left|\Phi^{-}\right\rangle_{B_1B_2}\left|\Psi^{+}\right\rangle_{C_1C_2}\\ &-\left|\Phi^{-}\right\rangle_{A_1A_2}\left|\Phi^{+}\right\rangle_{B_1B_2}\left|\Psi^{+}\right\rangle_{C_1C_2}\\ &-\left|\Phi^{-}\right\rangle_{A_1A_2}\left|\Phi^{-}\right\rangle_{B_1B_2}\left|\Psi^{-}\right\rangle_{C_1C_2}\big),\end{aligned} \tag{13}$$

where subscripts A_i, B_i, and C_i ($i=1,2$) denote three particles in the GHZ states, respectively.

According to formulas (6)–(13), each result of A_1A_2, B_1B_2, and C_1C_2 after the entanglement swapping does only correspond to one initial state among the above eight known initial states. Corresponding to formulas (6)–(13), eight collections composed by different results of A_1A_2, B_1B_2, and C_1C_2 after the entanglement swapping are coded as follows:

$$\begin{aligned}&\big\{\left|\Phi^{+}\right\rangle_{A_1A_2}\left|\Phi^{+}\right\rangle_{B_1B_2}\left|\Phi^{+}\right\rangle_{C_1C_2},\\ &\left|\Phi^{+}\right\rangle_{A_1A_2}\left|\Phi^{-}\right\rangle_{B_1B_2}\left|\Phi^{-}\right\rangle_{C_1C_2},\\ &\left|\Phi^{-}\right\rangle_{A_1A_2}\left|\Phi^{+}\right\rangle_{B_1B_2}\left|\Phi^{-}\right\rangle_{C_1C_2},\\ &\left|\Phi^{-}\right\rangle_{A_1A_2}\left|\Phi^{-}\right\rangle_{B_1B_2}\left|\Phi^{+}\right\rangle_{C_1C_2},\\ &\left|\Psi^{+}\right\rangle_{A_1A_2}\left|\Psi^{+}\right\rangle_{B_1B_2}\left|\Psi^{+}\right\rangle_{C_1C_2},\\ &\left|\Psi^{+}\right\rangle_{A_1A_2}\left|\Psi^{-}\right\rangle_{B_1B_2}\left|\Psi^{-}\right\rangle_{C_1C_2},\\ &\left|\Psi^{-}\right\rangle_{A_1A_2}\left|\Psi^{+}\right\rangle_{B_1B_2}\left|\Psi^{-}\right\rangle_{C_1C_2},\\ &\left|\Psi^{-}\right\rangle_{A_1A_2}\left|\Psi^{-}\right\rangle_{B_1B_2}\left|\Psi^{+}\right\rangle_{C_1C_2}\big\}\rightarrow 000,\end{aligned} \tag{14}$$

$$\begin{aligned}&\big\{\left|\Phi^{+}\right\rangle_{A_1A_2}\left|\Phi^{+}\right\rangle_{B_1B_2}\left|\Phi^{-}\right\rangle_{C_1C_2},\\ &\left|\Phi^{+}\right\rangle_{A_1A_2}\left|\Phi^{-}\right\rangle_{B_1B_2}\left|\Phi^{+}\right\rangle_{C_1C_2},\\ &\left|\Phi^{-}\right\rangle_{A_1A_2}\left|\Phi^{+}\right\rangle_{B_1B_2}\left|\Phi^{+}\right\rangle_{C_1C_2},\\ &\left|\Phi^{-}\right\rangle_{A_1A_2}\left|\Phi^{-}\right\rangle_{B_1B_2}\left|\Phi^{-}\right\rangle_{C_1C_2},\\ &\left|\Psi^{+}\right\rangle_{A_1A_2}\left|\Psi^{+}\right\rangle_{B_1B_2}\left|\Psi^{-}\right\rangle_{C_1C_2},\\ &\left|\Psi^{+}\right\rangle_{A_1A_2}\left|\Psi^{-}\right\rangle_{B_1B_2}\left|\Psi^{+}\right\rangle_{C_1C_2},\\ &\left|\Psi^{-}\right\rangle_{A_1A_2}\left|\Psi^{+}\right\rangle_{B_1B_2}\left|\Psi^{+}\right\rangle_{C_1C_2},\\ &\left|\Psi^{-}\right\rangle_{A_1A_2}\left|\Psi^{-}\right\rangle_{B_1B_2}\left|\Psi^{-}\right\rangle_{C_1C_2}\big\}\rightarrow 001,\end{aligned} \tag{15}$$

