Quantum Inf Process (2015) 14:4245–4254
DOI 10.1007/s11128-015-1110-1

Improving the security of protocols of quantum key agreement solely using Bell states and Bell measurement

Zhen-Chao Zhu[1,2] · **Ai-Qun Hu**[1] · **An-Min Fu**[3]

Received: 17 December 2014 / Accepted: 24 August 2015 / Published online: 1 September 2015

Abstract In a recent study, Shukla et al. (Quantum Inf Process 13:2391–2405, 2014) proposed two quantum key agreement protocols based on Bell state and Bell measurement, and they claimed that their two protocols were secure. However, in this study, we will show that the three-party protocol they proposed is not secure. Any participant in the protocol can directly obtain other two participants' secret keys. More seriously, two dishonest participants in the protocol can conclude to determine the shared key alone. Furthermore, we will show that there is another minor flaw in their two protocols; that is, eavesdroppers can flip any bit of the final key without introducing any error. In the end, some possible improvements are proposed to avoid these flaws.

Keywords Quantum key agreement · Bell states · Bell measurement · Participant attack

1 Introduction

In 2004, quantum key agreement (QKA), a new application of quantum mechanics in cryptography, was proposed by Zhou et al. [1]. With a QKA protocol, two or more participants can establish a secret key over unsafe public channels. In contrast to quantum key distribution (QKD), in which the sender determines the key and then distributes it to

✉ Zhen-Chao Zhu
zhuzc@seu.edu.cn

1 Information Security Research Center, Southeast University, Nanjing 210096, China

2 State Key Laboratory of Information Security, Institute of Information Engineering, Chinese Academy of Sciences, Beijing 100093, China

3 School of Computer Science and Technology, Nanjing University of Science and Technology, Nanjing 210094, China

the receiver, each participant in a QKA protocol contributes equally to the final key. The final key cannot be determined by any non-trivial subset of participants. We know that the security of most classical KA protocol [2–11] relies on some unproved assumptions of computation complexity, while the security of QKA protocol is guaranteed by quantum mechanics principles, such as Heisenberg's uncertainty principle and quantum no-cloning theorem; this security advantage makes QKA quickly become a research hotspot in recent years, and more and more QKA protocols [12–18] were proposed. However, the cryptanalysis of QKA protocol has not drawn enough attention. As that described by Gao et al. [19], cryptanalysis plays an important role in the development of cryptography, and it estimates a protocol's security level, finds potential loopholes and tries to overcome security issues. In the study of quantum cryptography, quite a few effective attack strategies have been proposed, such as entanglement-swapping attacks [20], channel-loss attacks [21], denial-of-service attacks [22], Trojan horse attacks [23] and participant attacks [24]. Deep learning of those attacks will be helpful for us to design new protocols with high security. In these kinds of attacks, we should pay more attention to the participant attacks. In contrast to an outside attacker, an inside participant, especially in a multi-party quantum cryptographic protocol, usually has more power to attack the protocol for her/his participant identity. Later studies showed that quite a number of quantum cryptographic protocols could not resist participant attacks [25–30].

Recently, Shukla et al. [31] proposed two QKA protocols based on Bell state and Bell measurement, and they claimed that their two protocols were secure against participant attack, and the security could mainly be assured by orthogonal-state-based eavesdropping checking technique. However, according to a widely accepted security definition for a multi-party QKA protocol proposed by Sun et al. [32], we find that Shukla et al.'s three-party QKA protocol is not secure. Any participant in the protocol can directly obtain other two participants' secret keys. More seriously, two dishonest participants in the protocol can conclude to determine the shared key alone. Furthermore, we will show that there is another minor flaw in their two protocols; that is, eavesdroppers can flip any bit of the final key without introducing any error. In the end, some possible improvements are proposed to avoid these flaws.

