Int J Theor Phys (2014) 53:1730–1737
DOI 10.1007/s10773-013-1971-y

Eavesdropping on Multiparty Quantum Secret Sharing Scheme Based on the Phase Shift Operations

Feng Liu · Qi Su · Qiao-yan Wen

Received: 16 August 2013 / Accepted: 19 December 2013 / Published online: 8 January 2014

Abstract In a recent paper (Du and Bao in Opt. Commun. 308:159, 2013), a scheme of multiparty quantum secret sharing based on the phase shift operations was presented. We study the security of this scheme and find that it is not secure for dishonest participants, who can illegally elicit all of the dealer's secret message without any error.

Keywords Quantum secret sharing (QSS) · Eavesdropping attack · Phase shift operation

1 Introduction

Quantum secret sharing (QSS) allows that a secret message is splitted into several pieces by a dealer (Alice), and each participant (Bob_i, $1 \leq i \leq n$) owns a piece, and no subset of participants can be sufficient to extract the dealer's secret message, but the whole set can. In 2007, Zhang et al. proposed a multiparty QSS scheme (ZGW scheme) [1] based on Einstein-Podolsky-Rosen (EPR) pairs and the five local unitary operations, which is more efficient and more feasible than the previous schemes. However, Lin et al. [2] showed that the last participant may solely obtain half of Alice's secret messages without introducing any error, moreover, they gave an improvement of ZGW scheme. Later on, Wang et al. [3] claimed that the three-party case in Lin et al. improved scheme [2] is secure, and pointed out that the n-party ($n \geq 4$) case is not secure. In the n-party case, Wang et al. showed that the first participant and the last participant may collaborate to eavesdrop Alice's secret messages without any error. In 2011, Gao [4] further studied the security of the improved n-party QSS scheme [2], and proposed an interesting attack on it. The attack given by Gao can obtain the entire secret, but it will introduce 25 % error rate [5]. Based on analyzing the reasons

F. Liu (✉) · Q. Su · Q.-y. Wen
State Key Laboratory of Networking and Switching Technology, Beijing University of Posts and Telecommunications, Beijing 100876, China
e-mail: liufeng23490@126.com

F. Liu
School of Mathematics and Statistics Science, Ludong University, Yantai 264025, China

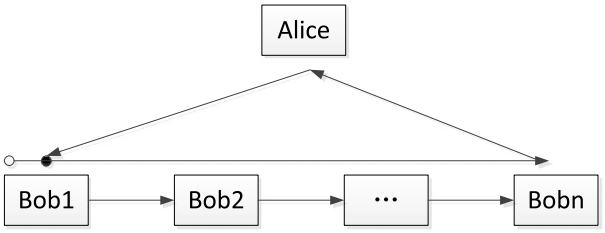

Fig. 1 The structure of DB scheme. $\circ - \bullet$ denotes the Bell state $|\varphi\rangle_{ts}$ prepared by Bob_1, of which the left one is photon s, and the right one is photon t

that make these schemes insecure, some possible improvements on the ZGW scheme have been proposed, i.e., ZGW-style schemes. In all the ZGW-style schemes, there are mainly Lin et al. improved scheme (Lin scheme) [2] and Gao modified scheme (Gao scheme) [4], by increasing the sample photons detections between the dealer and participants to improve the authentication of quantum channels. By contrast, Gao scheme is more secure than Lin scheme because of increasing the detection between Alice and Bob_n (the last participant).

Recently, Du and Bao [6] presented a novel collective eavesdropping attack strategy on Gao scheme. That is, Gao scheme can be successfully attacked by the first participant and the last two participants. They can obtain the entire secret messages without introducing any error, by attacking different photons from different participants separately. The strategy is also valid [6] to other ZGW-style schemes. Furthermore, they proposed a further improved multiparty QSS scheme (DB scheme) based on the 3-element phase shift operations set $\{U(0), U(2\pi/3), U(4\pi/3)\}$. It is claimed that DB scheme can resist not only the existing attacks on ZGW-style schemes, but also the Du and Bao collective eavesdropping attack strategy.

Cryptanalysis always plays an important role in the development of cryptography as pointed out by Gao et al. [7]. Up to now, quite a few effective attack strategies have been proposed in the study of quantum cryptography, such as the correlation-extractability attack [8], the intercept-resend attack [9], the entanglement swapping attack [10], and the participant attack [11] et al. Moreover, Qin et al. [11] pointed out that the attack power of dishonest participants is much stronger than outside eavesdroppers. In this paper, we study the security of DB scheme [6] and find that it is not secure against inside dishonest participants' attacks.