$$\begin{aligned}&\big\{\left|\Psi^{+}\right\rangle_{A_1A_2}\left|\Phi^{+}\right\rangle_{B_1B_2}\left|\Phi^{+}\right\rangle_{C_1C_2},\\ &\left|\Psi^{+}\right\rangle_{A_1A_2}\left|\Phi^{-}\right\rangle_{B_1B_2}\left|\Phi^{-}\right\rangle_{C_1C_2},\\ &\left|\Psi^{-}\right\rangle_{A_1A_2}\left|\Phi^{+}\right\rangle_{B_1B_2}\left|\Phi^{-}\right\rangle_{C_1C_2},\\ &\left|\Psi^{-}\right\rangle_{A_1A_2}\left|\Phi^{-}\right\rangle_{B_1B_2}\left|\Phi^{+}\right\rangle_{C_1C_2},\\ &\left|\Phi^{+}\right\rangle_{A_1A_2}\left|\Psi^{+}\right\rangle_{B_1B_2}\left|\Psi^{+}\right\rangle_{C_1C_2},\\ &\left|\Phi^{+}\right\rangle_{A_1A_2}\left|\Psi^{-}\right\rangle_{B_1B_2}\left|\Psi^{-}\right\rangle_{C_1C_2},\\ &\left|\Phi^{-}\right\rangle_{A_1A_2}\left|\Psi^{+}\right\rangle_{B_1B_2}\left|\Psi^{-}\right\rangle_{C_1C_2},\\ &\left|\Phi^{-}\right\rangle_{A_1A_2}\left|\Psi^{-}\right\rangle_{B_1B_2}\left|\Psi^{+}\right\rangle_{C_1C_2}\big\}\rightarrow 010,\end{aligned} \tag{16}$$

$$\begin{aligned}&\big\{\left|\Psi^{+}\right\rangle_{A_1A_2}\left|\Phi^{+}\right\rangle_{B_1B_2}\left|\Phi^{-}\right\rangle_{C_1C_2},\\ &\left|\Psi^{+}\right\rangle_{A_1A_2}\left|\Phi^{-}\right\rangle_{B_1B_2}\left|\Phi^{+}\right\rangle_{C_1C_2},\end{aligned}$$

$$
\begin{aligned}
&|\Psi^-\rangle_{A_1A_2}|\Phi^+\rangle_{B_1B_2}|\Phi^+\rangle_{C_1C_2},\\
&|\Psi^-\rangle_{A_1A_2}|\Phi^-\rangle_{B_1B_2}|\Phi^-\rangle_{C_1C_2},\\
&|\Phi^+\rangle_{A_2A_2}|\Psi^+\rangle_{B_1B_2}|\Psi^-\rangle_{C_1C_2},\\
&|\Phi^+\rangle_{A_1A_2}|\Psi^-\rangle_{B_1B_2}|\Psi^+\rangle_{C_1C_2},\\
&|\Phi^-\rangle_{A_1A_2}|\Psi^+\rangle_{B_1B_2}|\Psi^+\rangle_{C_1C_2},\\
&|\Phi^-\rangle_{A_1A_2}|\Psi^-\rangle_{B_1B_2}|\Psi^-\rangle_{C_1C_2}\} \rightarrow 011, \qquad (17)\\
&\{|\Phi^+\rangle_{A_1A_2}|\Psi^+\rangle_{B_1B_2}|\Phi^+\rangle_{C_1C_2},\\
&|\Phi^+\rangle_{A_1A_2}|\Psi^-\rangle_{B_1B_2}|\Phi^-\rangle_{C_1C_2},\\
&|\Phi^-\rangle_{A_1A_2}|\Psi^+\rangle_{B_1B_2}|\Phi^-\rangle_{C_1C_2},\\
&|\Phi^-\rangle_{A_1A_2}|\Psi^-\rangle_{B_1B_2}|\Phi^+\rangle_{C_1C_2},\\
&|\Psi^+\rangle_{A_1A_2}|\Phi^+\rangle_{B_1B_2}|\Psi^+\rangle_{C_1C_2},\\
&|\Psi^+\rangle_{A_1A_2}|\Phi^-\rangle_{B_1B_2}|\Psi^-\rangle_{C_1C_2},\\
&|\Psi^-\rangle_{A_1A_2}|\Phi^+\rangle_{B_1B_2}|\Psi^-\rangle_{C_1C_2},\\
&|\Psi^-\rangle_{A_1A_2}|\Phi^-\rangle_{B_1B_2}|\Psi^+\rangle_{C_1C_2}\} \rightarrow 100, \qquad (18)\\
&\{|\Phi^+\rangle_{A_1A_2}|\Psi^+\rangle_{B_1B_2}|\Phi^-\rangle_{C_1C_2},\\
&|\Phi^+\rangle_{A_1A_2}|\Psi^-\rangle_{B_1B_2}|\Phi^+\rangle_{C_1C_2},\\
&|\Phi^-\rangle_{A_1A_2}|\Psi^+\rangle_{B_1B_2}|\Phi^+\rangle_{C_1C_2},\\
&|\Phi^-\rangle_{A_1A_2}|\Psi^-\rangle_{B_1B_2}|\Phi^-\rangle_{C_1C_2},\\
&|\Psi^+\rangle_{A_1A_2}|\Phi^+\rangle_{B_1B_2}|\Psi^-\rangle_{C_1C_2},\\
&|\Psi^+\rangle_{A_1A_2}|\Phi^-\rangle_{B_1B_2}|\Psi^+\rangle_{C_1C_2},\\
&|\Psi^-\rangle_{A_1A_2}|\Phi^+\rangle_{B_1B_2}|\Psi^+\rangle_{C_1C_2},\\
&|\Psi^-\rangle_{A_1A_2}|\Phi^-\rangle_{B_1B_2}|\Psi^-\rangle_{C_1C_2}\} \rightarrow 101, \qquad (19)\\
&\{|\Psi^+\rangle_{A_1A_2}|\Psi^+\rangle_{B_1B_2}|\Phi^+\rangle_{C_1C_2},\\
&|\Psi^+\rangle_{A_1A_2}|\Psi^-\rangle_{B_1B_2}|\Phi^-\rangle_{C_1C_2},\\
&|\Psi^-\rangle_{A_1A_2}|\Psi^+\rangle_{B_1B_2}|\Phi^-\rangle_{C_1C_2},\\
&|\Psi^-\rangle_{A_1A_2}|\Psi^-\rangle_{B_1B_2}|\Phi^+\rangle_{C_1C_2},\\
&|\Phi^+\rangle_{A_1A_2}|\Phi^+\rangle_{B_1B_2}|\Psi^+\rangle_{C_1C_2},\\
&|\Phi^+\rangle_{A_1A_2}|\Phi^-\rangle_{B_1B_2}|\Psi^-\rangle_{C_1C_2},\\
&|\Phi^-\rangle_{A_1A_2}|\Phi^+\rangle_{B_1B_2}|\Psi^-\rangle_{C_1C_2},\\
&|\Phi^-\rangle_{A_1A_2}|\Phi^-\rangle_{B_1B_2}|\Psi^+\rangle_{C_1C_2}\} \rightarrow 110, \qquad (20)\\
&\{|\Psi^+\rangle_{A_1A_2}|\Psi^+\rangle_{B_1B_2}|\Phi^-\rangle_{C_1C_2},\\
&|\Psi^+\rangle_{A_1A_2}|\Psi^-\rangle_{B_1B_2}|\Phi^+\rangle_{C_1C_2},\\
&|\Psi^-\rangle_{A_1A_2}|\Psi^+\rangle_{B_1B_2}|\Phi^+\rangle_{C_1C_2},\\
&|\Psi^-\rangle_{A_1A_2}|\Psi^-\rangle_{B_1B_2}|\Phi^-\rangle_{C_1C_2},\\
&|\Phi^+\rangle_{A_1A_2}|\Phi^+\rangle_{B_1B_2}|\Psi^-\rangle_{C_1C_2},\\
&|\Phi^+\rangle_{A_1A_2}|\Phi^-\rangle_{B_1B_2}|\Psi^+\rangle_{C_1C_2},\\
&|\Phi^-\rangle_{A_1A_2}|\Phi^+\rangle_{B_1B_2}|\Psi^+\rangle_{C_1C_2},\\
&|\Phi^-\rangle_{A_1A_2}|\Phi^-\rangle_{B_1B_2}|\Psi^-\rangle_{C_1C_2}\} \rightarrow 111. \qquad (21)
\end{aligned}
$$

