Int J Theor Phys (2013) 52:2099–2111
DOI 10.1007/s10773-013-1504-8

An Improved Multiparty Quantum Secret Sharing with Bell States and Bell Measurement

Wenhua Wang · Huaixin Cao

Received: 8 October 2012 / Accepted: 21 January 2013 / Published online: 31 January 2013

Abstract A multiparty quantum secret sharing with Bell states and Bell measurement has been proposed by Shi et al., but it is not secure for two dishonest agents. In this paper, an improved scheme is proposed in order to prevent this attack and its security is also analyzed.

Keywords Quantum secret sharing · Bell state · Quantum entanglement

1 Introduction

Secret sharing is one of the useful tools in the cryptographic application field, which was firstly introduced by Blakely [1] and Shamir [2], respectively. It is a method to transmit the information but not being lost, destroyed, modified or into wrong hand. The main idea of secret sharing is to divide a secret into many shares such that only enough shares collaborate together can recover the secret.

With the development of quantum information processing, people began to consider the quantum secrete sharing (QSS). In 1999, Hillery et al. [3] proposed an original QSS for sharing a private key with three-particle and four-particle entangled Greenberger-Horne-Zeilinger (GHZ)states. Since then, a lot of QSS protocols [4–9] have been proposed, and the cryptanalysis of QSS has also attracted much attention [10, 11].

Recently, Shi et al. [13] proposed a multiparty quantum secret sharing protocol with Bell states and Bell measurement. In their scheme, only the dealer need to prepare EPR pairs and the agents just need to perform Bell measurement respectively, without performing any unitary operation to obtain the secret. This is more convenient than sharing an arbitrary two-qubit state in practical application [12], since EPR pairs are easily generated than GHZ states.

W. Wang · H. Cao (✉)
College of Mathematics and Information Science, Shaanxi Normal University, Xi'an 710062, China
e-mail: caohx@snnu.edu.cn

W. Wang
e-mail: wenhua@stu.snnu.edu.cn

Unfortunately, Wang et al. [14, 15] pointed out that this QSS scheme was not secure if there are two dishonest agents. Since the EPR pairs are entangled, and there must exist two agents who possess the particles which are entangled with the particles in the dealer's hand, and can collude to steal the dealer's secret without the help of the other agents. For example, suppose the four parties are Alice, Bob_1, Bob_2, Bob_3, where Alice is the sender and Bob_i $(i = 1, 2, 3)$ are the three agents. Alice shares 4 EPR pairs $|\phi^+\rangle_{12} \otimes |\phi^+\rangle_{34} \otimes |\phi^+\rangle_{56} \otimes |\phi^+\rangle_{78}$ with three agents. Assume that Alice holds two particles 1 and 8, and sends the two particles 2 and 3, 4 and 5, 6 and 7 to Bob_i $(i = 1, 2, 3)$, respectively. Since

$$\begin{aligned}|\phi^+\rangle_{34} \otimes |\phi^+\rangle_{56} =& \frac{1}{2}\big(|\phi^+\rangle_{36} \otimes |\phi^+\rangle_{45} + |\phi^-\rangle_{36} \otimes |\phi^-\rangle_{45} \\ &+ |\Psi^+\rangle_{36} \otimes |\Psi^+\rangle_{45} + |\Psi^-\rangle_{36} \otimes |\Psi^-\rangle_{45}\big)\end{aligned}$$

and

$$\begin{aligned}|\phi^+\rangle_{12} \otimes |\phi^+\rangle_{78} =& \frac{1}{2}\big(|\phi^+\rangle_{18} \otimes |\phi^+\rangle_{27} + |\phi^-\rangle_{18} \otimes |\phi^-\rangle_{27} \\ &+ |\Psi^+\rangle_{18} \otimes |\Psi^+\rangle_{27} + |\Psi^-\rangle_{18} \otimes |\Psi^-\rangle_{27}\big)\end{aligned}$$

so, we can get that Bob_1 can infer Bob_2's measurement outcome according to the correlation between the qubits 3, 6 and 4, 5, and Bob_3 can easily infer Alice's measurement outcome according to the correlation between the qubits 1, 8, and 2, 7. Accordingly, Bob_1 and Bob_3 can infer Alice's key if they cooperate. if Bob_1 and Bob_3 are dishonest, It is evident that this attack doesn't introduces any error since it happens after Alice's eavesdropping check. Therefore, Bob_1 and Bob_3 can collaborate to infer Alice's key without being detected in this four-party protocol and the scheme is not secure. At the same time, L. Joson [16] presented an enhancement of that scheme, which based on the idea that all agents possess two photons to share two classical bits, and an inside attack is prevented.

In this paper, we propose an another scheme to avoid that attack, and even there is only one dishonest agent, the probability of not being detected is less than Shi et al.'s protocol. Besides, after the communication, the particles owned by all parties are still entangled, thus they can be reused.

2 Theoretical Foundation of Multiparty Quantum Secret Sharing with Bell States

Before describing our scheme, we give a brief review about four Bell states and Pauli matrices.

Four Bell states are defined as follows:

$$\begin{aligned}|\phi^+\rangle &= \frac{1}{\sqrt{2}}\big(|00\rangle + |11\rangle\big), \qquad |\phi^-\rangle = \frac{1}{\sqrt{2}}\big(|00\rangle - |11\rangle\big), \\ |\psi^+\rangle &= \frac{1}{\sqrt{2}}\big(|01\rangle + |10\rangle\big), \qquad |\psi^-\rangle = \frac{1}{\sqrt{2}}\big(|01\rangle - |10\rangle\big),\end{aligned}$$

then $\{|\phi^+\rangle, |\phi^-\rangle, |\psi^+\rangle, |\psi^-\rangle\}$ forms an orthonormal basis for $\mathbb{C}^4$.

Four Pauli matrices are defined as follows:

$$\begin{aligned}I &= \begin{pmatrix}1 & 0\\ 0 & 1\end{pmatrix}, \qquad X = \begin{pmatrix}0 & 1\\ 1 & 0\end{pmatrix}, \\ Y &= \begin{pmatrix}0 & -i\\ i & 0\end{pmatrix}, \qquad Z = \begin{pmatrix}1 & 0\\ 0 & -1\end{pmatrix},\end{aligned}$$

which are the Hermitian unitary matrix, and $\{I, X, Y, Z\}$ is an orthonormal basis for M^2.

In this part, we introduce the relationship of all participants' measure results. We consider four-party QSS Scheme. Suppose they are Alice, Bob_1, Bob_2, Bob_3, where Alice is the sender and Bob_i $(i = 1, 2, 3)$ are the agents. Alice shares 4 EPR pairs $|\phi^+\rangle_{12} \otimes |\phi^+\rangle_{34} \otimes |\phi^+\rangle_{56} \otimes |\phi^+\rangle_{78}$ with three agents. Assume that Alice holds two particles 1 and 8, and sends the two particles 2 and 3, 4 and 5, 6 and 7 to Bob_i $(i = 1, 2, 3)$, respectively.

Firstly, we described the relationship of primary scheme [13] in mathematics as follows:

Theorem 2.1 *Define* $A : \mathbb{C}^6 \to \mathbb{C}^6$ *and* $B : \mathbb{C}^4 \to \mathbb{C}^4$ *by*

$$A(x_1, x_2, x_3, x_4, x_5, x_6) = (x_1, x_6, x_2, x_3, x_4, x_5), \quad \forall (x_1, x_2, x_3, x_4, x_5, x_6) \in C^6,$$
$$B\big|\phi^+\big\rangle = |00\rangle, \qquad B\big|\phi^-\big\rangle = |01\rangle, \qquad B\big|\psi^+\big\rangle = |10\rangle, \qquad B\big|\psi^-\big\rangle = |11\rangle.$$

Then A and B are unitary operators such that

$$(B \otimes B \otimes B)A\big(\big|\phi^+\big\rangle_{12} \otimes \big|\phi^+\big\rangle_{34} \otimes \big|\phi^+\big\rangle_{56}\big) = \sum_{k=1}^{16} \varepsilon_i \big(|a_k\rangle|b_k\rangle|c_k\rangle\big),$$

and $|a_k\rangle = |b_k\rangle \oplus |c_k\rangle \pmod 2$, *where* $\varepsilon_i \in \{-1, 1\}$, $|a_k\rangle, |b_k\rangle, |c_k\rangle \in \{|00\rangle, |01\rangle, |10\rangle, |11\rangle\}$ $(k = 1, 2, \ldots, 16)$.