2 The DB Scheme

Let us give a brief description of DB scheme [6] as follows (Fig. 1).

(1) Bob_1 prepares a photon pair $|\varphi\rangle_{ts}$ randomly in one of four Bell states, i.e. $|\phi^{\pm}\rangle = \frac{1}{\sqrt{2}}(|00\rangle \pm |11\rangle)$, $|\psi^{\pm}\rangle = \frac{1}{\sqrt{2}}(|01\rangle \pm |10\rangle)$. Then he stores the photon s in his lab and sends the other photon t to Bob_2.

(2) After receiving the photon t, Bob_2 ascertains whether the received photon is a single photon. If it is not a single photon, he aborts the communication; otherwise, he performs the local operation $U(\alpha_2)$ on the photon t, which is chosen randomly from the 3-element phase shift operations set $\{U(0), U(2\pi/3), U(4\pi/3)\}$. Here $U(\alpha) = \cos\alpha|0\rangle\langle 0| - \sin\alpha|0\rangle\langle 1| + \sin\alpha|1\rangle\langle 0| + \cos\alpha|1\rangle\langle 1|$, $\alpha \in \{0, \frac{2\pi}{3}, \frac{4\pi}{3}\}$. Then Bob_2 sends the photon t to Bob_3.

Bob_i $(i = 3, 4, \ldots, n)$ does the similar procedure as Bob_2 till Bob_n finishes his operation. At last, Bob_n sends the photon t to Alice.

(3) After receiving the photon t, Alice firstly confirms whether it is a single photon like Bob_2. Then she randomly switches between the control mode and the message mode. In the control mode, Alice randomly selects one action from the two choices: One is that she lets Bob_1 randomly use the measuring basis $Z = \{|0\rangle, |1\rangle\}$ or $X = \{|+\rangle, |-\rangle\}$ to measure the photon s, and then tell her his measurement outcome and the initial Bell state. Then Alice requires other participants to announce their unitary operations. The other is that she first lets Bob_2, $\mathrm{Bob}_3, \ldots, \mathrm{Bob}_n$ announce their operations. She then asks Bob_1 to perform a measurement on the photon s and tell her his measurement outcome and the initial Bell state. Next, Alice uses correct measuring basis to measure the photon t. By comparing her measurement outcome with the deduced outcome, Alice can judge whether the quantum channel is secure. If the quantum channel is attacked, the communication is aborted. Otherwise, the transmission goes on to Step (1). In the message mode, Alice encodes the secret by performing the Pauli operation on the photon t, according to the following definitions: $I(\sigma_x, \sigma_z, i\sigma_y)$ corresponds to two classical bits 00(10, 01, 11). After her encoding, Alice sends all the t-photons of message mode as a sequence (t-sequence) to Bob_1 in one communication.

(4) After receiving the t-sequence, all the participants can recover the secret by collaborating together: Bob_1 (or the other participant) collects all the participants' messages of operations, to deduce the compound operations and the correct measuring bases on these photons, and then he measures the pairs of photons in the corresponding positions of t-sequence and s-sequence to deduce the secret of Alice.

(5) At last, Alice announces a small part of the secret to participants to judge whether the t-sequence has been attacked. If it has, the eavesdropper cannot gain any useful information but destroy the communication.

3 Security Leak of the DB Scheme

In DB scheme [6], $\mathrm{Bob}_2, \mathrm{Bob}_3, \ldots, \mathrm{Bob}_n$ change their operations from the unitary operations set $\{I, \sigma_x, \sigma_z, i\sigma_y, H\}$ into the 3-element phase shift operations set $\{U(0), U(2\pi/3), U(4\pi/3)\}$ to resist the collective attack from the dishonest participants. By declaring false unitary operations on photon t by dishonest participants, Du and Bao [6] claimed that the collective attack strategy cannot escape from the eavesdropping detection.

