Three-party quantum secret sharing of secure direct communication based on χ-type entangled states*

Yang Yu-Guang(杨宇光)[a)†], Cao Wei-Feng(曹卫锋)[c)], and Wen Qiao-Yan(温巧燕)[b)]

[a)] *College of Computer Science and Technology, Beijing University of Technology, Beijing* 100124, *China*
[b)] *State Key Laboratory of Networking and Switching Technology, Beijing University of Posts and Telecommunications, Beijing* 100876, *China*
[c)] *College of Electric and Information Engineering, Zhengzhou University of Light Industry, Zhengzhou* 450002, *China*

(Received 14 July 2009; revised manuscript received 4 November 2009)

Based on χ-type entangled states and the two-step protocol [Deng F G, Long G L and Liu X S 2003 *Phys. Rev.* A **68** 042317], a quantum secret sharing protocol of secure direct communication based on χ-type entangled states $|\chi^{00}\rangle_{3214}$ is proposed. Using some interesting entanglement properties of this state, the agent entirety can directly obtain the secret message from the message sender only if they collaborate together. The security of the scheme is also discussed.

Keywords: quantum secret sharing, quantum secure direct communication, χ-type entangled states
PACC: 0367, 0365

1. Introduction

The introduction of quantum mechanics principles into cryptography forms quantum cryptography. Since Bennett and Brassard designed the original QKD protocol,[1] many branches of quantum cryptography have progressed quickly, including quantum key distribution (QKD),[1] quantum secure direct communication (QSDC),[2−26] quantum secret sharing (QSS),[27−48] and so on. The goal of QKD is to allow two legitimate parties, Alice and Bob, to generate a secret key over a long distance, in the presence of an eavesdropper, Eve, who interferes with the signals. Different from QKD, QSDC's object is to transmit the secret messages directly without first establishing a key to encrypt them. QSDC can be used in some special environments which have been shown by Boströem and Felbinger[3] and Deng *et al.*[4] QSS is the generalisation of classical secret sharing into quantum scenario. The basic idea of classical secret sharing in the simplest case is that the sender Alice splits the secret message into two shares and distributes them to two agents Bob and Charlie separately, such that the two agents can reconstruct the secret message only when they collaborate. QSS is likely to play a key role in both transmitting of classical message and protecting secret quantum information, e.g., in secure operations of distributed quantum computation, sharing difficult-to-construct ancilla states and joint sharing of quantum money, and so on. Hence, after HBB's pioneering work,[27] QSS, as an important branch of quantum communication, has so far attracted a great deal of attention.[27−48] These works can be divided into two kinds, classical message (i.e., bits) sharing[27−38] and quantum information (a quantum state) sharing.[27,39−48] The latter was clearly termed as quantum state sharing (QSTS) by Lance *et al.*[43] to differentiate from the QSS of classical message in 2004. More recently, a new kind of theoretical schemes, i.e., controlled quantum teleportation has been proposed.[49−54] In controlled teleportation, a sender transmits quantum message to a receiver via the control of agents in a network. Only when all agents collaborate, can the receiver restore

*Project supported by the National High-Tech Research and Development Program of China (Grant Nos. 2006AA01Z440, 2009AA012441 and 2009AA012437) and National Basic Research Program of China (Grant No. 2007CB311100), the National Natural Science Foundation of China (Grant Nos. 60873191 and 60821001), the Scientific Research Common Program of Beijing Municipal Commission of Education (Grant No. KM200810005004), Beijing Natural Science Foundation (Grant Nos. 1093015 and 1102004), the ISN Open Foundation, Specialized Research Fund for the Doctoral Programm of Higher Education (Grant No. 20091103120014).

†Corresponding author. E-mail: yangyang7357@bjut.edu.cn

© 2010 Chinese Physical Society and IOP Publishing Ltd

the original quantum state. If any agent does not cooperate, the original quantum information cannot be fully recovered. In this point of view, controlled teleportation is similar to QSTS and can be used for QSTS with a little or without modification.

In 2005, a new concept of quantum secret sharing of secure direct communication (QSS-SDC) was definitely presented by Zhang,[29] where the functions of both QSDC and QSS are combined and their advantages are included. Comparing with QSS of keys, QSS-SDC can be useful in some urgent circumstances, which allows the sender to transmit deterministic secret information (not a random key) to the agents only if they collaborate together. In fact, QSTS and controlled teleportation can be used for QSS-SDC with a little or without modification. As QSS-SDC schemes are useful in some urgent circumstances, many efforts have been made on them and lots of schemes were presented.[29−35] For example, Zhang and Man[30] proposed a multiparty QSS protocol of classical messages (QSSCM) by swapping quantum entanglement of Bell states. Based on the QSDC protocol,[6] Zhang *et al.*[31] proposed an (n,n)-threshold scheme of multiparty QSSCM using only single photons. Wang *et al.*[32] proposed an (n,n)-threshold scheme of multiparty QSS based on Greenberger–Horne–Zeilinger (GHZ) state and teleportation. Based on the protocol of Zhang *et al.*[31] and the concept of QSS-SDC, Han *et al.*[33] proposed a scheme for multiparty QSS-SDC using single photons and random phase shift operations (RPSOs) instead of some special discrete unitary operations to realise the sharing controls. However, Qin *et al.*[34] reexamined Han *et al.*'s protocol[33] and showed that it is insecure against a special attack.