Therefore, the sender's information can be uniquely deduced by all agents without any announcement. In this paper, we add an operator perform in the scheme, and the possible relationships of their measurement results can be show in the following:

Theorem 2.2 *Define* $A : \mathbb{C}^8 \to \mathbb{C}^8$ *and* $B : \mathbb{C}^4 \to \mathbb{C}^4$ *by*

$$A(x_1, x_2, x_3, x_4, x_5, x_6, x_7, x_8) = (x_1, x_8, x_2, x_3, x_4, x_5, x_6, x_7),$$
$$B\big|\phi^+\big\rangle = |00\rangle, \qquad B\big|\phi^-\big\rangle = |01\rangle, \qquad B\big|\psi^+\big\rangle = |10\rangle, \qquad B\big|\psi^-\big\rangle = |11\rangle.$$

Then A and B are unitary operators. Moreover, put

$$|\Psi\rangle := \big|\phi^+\big\rangle_{12} \otimes \big|\phi^+\big\rangle_{34} \otimes \big|\phi^+\big\rangle_{56} \otimes \big|\phi^+\big\rangle_{78}.$$

Then for every $T \in \{I, X, iY, Z\}$ (I, X, Y, Z *are Pauli matrices*), *we have*

$$B^{\otimes^4}\big(I^{\otimes^2} T^{\otimes^2} I^{\otimes^4}\big) A|\Psi\rangle = \sum_{i=1}^{64} \varepsilon_i |e_i\rangle_{18} |f_i\rangle_{23} |g_i\rangle_{45} |h_i\rangle_{67}, \tag{1}$$

where $\varepsilon_i \in \{-1, 1\}$, $|e_i\rangle_{18}, |f_i\rangle_{23}, |g_i\rangle_{45}, |h_i\rangle_{67} \in \{|00\rangle, |01\rangle, |10\rangle, |11\rangle\}$, *which satisfies*

$$|e_i\rangle_{18} = |f_i\rangle_{23} \oplus |g_i\rangle_{45} \oplus |h_i\rangle_{67} \quad (1 \le i \le 64).$$

(The proof is presented in the Appendix.)

3 Review of Shi et al.'s Multiparty QSS Protocol

In this section, we give a brief review of Shi et al.'s protocol [13]. A four-party QSS scheme in detail is described as follows (see also Figs. 1, 2, 3, 4):

(1) Alice prepares $4N$ EPR pairs, which are divided into N groups, and each group has three EPR pairs in the same Bell states $|\phi^+\rangle$ (i.e. $|\phi^-\rangle$, $|\psi^+\rangle$, $|\psi^-\rangle$). Moreover, Alice further divides these EPR particles into eight sequences:

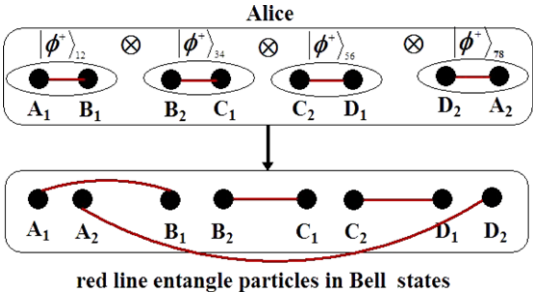

Fig. 1 Alice prepares 4N EPR pairs $|\phi^+\rangle$, and performs entanglement swapping

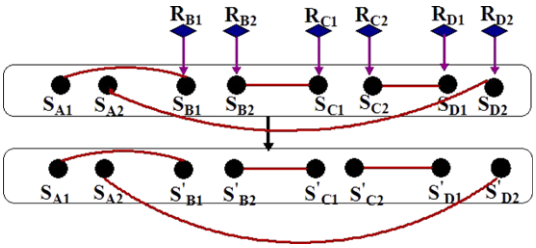

Fig. 2 Alice prepares six checking sets of sample particles randomly, and inserts them into $S_{B_1}, S_{B_2}, S_{C_1}, S_{C_2}, S_{D_1}, S_{D_2}$ in random position, respectively

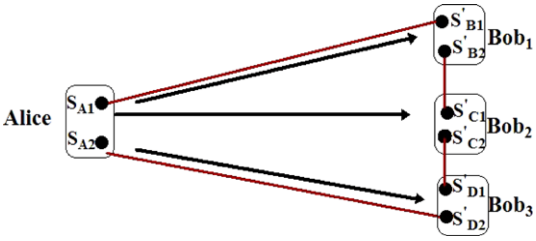

Fig. 3 Alice holds S_{A_1}, S_{A_2}, and sends $S_{B_1'}, S_{B_2'}, S_{C_1'}, S_{C_2'}, S_{D_1'}, S_{D_2'}$ to Bob_i $(i = 1, 2, 3)$, respectively

$$\begin{aligned}
&\big[P_1(A_1), P_2(A_1), \ldots, P_N(A_1)\big], \quad \big[P_1(A_2), P_2(A_2), \ldots, P_N(A_2)\big],\\
&\big[P_1(B_1), P_2(B_1), \ldots, P_N(B_1)\big], \quad \big[P_1(B_2), P_2(B_2), \ldots, P_N(B_2)\big],\\
&\big[P_1(C_1), P_2(C_1), \ldots, P_N(C_1)\big], \quad \big[P_1(C_2), P_2(C_2), \ldots, P_N(C_2)\big],\\
&\big[P_1(D_1), P_2(D_1), \ldots, P_N(D_1)\big], \quad \big[P_1(D_2), P_2(D_2), \ldots, P_N(D_2)\big],
\end{aligned}$$

which are denoted as $S_{A_1}, S_{A_2}, S_{B_1}, S_{B_2}, S_{C_1}, S_{C_2}, S_{D_1}$ and S_{D_2}, respectively.

(2) Alice prepares six checking sets $R_{B_1}, R_{B_2}, R_{C_1}, R_{C_2}, R_{D_1}$ and R_{D_2} of sample particles randomly from $\{|0\rangle, |1\rangle, |+\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle), |-\rangle = \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)\}$. Then Alice inserts these samples randomly into $S_{B_1}, S_{B_2}, S_{C_1}, S_{C_2}, S_{D_1}, S_{D_1}$ in random position, respectively. The new sequences are denoted as $S_{B_1'}, S_{B_2'}, S_{C_1'}, S_{C_2'}, S_{D_1'}, S_{D_2'}$, respectively.

(3) Alice sends $S_{B_1'}, S_{B_2'}, S_{C_1'}, S_{C_2'}, S_{D_1'}, S_{D_2'}$ to Bob_i $(i = 1, 2, 3)$, and retains the remaining sequences S_{A_1}, S_{A_2}.

(4) After confirming that Bob_i $(i = 1, 2, 3)$ have received the two sequences. Alice announces the positions and the measurement bases of sample particles $S_{B_1'}, S_{B_2'}$ to Bob_1, $S_{C_1'}$, $S_{C_2'}$ to Bob_2, and $S_{D_1'}, S_{D_2'}$ to Bob_3. Bob_i $(i = 1, 2, 3)$ measure the corresponding checking sets and tell Alice their measurement results, respectively. Alice analyzes the security of the transmissions. If the error rate is hight than the threshold determined by the channel noise, Alice terminates this scheme and restarts, or else they continue to the next step.

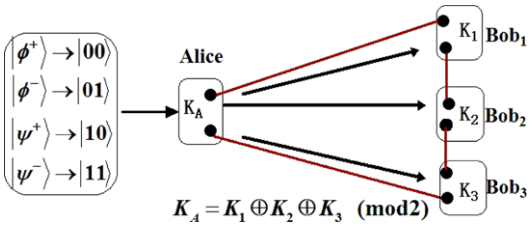

Fig. 4 Each measurement result defines the classical information, and they have the relationship

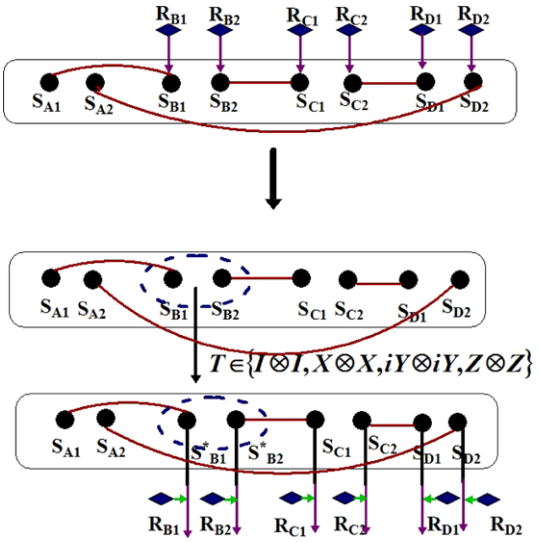

Fig. 5 Before the second step, we add a unitary transformation T

(5) Alice, Bob$_1$, Bob$_2$ and Bob$_3$ measure the jth ($j = 1, 2, \ldots, N$) two-particle pair ($P_j(A_1)$, $P_j(A_2)$), ($P_j(B_1)$, $P_j(B_2)$), ($P_j(C_1)$, $P_j(C_2)$), and ($P_j(D_1)$, $P_j(D_2)$) respectively. There are four kinds of measurement result in Bell states. Each measurement result defines the two bits of classical information: "00" if the result is $|\phi^+\rangle$, "01" if it is $|\phi^-\rangle$, "10" if it is $|\psi^+\rangle$, "11" if it is $|\psi^-\rangle$. Then Alice, Bob$_1$ Bob$_2$ and Bob$_3$ can transform their measured result sequences to classical bits strings K_A, K_1, K_2 and K_3, where K_A is the key of Alice, and K_i is the shared key of Bob$_i$ ($i = 1, 2, 3,$), respectively. Then Bob$_i$ ($i = 1, 2, 3$) can collaborate to infer Alice's key, since K_A, K_1, K_2 and K_3 satisfy the relationship: $K_A = K_1 \oplus K_2 \oplus K_3$ (mod 2).