However, there is a concealed condition in the Du and Bao attack strategy. That is, Bob_1 can only perform passive attacks in the eavesdropping process. For instance, Bob_1 only transfers his received false photons to Bob_{n-1} in the message mode. In fact, it is entirely possible for Bob_1 to perform active attacks, such as telling Alice a false initial state or sending a false photon to Alice in DB scheme. If Bob_1 only tells Alice the false initial state, the last two participants (Bob_{n-1} and Bob_n) can perform the intercept-and-resend attack to all photons, and tell lies based on entanglement swapping in the control mode. Finally, they can associate with Bob_1 to illegally elicit all of Alice's secret message without introducing any error, although the operations set is changed. The attack strategy is labeled by *the collective eavesdropping attack strategy* (Fig. 2). If Bob_1 tells Alice the false initial state and sends her false photons, he can solely perform the intercept-and-resend attack to all photons. Then, Bob_1 can tell lies based on entanglement swapping in the control mode. Finally, he can illegally elicit all of Alice's secret message without introducing any error. For the sake of distinction, the attack strategy is called *the individual eavesdropping attack strategy* (Fig. 3). In fact, the two attack strategies are all based on the entanglement swapping, which are similar to each other. To be precise, the second strategy can replace the first one completely.

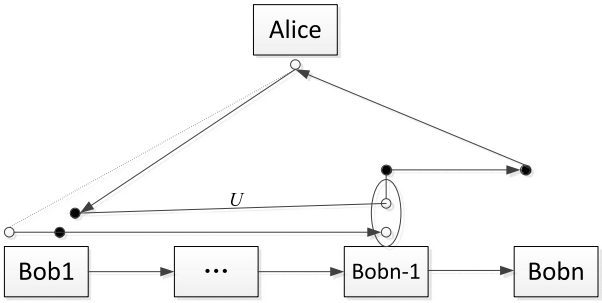

Fig. 2 The schematic diagram of the collective eavesdropping attack strategy

So the DB QSS scheme [6] is still not secure. In what follows, we will analyze in detail why it isn't secure.

3.1 The Collective Eavesdropping Attack Strategy

According to Step (1), Bob_i performs the local operation $U(\alpha_i)$ on the photon t and sends it to Bob_{i+1}, where $2 \le i \le n-2$. After receiving the photon t, Bob_{n-1} performs the local operation $U(\alpha_{n-1}^1)$ on the photon t. For the purpose of our discussion, let $U(\theta') = U(\alpha_{n-2}) \cdots U(\alpha_3)U(\alpha_2)$, $U(\theta) = U(\alpha_{n-1}^1)U(\theta')$, and Bob_{n-1} prepares one EPR photon pair $|\varphi\rangle_{t's'}$ randomly from four Bell states in advance. Then Bob_{n-1} stores t and replaces it by the photon t' from $|\varphi\rangle_{t's'}$. He sends t' to Bob_n. After receiving the photon t', Bob_n performs no operation on it. At last, Bob_n sends the photon t' to Alice.

When Alice is in the control mode, Bob_{n-1} performs the Bell measurement on the photon t and photon s'. Suppose that $|\psi\rangle_{ts} = (U(\theta) \otimes I)|\varphi\rangle_{ts}$ is the new entanglement state after the Bob_{n-1}'s operation. Obviously,

$$|\psi\rangle_{ts} \in \left\{\left|\phi^{\pm}\right\rangle^{0}, \left|\phi^{\pm}\right\rangle^{2\pi/3}, \left|\phi^{\pm}\right\rangle^{4\pi/3}; \left|\psi^{\pm}\right\rangle^{0}, \left|\psi^{\pm}\right\rangle^{2\pi/3}, \left|\psi^{\pm}\right\rangle^{4\pi/3}\right\}. \tag{1}$$

Here,

$$\left|\phi^{\pm}\right\rangle^{0} = \left(I \otimes U(0)\right)\left|\phi^{\pm}\right\rangle, \left|\phi^{\pm}\right\rangle^{2\pi/3} = \left(I \otimes U(2\pi/3)\right)\left|\phi^{\pm}\right\rangle,$$

$$\left|\phi^{\pm}\right\rangle^{4\pi/3} = \left(I \otimes U(4\pi/3)\right)\left|\phi^{\pm}\right\rangle; \left|\psi^{\pm}\right\rangle^{0} = \left(I \otimes U(0)\right)\left|\psi^{\pm}\right\rangle,$$

$$\left|\psi^{\pm}\right\rangle^{2\pi/3} = \left(I \otimes U(2\pi/3)\right)\left|\psi^{\pm}\right\rangle,$$