Further extending the initial state from $|\Psi_1\rangle$ to other seven GHZ states $|\Psi_k\rangle$ ($k = 2, \ldots, 8$), all the result collections composed by different results of A_1A_2, B_1B_2, and C_1C_2 after the entanglement swapping are listed in Table 1. Take the initial state of particles A_1, B_1, C_1 to be $|\Psi_2\rangle^{001}_{A_1B_1C_1}$ and the initial state of particles A_2, B_2, C_2 to be $|\Psi_6\rangle^{101}_{A_2B_2C_2}$ for example. The superscript in $|\Psi_2\rangle^{001}_{A_1B_1C_1}$ denotes that $|\Psi_2\rangle^{001}_{A_1B_1C_1}$ can be obtained by performing U_2 on the first and the second particles of $|\Psi_1\rangle^{000}_{A_1B_1C_1}$, while 100 denotes that the result collection composed by A_1A_2, B_1B_2, and C_1C_2 after the entanglement swapping from $|\Psi_2\rangle^{001}_{A_1B_1C_1}$ and $|\Psi_6\rangle^{101}_{A_2B_2C_2}$ corresponds to formula (18).

Table 1. Result collections of entanglement swapping between any two GHZ states (the superscript denotes the codes of U_k, and the subscript denotes the particles in the GHZ states).

	$\|\Psi_1\rangle^{000}_{A_2B_2C_2}$	$\|\Psi_2\rangle^{001}_{A_2B_2C_2}$	$\|\Psi_3\rangle^{010}_{A_2B_2C_2}$	$\|\Psi_4\rangle^{011}_{A_2B_2C_2}$	$\|\Psi_5\rangle^{100}_{A_2B_2C_2}$	$\|\Psi_6\rangle^{101}_{A_2B_2C_2}$	$\|\Psi_7\rangle^{110}_{A_2B_2C_2}$	$\|\Psi_8\rangle^{111}_{A_2B_2C_2}$
$\|\Psi_1\rangle^{000}_{A_1B_1C_1}$	000	001	010	011	100	101	110	111
$\|\Psi_2\rangle^{001}_{A_1B_1C_1}$	001	000	011	010	101	100	111	110
$\|\Psi_3\rangle^{010}_{A_1B_1C_1}$	010	011	000	001	110	111	100	101
$\|\Psi_4\rangle^{011}_{A_1B_1C_1}$	011	010	001	000	111	110	101	100
$\|\Psi_5\rangle^{100}_{A_1B_1C_1}$	100	101	110	111	000	001	010	011
$\|\Psi_6\rangle^{101}_{A_1B_1C_1}$	101	100	111	110	001	000	011	010
$\|\Psi_7\rangle^{110}_{A_1B_1C_1}$	110	111	100	101	010	011	000	001
$\|\Psi_8\rangle^{111}_{A_1B_1C_1}$	111	110	101	100	011	010	001	000