4 An Improved Multiparty Quantum Secret Sharing with Bell States and Bell Measurement

Now, we give the detail steps of our QSS scheme with Four-party in the following (see also Fig. 5):

(1) Alice prepares $4N$ EPR pairs $|\phi^+\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$, which are divided into N groups, and each group has four EPR pairs: $|\phi^+\rangle_{12}$, $|\phi^+\rangle_{34}$, $|\phi^+\rangle_{56}$, $|\phi^+\rangle_{78}$. Then she divides these particles into eight sequences:

$$S_1 = \{P_1(1), P_2(1), \ldots, P_N(1)\}, \qquad S_2 = \{P_1(2), P_2(2), \ldots, P_N(2)\},$$

$$S_3 = \{P_1(3), P_2(3), \ldots, P_N(3)\}, \qquad S_4 = \{P_1(4), P_2(4), \ldots, P_N(4)\},$$
$$S_5 = \{P_1(5), P_2(5), \ldots, P_N(5)\}, \qquad S_6 = \{P_1(6), P_2(6), \ldots, P_N(6)\},$$
$$S_7 = \{P_1(7), P_2(7), \ldots, P_N(7)\}, \qquad S_8 = \{P_1(8), P_2(8), \ldots, P_N(8)\}.$$

where $P_j(1) = P_j(2) = (a_1, a_2, \ldots, a_{16}), a_1 = a_2 = a_3 = a_4 = a_5 = a_6 = a_7 = a_8 = |0\rangle$, others are $|1\rangle$, $P_j(3) = P_j(4) = (b_1, b_2, \ldots, b_{16}), b_1 = b_2 = b_3 = b_4 = b_9 = b_{10} = b_{11} = b_{12} = |0\rangle$, others are $|1\rangle$, $P_j(5) = P_j(6) = (c_1, c_2, \ldots, c_{16}), c_1 = c_2 = c_5 = c_6 = c_9 = c_{10} = c_{13} = c_{14} = |0\rangle$, others are $|1\rangle$, $P_j(7) = P_j(8) = (d_1, d_2, \ldots, d_{16}), d_1 = d_3 = d_5 = d_7 = d_9 = d_{11} = d_{13} = d_{15} = |0\rangle$, others are $|1\rangle$, $(j = 1, 2, \ldots, N)$.

(2) Alice chooses an operator T from $\{I, X, Z, iY, \}$ randomly, and transforms $P_j(2) \otimes P_j(3)$ to $P_j(2^*) \otimes P_j(3^*)$ $(j = 1, 2, \ldots, N)$, where, $P_j(2^*) \otimes P_j(3^*) = (T \otimes T)(P_j(2) \otimes P_j(3))$ $(j = 1, 2, \ldots, N)$. Then S_2 and S_3 are transformed into S_2^* and S_3^*, while the others are unchanged.

(3) Alice prepares six sets of particles as well which are sufficient for statistical analysis of eavesdropping as the sample sets and stems randomly from $\{|0\rangle, |1\rangle, |+\rangle, |-\rangle\}$. Then Alice inserts these samples randomly into $S_2^*, S_3^*, S_4, S_5, S_6, S_7$, respectively, each sample particle is distributed in a random position. The new sequences are denoted as $S_2^{\clubsuit}, S_3^{\clubsuit}, S_4^{\clubsuit}, S_5^{\clubsuit}, S_6^{\clubsuit}, S_7^{\clubsuit}$, and Alice makes a record of the insertion positions.

(4) Alice sends $S_2^{\clubsuit}, S_3^{\clubsuit}$ to Bob_1, $S_4^{\clubsuit}, S_5^{\clubsuit}$ to Bob_2,$S_6^{\clubsuit}, S_7^{\clubsuit}$ to Bob_3, and retains the remaining sequences S_1, S_8, Alice has to confirm that each agent has actually received two sequences via classical communication.

(5) After being notified when Bob_i $(i = 1, 2, 3)$ has received the two sequences, respectively. Alice announces the positions of the sample particles. Bob_i $(i = 1, 2, 3)$ choosing measurement basis $\{|0\rangle, |1\rangle\}$ or $\{|+\rangle, |-\rangle\}$ randomly, measure the sample particles according to Alice's announcement and tell Alice measurement basis and measurement results, respectively. Alice compares the measurement results of the agents with the initial states of the particles in the samples sets and analyzes the security of the transmissions. If the error rate is hight than the threshold determined by the channel noise, Alice terminates this scheme and restarts, or else they continue to the next step.

(6) Alice, Bob_1, Bob_2 and Bob_3 measure the jth $(j = 1, 2, \ldots, N)$ two-particle pair $(P_j(1) \otimes P_j(8))$, $(P_j(2) \otimes P_j(3))$, $(P_j(4) \otimes P_j(5))$, and $(P_j(6) \otimes P_j(7))$, respectively. Each measurement result defines the two bits of classical information: "00" if the result is $|\phi^+\rangle$, "01" if it is $|\phi^-\rangle$, "10" if it is $|\psi^+\rangle$, "11" if it is $|\psi^-\rangle$. Then Alice, Bob_1, Bob_2, Bob_3 can transform their measured result sequences to classical bits strings K_A, K_1, K_2, K_3 where K_A is the key of Alice, and K_i is the shared key of Bob_i $(i = 1, 2, 3)$, respectively. Then Bob_i $(i = 1, 2, 3)$ can collaborate to infer Alice's key, since K_A, K_1, K_2 and K_3 satisfy the relationship: $K_A = K_1 \oplus K_2 \oplus K_3 \pmod 2$.

Remark In step (2), if Alice chooses the operator T to perform $P_j(6) \otimes P_j(7)$ $(j = 1, 2, \ldots, N)$, this is considered the same. That is, as long as Alice perform a agent's two-particles which have one entangled with the sender's, the scheme is believed the same.

In the following, we generalize this four-party QSS scheme into n-party case. Suppose they are Alice, Bob_1, Bob_2, $\text{Bob}_3, \ldots, \text{Bob}_{n-1}$, Alice is the sender and Bob_i, $(i = 1, 2, \ldots, n-1)$ are agents. The multiparty QSS can be described as following:

(1) Alice prepares nN EPR pairs $|\phi^+\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$, which are divided into N groups, and each group has n EPR parties: $|\phi^+\rangle_{12}, |\phi^+\rangle_{34}, \ldots, |\phi^+\rangle_{2n-1,2n}$. Then she divided these particles into $2n$ sequences:

$$S_1 = \{P_1(1), P_2(1), \ldots, P_N(1)\}, \qquad S_2 = \{P_1(2), P_2(2), \ldots, P_N(2)\},$$
$$S_3 = \{P_1(3), P_2(3), \ldots, P_N(3)\}, \qquad S_4 = \{P_1(4), P_2(4), \ldots, P_N(4)\},$$
$$\vdots$$
$$S_{2n-1} = \{P_1(2n-1), P_2(2n-1), \ldots, P_N(2n-1)\},$$
$$S_{2n} = \{P_1(2n), P_2(2n), \ldots, P_N(2n)\}.$$

(2) Alice chooses operator from $\{I \otimes I, X \otimes X, Z \otimes Z, iY \otimes iY, \}$ randomly,and transform $P_j(2) \otimes P_j(3)$ to $P_j(2^*) \otimes P_j(3^*)$ $(j = 1, 2, \ldots, N)$, then S_2 and S_3 are transmitted into S_2^* and S_3^*, while the rest unchanged.

(3) Alice prepares $2n-2$ sets of particles which are sufficient for statistical analysis of eavesdropping as the sample sets and selected randomly from $\{|0\rangle, |1\rangle, |+\rangle, |-\rangle\}$. Then Alice inserts these samples randomly into $S_2^*, S_3^*, S_4, \ldots, S_{2n-2}, S_{2n-1}$, respectively, each sample particle is distributed in a random position. The new sequences are denoted as $S_2^{\clubsuit}$, $S_3^{\clubsuit}, \ldots, S_{2n-2}^{\clubsuit}, S_{2n-1}^{\clubsuit}$, and Alice makes a record of the insertion positions and the measurement basis of the sample particles.