$$\left|\psi^{\pm}\right\rangle^{4\pi/3} = \left(I \otimes U(4\pi/3)\right)\left|\psi^{\pm}\right\rangle$$

and

$$U(2\pi/3)U(4\pi/3) = U(4\pi/3)U(2\pi/3) = U(0),$$
$$\left(U(2\pi/3)\right)^3 = \left(U(4\pi/3)\right)^3 = U(0);$$

$$\left\{\left|\phi^{\pm}\right\rangle^{0}, \left|\psi^{\pm}\right\rangle^{0}\right\}, \left\{\left|\phi^{\pm}\right\rangle^{2\pi/3}, \left|\psi^{\pm}\right\rangle^{2\pi/3}\right\}, \left\{\left|\phi^{\pm}\right\rangle^{4\pi/3}, \left|\psi^{\pm}\right\rangle^{4\pi/3}\right\}$$

are orthonormal basis respectively.

Based on the principle of entanglement swapping,

$$|\psi\rangle_{ts} \otimes |\varphi\rangle_{t's'} \mapsto (I \otimes U)|\varphi\rangle_{ts'} \otimes (I \otimes U)|\psi\rangle_{t's} \tag{2}$$

where $U \in \{I, \sigma_x, i\sigma_y, \sigma_z\}$, the photon t' and photon s will establish the new entanglement state $|\psi'\rangle_{ts}$.

Suppose that Bob_{n-1}'s Bell state measurement outcome on photons t and s' is $(I \otimes U)|\varphi\rangle_{ts'}$. Bob_{n-1} makes a comparison for $(I \otimes U)|\varphi\rangle_{ts'}$ and $|\varphi\rangle_{t's'}$, and gets the unitary operation U. This kind of Bell state comparison method and its comparison steps can be consulted in the paper [12]. According to Eq. (2), photons t' and s must be in $|\psi'\rangle_{ts} = (I \otimes U)|\psi\rangle_{t's} = (U(\theta) \otimes U)|\varphi\rangle_{ts}$, which is the real shared state between Alice and Bob_1. Bob_{n-1} tells Bob_1 the unitary operation U. Bob_1 uses $\{|0\rangle, |1\rangle\}$ or $\{|+\rangle, |-\rangle\}$ to measure the photon s and tells Alice his single-qubit measurement outcome. According to Step (3), Bob_1 still needs to tell Alice his initial Bell state. In order that Bob_{n-1}'s replacing trick is not detected by Alice, Bob_1 may not directly say that the initial Bell state is $|\varphi\rangle_{ts}$, but should tell the lie that it is $(I \otimes U)|\varphi\rangle_{ts}$ (U is just the gotten operator that Bob_{n-1} makes the Bell state comparison). At that time, Bob_{n-1} declares he performed $U(\alpha_{n-1}^2)$ and Bob_n declares $U(\alpha_n)$ operation, which satisfy

$$U(\alpha_n)U\left(\alpha_{n-1}^2\right) = U\left(\alpha_{n-1}^1\right), \alpha_{n-1}^2, \alpha_n \in \{0, 2\pi/3, 4\pi/3\}. \tag{3}$$

So, Bob_{n-1}'s replacing action will not be detected by Alice.

Next, we prove that there is no probabilistic error of the collective eavesdropping attack. Continuing to analyze, the key reason will be obtained. We know that Alice deduces $|\varphi\rangle_{ts'}$ from the information published by $\mathrm{Bob}_1, \mathrm{Bob}_2, \ldots, \mathrm{Bob}_n$. Only if it is satisfied the following two conditions, Bob_{n-1}'s replacing trick cannot be detected by Alice. The one condition is that the deduced state by Alice satisfies Eq. (1), and the other condition is that Alice's deducing state and $(U(\theta) \otimes U)|\varphi\rangle_{ts}$ are the same state. From the above content, Alice can obtain the initial state published by Bob_1 is $(I \otimes U)|\varphi\rangle_{ts}$, and the operations published by Bob_{n-1} is $U(\alpha_{n-1}^2)$ and Bob_n is $U(\alpha_n)$ respectively. If the compound operation of other participants is $U(\theta')$, Alice can only deduce as follows:

$$\begin{aligned} |\varphi\rangle_{ts} &\mapsto \left(U(\alpha_n)U\left(\alpha_{n-1}^2\right)U\left(\theta'\right) \otimes I\right)(I \otimes U)|\varphi\rangle_{ts} \\ &= \left(U\left(\alpha_{n-1}^1\right)U\left(\theta'\right) \otimes U\right)|\varphi\rangle_{ts} = \left(U(\theta) \otimes U\right)|\varphi\rangle_{ts}. \end{aligned} \tag{4}$$