2 Brief review of Shukla et al.'s three-party QKA protocol

To maintain the integrity of the paper, let us first give a brief review of Shukla et al.'s three-party QKA protocol [31]. In the protocol, three participants Alice, Bob and Charlie want to equally establish a final secret key. Four Bell states $\left|\psi^{+}\right\rangle$, $\left|\psi^{-}\right\rangle$, $\left|\phi^{+}\right\rangle$ and $\left|\phi^{-}\right\rangle$ will be used in the protocol, where, $\left|\psi^{\pm}\right\rangle = \frac{1}{\sqrt{2}}\left(|00\rangle \pm |11\rangle\right)$, $\left|\phi^{\pm}\right\rangle = \frac{1}{\sqrt{2}}\left(|01\rangle \pm |10\rangle\right)$. The details of the protocol are as follows.

Step 1 Alice (Bob, Charlie) generates n EPR pairs which are all in state $\left|\psi^{+}\right\rangle$. Alice (Bob, Charlie) takes one particle from each pair to form sequence p_{A} (p_{B}, p_{C}); the remained particles in each pair compose sequence q_{A} (q_{B}, q_{C}). Alice (Bob, Charlie) randomly generates another binary bit sequence K_{A} (K_{B}, K_{C}) $= \left(K_{\mathrm{A}}^{1}, \ldots, K_{\mathrm{A}}^{n}\right)$ $\left(\left(K_{\mathrm{B}}^{1}, \ldots, K_{\mathrm{B}}^{n}\right), \left(K_{\mathrm{C}}^{1}, \ldots, K_{\mathrm{C}}^{n}\right)\right)$ as her /his secret key.

Step 2 Alice (Bob, Charlie) prepares $n/2$ EPR pairs which are all in state $\left|\psi^{+}\right\rangle$ as decoy photons. Then Alice (Bob, Charlie) concatenates these decoy photons with sequence q_{A} (q_{B}, q_{C}) to get sequence q'_{A} $\left(q'_{\mathrm{B}}, q'_{\mathrm{C}}\right)$. Subsequently, Alice (Bob, Charlie) applies a permutation operator $(\Pi_{2n})_{\mathrm{A}}$ $((\Pi_{2n})_{\mathrm{B}}$, $(\Pi_{2n})_{\mathrm{C}})$ on the sequence q'_{A} $\left(q'_{\mathrm{B}}, q'_{\mathrm{C}}\right)$ to get sequence q''_{A} $\left(q''_{\mathrm{B}}, q''_{\mathrm{C}}\right)$ and then sends the new sequence to Bob (Charlie, Alice).

Step 3 Bob (Charlie, Alice) sends an authentic acknowledgment of receipt to Alice (Bob, Charlie) through an ordinary public communications channel. As that described by Bennett and Brassard [33], the channel is assumed to be susceptible to eavesdropping but not to the injection or alteration of messages. Alice (Bob, Charlie) announces the details of permutation operator $(\Pi_{2n})_{\mathrm{A}}$ $((\Pi_{2n})_{\mathrm{B}}$, $(\Pi_{2n})_{\mathrm{C}})$. Bob (Charlie, Alice) computes error rate. If all three error rates are found to be within a tolerable limit, they continue to the next step, otherwise they stop the protocol. In a real-life quantum cryptographic system, the photons in the transmission will inevitably interact with environment. The tolerable limit tells us the theoretical bound of error rate, and a quantum cryptographic protocol can tolerate. The limit mainly depends on the type of protocol and the way of classical post-processing. Gottesman and Lo showed that BB84 protocol [33] with two-way classical communications during post-processing can tolerate a bit error rate of up to 18.9 %, while the BB84 protocol with one-way classical communications only can tolerate a bit error rate of 11.1 %. A similar six-state QKD protocol with two-way classical communications can tolerate a bit error rate of up to 26.4 % [34].

Step 4 After having discarded all decoy photons, according to the ith bit K_{B}^{i} $\left(K_{\mathrm{C}}^{i}, K_{\mathrm{A}}^{i}\right)$, Bob (Charlie, Alice) performs I or X on the ith particle in q_{A} (q_{B}, q_{C}) to obtain a new sequence r_{B} (r_{C}, r_{A}). Bob (Charlie, Alice) prepares another $n/2$ EPR pairs which are all in state $\left|\psi^{+}\right\rangle$ as decoy photons. Bob (Charlie, Alice) concatenates these $n/2$ EPR pairs with r_{B} (r_{C}, r_{A}) and then applies $(\Pi_{2n})'_{\mathrm{B}}$ $\left((\Pi_{2n})'_{\mathrm{C}}\right.$, $\left.(\Pi_{2n})'_{\mathrm{A}}\right)$ on the sequence to obtain a new sequence r'_{B} $\left(r'_{\mathrm{C}}, r'_{\mathrm{A}}\right)$. Bob (Charlie, Alice) sends the new sequence to Charlie (Alice, Bob).