(4) Alice sends $S_2^{\clubsuit}, S_3^{\clubsuit}$ to Bob_1, $S_4^{\clubsuit}, S_5^{\clubsuit}$ to $\text{Bob}_2, \ldots, S_{2n-2}^{\clubsuit}, S_{2n-1}^{\clubsuit}$ to Bob_{n-1}, and retains the remaining sequences S_1, S_{2n}, Alice has to confirm that each agent has actually received two sequences via classical communication.

(5) Alice being notified that Bob_i $(i = 1, 2, \ldots, n-1)$ has received the two sequences respectively announces the positions of the sample particles. Bob_i $(i = 1, 2, 3)$ choosing measurement basis $\{|0\rangle, |1\rangle\}$ or $\{|+\rangle, |-\rangle\}$ randomly, measure the sample particles according to Alice's announcement and tell Alice measurement basis and measurement results, respectively. Alice compares the measurement results of the agents with the initial states of the particles in the samples sets and analyzes the security of the transmissions. If the error rate is hight than the threshold determined by the channel noise, Alice terminates this scheme and restarts, or else they continue to the next step.

(6) Alice, $\text{Bob}_1, \text{Bob}_2, \ldots, \text{Bob}_{n-1}$ measure the jth $(j = 1, 2 \ldots, N)$ two-particle pair $(P_j(1) \otimes P_j(2n)), (P_j(2) \otimes P_j(3)), \ldots, (P_j(2n-2) \otimes P_j(2n-1))$ with Bell basis, respectively. Each measurement result with Bell basis defines the two bits of classical information: "00" if the result is $|\phi^+\rangle$, "01" if it is $|\phi^-\rangle$, "10" if it is $|\psi^+\rangle$, "11" if it is $|\psi^-\rangle$. Then Alice, $\text{Bob}_1, \text{Bob}_2, \ldots, \text{Bob}_{n-1}$ can transform their measurement result sequences to classical bits strings $K_A, K_1, K_2, \ldots, K_{n-1}$ where K_A is the key of Alice, and K_i is the shared key of Bob_i $(i = 1, 2, \ldots, n-1)$, respectively. Then Bob_i $(i = 1, 2, \ldots, n-1)$ can collaborate to infer Alice's key, since $K_A, K_1, K_2, \ldots, K_{n-1}$ satisfy the relationship: $K_A = K_1 \oplus K_2 \oplus \cdots \oplus K_{n-1} \pmod 2$.

5 Security Analysis

Now we begin to analyze the security of the present scheme. We take the four-party QSS scheme for the case. As mentioned in [12, 13], a dishonest agent has more power to attack than an outside eavesdropper, since he knows partial information legally and tells a lie in the detected proceeding to avoid introducing errors, so our main goal is to prevent the dishonest agents in QSS protocol from finding the secret without other agents. In other word, if all dishonest agents fail to cheat in a QSS scheme, then the scheme is said to be secure.

Suppose there are dishonest agents and they can intercept the particle sequences transmitted from Alice to other agents and resend the fake sequences prepared by themselves

to the other agents. Thus they can get the initial particles S_i $(i = 2, 3, \ldots, 7)$, after Alice announcing the positions of sample particles, then they can get the information of Alice. But in step (3), Alice inserts randomly some samples in the transmitted sequences, requires the agents to measure them later and checks their measurement results. In fact, the dishonest agents don't know the sample particles and their positions in the transmitted sequences. therefore whatever fake sequences prepared by dishonest agents, they all bring the error, since each sample particle is randomly selected in four states $\{|0\rangle, |1\rangle, |+\rangle, |-\rangle\}$. Besides in step (5), each agent selects measurement basis randomly to measure the sample sets, so the successful probability is less than $(\frac{1}{4} \times \frac{1}{2})^m$, where m is the number of the sample particles in each sequences transmitted to other agent. That is less than the Shi et al.'s QSS protocol.

Furthermore, we analyze the two dishonest agents:

If Bob_1 and Bob_2 are dishonest or Bob_3 and Bob_2 are dishonest. Since Bob_2 received the particles 4 and 5, they have no relation with Alice's particles 1 and 8. So the two agents collusion attack get no information about Alice's ,thus the scheme is secure.

If Bob_1 and Bob_3 are dishonest. As the particle 2 owned by Bob_1 and the particle 7 owned by Bob_3 are entangled with the particles 1 and 8 of Alice's.

In the step (2), Alice performed the particle 2 in $P_i(2)$ $(i = 1, 2, \ldots, N)$ by operator from $\{I, X, iY, Z\}$, randomly.

(i) When I was selected, for $1 \leq j \leq$ N:

$$\begin{aligned}\big((I \otimes I)|\phi^+\rangle_{12}\big) \otimes |\phi^+\rangle_{78} = \frac{1}{2}\big(&|\phi^+\rangle_{18}|\phi^+\rangle_{27} + |\phi^-\rangle_{18}|\phi^-\rangle_{27} \\ &+ |\psi^+\rangle_{18}|\psi^+\rangle_{27} + |\psi^-\rangle_{18}|\psi^-\rangle_{27}\big).\end{aligned}$$

(ii) When X was selected, for $1 \leq j \leq$ N:

$$\begin{aligned}\big((I \otimes X)|\phi^+\rangle_{12}\big) \otimes |\phi^+\rangle_{78} = \frac{1}{2}\big(&|\phi^+\rangle_{18}|\psi^+\rangle_{27} - |\phi^-\rangle_{18}|\psi^-\rangle_{27} \\ &+ |\psi^+\rangle_{18}|\phi^+\rangle_{27} - |\psi^-\rangle_{18}|\phi^-\rangle_{27}\big).\end{aligned}$$

(iii) When iY was selected, for $1 \leq j \leq$ N:

$$\begin{aligned}\big((I \otimes iY)|\phi^+\rangle_{12}\big) \otimes |\phi^+\rangle_{78} = \frac{1}{2}\big(&|\phi^+\rangle_{18}|\psi^-\rangle_{27} - |\phi^-\rangle_{18}|\psi^+\rangle_{27} \\ &+ |\psi^+\rangle_{18}|\phi^-\rangle_{27} - |\psi^-\rangle_{18}|\phi^+\rangle_{27}\big).\end{aligned}$$

(iv) When Z was selected, for $1 \leq j \leq$ N:

$$\begin{aligned}\big((I \otimes Z)|\phi^+\rangle_{12}\big) \otimes |\phi^+\rangle_{78} = \frac{1}{2}\big(&|\phi^+\rangle_{18}|\phi^-\rangle_{27} + |\phi^-\rangle_{18}|\phi^+\rangle_{27} \\ &+ |\psi^+\rangle_{18}|\psi^-\rangle_{27} + |\psi^-\rangle_{18}|\psi^+\rangle_{27}\big).\end{aligned}$$

Since the operator is randomly in one of four operators $\{I, X, iY, Z\}$, the probability of right information deduced by Bob_1 and Bob_3 is $(\frac{1}{4})^N$. where N is the number of groups in the first step, therefore, the present scheme is secure for two dishonest agents.

6 Conclusion

To summarize, we present a multiparty QSS scheme suing entanglement swapping theory and we analyze its security. In this scheme, all agents are not required to prepared entangled states or perform any unitary operation, and the sender check the security only need the agents' measure results. After the communication, all participants' particles are entangled and they can be reused.

Acknowledgements This work was supported by the NNSFs of China (Nos. 10871224, 11171197).