In the above QSS-SDC schemes, the states as quantum channel are Einstein–Podolsky–Rosen (EPR) pairs, GHZ class states, W class states or single photons. In this paper, an efficient QSS-SDC protocol is proposed, based on the idea of the transmission of quantum data block[55] and four-qubit χ-type entangled states[56,57]

$$\begin{aligned}&|\chi^{00}\rangle_{3214}\\ =\ &\frac{1}{2\sqrt{2}}(|0000\rangle-|0011\rangle-|0101\rangle+|0110\rangle\\ &+|1001\rangle+|1010\rangle+|1100\rangle+|1111\rangle)_{3214},\end{aligned}\quad(1)$$

where the subscripts 3, 2, 1, and 4 denote different particles in a χ-type entangled state. Then we analyse the security of the scheme.

2. The QSS-SDC scheme with χ-type entangled states

The genuine four-qubit entangled state $|\chi^{00}\rangle_{3214}$ does not belong to the well-known three types of multipartite entangled states, i.e., GHZ state,[58] W state,[59] and linear cluster state,[60] in terms of stochastic local operations and classical communication. And it is not reducible to a pair of Bell states. Its properties were compared and contrasted with those of the four-party GHz and W states in Ref. [56].

The state $|\chi^{00}\rangle_{3214}$ has many interesting properties. For example, performing Pauli operation on qubits 3 and 1, respectively, can construct an orthonormal basis set FMB $=\{|\chi^{ij}\rangle_{3214}=\sigma_3^i\sigma_1^j|\chi^{00}\rangle_{3214}|i,j=0,1,2,3\}$ for the four-qubit Hilbert space. Here, σ^i is one of the four Pauli operators, i.e., $\sigma^0=I=|0\rangle\langle 0|+|1\rangle\langle 1|$, $\sigma^1=|0\rangle\langle 0|-|1\rangle\langle 1|$, $\sigma^2=|0\rangle\langle 1|+|1\rangle\langle 0|$, $\sigma^3=|0\rangle\langle 1|-|1\rangle\langle 0|$. Meanwhile, these states are maximally entangled states and both the corresponding reduced density matrices of the qubits (3, 1) and (2, 4), are equal to the complete mixture, $\rho=(|00\rangle\langle 00|+|01\rangle\langle 01|+|10\rangle\langle 10|+|11\rangle\langle 11|)/4$ and indistinguishable. But a perfect four-particle projective measurement can successfully discriminate the state of particles (3, 2, 1, 4). Because of the interesting entanglement properties of $|\chi^{00}\rangle_{3214}$, it has been used in many aspects, such as teleportation and dense coding,[56] QSDC,[61] deterministic secure quantum communication.[62]

Due to the orthogonal properties of χ-type entangled states, the four particles cannot be transmitted simultaneously in the quantum channel. So, similar to Ref. [61], the transmission can be performed by two steps. In addition, the state $|\chi^{00}\rangle_{3214}$ may be rewritten in the following way, simply by regrouping terms,

$$\begin{aligned}|\chi^{00}\rangle_{3214}=\ &\frac{1}{2}(|\Phi_1^-\rangle|0+\rangle+|\Phi_1^+\rangle|0-\rangle+|\Psi_1^-\rangle|1\\ &+\rangle+|\Psi_1^+\rangle|1-\rangle)_{3214}.\end{aligned}\quad(2)$$

Similarly, $|\chi^{00}\rangle_{3214}$ can be rewritten in another form

$$\begin{aligned}|\chi^{00}\rangle_{3214}=\ &\frac{1}{2}(|\Phi_2^+\rangle|+0\rangle+|\Phi_2^-\rangle|-0\rangle\\ &-|\Psi_2^+\rangle|+1\rangle-|\Psi_2^-\rangle|-1\rangle)_{3214},\end{aligned}\quad(3)$$

here, $|\Phi_1^\pm\rangle=(|\phi^+\rangle\pm|\psi^-\rangle)/\sqrt{2}$, $|\Psi_1^\pm\rangle=(|\psi^+\rangle\pm|\phi^-\rangle)/\sqrt{2}$, $|\Phi_2^\pm\rangle=(|\phi^+\rangle\pm|\psi^+\rangle)/\sqrt{2}$, $|\Psi_2^\pm\rangle=(|\psi^-\rangle\pm|\phi^-\rangle)/\sqrt{2}$, where $|\phi^\pm\rangle=(|00\rangle\pm|11\rangle)/\sqrt{2}$ and $|\psi^\pm\rangle=(|01\rangle\pm|10\rangle)/\sqrt{2}$ are the four Bell states. The four states $|\Phi_1^\pm\rangle$ and $|\Psi_1^\pm\rangle$ form an orthonormal basis AMB_1 for the two-qubit Hilbert

space. And the states $|\Phi_2^{\pm}\rangle$ and $|\Psi_2^{\pm}\rangle$ form another orthonormal basis AMB_2 for the two-qubit Hilbert space. One can easily see that there are four possible results $|\Phi_1^-\rangle|0+\rangle, |\Phi_1^+\rangle|0-\rangle, |\Psi_1^-\rangle|1+\rangle$, and $|\Psi_1^+\rangle|1-\rangle$ with equal probability of 1/4 if we measure the qubits (3, 1) and (2, 4) in the basis $\mathrm{AMB}_1 = \{|\Phi_1^{\pm}\rangle, |\Psi_1^{\pm}\rangle\}$ and $\mathrm{BMB}_1 = \{|0+\rangle, |0-\rangle, |1+\rangle, |1-\rangle || \pm\rangle = (|0\rangle \pm |1\rangle)/\sqrt{2}\}$, respectively. Obviously, there exists the similar correlation of the measurement results if we measure the qubits (3, 1) and (2, 4) in the basis $\mathrm{AMB}_2 = \{|\Phi_2^{\pm}\rangle, |\Psi_2^{\pm}\rangle\}$ and $\mathrm{BMB}_2 = \{|+0\rangle, |-0\rangle, |+1\rangle, |-1\rangle\}$, respectively. The correlation property of the measurement results can be utilised to check eavesdropping.