Using the relationships after Eq. (1), it is easy to verify that the final entanglement state $(U(\theta) \otimes U)|\varphi\rangle_{ts}$ satisfies Eq. (1). Moreover, the $(U(\theta) \otimes U)|\varphi\rangle_{ts}$ and $|\psi'\rangle_{ts}$ are the same state. Hence, Bob_{n-1}'s replacing trick does not introduce any error. Meanwhile, because Bob_{n-1} has replaced all the photons by his false photons, he can associate with Bob_n and Bob_1 to get Alice's entire secret messages. In conclusion, the main reason for the success of Bob_{n-1}'s replacing action is that Bob_1 knows the initial Bell state of the scheme, and can announce a false initial state according to Bob_{n-1}'s measurement result.

When Alice is in the message mode, she encodes her secret message by performing a unitary operation $U_A \in \{I, \sigma_x, i\sigma_y, \sigma_z\}$ on photon t'. Then, she sends photon t' back to Bob_1. Bob_1 can associate with both Bob_{n-1} and Bob_n to make Bell state measurement on photons t' and s', finally to deduce Alice's secret.

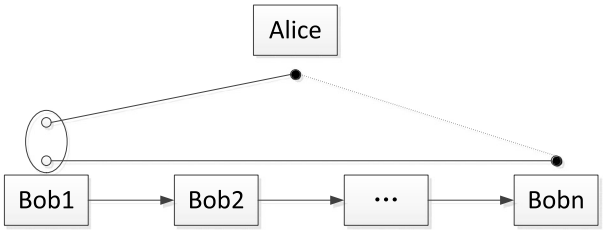

Fig. 3 The schematic diagram of the individual eavesdropping attack strategy

Example Suppose $|\varphi\rangle_{ts} = |\phi^+\rangle$, $|\varphi\rangle_{t's'} = |\psi^+\rangle$, $|\varphi'\rangle_{ts} = |\varphi\rangle_{ts'} = (I \otimes i\sigma_y)|\phi^+\rangle = -|\psi^-\rangle$, $U(\theta') = I$, $U(\alpha_{n-1}^1) = U(2\pi/3)$, and $U(\alpha_n)U(\alpha_{n-1}^2) = U(2\pi/3)$, then the real entanglement state between Alice and Bob_1 should be

$$\begin{aligned}\big|\psi'\big\rangle_{ts} &= \big(U\big(\alpha_{n-1}^1\big)U\big(\theta'\big) \otimes i\sigma_y\big)|\varphi\rangle_{ts} \\ &= \frac{U(2\pi/3) \otimes i\sigma_y}{\sqrt{2}}\big(|00\rangle + |11\rangle\big) = -\frac{1}{\sqrt{2}}\left(\frac{1}{2}\big|\psi^-\big\rangle + \frac{\sqrt{3}}{2}\big|\phi^+\big\rangle\right).\end{aligned}$$

According to the information published by participants, Alice can only deduce the following state.

$$\begin{aligned}\big(U(\alpha_n)U\big(\alpha_{n-1}^2\big)U\big(\theta'\big) \otimes I\big)\big|\varphi'\big\rangle_{ts} &= \big(U(2\pi/3)U\big(\theta'\big) \otimes i\sigma_y\big)|\varphi\rangle_{ts} \\ &= -\frac{1}{\sqrt{2}}\left(\frac{1}{2}\big|\psi^-\big\rangle + \frac{\sqrt{3}}{2}\big|\phi^+\big\rangle\right).\end{aligned}$$

It is easy to verify that $|\psi'\rangle_{ts}$ conforms to the constraint of Eq. (1). Moreover, the real entanglement state $|\psi'\rangle_{ts}$ between Alice and Bob_1 and the deduced state from Alice are all equivalent to $\frac{1}{2}|\psi^-\rangle + \frac{\sqrt{3}}{2}|\phi^+\rangle$. In a word, Bob_{n-1}'s replacing action will not be detected by Alice.