Appendix: The Proof of Theorem 2.2

Proof Since $|\Psi\rangle := |\phi^+|\rangle_{12} \otimes \phi^+\rangle_{34} \otimes |\phi^+\rangle_{56} \otimes |\phi^+\rangle_{78}$, and

$$
\begin{aligned}
&A|\Psi\rangle \\
&= \frac{1}{4}\big(|00\rangle_{18}|00\rangle_{23}|00\rangle_{45}|00\rangle_{67} + |01\rangle_{18}|00\rangle_{23}|00\rangle_{45}|01\rangle_{67} + |00\rangle_{18}|00\rangle_{23}|01\rangle_{45}|10\rangle_{67} \\
&\quad + |01\rangle_{18}|00\rangle_{23}|01\rangle_{45}|11\rangle_{67} + |00\rangle_{18}|01\rangle_{23}|10\rangle_{45}|00\rangle_{67} + |01\rangle_{18}|01\rangle_{23}|10\rangle_{45}|01\rangle_{67} \\
&\quad + |00\rangle_{18}|01\rangle_{23}|11\rangle_{45}|10\rangle_{67} + |01\rangle_{18}|01\rangle_{23}|11\rangle_{45}|11\rangle_{67} + |10\rangle_{18}|10\rangle_{23}|00\rangle_{45}|00\rangle_{67} \\
&\quad + |11\rangle_{18}|10\rangle_{23}|00\rangle_{45}|01\rangle_{67} + |10\rangle_{18}|10\rangle_{23}|01\rangle_{45}|10\rangle_{67} + |11\rangle_{18}|10\rangle_{23}|01\rangle_{45}|11\rangle_{67} \\
&\quad + |10\rangle_{18}|11\rangle_{23}|10\rangle_{45}|00\rangle_{67} + |11\rangle_{18}|11\rangle_{23}|10\rangle_{45}|01\rangle_{67} + |10\rangle_{18}|11\rangle_{23}|11\rangle_{45}|10\rangle_{67} \\
&\quad + |11\rangle_{18}|11\rangle_{23}|11\rangle_{45}|11\rangle_{67}\big).
\end{aligned}
$$

(i) When $A|\Psi\rangle$ is performed by $I^{\otimes^8} = I \otimes I \otimes I \otimes I \otimes I \otimes I \otimes I \otimes I$, we get follows:

$$
\begin{aligned}
&B^{\otimes^4} I^{\otimes^8} A|\Psi\rangle \\
&= \frac{1}{8}(|00\rangle_{18}|00\rangle_{23}|00\rangle_{45}|00\rangle_{67} + |00\rangle_{18}|00\rangle_{23}|01\rangle_{45}|01\rangle_{67} + |00\rangle_{18}|01\rangle_{23}|00\rangle_{45}|01\rangle_{67} \\
&\quad + |00\rangle_{18}|01\rangle_{23}|01\rangle_{45}|00\rangle_{67} + |01\rangle_{18}|00\rangle_{23}|00\rangle_{45}|01\rangle_{67} + |01\rangle_{18}|00\rangle_{23}|01\rangle_{45}|00\rangle_{67} \\
&\quad + |01\rangle_{18}|01\rangle_{23}|00\rangle_{45}|00\rangle_{67} + |01\rangle_{18}|01\rangle_{23}|01\rangle_{45}|01\rangle_{67} + |10\rangle_{18}|00\rangle_{23}|00\rangle_{45}|10\rangle_{67} \\
&\quad + |10\rangle_{18}|00\rangle_{23}|01\rangle_{45}|11\rangle_{67} + |10\rangle_{18}|01\rangle_{23}|00\rangle_{45}|11\rangle_{67} + |10\rangle_{18}|01\rangle_{23}|01\rangle_{45}|10\rangle_{67} \\
&\quad + |11\rangle_{18}|00\rangle_{23}|00\rangle_{45}|11\rangle_{67} + |11\rangle_{18}|00\rangle_{23}|01\rangle_{45}|10\rangle_{67} + |11\rangle_{18}|01\rangle_{23}|00\rangle_{45}|10\rangle_{67} \\
&\quad + |11\rangle_{18}|01\rangle_{23}|01\rangle_{45}|11\rangle_{67} + |00\rangle_{18}|00\rangle_{23}|10\rangle_{45}|10\rangle_{67} - |00\rangle_{18}|00\rangle_{23}|11\rangle_{45}|11\rangle_{67} \\
&\quad - |00\rangle_{18}|01\rangle_{23}|10\rangle_{45}|11\rangle_{67} + |00\rangle_{18}|01\rangle_{23}|11\rangle_{45}|10\rangle_{67} - |01\rangle_{18}|00\rangle_{23}|10\rangle_{45}|11\rangle_{67} \\
&\quad + |01\rangle_{18}|00\rangle_{23}|11\rangle_{45}|10\rangle_{67} + |01\rangle_{18}|01\rangle_{23}|10\rangle_{45}|10\rangle_{67} - |01\rangle_{18}|01\rangle_{23}|11\rangle_{45}|11\rangle_{67} \\
&\quad + |10\rangle_{18}|00\rangle_{23}|10\rangle_{45}|00\rangle_{67} - |10\rangle_{18}|00\rangle_{23}|11\rangle_{45}|01\rangle_{67} - |10\rangle_{18}|01\rangle_{23}|10\rangle_{45}|01\rangle_{67} \\
&\quad + |10\rangle_{18}|01\rangle_{23}|11\rangle_{45}|00\rangle_{67} - |11\rangle_{18}|00\rangle_{23}|10\rangle_{45}|01\rangle_{67} + |11\rangle_{18}|00\rangle_{23}|11\rangle_{45}|00\rangle_{67} \\
&\quad + |11\rangle_{18}|01\rangle_{23}|10\rangle_{45}|00\rangle_{67} - |11\rangle_{18}|01\rangle_{23}|11\rangle_{45}|01\rangle_{67} + |00\rangle_{18}|10\rangle_{23}|10\rangle_{45}|00\rangle_{67} \\
&\quad - |00\rangle_{18}|10\rangle_{23}|11\rangle_{45}|01\rangle_{67} + |00\rangle_{18}|11\rangle_{23}|10\rangle_{45}|01\rangle_{67} - |00\rangle_{18}|11\rangle_{23}|11\rangle_{45}|00\rangle_{67} \\
&\quad + |00\rangle_{18}|10\rangle_{23}|10\rangle_{45}|01\rangle_{67} - |01\rangle_{18}|10\rangle_{23}|11\rangle_{45}|00\rangle_{67} + |01\rangle_{18}|11\rangle_{23}|10\rangle_{45}|00\rangle_{67} \\
&\quad - |01\rangle_{18}|11\rangle_{23}|11\rangle_{45}|01\rangle_{67} + |10\rangle_{18}|10\rangle_{23}|10\rangle_{45}|10\rangle_{67} + |10\rangle_{18}|10\rangle_{23}|11\rangle_{45}|11\rangle_{67} \\
&\quad - |10\rangle_{18}|11\rangle_{23}|10\rangle_{45}|11\rangle_{67} - |10\rangle_{18}|11\rangle_{23}|11\rangle_{45}|10\rangle_{67} - |11\rangle_{18}|10\rangle_{23}|11\rangle_{45}|10\rangle_{67} \\
&\quad - |11\rangle_{18}|10\rangle_{23}|10\rangle_{45}|11\rangle_{67} + |11\rangle_{18}|11\rangle_{23}|10\rangle_{45}|10\rangle_{67} + |11\rangle_{18}|11\rangle_{23}|11\rangle_{45}|11\rangle_{67} \\
&\quad + |00\rangle_{18}|10\rangle_{23}|00\rangle_{45}|10\rangle_{67} + |00\rangle_{18}|10\rangle_{23}|01\rangle_{45}|11\rangle_{67} - |00\rangle_{18}|11\rangle_{23}|00\rangle_{45}|11\rangle_{67} \\
&\quad - |00\rangle_{18}|11\rangle_{23}|01\rangle_{45}|10\rangle_{67} - |01\rangle_{18}|10\rangle_{23}|00\rangle_{45}|11\rangle_{67} - |01\rangle_{18}|10\rangle_{23}|01\rangle_{45}|10\rangle_{67} \\
&\quad + |01\rangle_{18}|11\rangle_{23}|00\rangle_{45}|10\rangle_{67} + |01\rangle_{18}|11\rangle_{23}|01\rangle_{45}|11\rangle_{67} + |10\rangle_{18}|10\rangle_{23}|00\rangle_{45}|00\rangle_{67} \\
&\quad + |10\rangle_{18}|10\rangle_{23}|01\rangle_{45}|01\rangle_{67} - |10\rangle_{18}|11\rangle_{23}|00\rangle_{45}|01\rangle_{67} - |10\rangle_{18}|11\rangle_{23}|01\rangle_{45}|00\rangle_{67}
\end{aligned}
$$

$$
\begin{aligned}
&- |11\rangle_{18}|10\rangle_{23}|00\rangle_{45}|01\rangle_{67} - |11\rangle_{18}|10\rangle_{23}|01\rangle_{45}|00\rangle_{67} + |11\rangle_{18}|11\rangle_{23}|00\rangle_{45}|00\rangle_{67}\\
&+ |11\rangle_{18}|11\rangle_{23}|01\rangle_{45}|01\rangle_{67}),
\end{aligned}
$$

which can be written as

$$B^{\otimes^4} I^{\otimes^8} A|\Psi\rangle = \sum_{i=1}^{64} \varepsilon_i |e_i\rangle_{18}|f_i\rangle_{23}|g_i\rangle_{45}|h_i\rangle_{67},$$

where

$$\varepsilon_i \in \{-1, 1\}, |e_i\rangle_{18}, |f_i\rangle_{23}, |g_i\rangle_{45}, |h_i\rangle_{67} \in \big\{|00\rangle, |01\rangle, |10\rangle, |11\rangle\big\},$$

which satisfies $|e_i\rangle_{18} = |f_i\rangle_{23} \oplus |g_i\rangle_{45} \oplus |h_i\rangle_{67}$ $(1 \le i \le 64)$. Thus, Eq. (1) holds.