Step 5 After having received the authentic acknowledgment of the receipt of sequence r'_{B} $\left(r'_{\mathrm{C}}, r'_{\mathrm{A}}\right)$ from Charlie (Alice, Bob), Bob (Charlie, Alice) announces the coordinates of the decoy photons. Charlie (Alice, Bob) computes error rate. If the computed error rates are found to be within the tolerable limit, Bob (Charlie, Alice) announces the coordinates of the message qubits, otherwise they stop the protocol.

Step 6 After having discarded all decoy photons, according to the ith bit K_{C}^{i} $\left(K_{\mathrm{A}}^{i}, K_{\mathrm{B}}^{i}\right)$, Charlie (Alice, Bob) performs I or Z on the ith particle in r_{B} (r_{C}, r_{A}) to obtain a new sequence s_{C} (s_{A}, s_{B}). Charlie (Alice, Bob) prepares another $n/2$ EPR pairs which are all in state $\left|\psi^{+}\right\rangle$ as decoy photons. Charlie (Alice, Bob) concatenates these $n/2$ EPR pairs with s_{C} (s_{A}, s_{B}) and then applies $(\Pi_{2n})''_{\mathrm{C}}$ $\left((\Pi_{2n})''_{\mathrm{A}}\right.$, $\left.(\Pi_{2n})''_{\mathrm{B}}\right)$on the sequence to obtain sequence s'_{C} $\left(s'_{\mathrm{A}}, s'_{\mathrm{B}}\right)$. Charlie (Alice, Bob) sends the new sequence to Alice (Bob, Charlie).

Step 7 Charlie (Alice, Bob) and Alice (Bob, Charlie) check the security of the transmission as that in **Step 5**.

Step 8 After having discarded all decoy photons, Alice (Bob, Charlie) rearranges the received sequence and then performs Bell state measurements on the particle

pairs in sequences p_A (p_B, p_C) and s_C (s_A, s_B) to obtain other two participants' secret keys.

3 Security analysis of Shukla et al.'s three-party QKA protocol

Shukla et al. claimed that the protocol was secure as it was designed along the line of existing protocol [15] with a modified strategy of eavesdropping checking [35,36]. However, in this section, we will show that Shukla et al.'s three-party QKA protocol is not secure, and the protocol cannot achieve privacy and fairness properties. Then, we will show that there is another minor flaw in Shukla et al.'s two protocols; that is, eavesdroppers can flip any bit of the final key without introducing any error. As that described in Ref. [32], a secure multi-party QKA protocol should satisfy following four security properties.

Correctness Each participant involved in the protocol could get the correct shared key.
Security An outside eavesdropper cannot get any useful information about the final shared key without being detected.
Privacy Each participant in the protocol cannot learn any useful information about other participant's secret key, i.e., the sub-secret keys of the participants can be kept secret in the protocol. In the view of information theory, the probability that each participant can succeed in deducing any one bit of other participant's sub-secret key is 50 %.
Fairness All involved participants are entirely peer entities and can equally influence the final shared key. In the view of information theory, the probability that non-trivial subset of the participants can succeed in determining the shared key alone can be negligible.