When the message mode is switched into, since Alice doesn't know that a replacing trick has been done by dishonest participants, she encodes her secret messages by performing a unitary operation on the received photon t'. Suppose that Alice encodes the secret message by performing the operation $U_A = \sigma_z$ on photon t', then the final entanglement state should be

$$(\sigma_z \otimes I)|\varphi\rangle_{t's'} = \big|\psi^-\big\rangle_{t's'}. \tag{5}$$

After Bob_1 receives photon t', he performs a Bell state measurement on photons t' and s'. Bob_{n-1} tells Bob_1 the initial state of photons t' and s', he very easily gets the operation $U_A = \sigma_z$ which represents Alice's secret message "01".

3.2 The Individual Eavesdropping Attack Strategy

The DB scheme [6] reduces two detections of sample photons compared with the Gao scheme [4], in order to decrease the numbers of message communications and quantum states preparations. In this case, we will show that Bob_1 may solely obtain the entire of Alice's secret messages without the other participants' help.

In advance, Bob_1 prepares two EPR photon pairs. Suppose that one pair is in $|\phi^-\rangle_{ts}$ and the other $|\psi^+\rangle_{t's'}$. According to Step (1), Bob_i sends photon t to Bob_{i+1}. After receiving photon t, Bob_{i+1} performs one local operation $U(\alpha_i) \in \{U(0), U(2\pi/3), U(4\pi/3)\}$ on it.

Here, $1 \le i \le n-1$. Finally, Bob_n sends photon t to Alice. When photon t is traveling between Bob_n and Alice, Bob_1 intercepts it, and stores it well. At the same time, Bob_1 sends photon t' (that is from $|\psi^+\rangle_{t's'}$), instead of photon t, to Alice. Alice randomly switches the control mode and the message mode. In the control mode, when Alice requires Bob_1 to make single-photon measurement on photon s, Bob_1 immediately makes Bell state measurement on photons s and s'. Obviously, this is the entangle swapping process of Bell states. Suppose that the operation performed by $\mathrm{Bob}_2, \mathrm{Bob}_3, \ldots$, and Bob_n is $U(2\pi/3) = U(\alpha_n)\cdots U(\alpha_2)$, then the whole system state can be written as follows:

$$
\begin{aligned}
&|\phi^-\rangle_{ts} \otimes |\psi^+\rangle_{t's'} \\
&\quad \to \big(U(2\pi/3) \otimes I\big)|\phi^-\rangle_{ts} \otimes |\psi^+\rangle_{t's'} \\
&\qquad = \frac{1}{2}\Bigg[|\phi^+\rangle_{ss'}\left(\frac{1}{2}|\psi^-\rangle + \frac{\sqrt{3}}{2}|\phi^+\rangle\right)_{tt'} + |\phi^-\rangle_{ss'}\left(\frac{1}{2}|\psi^+\rangle - \frac{\sqrt{3}}{2}|\phi^-\rangle\right)_{tt'} \\
&\qquad\quad + |\psi^+\rangle_{ss'}\left(\frac{1}{2}|\phi^-\rangle + \frac{\sqrt{3}}{2}|\psi^+\rangle\right)_{tt'} + |\psi^-\rangle_{ss'}\left(\frac{1}{2}|\phi^+\rangle - \frac{\sqrt{3}}{2}|\psi^-\rangle\right)_{tt'}\Bigg]. \qquad (6)
\end{aligned}
$$

Suppose that Bob_1's Bell state measurement outcome on photons s and s' is $|\psi^-\rangle_{ss'}$. According to Eq. (6), photons t and t' must be in $(\frac{1}{2}|\phi^+\rangle - \frac{\sqrt{3}}{2}|\psi^-\rangle)_{tt'}$. Next, Bob_1 makes a comparison for $|\psi^-\rangle_{ss'}$ and $|\psi^+\rangle_{t's'}$, and gets the unitary operation $U = \sigma_z$. After making Bell state measurement, Bob_1 uses $\{|0\rangle, |1\rangle\}$ or $\{|+\rangle, |-\rangle\}$ to measure photon t and tells Alice his single-qubit measurement outcome. According to Step (3), Bob_1 still needs to tell Alice his initial Bell state. In order that his replacing trick is not detected by Alice, Bob_1 may not directly say that the initial Bell state is $|\psi^+\rangle_{t's'}$, but should tell the lie that it is $(I \otimes \sigma_z)|\psi^+\rangle_{t's'} = |\psi^-\rangle_{t's'}$. So his replacing action will not be detected by Alice.