If the $\boldsymbol{H}$ operation is performed on qubits 2 and 4, then Eq. (2) is transformed into

$$\begin{aligned}&(I_3 \otimes I_1 \otimes H_2 \otimes H_4)|\chi^{00}\rangle_{3214}\\ &= \frac{1}{2}(|\Phi_1^-\rangle|+0\rangle + |\Phi_1^+\rangle|+1\rangle + |\Psi_1^-\rangle|-0\rangle\\ &\quad +|\Psi_1^+\rangle|-1\rangle)_{3214}, \end{aligned} \tag{4}$$

and Eq. (3) into

$$\begin{aligned}&(I_3 \otimes I_1 \otimes H_2 \otimes H_4)|\chi^{00}\rangle_{3214}\\ &= \frac{1}{2}(|\Phi_2^+\rangle|0+\rangle - |\Psi_2^+\rangle|0-\rangle + |\Phi_2^-\rangle|1+\rangle\\ &\quad -|\Psi_2^-\rangle|1-\rangle)_{3214}. \end{aligned} \tag{5}$$

Here $H = (|0\rangle\langle 0| + |1\rangle\langle 0| + |0\rangle\langle 1| - |1\rangle\langle 1|)/\sqrt{2}$. The correlation measurement results of qubits (3, 1) and (2, 4) in the state $|\chi^{00}\rangle_{3214}$ in different bases after performing the $\boldsymbol{H}$ or $\boldsymbol{I}$ operation on qubits 2 and 4 are summarised in Table 1.

Table 1. The correlation measurement results of qubits (3, 1) and (2, 4) in the state $|\chi^{00}\rangle_{3214}$ in different bases after performing the $\boldsymbol{H}$ or $\boldsymbol{I}$ operation on qubits 2 and 4.

Eq. (2) $\mapsto \boldsymbol{I}$,	AMB_1, BMB_1	$\|\Phi_1^-\rangle\|0+\rangle, \|\Phi_1^+\rangle\|0-\rangle, \|\Psi_1^-\rangle\|1+\rangle, \|\Psi_1^+\rangle\|1-\rangle$
Eq. (3) $\mapsto \boldsymbol{I}$,	AMB_2, BMB_2	$\|\Phi_2^+\rangle\|+0\rangle, \|\Phi_2^-\rangle\|-0\rangle, \|\Psi_2^+\rangle\|+1\rangle, \|\Psi_2^-\rangle\|-1\rangle$
Eq. (4) $\mapsto \boldsymbol{H}$,	AMB_1, BMB_2	$\|\Phi_1^-\rangle\|+0\rangle, \|\Phi_1^+\rangle\|+1\rangle, \|\Psi_1^-\rangle\|-0\rangle, \|\Psi_1^+\rangle\|-1\rangle$
Eq. (5) $\mapsto \boldsymbol{H}$,	AMB_2, BMB_1	$\|\Phi_2^+\rangle\|0+\rangle, \|\Psi_2^+\rangle\|0-\rangle, \|\Phi_2^-\rangle\|1+\rangle, \|\Psi_2^-\rangle\|1-\rangle$

Equations (2)–(5) correspond to the first, second, third and fourth row in Table 1, respectively. And the first column represents the unitary operation performed on qubits (2, 4) by Bob. Accordingly, the second column and the third column denote the measuring bases and the correlation measurement results of qubits (3, 1) and (2, 4) in the state $|\chi^{00}\rangle_{3214}$ after performing the $\boldsymbol{H}$ or $\boldsymbol{I}$ operation on qubits 2 and 4, respectively.

Let us give an explicit description of the QSS-SDC protocol as follows:

(1) Alice and her agents, Bob and Charlie agree that each of the 16 mutually orthogonal χ-type entangled states represents four-bit classical information, i.e., $|\chi^{ij}\rangle_{3214}$ correspond to $'ij'(i, j = 0, 1, 2, 3)$.

(2) First, Alice prepares an ordered N four-qubit χ-type entangled state sequence $[(P_1^1, P_2^1, P_3^1, P_4^1), (P_1^2, P_2^2, P_3^2, P_4^2), \ldots, (P_1^N, P_2^N, P_3^N, P_4^N)]$ according to her secret message. Here, the subscripts 1, 2, 3, and 4 represent four different particles in one χ-type entangled state and the superscripts 1, 2, 3, ..., and n indicate the entangled quartet orders in the sequence. Then she prepares $i + k + j$ entangled particle quartets all in the state $|\chi^{00}\rangle_{3214}$ used for eavesdropping check. Alice randomly inserts each of the $i + k + j$ checking photon quartets one by one into the ordered N photon quartet sequence and records each position. We denote the ordered $N + i + k + j$ quartet sequence with $[(P_1^1, P_2^1, P_3^1, P_4^1), (P_1^2, P_2^2, P_3^2, P_4^2), \ldots, (P_1^{N+i+k+j}, P_2^{N+i+k+j}, P_3^{N+i+k+j}, P_4^{N+i+k+j})]$. Alice takes one particle from each entangled quartet to form four ordered particle sequences: $S_1 : [P_1^1, P_1^2, \ldots, P_1^{N+i+k+j}]$, $S_2 : [P_2^1, P_2^2, \ldots, P_2^{N+i+k+j}]$, $S_3 : [P_3^1, P_3^2, \ldots, P_3^{N+i+k+j}]$, $S_4 : [P_4^1, P_4^2, \ldots, P_4^{N+i+k+j}]$. She keeps particle sequences S_1 and S_3, and sends the particles in sequences S_2 and S_4 to Bob.