3. Quantum steganography protocol

Our quantum steganography protocol integrates the original QSDC adopting the dense coding of the GHZ states, which is inspired by Refs. [7] and [9], and the entanglement swapping of the GHZ states together. In the schemes of Refs. [7] and [9], all particles are eventually transmitted from one communication party to the other communication party. However, in that original QSDC, the third particle from each GHZ triplet is always kept intact in one communication party's hand, while the first and the second particles are transmitted between the two communication parties. The basic idea of the original QSDC is as follows. (i) Bob keeps the sequence of the third particle from each GHZ triplet in hand, and sends the se-

quences of the first and the second particles to Alice one by one. In order to ensure security, the eavesdropper detection is implemented in each transmission. (ii) According to the bits sequence of information, Alice then adopts the dense coding of the GHZ states to perform unitary operations on the two sequences. Afterward, Alice sends the two encoded sequences back to Bob. (iii) Finally, Bob implements the GHZ-basis measurement on each GHZ triplet to recover the information. Due to the dense coding of the GHZ states, the original QSDC can transmit three bits information per round communication. Now, we demonstrate our quantum steganography protocol in detail as follows.

S1) Bob prepares a large number (n) of $|\Psi_1\rangle_{\rm ABC}$. Let $G_{\rm A}$, $G_{\rm B}$, and $G_{\rm C}$ denote the particle groups of A, B, and C, respectively. Accordingly, $G_{\rm A}=[{\rm A}_1,{\rm A}_2,\ldots,{\rm A}_n]$, $G_{\rm B}=[{\rm B}_1,{\rm B}_2,\ldots,{\rm B}_n]$, and $G_{\rm C}=[{\rm C}_1,{\rm C}_2,\ldots,{\rm C}_n]$, where the subscript denotes the number of GHZ states.

S2) Bob sends $G_{\rm A}$ and $G_{\rm B}$ to Alice by a quantum channel in two steps. (i) Bob sends $G_{\rm A}$ to Alice while keeping $G_{\rm B}$ and $G_{\rm C}$ to himself. For eavesdropper detection, Alice selects a large enough subgroup from $G_{\rm A}$, and chooses randomly a measurement basis, Z-basis ($|0\rangle$, $|1\rangle$) or X-basis ($|+\rangle$, $|-\rangle$), to measure particle A in the subgroup from $G_{\rm A}$. Alice publishes her measurement basis and measurement results to Bob. After obtaining Alice's results, Bob measures particle B from the corresponding subgroup of $G_{\rm B}$ and particle C from the corresponding subgroup of $G_{\rm C}$ under the same measurement basis. According to formula (22), by comparing with Alice's measurement results, Bob can know whether there is an eavesdropper or not. If the channel is safe, their measurement results are highly correlated. If Alice and Bob use the Z-basis, Bob's measurement result should be $|0\rangle|0\rangle$ ($|1\rangle|1\rangle$) when Alice gets the measurement result $|0\rangle$ ($|1\rangle$). If Alice and Bob use the X-basis, Bob's measurement result should be $|+\rangle|+\rangle$ or $|-\rangle|-\rangle$ ($|+\rangle|-\rangle$ or $|-\rangle|+\rangle$) when Alice gets the measurement result $|+\rangle$ ($|-\rangle$). If Bob confirms that there is an eavesdropper, they abort the communication; otherwise, they enter the following step (ii). (ii) Bob sends $G_{\rm B}$ to Alice while keeping $G_{\rm C}$ to himself. For eavesdropper detection, Alice selects a large enough subgroup from $G_{\rm A}$ and a large enough corresponding subgroup from $G_{\rm B}$, and chooses a measurement basis randomly, Z-basis ($|0\rangle$,$|1\rangle$) or X-basis ($|+\rangle$, $|-\rangle$), to measure particles A and B. Alice publishes her measurement basis and measurement results to Bob. After obtaining Alice's results, Bob measures particle C from the corresponding subgroup of $G_{\rm C}$ under the same measurement basis. According to formula (22), by comparing with Alice's measurement results, Bob can know whether there is an eavesdropper or not. If the channel is safe, their measurement results are highly correlated. Then, if Bob confirms that there is an eavesdropper, they abort the communication; otherwise, they enter information transmission mode S3).