(ii) When $A|\Psi\rangle$ is performed by $I^{\otimes^2} X^{\otimes^2} I^{\otimes^4} = I \otimes I \otimes X \otimes X \otimes I \otimes I \otimes I \otimes I$, we get

$$
\begin{aligned}
&B^{\otimes^4} I^{\otimes^2} X^{\otimes^2} I^{\otimes^4} A|\Psi\rangle\\
&= \frac{1}{8}(|00\rangle_{18}|00\rangle_{23}|00\rangle_{45}|00\rangle_{67} + |00\rangle_{18}|00\rangle_{23}|01\rangle_{45}|01\rangle_{67} - |00\rangle_{18}|01\rangle_{23}|00\rangle_{45}|01\rangle_{67}\\
&- |00\rangle_{18}|01\rangle_{23}|01\rangle_{45}|00\rangle_{67} + |01\rangle_{18}|00\rangle_{23}|00\rangle_{45}|01\rangle_{67} + |01\rangle_{18}|00\rangle_{23}|01\rangle_{45}|00\rangle_{67}\\
&- |01\rangle_{18}|01\rangle_{23}|00\rangle_{45}|00\rangle_{67} - |01\rangle_{18}|01\rangle_{23}|01\rangle_{45}|01\rangle_{67} + |10\rangle_{18}|00\rangle_{23}|00\rangle_{45}|10\rangle_{67}\\
&+ |10\rangle_{18}|00\rangle_{23}|01\rangle_{45}|11\rangle_{67} - |10\rangle_{18}|01\rangle_{23}|00\rangle_{45}|11\rangle_{67} - |10\rangle_{18}|01\rangle_{23}|01\rangle_{45}|10\rangle_{67}\\
&+ |11\rangle_{18}|00\rangle_{23}|00\rangle_{45}|11\rangle_{67} + |11\rangle_{18}|00\rangle_{23}|01\rangle_{45}|10\rangle_{67} - |11\rangle_{18}|01\rangle_{23}|00\rangle_{45}|10\rangle_{67}\\
&- |11\rangle_{18}|01\rangle_{23}|01\rangle_{45}|11\rangle_{67} + |00\rangle_{18}|00\rangle_{23}|10\rangle_{45}|10\rangle_{67} - |00\rangle_{18}|00\rangle_{23}|11\rangle_{45}|11\rangle_{67}\\
&+ |00\rangle_{18}|01\rangle_{23}|10\rangle_{45}|11\rangle_{67} - |00\rangle_{18}|01\rangle_{23}|11\rangle_{45}|10\rangle_{67} - |01\rangle_{18}|00\rangle_{23}|10\rangle_{45}|11\rangle_{67}\\
&+ |01\rangle_{18}|00\rangle_{23}|11\rangle_{45}|10\rangle_{67} - |01\rangle_{18}|01\rangle_{23}|10\rangle_{45}|10\rangle_{67} + |01\rangle_{18}|01\rangle_{23}|11\rangle_{45}|11\rangle_{67}\\
&+ |10\rangle_{18}|00\rangle_{23}|10\rangle_{45}|00\rangle_{67} - |10\rangle_{18}|00\rangle_{23}|11\rangle_{45}|01\rangle_{67} + |10\rangle_{18}|01\rangle_{23}|10\rangle_{45}|01\rangle_{67}\\
&- |10\rangle_{18}|01\rangle_{23}|11\rangle_{45}|00\rangle_{67} - |11\rangle_{18}|00\rangle_{23}|10\rangle_{45}|01\rangle_{67} + |11\rangle_{18}|00\rangle_{23}|11\rangle_{45}|00\rangle_{67}\\
&- |11\rangle_{18}|01\rangle_{23}|10\rangle_{45}|00\rangle_{67} + |11\rangle_{18}|01\rangle_{23}|11\rangle_{45}|01\rangle_{67} + |00\rangle_{18}|10\rangle_{23}|10\rangle_{45}|00\rangle_{67}\\
&- |00\rangle_{18}|10\rangle_{23}|11\rangle_{45}|01\rangle_{67} - |00\rangle_{18}|11\rangle_{23}|10\rangle_{45}|01\rangle_{67} + |00\rangle_{18}|11\rangle_{23}|11\rangle_{45}|00\rangle_{67}\\
&+ |00\rangle_{18}|10\rangle_{23}|10\rangle_{45}|01\rangle_{67} - |01\rangle_{18}|10\rangle_{23}|11\rangle_{45}|00\rangle_{67} - |01\rangle_{18}|11\rangle_{23}|10\rangle_{45}|00\rangle_{67}\\
&+ |01\rangle_{18}|11\rangle_{23}|11\rangle_{45}|01\rangle_{67} + |10\rangle_{18}|10\rangle_{23}|10\rangle_{45}|10\rangle_{67} + |10\rangle_{18}|10\rangle_{23}|11\rangle_{45}|11\rangle_{67}\\
&+ |10\rangle_{18}|11\rangle_{23}|10\rangle_{45}|11\rangle_{67} + |10\rangle_{18}|11\rangle_{23}|11\rangle_{45}|10\rangle_{67} - |11\rangle_{18}|10\rangle_{23}|11\rangle_{45}|10\rangle_{67}\\
&- |11\rangle_{18}|10\rangle_{23}|10\rangle_{45}|11\rangle_{67} - |11\rangle_{18}|11\rangle_{23}|10\rangle_{45}|10\rangle_{67} - |11\rangle_{18}|11\rangle_{23}|11\rangle_{45}|11\rangle_{67}\\
&+ |00\rangle_{18}|10\rangle_{23}|00\rangle_{45}|10\rangle_{67} + |00\rangle_{18}|10\rangle_{23}|01\rangle_{45}|11\rangle_{67} + |00\rangle_{18}|11\rangle_{23}|00\rangle_{45}|11\rangle_{67}\\
&+ |00\rangle_{18}|11\rangle_{23}|01\rangle_{45}|10\rangle_{67} - |01\rangle_{18}|10\rangle_{23}|00\rangle_{45}|11\rangle_{67} - |01\rangle_{18}|10\rangle_{23}|01\rangle_{45}|10\rangle_{67}\\
&- |01\rangle_{18}|11\rangle_{23}|00\rangle_{45}|10\rangle_{67} - |01\rangle_{18}|11\rangle_{23}|01\rangle_{45}|11\rangle_{67} + |10\rangle_{18}|10\rangle_{23}|00\rangle_{45}|00\rangle_{67}\\
&+ |10\rangle_{18}|10\rangle_{23}|01\rangle_{45}|01\rangle_{67} + |10\rangle_{18}|11\rangle_{23}|00\rangle_{45}|01\rangle_{67} + |10\rangle_{18}|11\rangle_{23}|01\rangle_{45}|00\rangle_{67}\\
&- |11\rangle_{18}|10\rangle_{23}|00\rangle_{45}|01\rangle_{67} - |11\rangle_{18}|10\rangle_{23}|01\rangle_{45}|00\rangle_{67} - |11\rangle_{18}|11\rangle_{23}|00\rangle_{45}|00\rangle_{67}\\
&- |11\rangle_{18}|11\rangle_{23}|01\rangle_{45}|01\rangle_{67}),
\end{aligned}
$$

which can be written as

$$B^{\otimes^4} I^{\otimes^2} X^{\otimes^2} I^{\otimes^4} A|\Psi\rangle = \sum_{i=1}^{64} \varepsilon_i |e_i\rangle_{18}|f_i\rangle_{23}|g_i\rangle_{45}|h_i\rangle_{67},$$

where

$$\varepsilon_i \in \{-1, 1\}, |e_i\rangle_{18}, |f_i\rangle_{23}, |g_i\rangle_{45}, |h_i\rangle_{67} \in \big\{|00\rangle, |01\rangle, |10\rangle, |11\rangle\big\},$$

which satisfies $|e_i\rangle_{18} = |f_i\rangle_{23} \oplus |g_i\rangle_{45} \oplus |h_i\rangle_{67}$ $(1 \le i \le 64)$. Thus, Eq. (1) holds.