(3) Bob first inserts a filter in front of his devices to filter out the photon signals with an illegitimate wavelength to prevent the invisible photon eavesdropping (IPE) Trojan horse attack strategies.[63,64] Then he splits the photon signals with some photon number splitters (PNSs: 50/50) and measures the two signals after the PNS with the two measuring bases (MBs), Z-basis and X-basis, chosen randomly. If the multipho-

ton rate is unreasonably high, he terminates the transmission and repeats the communication from the beginning. After Bob receives the S_2 and S_4 sequences, Alice publicly announces the positions of i checking entanglement quartets. For each of these i checking entanglement quartets, Alice first lets Bob measure the corresponding checking photons in his lab by using the BMB_1 basis or the BMB_2 basis randomly and publish his measurement outcome. Then she measures the corresponding photons using the AMB_1 basis or the AMB_2 basis according to the first and second rows in Table 1. If the error rate exceeds the threshold, the process is aborted. Otherwise, for each two photons in the same positions in sequences S_2 and S_4 Bob generates three classical bits B_1, B_2, B_3, B_4, and B_5 randomly. According to the values of B_1, B_2, B_3 and B_4, he applies the operation $\sigma^{2B_1+B_2}$ and $\sigma^{2B_3+B_4}$ on the qubits 2 and 4, respectively. Then he encrypts the particles by performing the operation H^{B_5} respectively. At last, Bob sends the ordered S_2 and S_4 sequences to Charlie.

(4) Charlie first inserts a filter in front of his devices to filter out the photon signals with an illegitimate wavelength to prevent the IPE Trojan horse attack strategies.[63,64] Then he splits the photon signals with some PNSs and measures the two signals after the PNS with the two MBs Z-basis and X-basis chosen randomly. If the multiphoton rate is unreasonably high, he terminates the transmission and repeats the communication from the beginning. After confirming that Charlie has received the ordered S_2 and S_4 sequences, Alice publicly announces the positions of k checking entanglement quartets. For each of these k checking entanglement quartets, Alice first lets Charlie measure the corresponding checking photons in his lab by using the BMB_1 basis or the BMB_2 basis randomly and publish his measurement outcome. Then Alice lets Bob publish which unitary operation he has performed on the checking photons when they pass by him. If Bob's unitary operation is $\boldsymbol{H}$, then Alice measures the corresponding checking photons in her lab by using the corresponding basis according to the third and fourth rows in Table 1. Otherwise, she measures the photons using the corresponding basis according to the first and second rows in Table 1. If the error rate exceeds the threshold, the process is aborted. Otherwise, the process continues and Alice sends the retained $N+j$ ordered S_1' and S_3' (S_1' and S_3' denote the remainder photons in the S_1 and S_3 sequences except for eavesdropping check) sequences to Charlie.

(5) After Charlie receives the photons, if Bob and Charlie collaborate, both Bob and Charlie can obtain a raw secret message including Alice's secret message and additional $4j$ useless bits. The detailed procedure is as follows. For each photon quartet, if Bob's unitary operation is $\boldsymbol{I}$, then Bob and Charlie directly measure the particles in his site in the basis FMB. If Bob's unitary operation is $\boldsymbol{H}$, then they first perform a Hardamard operation on the S_2' and S_4' (S_2' and S_4' denote the remainder photons in the S_2 and S_4 sequences except for eavesdropping check) photons and then perform a measurement on the four-qubit quartet in the basis FMB. According to their measurement outcome they can deduce the four secret bits Alice imposed on this photon quartet. On the other hand, if Bob and Charlie do not collaborate, then neither of them can get access to Alice's secret message.

(6) Alice publicly announces the positions of the retained j checking quartets for Bob and Charlie to extract her exact secret message from the raw secret message and to check whether the $N+j$ S_1 and S_3' photons traveling from Alice site to Charlie's site have been attacked, which is called message authentication. Even if the photons are attacked, the eavesdropper Eve cannot get access to any useful information but interrupt the transmissions quantum channel between Alice and Charlie.

3. Security analysis

So far we have proposed the three-party QSS-SDC protocol based on χ-type entangled states. Now let us discuss its security proof. The proof of our protocol is based on the security for the transmission of the S_2 and S_4 sequences. As pointed out in Refs. [65]–[67], a participant generally has more advantages in an attack than an outside eavesdropper in QSS protocols. If a QSS protocol is secure for a dishonest participant, it is secure for any eavesdropper. So the participant attack is paid more attention to in the security analysis of a QSS protocol. For the transmission of the S_2 and S_4 sequences, there are two main means of eavesdropping. One is the intercept and resend attack and the other is that using an auxiliary particle to interact with the particles carrying messages and measuring the auxiliary photon to gain some useful information. Suppose the dishonest participant is Charlie*. For the first intercept and resend attack, because Alice's secret message is encoded into four-particle entangled

states and the quartets are transmitted by two steps, Charlie*'s intercept and measurements will result in no relation between the outcomes of qubits (3, 1) and those of qubits (2, 4), and would be found by using the checking procedure in step (3) based on the qubit correlation of each χ-type entangled state. To gain Alice's secret message without being detected, Charlie* will adopt a general attack strategy as follows. Charlie* prepares an ancilla E in the initial state $|\varepsilon\rangle$. When the qubits 2 and 4 are transmitted from Alice to Bob, Charlie* intercepts the travel particles, and makes the ancilla E interact unitarily with the qubits 2 and 4. Then, she sends these two qubits to Bob. When the encoding particles are transmitted to her, Charlie* makes a joint measurement on the encoding particles and the ancilla. In this way, she may gain information about the secret message. Later, it will be shown that Eve cannot achieve any information about the message in the condition that no errors are to occur.