$$\begin{aligned}|\Psi_1\rangle_{\rm ABC} &= \frac{1}{\sqrt{2}}(|000\rangle_{\rm ABC}+|111\rangle_{\rm ABC})\\ &= \frac{1}{2}\big[|+\rangle_{\rm A}(|+\rangle_{\rm B}|+\rangle_{\rm C}+|-\rangle_{\rm B}|-\rangle_{\rm C})\\ &\quad +|-\rangle_{\rm A}(|+\rangle_{\rm B}|-\rangle_{\rm C}+|-\rangle_{\rm B}|+\rangle_{\rm C})\big]\\ &= \frac{1}{2}\big[(|+\rangle_{\rm A}|+\rangle_{\rm B}+|-\rangle_{\rm A}|-\rangle_{\rm B})|+\rangle_{\rm C}\\ &\quad +(|+\rangle_{\rm A}|-\rangle_{\rm B}+|-\rangle_{\rm A}|+\rangle_{\rm B})|-\rangle_{\rm C}\big]. \qquad (22)\end{aligned}$$

S3) **Information transmission mode** (i) According to the bits sequence of information, Alice performs U_k on the pairs of particles in $G_{\rm A}$ and $G_{\rm B}$. Note that after performed with U_k, $G_{\rm A}$ and $G_{\rm B}$ become $G'_{\rm A}$ and $G'_{\rm B}$, respectively. Although no unitary operations have been performed on the particle in $G_{\rm C}$, for consistence, $G'_{\rm C}$ is still used to represent the original $G_{\rm C}$. Accordingly, $G'_{\rm C}$ is the same as $G_{\rm C}$. (ii) According to secret messages, Alice chooses four particles ${\rm A}'_m$, ${\rm A}'_{m+1}$, ${\rm B}'_m$, ${\rm B}'_{m+1}$ from $G'_{\rm A}$ and $G'_{\rm B}$, respectively, and enters the secret message hiding mode. (iii) Alice sends $G'_{\rm A}$ and $G'_{\rm B}$ back to Bob by a quantum channel.

S4) **Secret message hiding mode** (i) According to secret messages, Alice chooses four particles ${\rm A}'_m$, ${\rm A}'_{m+1}$, ${\rm B}'_m$, ${\rm B}'_{m+1}$ from $G'_{\rm A}$ and $G'_{\rm B}$, respectively, where subscript m represents the position of particle ${\rm A}'_m$ in $G'_{\rm A}$ and the position of particle ${\rm B}'_m$ in $G'_{\rm B}$. The m must satisfy the consistent condition, which means two GHZ states formed by ${\rm A}'_{m-1}{\rm B}'_{m-1}{\rm C}'_{m-1}$ and ${\rm A}'_m{\rm B}'_m{\rm C}'_m$ must be consistent with the secret messages, as shown in Table 1 (an appropriate m can be decided by Alice in advance before sending it to Bob by implementing QSDC, QKD, or a one-time pad through the classical channel[23]). (ii) By performing the same U_k on ${\rm A}_{m+1}$ and ${\rm B}_{m+1}$ in advance, ${\rm A}'_{m+1}{\rm B}'_{m+1}{\rm C}'_{m+1}$ can copy the information carried by ${\rm A}'_{m-1}{\rm B}'_{m-1}{\rm C}'_{m-1}$. Consequently, ${\rm A}'_{m+1}{\rm B}'_{m+1}{\rm C}'_{m+1}$ does not normally transmit information but acts as an auxiliary GHZ state to help hide the secret messages.

S5) **Secret message decoding mode** (i) Bob gets the value of m. (ii) Bob performs the GHZ-basis measurement on ${\rm A}'_{m-1}{\rm B}'_{m-1}{\rm C}'_{m-1}$ to recover the information. (iii) Bob performs the Bell-basis measurement on ${\rm A}'_m{\rm A}'_{m+1}$, ${\rm B}'_m{\rm B}'_{m+1}$, and ${\rm C}'_m{\rm C}'_{m+1}$ respectively. (iv) Then, Bob decodes the secret messages sent by Alice according to formulas (14)–(21). Moreover, through the decoded secret messages and the state of ${\rm A}'_{m-1}{\rm B}'_{m-1}{\rm C}'_{m-1}$, Bob can also recover the information carried by ${\rm A}'_m{\rm B}'_m{\rm C}'_m$ according to Table 1.

We use an example to further explain secret message hiding mode S4) and secret message decoding S5) in our quantum steganography protocol. Assume that the secret messages Alice wants to send to Bob are 100, and the information sequence $\cdots 000_{100}\cdots 001_{101}\cdots 010_{110}\cdots 011_{111}\cdots 100_{000}\cdots 101_{001}\cdots 110_{010}\cdots 111_{011}\cdots$ is generated