(iii) When $A|\Psi\rangle$ is performed by $I^{\otimes^2} Z^{\otimes^2} I^{\otimes^4} = I \otimes I \otimes Z \otimes Z \otimes I \otimes I \otimes I \otimes I$, we get

$$\begin{aligned}
&B^{\otimes^4} I^{\otimes^2} Z^{\otimes^2} I^{\otimes^4} A|\Psi\rangle \\
&= \frac{1}{8}(|00\rangle_{18}|00\rangle_{23}|00\rangle_{45}|00\rangle_{67} + |00\rangle_{18}|00\rangle_{23}|01\rangle_{45}|01\rangle_{67} + |00\rangle_{18}|01\rangle_{23}|00\rangle_{45}|01\rangle_{67} \\
&\quad + |00\rangle_{18}|01\rangle_{23}|01\rangle_{45}|00\rangle_{67} + |01\rangle_{18}|00\rangle_{23}|00\rangle_{45}|01\rangle_{67} + |01\rangle_{18}|00\rangle_{23}|01\rangle_{45}|00\rangle_{67} \\
&\quad + |01\rangle_{18}|01\rangle_{23}|00\rangle_{45}|00\rangle_{67} + |01\rangle_{18}|01\rangle_{23}|01\rangle_{45}|01\rangle_{67} + |10\rangle_{18}|00\rangle_{23}|00\rangle_{45}|10\rangle_{67} \\
&\quad + |10\rangle_{18}|00\rangle_{23}|01\rangle_{45}|11\rangle_{67} + |10\rangle_{18}|01\rangle_{23}|00\rangle_{45}|11\rangle_{67} + |10\rangle_{18}|01\rangle_{23}|01\rangle_{45}|10\rangle_{67} \\
&\quad + |11\rangle_{18}|00\rangle_{23}|00\rangle_{45}|11\rangle_{67} + |11\rangle_{18}|00\rangle_{23}|01\rangle_{45}|10\rangle_{67} + |11\rangle_{18}|01\rangle_{23}|00\rangle_{45}|10\rangle_{67} \\
&\quad + |11\rangle_{18}|01\rangle_{23}|01\rangle_{45}|11\rangle_{67} + |00\rangle_{18}|00\rangle_{23}|10\rangle_{45}|10\rangle_{67} - |00\rangle_{18}|00\rangle_{23}|11\rangle_{45}|11\rangle_{67} \\
&\quad - |00\rangle_{18}|01\rangle_{23}|10\rangle_{45}|11\rangle_{67} + |00\rangle_{18}|01\rangle_{23}|11\rangle_{45}|10\rangle_{67} - |01\rangle_{18}|00\rangle_{23}|10\rangle_{45}|11\rangle_{67} \\
&\quad + |01\rangle_{18}|00\rangle_{23}|11\rangle_{45}|10\rangle_{67} + |01\rangle_{18}|01\rangle_{23}|10\rangle_{45}|10\rangle_{67} - |01\rangle_{18}|01\rangle_{23}|11\rangle_{45}|11\rangle_{67} \\
&\quad + |10\rangle_{18}|00\rangle_{23}|10\rangle_{45}|00\rangle_{67} - |10\rangle_{18}|00\rangle_{23}|11\rangle_{45}|01\rangle_{67} - |10\rangle_{18}|01\rangle_{23}|10\rangle_{45}|01\rangle_{67} \\
&\quad + |10\rangle_{18}|01\rangle_{23}|11\rangle_{45}|00\rangle_{67} - |11\rangle_{18}|00\rangle_{23}|10\rangle_{45}|01\rangle_{67} + |11\rangle_{18}|00\rangle_{23}|11\rangle_{45}|00\rangle_{67} \\
&\quad + |11\rangle_{18}|01\rangle_{23}|10\rangle_{45}|00\rangle_{67} - |11\rangle_{18}|01\rangle_{23}|11\rangle_{45}|01\rangle_{67} - |00\rangle_{18}|10\rangle_{23}|10\rangle_{45}|00\rangle_{67} \\
&\quad + |00\rangle_{18}|10\rangle_{23}|11\rangle_{45}|01\rangle_{67} - |00\rangle_{18}|11\rangle_{23}|10\rangle_{45}|01\rangle_{67} + |00\rangle_{18}|11\rangle_{23}|11\rangle_{45}|00\rangle_{67} \\
&\quad - |00\rangle_{18}|10\rangle_{23}|10\rangle_{45}|01\rangle_{67} + |01\rangle_{18}|10\rangle_{23}|11\rangle_{45}|00\rangle_{67} - |01\rangle_{18}|11\rangle_{23}|10\rangle_{45}|00\rangle_{67} \\
&\quad + |01\rangle_{18}|11\rangle_{23}|11\rangle_{45}|01\rangle_{67} - |10\rangle_{18}|10\rangle_{23}|10\rangle_{45}|10\rangle_{67} - |10\rangle_{18}|10\rangle_{23}|11\rangle_{45}|11\rangle_{67} \\
&\quad + |10\rangle_{18}|11\rangle_{23}|10\rangle_{45}|11\rangle_{67} + |10\rangle_{18}|11\rangle_{23}|11\rangle_{45}|10\rangle_{67} + |11\rangle_{18}|10\rangle_{23}|11\rangle_{45}|10\rangle_{67} \\
&\quad + |11\rangle_{18}|10\rangle_{23}|10\rangle_{45}|11\rangle_{67} - |11\rangle_{18}|11\rangle_{23}|10\rangle_{45}|10\rangle_{67} - |11\rangle_{18}|11\rangle_{23}|11\rangle_{45}|11\rangle_{67} \\
&\quad - |00\rangle_{18}|10\rangle_{23}|00\rangle_{45}|10\rangle_{67} - |00\rangle_{18}|10\rangle_{23}|01\rangle_{45}|11\rangle_{67} + |00\rangle_{18}|11\rangle_{23}|00\rangle_{45}|11\rangle_{67} \\
&\quad + |00\rangle_{18}|11\rangle_{23}|01\rangle_{45}|10\rangle_{67} + |01\rangle_{18}|10\rangle_{23}|00\rangle_{45}|11\rangle_{67} + |01\rangle_{18}|10\rangle_{23}|01\rangle_{45}|10\rangle_{67} \\
&\quad - |01\rangle_{18}|11\rangle_{23}|00\rangle_{45}|10\rangle_{67} - |01\rangle_{18}|11\rangle_{23}|01\rangle_{45}|11\rangle_{67} - |10\rangle_{18}|10\rangle_{23}|00\rangle_{45}|00\rangle_{67} \\
&\quad - |10\rangle_{18}|10\rangle_{23}|01\rangle_{45}|01\rangle_{67} + |10\rangle_{18}|11\rangle_{23}|00\rangle_{45}|01\rangle_{67} + |10\rangle_{18}|11\rangle_{23}|01\rangle_{45}|00\rangle_{67} \\
&\quad + |11\rangle_{18}|10\rangle_{23}|00\rangle_{45}|01\rangle_{67} + |11\rangle_{18}|10\rangle_{23}|01\rangle_{45}|00\rangle_{67} - |11\rangle_{18}|11\rangle_{23}|00\rangle_{45}|00\rangle_{67} \\
&\quad - |11\rangle_{18}|11\rangle_{23}|01\rangle_{45}|01\rangle_{67}),
\end{aligned}$$

which can be written as

$$B^{\otimes^4} I^{\otimes^2} Z^{\otimes^2} I^{\otimes^4} A|\Psi\rangle = \sum_{i=1}^{64} \varepsilon_i |e_i\rangle_{18}|f_i\rangle_{23}|g_i\rangle_{45}|h_i\rangle_{67},$$

where

$$\varepsilon_i \in \{-1, 1\},\ |e_i\rangle_{18}, |f_i\rangle_{23}, |g_i\rangle_{45}, |h_i\rangle_{67} \in \big\{|00\rangle, |01\rangle, |10\rangle, |11\rangle\big\},$$

which satisfies $|e_i\rangle_{18} = |f_i\rangle_{23} \oplus |g_i\rangle_{45} \oplus |h_i\rangle_{67}$ $(1 \le i \le 64)$. Thus, Eq. (1) holds.