As for the other Bell states that Bob_1's measurement outcomes on photons s and s' are, the law exists as of old. So Bob_1 may evade Alice's security-check successfully in the case that $\mathrm{Bob}_2, \mathrm{Bob}_3, \ldots$, and Bob_n's compound operation is $U(2\pi/3)$. Similarly, if the compound operation is $U(0)$ or $U(4\pi/3)$, Bob_1's replacing trick is also feasible. In a word, no matter what $\mathrm{Bob}_2, \mathrm{Bob}_3, \ldots$, and Bob_n's operation is, Bob_1's replacing trick is not detected by Alice in the control mode [4].

When the message mode is switched into, since Alice doesn't know that Bob_1 has done the replacing trick and regards photon t' as photon t as of old, she encodes her secret messages by performing a unitary operation $U_A \in \{I, \sigma_x, i\sigma_y, \sigma_z\}$ on photon t'. Then she sends photon t' back to Bob_1. Bob_1 very easily gets Alice's secret messages by making Bell state measurement on photons s' and t' without other participants' help.

4 Conclusions

In summary, we have shown that the multiparty quantum secret sharing scheme [6] based on the 3-element phase shift operations is not secure against the collective eavesdropping attack strategy and the individual eavesdropping attack strategy. We hope that these problems are noticed in the following research.

Acknowledgements This work is supported by NSFC (Grant Nos. 61272057, 61202434, 61170270, 61100203, 61003286, 61121061), NCET (Grant No. NCET-10-0260), Beijing Natural Science Foundation (Grant Nos. 4112040, 4122054), the Fundamental Research Funds for the Central Universities (Grant No. 2012RC0612, 2011YB01).

References

1. Zhang, Z.J., Gao, G., Wang, X., Han, L.F., Shi, S.H.: Multiparty quantum secret sharing based on the improved Boström-Felbinger protocol. Opt. Commun. **269**(2), 418 (2007)
2. Lin, S., Wen, Q.Y., Gao, F., Zhu, F.C.: Improving the security of multiparty quantum secret sharing based on the improved Boström-Felbinger protocol. Opt. Commun. **281**(17), 4553 (2008)
3. Wang, T.Y., Wen, Q.Y., Gao, F., Lin, S., Zhu, F.C.: Cryptanalysis and improvement of multiparty quantum secret sharing schemes. Phys. Lett. A **373**(1), 65 (2008)
4. Gao, G.: Eavesdropping on the improved three-party quantum secret sharing protocol. Opt. Commun. **284**(3), 902 (2011)
5. Wang, T.Y., Wen, Q.Y., Zhu, F.C.: Cryptanalysis of multiparty quantum secret sharing with Bell states and Bell measurements. Opt. Commun. **284**(6), 1711 (2011)
6. Du, Y.T., Bao, W.S.: Multiparty quantum secret sharing scheme based on the phase shift operations. Opt. Commun. **308**, 159 (2013)
7. Gao, F., Qin, S.J., Guo, F.Z., et al.: Cryptanalysis of the arbitrated quantum signature protocols. Phys. Rev. A **84**(2), 022344 (2011)
8. Qin, S.J., Gao, F., Guo, F.Z., et al.: Comment on "Two-way protocols for quantum cryptography with a nonmaximally entangled qubit pair". Phys. Rev. A **82**(3), 036301 (2010)
9. Gao, F., Guo, F.Z., Wen, Q.Y., et al.: Comment on "Colloidal interactions and transport in nematic liquid crystals". Phys. Rev. Lett. **101**(2), 208901 (2008)
10. Gao, F., Qin, S.J., Wen, Q.Y., et al.: A simple participant attack on the Bradler-Dusek protocol. Quantum Inf. Comput. **7**(4), 329 (2007)
11. Qin, S.J., Gao, F., Wen, Q.Y., et al.: Cryptanalysis of the Hillery-Buzek-Berthiaume quantum secret sharing protocol. Phys. Rev. A **76**(6), 062324 (2007)
12. Gao, G.: Quantum key distribution by comparing Bell states. Opt. Commun. **281**(4), 876 (2008)