by Alice (the information is divided by six bits, since two U_k denote six bits information). Assume that the group numbers of 000_{100}, 001_{101}, 010_{110}, 011_{111}, 100_{000}, 101_{001}, 110_{010}, and 111_{011} in the information sequence are Nos. 7, 10, 13, 16, 20, 25, 28, and 32, respectively. In S3), Alice can make $m = 7$, 10, 13, 16, 20, 25, 28, or 32 to satisfy the consistency in Table 1. If $m = 7$, $A'_6B'_6C'_6$ will be $|\Psi_1\rangle$ and $A'_7B'_7C'_7$ will be $|\Psi_5\rangle$. Accordingly, the secret messages 100 are transmitted by the entanglement swapping between $A'_7B'_7C'_7$ and $A'_8B'_8C'_8$. The secret messages 100 can also be transmitted in the same way, if $m = 10$, 13, 16, 20, 25, 28, or 32. Note that $A'_8B'_8C'_8$ can not be used to transmit the information like the other normal GHZ states, and acts as an auxiliary GHZ state to help hide the secret messages. In S6), Bob obtains the value of m at first. Afterward, Bob performs the GHZ-basis measurement on $A'_6B'_6C'_6$. Then, Bob performs the Bell-basis measurement on $A'_7A'_8$, $B'_7B'_8$, and $C'_7C'_8$ respectively. According to formulas (14)–(21), Bob can decode that the secret messages are 100. Then, according to the state of $A'_6B'_6C'_6$ ($|\Psi_1\rangle$) , the secret messages 100, and Table 1, Bob can easily know that the information carried by $A'_7B'_7C'_7$ is 100.

4. Analysis

4.1. Capacity

In the above quantum steganography protocol, three bits secret messages are transmitted by the entanglement swapping between $A'_{m+1}B'_{m+1}C'_{m+1}$ and $A'_mB'_mC'_m$. In addition, $A'_{m+1}B'_{m+1}C'_{m+1}$ copies the information carried by $A'_{m-1}B'_{m-1}C'_{m-1}$ and acts as an auxiliary GHZ state to help hide the secret messages. Accordingly, the information carried by $A'_mB'_mC'_m$ is recovered, while $A'_{m+1}B'_{m+1}C'_{m+1}$ is consumed. Moreover, it is clear that three bits secret messages can be transmitted by eight different kinds of initial states. For example, according to Table 1, messages 100 can be transmitted by eight different kinds of initial states

$$\left\{|\Psi_1\rangle^{000}_{A_1B_1C_1}, |\Psi_5\rangle^{100}_{A_2B_2C_2}\right\}, \quad \left\{|\Psi_2\rangle^{001}_{A_1B_1C_1}, |\Psi_6\rangle^{101}_{A_2B_2C_2}\right\},$$
$$\left\{|\Psi_3\rangle^{010}_{A_1B_1C_1}, |\Psi_7\rangle^{110}_{A_2B_2C_2}\right\}, \quad \left\{|\Psi_4\rangle^{011}_{A_1B_1C_1}, |\Psi_8\rangle^{111}_{A_2B_2C_2}\right\},$$
$$\left\{|\Psi_5\rangle^{100}_{A_1B_1C_1}, |\Psi_1\rangle^{000}_{A_2B_2C_2}\right\}, \quad \left\{|\Psi_6\rangle^{101}_{A_1B_1C_1}, |\Psi_2\rangle^{001}_{A_2B_2C_2}\right\},$$
$$\left\{|\Psi_7\rangle^{110}_{A_1B_1C_1}, |\Psi_3\rangle^{010}_{A_2B_2C_2}\right\}, \quad \left\{|\Psi_8\rangle^{111}_{A_1B_1C_1}, |\Psi_4\rangle^{011}_{A_2B_2C_2}\right\}.$$

After coding these eight different kinds of initial states by formula (23), the capacity of the quantum channel in the above quantum steganography protocol can be increased to six bits. Consequently, the quantum channel capacity is six times of that in Refs. [19]– [22], and one and half times of that in Ref. [23]. The reason why the quantum channel capacity is larger than that in Ref. [23] lies in two facts. (i) The entanglement swapping between two GHZ states transmits three bits in our quantum steganography protocol, while the entanglement swapping between two Bell states only transmits two bits in Ref. [23]. (ii) Each three bits secret message corresponds to eight different kinds of initial states in our quantum steganography protocol, while each two bit secret message corresponds to four different kinds of initial states in Ref. [23].

$$\begin{aligned} &000100 \to 000, 001101 \to 001, 010110 \to 010, \\ &011111 \to 011, 100000 \to 100, 101001 \to 101, \\ &110010 \to 110, 111011 \to 111. \end{aligned} \tag{23}$$

Based on the above analysis, our quantum steganography protocol can transmit six bits per round covert communication. In fact, our quantum steganography protocol transmits secret messages by building up a hidden channel within the original QSDC. However, the original QSDC only transmits three bits per round covert communication. Thus, the transmission efficiency of our quantum steganography protocol is twice of that of the original QSDC. It can be concluded that the super quantum channel integrating the original quantum channel of the QSDC and the hidden channel in our quantum steganography protocol can enlarge the capacity of the quantum channel. It is also possible to apply the idea of our quantum steganography protocol to QSS and QKD based on the GHZ states to enlarge the transmission efficiency of the original quantum channel.

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 $A'_{m-1}B'_{m-1}C'_{m-1}$, $A'_mB'_mC'_m$, and secret messages. Consequently, the imperceptibility mainly depends on the difficulty of knowing m by Eve. As pointed out in Ref. [23], choosing m can still be treated as an arbitrary behavior for Eve, since both information and secret messages can be regarded to be random or pseudo-random. If the information or secret messages do not distribute randomly in advance, a pseudo-random sequence encryption can be adopted to make its distribution randomized.