(iv) When $A|\Psi\rangle$ is performed by $I^{\otimes^2} iY^{\otimes^2} I^{\otimes^4} = I \otimes I \otimes iY \otimes iY \otimes I \otimes I \otimes I \otimes I$, we get

$$
\begin{aligned}
&B^{\otimes^4} I^{\otimes^2} iY^{\otimes^2} I^{\otimes^4} A|\Psi\rangle \\
&\quad = \frac{1}{8}(|00\rangle_{18}|00\rangle_{23}|00\rangle_{45}|00\rangle_{67} + |00\rangle_{18}|00\rangle_{23}|01\rangle_{45}|01\rangle_{67} - |00\rangle_{18}|01\rangle_{23}|00\rangle_{45}|01\rangle_{67} \\
&\qquad - |00\rangle_{18}|01\rangle_{23}|01\rangle_{45}|00\rangle_{67} + |01\rangle_{18}|00\rangle_{23}|00\rangle_{45}|01\rangle_{67} + |01\rangle_{18}|00\rangle_{23}|01\rangle_{45}|00\rangle_{67} \\
&\qquad - |01\rangle_{18}|01\rangle_{23}|00\rangle_{45}|00\rangle_{67} - |01\rangle_{18}|01\rangle_{23}|01\rangle_{45}|01\rangle_{67} + |10\rangle_{18}|00\rangle_{23}|00\rangle_{45}|10\rangle_{67} \\
&\qquad + |10\rangle_{18}|00\rangle_{23}|01\rangle_{45}|11\rangle_{67} - |10\rangle_{18}|01\rangle_{23}|00\rangle_{45}|11\rangle_{67} - |10\rangle_{18}|01\rangle_{23}|01\rangle_{45}|10\rangle_{67} \\
&\qquad + |11\rangle_{18}|00\rangle_{23}|00\rangle_{45}|11\rangle_{67} + |11\rangle_{18}|00\rangle_{23}|01\rangle_{45}|10\rangle_{67} - |11\rangle_{18}|01\rangle_{23}|00\rangle_{45}|10\rangle_{67} \\
&\qquad - |11\rangle_{18}|01\rangle_{23}|01\rangle_{45}|11\rangle_{67} + |00\rangle_{18}|00\rangle_{23}|10\rangle_{45}|10\rangle_{67} - |00\rangle_{18}|00\rangle_{23}|11\rangle_{45}|11\rangle_{67} \\
&\qquad + |00\rangle_{18}|01\rangle_{23}|10\rangle_{45}|11\rangle_{67} - |00\rangle_{18}|01\rangle_{23}|11\rangle_{45}|10\rangle_{67} - |01\rangle_{18}|00\rangle_{23}|10\rangle_{45}|11\rangle_{67} \\
&\qquad + |01\rangle_{18}|00\rangle_{23}|11\rangle_{45}|10\rangle_{67} - |01\rangle_{18}|01\rangle_{23}|10\rangle_{45}|10\rangle_{67} + |01\rangle_{18}|01\rangle_{23}|11\rangle_{45}|11\rangle_{67} \\
&\qquad + |10\rangle_{18}|00\rangle_{23}|10\rangle_{45}|00\rangle_{67} - |10\rangle_{18}|00\rangle_{23}|11\rangle_{45}|01\rangle_{67} + |10\rangle_{18}|01\rangle_{23}|10\rangle_{45}|01\rangle_{67} \\
&\qquad - |10\rangle_{18}|01\rangle_{23}|11\rangle_{45}|00\rangle_{67} - |11\rangle_{18}|00\rangle_{23}|10\rangle_{45}|01\rangle_{67} + |11\rangle_{18}|00\rangle_{23}|11\rangle_{45}|00\rangle_{67} \\
&\qquad - |11\rangle_{18}|01\rangle_{23}|10\rangle_{45}|00\rangle_{67} + |11\rangle_{18}|01\rangle_{23}|11\rangle_{45}|01\rangle_{67} - |00\rangle_{18}|10\rangle_{23}|10\rangle_{45}|00\rangle_{67} \\
&\qquad + |00\rangle_{18}|10\rangle_{23}|11\rangle_{45}|01\rangle_{67} + |00\rangle_{18}|11\rangle_{23}|10\rangle_{45}|01\rangle_{67} - |00\rangle_{18}|11\rangle_{23}|11\rangle_{45}|00\rangle_{67} \\
&\qquad - |00\rangle_{18}|10\rangle_{23}|10\rangle_{45}|01\rangle_{67} + |01\rangle_{18}|10\rangle_{23}|11\rangle_{45}|00\rangle_{67} + |01\rangle_{18}|11\rangle_{23}|10\rangle_{45}|00\rangle_{67} \\
&\qquad - |01\rangle_{18}|11\rangle_{23}|11\rangle_{45}|01\rangle_{67} - |10\rangle_{18}|10\rangle_{23}|10\rangle_{45}|10\rangle_{67} - |10\rangle_{18}|10\rangle_{23}|11\rangle_{45}|11\rangle_{67} \\
&\qquad - |10\rangle_{18}|11\rangle_{23}|10\rangle_{45}|11\rangle_{67} - |10\rangle_{18}|11\rangle_{23}|11\rangle_{45}|10\rangle_{67} + |11\rangle_{18}|10\rangle_{23}|11\rangle_{45}|10\rangle_{67} \\
&\qquad + |11\rangle_{18}|10\rangle_{23}|10\rangle_{45}|11\rangle_{67} + |11\rangle_{18}|11\rangle_{23}|10\rangle_{45}|10\rangle_{67} + |11\rangle_{18}|11\rangle_{23}|11\rangle_{45}|11\rangle_{67} \\
&\qquad - |00\rangle_{18}|10\rangle_{23}|00\rangle_{45}|10\rangle_{67} - |00\rangle_{18}|10\rangle_{23}|01\rangle_{45}|11\rangle_{67} - |00\rangle_{18}|11\rangle_{23}|00\rangle_{45}|11\rangle_{67} \\
&\qquad - |00\rangle_{18}|11\rangle_{23}|01\rangle_{45}|10\rangle_{67} + |01\rangle_{18}|10\rangle_{23}|00\rangle_{45}|11\rangle_{67} + |01\rangle_{18}|10\rangle_{23}|01\rangle_{45}|10\rangle_{67} \\
&\qquad + |01\rangle_{18}|11\rangle_{23}|00\rangle_{45}|10\rangle_{67} + |01\rangle_{18}|11\rangle_{23}|01\rangle_{45}|11\rangle_{67} - |10\rangle_{18}|10\rangle_{23}|00\rangle_{45}|00\rangle_{67} \\
&\qquad - |10\rangle_{18}|10\rangle_{23}|01\rangle_{45}|01\rangle_{67} - |10\rangle_{18}|11\rangle_{23}|00\rangle_{45}|01\rangle_{67} - |10\rangle_{18}|11\rangle_{23}|01\rangle_{45}|00\rangle_{67} \\
&\qquad + |11\rangle_{18}|10\rangle_{23}|00\rangle_{45}|01\rangle_{67} + |11\rangle_{18}|10\rangle_{23}|01\rangle_{45}|00\rangle_{67} + |11\rangle_{18}|11\rangle_{23}|00\rangle_{45}|00\rangle_{67} \\
&\qquad + |11\rangle_{18}|11\rangle_{23}|01\rangle_{45}|01\rangle_{67}),
\end{aligned}
$$

which can be written as

$$
B^{\otimes^4} I^{\otimes^2} iY^{\otimes^2} I^{\otimes^4} A|\Psi\rangle = \sum_{i=1}^{64} \varepsilon_i |e_i\rangle_{18}|f_i\rangle_{23}|g_i\rangle_{45}|h_i\rangle_{67},
$$

where

$$
\varepsilon_i \in \{-1, 1\}, |e_i\rangle_{18}, |f_i\rangle_{23}, |g_i\rangle_{45}, |h_i\rangle_{67} \in \big\{|00\rangle, |01\rangle, |10\rangle, |11\rangle\big\},
$$

which satisfies $|e_i\rangle_{18} = |f_i\rangle_{23} \oplus |g_i\rangle_{45} \oplus |h_i\rangle_{67}$ $(1 \le i \le 64)$. Thus, Eq. (1) holds. The proof is completed. □

References

1. Blakley, G.R.: In: Proc. AFIPS 1979 NCC, vol. 48, p. 313 (1979)
2. Shamir, A.: Commun. ACM **22**, 612 (1979)
3. Hillery, M., Buek, V., Berthiaume, A.: Phys. Rev. A **59**, 1829 (1999)
4. Karlsson, A., Koashi, M., Imoto, N.: Phys. Rev. A **59**, 162 (1999)

5. Hillery, M., Buzek, V., Bethillme, A.: Phys. Rev. A **59**, 1829 (1999)
6. Bagherineahad, S., Karimipour, V.: Phys. Rev. A **67**, 044302 (2003)
7. Zhang, Z.J., Man, Z.X.: Phys. Rev. A **72**, 022303 (2005)
8. Deng, F.G., Zhou, H.Y., Long, G.L.: J. Phys. A, Math. Gen. **39**, 14089 (2006)
9. Deng, F.G., Long, G.L., Zhou, H.Y.: Phys. Lett. A **43**, 340 (2005)
10. Deng, F.G., Li, X.H., Li, C.Y., et al.: Phys. Rev. A **72**, 044301 (2005)
11. Sun, Y., Wen, Q.Y., Gao, F., et al.: Opt. Commun. **282**, 3647 (2009)
12. Shi, R.H., Huang, L.S., Yang, W., et al.: Opt. Commun. **283**, 2762 (2010)
13. Shi, R.H., Huang, L.S., Yang, W., et al.: Opt. Commun. **283**, 2476 (2010)
14. Wang, S.H., Chong, S.K., Hwang, T.: Opt. Commun. **283**, 4405 (2010)
15. Wang, T.Y., Wen, Q.Y., Zhu, F.C.: Opt. Commun. **284**, 1711 (2011)
16. Lin, J., Hwang, T.: Opt. Commun. **284**, 1468 (2011)