3.1 The defect on privacy

We first show that Shukla et al.'s three-party QKA protocol cannot achieve privacy property. In the step 8, Alice (Bob, Charlie) performs Bell-state measurements on the corresponding particle pairs in p_A (p_B, p_C) and s_C (s_A, s_B). If the measurement result is $|\psi^+\rangle$, Alice (Bob, Charlie) can deduce that the first operator applied by Bob (Charlie, Alice) and the second operator applied by Charlie (Alice, Bob) are I and I, respectively. Then Alice (Bob, Charlie) can further deduce that the corresponding bits in Bob's (Charlie's, Alice's) sub-key and Charlie's (Alice's, Bob's) sub-key are 0 and 0, respectively. If the measurement result is $|\psi^-\rangle$, Alice (Bob, Charlie) can deduce that the corresponding bits in Bob's (Charlie's, Alice's) sub-key and Charlie's (Alice's, Bob's) sub-key are 0 and 1, respectively. If the measurement result is $|\phi^+\rangle$, Alice (Bob, Charlie) can deduce that the corresponding bits in Bob's (Charlie's, Alice's) sub-key and Charlie's (Alice's, Bob's) sub-key are 1 and 0, respectively. If the measurement result is $|\phi^-\rangle$, Alice (Bob, Charlie) can deduce that the corresponding bits in Bob's (Charlie's, Alice's) sub-key and Charlie's (Alice's, Bob's) sub-key are 1 and 1, respectively. So it is obviously that the protocol cannot achieve privacy property.

3.2 The defect on fairness

In the next, we will show that any two dishonest participants in the protocol can conclude to determine the shared secret key, and the protocol cannot achieve fairness property. Without loss of generality, we suppose that Alice and Bob are two dishonest participants. In step 4, Alice (Bob) first performs unitary operations on the particles in q_C (q_A) according to the corresponding bit in K_A (K_B) to get r_A (r_B). Alice (Bob) concatenates r_A (r_B) with new prepared $n/2$ decoy photons and then applies $(\Pi_{2n})'_A$ $\left((\Pi_{2n})'_B\right)$on the sequence to obtain r'_A $\left(r'_B\right)$. Alice (Bob) sends r'_A $\left(r'_B\right)$ to Bob (Charlie). In the same time, Charlie generates r'_C and then sends the sequence to Alice. In the end of step 5, Alice and Bob can deduce Charlie's unitary operations through performing Bell-state measurement on the corresponding particle pairs in p_B and r_C. Then they can further deduce the corresponding bit in Charlie's secret key. For example, if Alice and Bob get $\left|\psi^+\right\rangle$, they deduce that Charlie's unitary operation is I, which means that the corresponding bit in Charlie's secret key is 0. If Alice and Bob get $\left|\phi^+\right\rangle$, they deduce that the corresponding bit in Charlie's secret key is 1.

In step 6, if Alice and Bob do not want to determine the shared key alone, they perform I or Z on the corresponding particles in r_C and r_A to get s_A and s_B, respectively. Alice (Bob) prepares $n/2$ decoy photons and then inserts them into s_A (s_B). Alice (Bob) applies $(\Pi_{2n})''_A$ $\left((\Pi_{2n})''_B\right)$ on the mixed sequence to obtain s'_A $\left(s'_B\right)$ and then sends the sequence to Bob (Charlie). In the same time, Charlie performs I or Z on the corresponding particle in r_B to get s_C. After having inserted decoy photons into s_C, Charlie applies $(\Pi_{2n})''_C$ on the mixed sequence to obtain s'_C and then sends the sequence to Alice. In step 8, after having discarded all decoy photons, Alice (Bob, Charlie) can deduce other two participants' secret keys through performing Bell-state measurement on the corresponding particle pairs in p_A (p_B, p_C) and s_C (s_A, s_B). Table 1 shows the relations between Alice's (Bob's, Charlie's) first unitary operations, Bob's (Charlie's, Alice's) second unitary operations and Charlie's (Alice's, Bob's) measurement results.

However, if Alice and Bob want to determine the shared key alone, in the next, we will show how they can do this. We know that Alice and Bob can deduce Charlie's secret key through performing Bell-state measurement on the particle pairs in p_B and r_C in the end of step 5. In step 6, Bob can choose a different unitary operation $U_i^\dagger = U_{2K_C^i} U_{2K_B^i}$ to perform on the ith particle in r_A to get $s_B^\dagger$, and the corresponding particle pair in p_C and $s_B^\dagger$ will be in state $\left(I \otimes U_i^\dagger\right)\left(I \otimes U_{K_A^i}\right)\left|\psi^+\right\rangle$; for the sake of clarity, we use U_0, U_1 and U_2 to represent I, X and Z, respectively. Table 2 shows