For example, if the secret messages Alice wants to send to Bob are 100, in order to choose m, Alice needs to find out all the group numbers of 000_{100}, 001_{101}, 010_{110}, 011_{111}, 100_{000}, 101_{001}, 110_{010}, 111_{011} in the information sequence. Accordingly, the GHZ states $A'_{m-1}B'_{m-1}C'_{m-1}$ and $A'_mB'_mC'_m$ will be $|\Psi_1\rangle|\Psi_5\rangle$, $|\Psi_2\rangle|\Psi_6\rangle$, $|\Psi_3\rangle|\Psi_7\rangle$, $|\Psi_4\rangle|\Psi_8\rangle$, $|\Psi_5\rangle|\Psi_1\rangle$, $|\Psi_6\rangle|\Psi_2\rangle$, $|\Psi_7\rangle|\Psi_3\rangle$, and $|\Psi_8\rangle|\Psi_4\rangle$ respectively. If the information distributes evenly, probability of 000_{100}, 001_{101}, 010_{110}, 011_{111}, 100_{000}, 101_{001}, 110_{010}, 111_{011} will be $1/64$ each. Consequently, their total probability is $1/8$. It is similar if the secret messages are 000, 001, 010, 011, 101, 110, or 111. 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 Ref. [23]. Consequently, m can be regarded as a random number for Eve. It means that the imperceptibility of our quantum steganography protocol is good.

4.3. Security

The security of our protocol can be proved via the security of the original QSDC. The original QSDC uses the GHZ states, and its security is similar to the scheme using the Bell states in Ref. [7]. The security of the original QSDC is based on the security for the transmission of $G_{\rm A}$ and $G_{\rm B}$ from Bob to Alice.

Now we analyze the security for the transmission of $G_{\rm A}$ against the entanglement-and-measurement attack at first. According to the Stinespring dilation theorem, Eve's eavesdropping can be realized by a unitary operation $\hat{E}$ on a larger Hilbert space, $|x,E\rangle \equiv |x\rangle\,|E\rangle$. Therefore, the state of the composite system will be

$$\begin{aligned}|\psi\rangle \;=\; & \frac{1}{\sqrt{2}}\big[(\alpha_1\,|0\rangle\,|\varepsilon_{00}\rangle+\beta_1\,|1\rangle\,|\varepsilon_{01}\rangle)\,|00\rangle \\ & +\left(\beta_1'\,|0\rangle\,|\varepsilon_{10}\rangle+\alpha_1'\,|1\rangle\,|\varepsilon_{11}\rangle\right)|11\rangle\big],\end{aligned} \tag{24}$$

where ε_{00}, ε_{01}, ε_{10}, ε_{11} are Eve's states, and $\hat{E}=\begin{pmatrix}\alpha_1 & \beta_1'\\ \beta_1 & \alpha_1'\end{pmatrix}$ is Eve's probe operator. Since $\hat{E}$ is a unitary operator, we can obtain that the error rate introduced by Eve's eavesdropping on $G_{\rm A}$ is $\tau_1=|\beta_1|^2=|\beta_1'|^2=1-|\alpha_1|^2=1-|\alpha_1'|^2$. The security for the transmission of $G_{\rm B}$ against the entanglement-and-measurement attack can be analyzed in a similar way as above. After Eve eavesdrops $G_{\rm B}$ before the second checking, the state of the composite system will be

$$\begin{aligned}|\psi\rangle \;=\; & \frac{1}{\sqrt{2}}\big[|0\rangle\,(\alpha_2\,|0\rangle\,|\varepsilon_{00}\rangle+\beta_2\,|1\rangle\,|\varepsilon_{01}\rangle)\,|0\rangle \\ & +|1\rangle\left(\beta_2'\,|0\rangle\,|\varepsilon_{10}\rangle+\alpha_2'\,|1\rangle\,|\varepsilon_{11}\rangle\right)|1\rangle\big].\end{aligned} \tag{25}$$

We can obtain that the error rate introduced by Eve's eavesdropping on $G_{\rm B}$ will be $\tau_2=|\beta_2|^2=|\beta_2'|^2=1-|\alpha_2|^2=1-|\alpha_2'|^2$.

Without loss of generality, we turn to analyze the measure-resend attack on $G_{\rm A}$. Eve intercepts particle A in $G_{\rm A}$, measures it in Z-basis or X-basis, and resends its measurement result to Alice. If Eve performs the Z-basis measurement, the state of the whole system will collapse to $|000\rangle$ or $|111\rangle$ each with probability $1/2$. Take the state to be $|000\rangle_{\rm ABC}$ for example. Accordingly, Eve resends $|0\rangle_{\rm A}$ to Alice. Then, if Alice performs the Z-basis measurement to check eavesdropping, no error will be introduced by Eve. If Alice performs the X-basis measurement, the state will collapse to $|opq\rangle_{\rm ABC}$ $(o,p,q=+,-)$ each with probability $1/8$. According to formula (22), the error rate introduced by Eve will be 50%. Therefore, the total error rate in this case is 25%. If Eve uses X-basis, the total error rate in this case is 37.5%. Therefore, the random Z-basis or X-basis measurement guarantees that Eve's attack can be found out by eavesdropping check.