In the eavesdropping process, Charlie* adds the ancilla E, and performs the unitary operation $\boldsymbol{U}$ on the particle 2, 4, and E. The most general operation Charlie* can do is able to be written as

$$\begin{aligned}
\boldsymbol{U}:|00,\varepsilon\rangle &\rightarrow |00,\varepsilon_{00}\rangle+|01,\varepsilon_{01}\rangle+|10,\varepsilon_{02}\rangle\\
&\quad+|11,\varepsilon_{03}\rangle,\\
|01,\varepsilon\rangle &\rightarrow |00,\varepsilon_{10}\rangle+|01,\varepsilon_{11}\rangle+|10,\varepsilon_{12}\rangle\\
&\quad+|11,\varepsilon_{13}\rangle,\\
|10,\varepsilon\rangle &\rightarrow |00,\varepsilon_{20}\rangle+|01,\varepsilon_{21}\rangle+|10,\varepsilon_{22}\rangle\\
&\quad+|11,\varepsilon_{23}\rangle,\\
|11,\varepsilon\rangle &\rightarrow |00,\varepsilon_{30}\rangle+|01,\varepsilon_{31}\rangle+|10,\varepsilon_{32}\rangle\\
&\quad+|11,\varepsilon_{33}\rangle, \qquad (6)
\end{aligned}$$

where $|\varepsilon_{ij}\rangle(i,j\in\{0,1,2,3\})$ are pure ancilla states uniquely determined by $\boldsymbol{U}$. After this unitary interaction, the whole quantum system is in the state

$$\begin{aligned}
&|\varphi\rangle\\
&=\frac{1}{2}[|\phi^+\rangle(|00,\varepsilon_{00}\rangle+|01,\varepsilon_{01}\rangle+|10,\varepsilon_{02}\rangle+|11,\varepsilon_{03}\rangle)\\
&\quad-|\psi^-\rangle(|00,\varepsilon_{10}\rangle+|01,\varepsilon_{11}\rangle+|10,\varepsilon_{12}\rangle+|11,\varepsilon_{13}\rangle)\\
&\quad+|\psi^+\rangle(|00,\varepsilon_{20}\rangle+|01,\varepsilon_{21}\rangle+|10,\varepsilon_{22}\rangle+|11,\varepsilon_{23}\rangle)\\
&\quad-|\phi^-\rangle(|00,\varepsilon_{30}\rangle+|01,\varepsilon_{31}\rangle+|10,\varepsilon_{32}\rangle\\
&\quad+|11,\varepsilon_{33}\rangle)]_{3214E}. \qquad (7)
\end{aligned}$$

Then, four cases will be discussed, in which Charlie* measures qubits 2 and 4 in different bases, and Bob performs on qubits 2 and 4 the identity operation or $\boldsymbol{H}$ operation.

(i) **Case 1** Bob performs the identity operation on qubits 2 and 4, separately, and Alice and Charlie* measures qubits (3, 1) and (2, 4) in the basis AMB_1 and BMB_1, respectively. Here, the state $|\varphi\rangle$ can be rewritten as follows:

$$\begin{aligned}
|\varphi\rangle &= \frac{1}{2}(|v_1\rangle|0+\rangle+|v_2\rangle|0-\rangle+|v_3\rangle|1+\rangle\\
&\quad+|v_4\rangle|1-\rangle)_{31E24}, \qquad (8)
\end{aligned}$$

where

$$\begin{aligned}
|v_1\rangle &= \frac{1}{\sqrt{2}}(|\phi^+\rangle|\varepsilon_{00}\rangle+|\phi^+\rangle|\varepsilon_{01}\rangle-|\psi^-\rangle|\varepsilon_{10}\rangle\\
&\quad-|\psi^-\rangle|\varepsilon_{11}\rangle+|\psi^+\rangle|\varepsilon_{20}\rangle+|\psi^+\rangle|\varepsilon_{21}\rangle\\
&\quad-|\phi^-\rangle|\varepsilon_{30}\rangle-|\phi^-\rangle|\varepsilon_{31}\rangle)_{31E},\\
|v_2\rangle &= \frac{1}{\sqrt{2}}(|\phi^+\rangle|\varepsilon_{00}\rangle-|\phi^+\rangle|\varepsilon_{01}\rangle-|\psi^-\rangle|\varepsilon_{10}\rangle\\
&\quad+|\psi^-\rangle|\varepsilon_{11}\rangle+|\psi^+\rangle|\varepsilon_{20}\rangle-|\psi^+\rangle|\varepsilon_{21}\rangle\\
&\quad-|\phi^-\rangle|\varepsilon_{30}\rangle+|\phi^-\rangle|\varepsilon_{31}\rangle)_{31E},\\
|v_3\rangle &= \frac{1}{\sqrt{2}}(|\phi^+\rangle|\varepsilon_{02}\rangle+|\phi^+\rangle|\varepsilon_{03}\rangle-|\psi^-\rangle|\varepsilon_{12}\rangle\\
&\quad-|\psi^-\rangle|\varepsilon_{13}\rangle+|\psi^+\rangle|\varepsilon_{22}\rangle+|\psi^+\rangle|\varepsilon_{23}\rangle\\
&\quad-|\phi^-\rangle|\varepsilon_{32}\rangle-|\phi^-\rangle|\varepsilon_{33}\rangle)_{31E},\\
|v_4\rangle &= \frac{1}{\sqrt{2}}(|\phi^+\rangle|\varepsilon_{02}\rangle-|\phi^+\rangle|\varepsilon_{03}\rangle-|\psi^-\rangle|\varepsilon_{12}\rangle\\
&\quad+|\psi^-\rangle|\varepsilon_{13}\rangle+|\psi^+\rangle|\varepsilon_{22}\rangle-|\psi^+\rangle|\varepsilon_{23}\rangle\\
&\quad-|\phi^-\rangle|\varepsilon_{32}\rangle+|\phi^-\rangle|\varepsilon_{33}\rangle)_{31E}\,. \qquad (9)
\end{aligned}$$

According to Eq. (2), the following conditions should be satisfied to avoid introducing error:

$$\begin{aligned}
&\langle\Phi_1^+|v_1\rangle=\langle\Psi_1^-|v_1\rangle=\langle\Psi_1^+|v_1\rangle=0,\\
&\langle\Phi_1^-|v_2\rangle=\langle\Psi_1^-|v_2\rangle=\langle\Psi_1^+|v_2\rangle=0,\\
&\langle\Phi_1^-|v_3\rangle=\langle\Phi_1^+|v_3\rangle=\langle\Psi_1^+|v_3\rangle=0,\\
&\langle\Phi_1^-|v_4\rangle=\langle\Phi_1^+|v_4\rangle=\langle\Psi_1^-|v_4\rangle=0. \qquad (10)
\end{aligned}$$

From Eqs.(9) and (10), we obtain

$$\begin{aligned}
&|\varepsilon_{00}\rangle=|\varepsilon_{11}\rangle,\quad |\varepsilon_{22}\rangle=|\varepsilon_{33}\rangle,\\
&|\varepsilon_{01}\rangle=|\varepsilon_{10}\rangle,\quad |\varepsilon_{23}\rangle=|\varepsilon_{32}\rangle,\\
&|\varepsilon_{20}\rangle=|\varepsilon_{21}\rangle=|\varepsilon_{30}\rangle=|\varepsilon_{31}\rangle=\boldsymbol{O},\\
&|\varepsilon_{02}\rangle=|\varepsilon_{03}\rangle=|\varepsilon_{12}\rangle=|\varepsilon_{13}\rangle=\boldsymbol{O}, \qquad (11)
\end{aligned}$$

where $\boldsymbol{O}$ denotes a zero vector.

(ii) **Case 2** Bob performs the identity operation on qubits 2 and 4, separately, and Alice and Charlie* measures qubits (3, 1) and (2, 4) in the basis AMB_2 and BMB_2, respectively.

According to Eq. (3) and the method used above, the following constraints can be deduced,

$$|\varepsilon_{00}\rangle=|\varepsilon_{22}\rangle,\quad |\varepsilon_{11}\rangle=|\varepsilon_{33}\rangle,$$

$$|\varepsilon_{02}\rangle = |\varepsilon_{20}\rangle, \quad |\varepsilon_{13}\rangle = |\varepsilon_{31}\rangle,$$
$$|\varepsilon_{10}\rangle = |\varepsilon_{12}\rangle = |\varepsilon_{30}\rangle = |\varepsilon_{32}\rangle = \boldsymbol{O},$$
$$|\varepsilon_{01}\rangle = |\varepsilon_{03}\rangle = |\varepsilon_{21}\rangle = |\varepsilon_{23}\rangle = \boldsymbol{O}. \quad (12)$$

(iii) **Case 3** Bob performs the identity operation on qubits 2 and 4, separately, and Alice and Charlie* measures qubits (3, 1) and (2, 4) in the basis AMB_1 and BMB_2, respectively.

According to Eq. (4) and the method used above, the following constraints can be deduced,

$$|\varepsilon_{00}\rangle = |\varepsilon_{02}\rangle, \quad |\varepsilon_{01}\rangle = |\varepsilon_{03}\rangle,$$
$$|\varepsilon_{32}\rangle = |\varepsilon_{30}\rangle, \quad |\varepsilon_{31}\rangle = |\varepsilon_{33}\rangle,$$
$$|\varepsilon_{00}\rangle + |\varepsilon_{02}\rangle = |\varepsilon_{10}\rangle + |\varepsilon_{12}\rangle,$$
$$|\varepsilon_{20}\rangle = |\varepsilon_{22}\rangle = |\varepsilon_{21}\rangle = |\varepsilon_{23}\rangle = \boldsymbol{O},$$
$$|\varepsilon_{01}\rangle = |\varepsilon_{03}\rangle = |\varepsilon_{11}\rangle = |\varepsilon_{13}\rangle = \boldsymbol{O}. \quad (13)$$

(iv) **Case 4** Bob performs the identity operation on qubits 2 and 4, Separately, and Alice and Charlie* measures qubits (3, 1) and (2, 4) in the basis AMB_2 and BMB_1, respectively.