Further, we consider the influence caused by the leakage of m. Assume that Eve not only obtains m but also gets $\mathrm{A}'_m\mathrm{A}'_{m+1}$ and $\mathrm{B}'_m\mathrm{B}'_{m+1}$ through some advance eavesdropping attacks (it is possible for Eve to eavesdrop $\mathrm{A}'_m\mathrm{A}'_{m+1}$ and $\mathrm{B}'_m\mathrm{B}'_{m+1}$, since particles A and B are travel particles). However, Eve still can not get secret messages according to formulas (14)–(21), because only knowing $\mathrm{A}'_m\mathrm{A}'_{m+1}$ and $\mathrm{B}'_m\mathrm{B}'_{m+1}$ is not enough to decode the secret messages.

5. Discussion and conclusion

As analyzed in Subsection 4.1, the capacity of the super quantum channel in our quantum steganography protocol achieves six bits, and is twice of that of the original QSDC. The reason lies in that the super quantum channel is formed by building up a hidden channel within the original QSDC. However, the hidden channel works at the cost of transmitting m. Transmitting m means to transmit $\log_2 m$ bits. If m is great enough, transmitting m may consume more bits than the secret messages. Fortunately, as pointed out in Ref. [23], since m can be decided and transmitted by implementing QSDC, QKD, or a one-time pad through the classical channel in advance, it is unnecessary to overemphasize the cost of transmitting m. Furthermore, since m and the secret messages tend to have different security levels, it is reasonable to consume a certain resource to achieve the covert communication for secret messages.

To sum up, a quantum steganography protocol with a large payload is proposed based on the dense coding and the entanglement swapping of the GHZ states. Its super quantum channel is formed by building up a hidden channel within the original QSDC. Based on the original QSDC, secret messages are transmitted by integrating the dense coding and the entanglement swapping of the GHZ states. It can transmit six bits per round covert communication, much higher than the previous quantum steganography protocols. Since the information and the secret messages can be regarded to be random or pseudo-random, its imperceptibility is good. Moreover, its security is proved to be reliable. In the future, our research of quantum steganography will concentrate on two aspects, i.e., using quantum error-correcting code to hide secret messages and applying quantum Fourier transform into the literature of steganography.

References

[1] Bennett C H and Brassard G 1984 *International Conference on Computers, Systems & Signal Processing,* December 10–19, 1984 Bangalore India, p. 175
[2] Bennett C H, Brassard G and Mermin N D 1992 *Phys. Rev. Lett.* **68** 557
[3] Cabell A 2000 *Phys. Rev. Lett.* **85** 5635
[4] Long G L and Liu X S 2002 *Phys. Rev. A* **65** 032302
[5] Beige A, Englert B G and Kurtsiefer C 2002 *Acta Physica Polonica A* **101** 357
[6] Bostrom K and Felbinger T 2002 *Phys. Rev. Lett.* **89** 187902
[7] Deng F G, Long G L and Liu X S 2003 *Phys. Rev. A* **68** 042317
[8] Cai Q Y and Li B W 2004 *Phys. Rev. A* **69** 054301
[9] Wang C, Deng F G and Long G L 2005 *Opt. Commun.* **253** 15
[10] Gao T, Yan F L and Wang Z X 2005 *Chin. Phys. Lett.* **22** 2473
[11] Sun Y, Wen Q Y and Zhu F C 2008 *Chin. Phys. Lett.* **25** 828
[12] Chen X B, Wang T Y, Du J Z, Wen Q Y and Zhu F C 2008 *Int. J. Quant. Inform.* **6** 543
[13] Chen X B, Wen Q Y, Guo F Z, Sun Y, Xu G and Zhu F C 2008 *Int. J. Quant. Inform.* **6** 899
[14] Huang W, Wen Q Y, Jia H Y, Qin S J and Gao F 2012 *Chin. Phys. B* **21** 100308
[15] Hillery M, Buzek V and Berthiaume A 1999 *Phys. Rev. A* **59** 1829
[16] Guo G P and Guo G C 2003 *Phys. Lett. A* **310** 247
[17] Chen X B, Yang S, Su Y and Yang Y X 2012 *Phys. Scr.* **86** 055002
[18] Chen X B, Niu X X, Zhou X J and Yang Y X 2013 *Quantum Inf. Process.* **12** 365
[19] Gea-Banacloche J 2002 *J. Math. Phys.* **43** 4531
[20] Worley III G G 2004 arXiv: ph/0401041v2
[21] Martin K 2007 *IH2007 LNCS* **4567** 32
[22] Liao X, Wen Q Y, Sun Y and Zhang J 2010 *J. Syst. Software* **83** 1801
[23] Qu Z G, Chen X B, Zhou X J, Niu X X and Yang Y X 2010 *Opt. Commun.* **283** 4782
[24] Lee H J, Ahn D and Hwang S W 2002 *Phys. Rev. A* **66** 024304
[25] Bennett C H and Wiesner S J 1992 *Phys. Rev. Lett.* **69** 2881