According to Eq. (5) and the method used above, the following constraints can be deduced,

$$|\varepsilon_{00}\rangle = |\varepsilon_{01}\rangle, |\varepsilon_{02}\rangle = |\varepsilon_{03}\rangle, |\varepsilon_{32}\rangle = |\varepsilon_{33}\rangle,$$
$$|\varepsilon_{00}\rangle + |\varepsilon_{01}\rangle = |\varepsilon_{20}\rangle + |\varepsilon_{21}\rangle,$$
$$|\varepsilon_{11}\rangle + |\varepsilon_{30}\rangle = |\varepsilon_{10}\rangle + |\varepsilon_{31}\rangle,$$
$$|\varepsilon_{10}\rangle = |\varepsilon_{11}\rangle = |\varepsilon_{30}\rangle = |\varepsilon_{31}\rangle = \boldsymbol{O},$$
$$|\varepsilon_{12}\rangle = |\varepsilon_{13}\rangle = |\varepsilon_{02}\rangle = |\varepsilon_{03}\rangle$$
$$= |\varepsilon_{22}\rangle = |\varepsilon_{23}\rangle = \boldsymbol{O}. \quad (14)$$

As a result, from Eqs. (11)–(14), we find that the whole system is in the state

$$|\varphi\rangle = |\chi^{00}\rangle_{3214}|\varepsilon_{00}\rangle_E. \quad (15)$$

From the above equation, it is evident that $|\varphi\rangle$ is a product of a χ-type entangled state $|\chi^{00}\rangle_{3214}$ and the ancilla. This implies that it is impossible for Charlie* to pass the security test in step (iv) by entangling the ancilla with χ-type entangled state and measuring it without introducing any error. Once the security for the transmission of the S_2 and S_4 sequences is not ensured, Alice will abort the transmission of the S_3 and S_1 sequences, thereby no information will be leaked to the eavesdropper. Same as in the two-step protocol,[4] the transmission and the security check of the S_2 and S_4 sequences in our protocol is also very similar to the procedure in BBM92 QKD protocol,[68] where one qubit in an EPR pair is sent to a party and another is sent to another party. The difference is that the quantum information carriers are replaced by χ-type entangled states. Here the S_3 and S_1 sequences are retained securely in Alice's lab and Eve (or an insider) cannot get access to it at all before Alice's eavesdropping detection. Hence our protocol can stand against the participant attack in an ideal condition.

Now, let us consider a special case, in which Charlie* executes a participant attack that may not be the optimal one. In this case, Charlie* will obtain no information if he tries to take an invisible photon eavesdropping (IPE) Trojan horse attack[63,64] as Bob inserts a filter to filter out the photon signal with an illegitimate wavelength. If Charlie* tries to take a delay-photon Trojan horse attack,[64] the eavesdropping check in step (iii) can defeat the delay-photon Trojan horse attack by Bob. The delay-photon Trojan horse attack[64] is inserting a spy photon in a legitimate signal with a delay time, shorter than the time windows. Different from the IPE attack, the delay spy photon has the same wavelength as the legitimate photon. Therefore, the spy photon will carry the same information as the legitimate qubit

4. Discussion and summary

Compared with other QSS protocol, one distinct feature of our protocol is its high efficiency. According to Ref. [69], a natural definition of efficiency η is

$$\eta = \frac{b_s}{q_t + b_t}, \quad (16)$$

where b_s is the number of secret bits, q_t and b_t are the number of transmitted qubits and bits, respectively. Using Eq. (16), the efficiency of the most famous QSS protocol, HBB protocol, is 11.25%.[27] In the present protocol, to share four classical bits ($b_s = 4$), 4 qubits and 1 bit need to be transmitted. Thus, the efficiency of this protocol is $4/(4+1) = 80\%$. Obviously, the efficiency of the present protocol is far higher than that of HBB protocol.

In summary, based on χ-type entangled states and the idea of quantum data block transmission, we introduce a three-party QSS-SDC protocol based on χ-type entangled states $|\chi^{00}\rangle_{3214}$. Using some interesting entanglement properties of this state, the agent entirety can directly obtain the secret message from the message sender only if they collaborate together. In addition, this protocol is scalable since the number of participants can be arbitrarily high.

References

[1] Bennett C H and Brassard G 1984 *Proc. IEEE Int. Conf. Computers, Systems, and Signal Processing* (India: Bangalore) p175

[2] Beige A, Englert B G, Kurtsiefer C and Weinfurter H 2002 *Acta Phys. Pol.* A **101** 357

[3] Boström K and Felbinger T 2002 *Phys. Rev. Lett.* **89** 187902

[4] Deng F G, Long G L and Liu X S 2003 *Phys. Rev.* A **68** 042317

[5] Zhang Z J, Man Z X and Li Y 2004 *Phys. Lett.* A **333** 46

[6] Deng F G and Long G L 2004 *Phys. Rev.* A **69** 052319

[7] Nguyen B A 2004 *Phys. Lett.* A **328** 6

[8] Man Z X, Zhang Z J and Li Y 2005 *Chin. Phys. Lett.* **22** 18

[9] Lucamarini M and Mancini S 2005 *Phys. Rev. Lett.* **94** 140501

[10] Deng F G and Long G L 2006 *Commun. Theor. Phys.* **46** 443

[11] Wang J, Zhang Q and Tang C J 2006 *Phys. Lett.* A **358** 256

[12] Man Z X, Zhang Z J and Li Y 2005 *Chin. Phys. Lett.* **22** 22

[13] Zhu A D, Xia Y, Fan Q B and Zhang S 2006 *Phys. Rev.* A **73** 022338

[14] Xia Y, Fu C B, Zhang S, Hong S K, Yeon K H and Um C I 2006 *J. Korean Phys. Soc.* **48** 24

[15] Chen P, Deng F G and Long G L 2006 *Chin. Phys.* **15** 2228

[16] Chen P, Li Y S, Deng F G and Long G L 2007 *Commun.Theor. Phys.* **47** 49

[17] Wang C, Deng F G, Li Y S, Liu X S and Long G L 2005 *Phys. Rev.* A **71** 044305

[18] Li X H, Deng F G and Zhou H Y 2006 *Phys. Rev.* A **74** 054302

[19] Deng F G, Li X H, Li C Y, Zhou P and Zhou H Y 2006 *Phys. Lett.* A **359** 359

[20] Deng F G, Long G L and Zhou H Y 2005 *Phys. Lett.* A **340** 43

[21] Deng F G, Li X H, Li C Y, Zhou P and Zhou H Y 2006 *Phys. Lett.* A **354** 190

[22] Yang Y G and Wen Q Y 2007 *Sci. Chin.* G: *Phys. Mech. Astron.* **50** 558

[23] Yang Y G, Wen Q Y and Zhu F C 2007 *Chin. Phys.* **16** 1838

[24] Zhang Z J, Liu J, Wang D and Shi S 2007 *Phys. Rev.* A **75** 026301

[25] Zhang Z J 2005 *Phys. Lett.* A **342** 60

[26] Zhang Z J, Li Y and Man Z X 2005 *Phys. Lett.* A **341** 385

[27] Hillery M, Buzek V and Berthiaume A 1999 *Phys. Rev.* A **59** 1829

[28] Karlsson A, Koashi M and Imoto N 1999 *Phys. Rev.* A **59** 162

[29] Zhang Z J 2005 *Phys. Lett.* A **342** 60

[30] Zhang Z J and Man Z X 2005 *Phys. Rev.* A **72** 022303

[31] Zhang Z J, Li Y and Man Z X 2005 *Phys. Rev.* A **71** 044301

[32] Wang J, Zhang Q and Tang C J 2007 *Commun. Theor. Phys.* **47** 454

[33] Han L F, Liu Y M, Liu J and Zhang Z J 2008 *Opt. Commun.* **281** 2690

[34] Qin S J, Gao F, Wen Q Y and Zhu F C 2008 *Opt. Commun.* **281** 5472

[35] Wang T Y, Wen Q Y, Chen X B, Guo F Z and Zhu F C 2008 *Opt. Commun.* **281** 6130

[36] Li B K, Yang Y G and Wen Q Y 2009 *Chin. Phys. Lett.* **26** 010302

[37] Yang Y G and Wen Q Y 2008 *Sci. Chin.* G: *Phys. Mech. Astron.* **51** 1308

[38] Yang Y G and Wen Q Y 2008 *Chin. Phys.* B **17** 419

[39] Zhang Z J 2006 *Opt. Commun.* **261** 199

[40] Cleve R, Gottesman D and Lo H K 1999 *Phys. Rev. Lett.* **83** 648

[41] Bandyopadhyay S 2000 *Phys. Rev.* A **62** 012308

[42] Hsu L Y 2003 *Phys. Rev.* A **68** 022306

[43] Lance A M, Symul T, Bowen W P, Sanders B C and Lam P K 2004 *Phys. Rev. Lett.* **92** 177903

[44] Yang Y G and Wen Q Y 2009 *Int. J. Quantum Inform.* **7** 1249

[45] Deng F G, Zhou H Y and Long G L 2005 *Phys. Lett.* A **337** 329

[46] Deng F G, Li X H, Zhou H Y and Zhang Z J 2005 *Phys. Rev.* A **72** 044302

[47] Zhang Z J, Yang J, Man Z X and Li Y 2005 *Eur. Phys. J.* D **33** 133

[48] Lance A M, Symul T, Bowen W P, Sanders B C, Tyc T, Ralph T C and Lam P K 2005 *Phys. Rev.* A **71** 033814

[49] Li X H, Deng F G, Zhou H Y 2007 *Chin. Phys. Lett.* **24** 1151

[50] Yang J and Liu J 2008 *Commun. Theor. Phys.* **49** 338

[51] Zhou P, Li X H, Deng F G and Zhou H Y 2007 *J. Phys.* A*: Math.Theor.* **40** 13121

[52] Zhan Y B 2007 *Chin. Phys.* **16** 2557

[53] Ji H, Zhan X G and Zeng H S 2007 *Chin. Phys. Lett.* **24** 2724

[54] Li X H and Deng F G 2008 *Front. Comput. Sci. China* **2** 147

[55] Long G L and Liu X S 2002 *Phys. Rev.* A **65** 032302

[56] Yeo Y and Chua W K 2006 *Phys. Rev.Lett.* **96** 060502

[57] Wang X W and Yang G J 2008 *Phys. Rev.* A **78** 024301

[58] Greenberger D M, Horne M A, Shimony A and Zeilinger A 1990 *Am. J. Phys.* **58** 1131

[59] Dür W, Vidal G and Cirac J I 2000 *Phys. Rev.* A **62** 062314

[60] Briegel H J and Raussendorf R 2001 *Phys. Rev. Lett.* **86** 910

[61] Lin S, Wen Q Y, Gao F and Zhu F C 2008 *Phys. Rev.* A **78** 064304

[62] Xiu X M, Dong H K, Dong L, Gao Y J and Chi F 2009 *Opt. Commun.* **282** 2457

[63] Cai Q Y 2006 *Phys. Lett.* A **351** 23

[64] Li X H, Deng F G and Zhou H Y 2006 *Phys. Rev.* A **74** 054302

[65] Qin S J, Gao F, Wen Q Y and Zhu F C 2006 *Phys. Lett.* A **357** 101

[66] Deng F G, Li X H, Zhou H Y and Zhang Z J 2005 *Phys. Rev.* A **72** 044302.

[67] Gao F, Qin S J, Wen Q Y and Zhu F C 2007 *Quantum Inf. Comput.* **7** 329

[68] Bennett C H, Brassard G and Mermin N D 1992 *Phys. Rev. Lett.* **68** 557

[69] Cabello A 2000 *Phys. Rev. Lett.* **85** 5635