Table 1 Relations between Alice's (Bob's, Charlie's) first unitary operations, Bob's (Charlie's, Alice's) second unitary operations and Charlie's (Alice's, Bob's) measurement results

	I (0)	Z (1)
I (0)	$\left\|\psi^+\right\rangle$	$\left\|\psi^-\right\rangle$
X (1)	$\left\|\phi^+\right\rangle$	$\left\|\phi^-\right\rangle$

Alice's (Bob's, Charlie's) first unitary operations are listed in the first column, Bob's (Charlie's, Alice's) second unitary operations are listed in the first row

Table 2 Relations between Alice's secret key, Bob's secret key, Charlie's secret key and Charlie's measurement results after Bob has performed $U_i^\dagger$ on the corresponding particles in sequence r_A

	00	01	10	11
0	$\left\|\psi^+\right\rangle(00)$	$\left\|\psi^-\right\rangle(01)$	$\left\|\phi^+\right\rangle(10)$	$\left\|\phi^-\right\rangle(11)$
1	$\left\|\psi^-\right\rangle(01)$	$\left\|\psi^+\right\rangle(00)$	$\left\|\phi^-\right\rangle(11)$	$\left\|\phi^+\right\rangle(10)$

Charlie's secret key is listed in the first column, Alice's secret key and Bob's secret key are listed in the first row

the relations between Alice's secret key, Bob's secret key, Charlie's secret key and Charlie's measurement results after Bob has performed $U_i^\dagger$ on the ith particle in r_A. After having inserted decoy photons into $s_B^\dagger$, Bob applies $(\Pi_{2n})_B''$ to the mixed sequence to obtain sequence $s_B^{\dagger\dagger}$ and then sends $s_B^{\dagger\dagger}$ instead of s_B' to Charlie. After having checked the security of the transmission through discussing with Bob, Charlie performs Bell-state measurement on the corresponding particle pairs in p_C and $s_B^\dagger$ to deduce other two participants' secret keys.

Through analyzing Table 2, we find that Alice and Bob can totally offset the role of Charlie in the generation of the final key through performing a different unitary operation $U_i^\dagger$ on the ith particle in sequence r_A, the final key is determined by Alice and Bob, Charlie cannot equally influence the final shared key, and the protocol cannot achieve fairness property. We take a generation process of 4-bit key as an example to show the attack; without loss of generality, we suppose that Alice and Bob want to generate a shared key $K = 1111$ alone. Alice first generates a 4-bit sequence 0101 as her secret key, in other words, $K_A = 0101$, $K_B = K \oplus K_A = 1010$. Without loss of generality, we suppose that Charlie's secret key $K_C = 1101$. In step 4, after having discarded all decoy photons, Alice (Bob, Charlie) performs $U_{K_A^i}\left(U_{K_B^i}, U_{K_C^i}\right)$ $(i = 1, 2, 3, 4)$ on the i^{th} particles in q_C (q_A, q_B), where, $K_A^1 = 0, K_A^2 = 1, K_A^3 = 0, K_A^4 = 1$, $K_B^1 = 1, K_B^2 = 0, K_B^3 = 1, K_B^4 = 0$, $K_C^1 = 1, K_C^2 = 1, K_C^3 = 0$ and $K_C^4 = 1$. The states of the corresponding particle pairs in p_B and r_C will be changed to $\left|\phi^+\right\rangle, \left|\phi^+\right\rangle, \left|\psi^+\right\rangle$ and $\left|\phi^+\right\rangle$, respectively. In the end of step 5, Alice and Bob first perform Bell-state measurement on the corresponding particle pairs in p_B and r_C to get Charlie's secret key 1101. In step 6, Bob performs $U_i^\dagger = U_{2K_C^i} U_{2K_B^i}$ on the ith particles in r_A to get sequence $s_B^\dagger$. According to Table 2, we can deduce that the states of the corresponding particle pairs in p_C and $s_B^\dagger$ are $\left|\psi^+\right\rangle, \left|\phi^-\right\rangle, \left|\psi^-\right\rangle$ and $\left|\phi^-\right\rangle$, respectively. After having performed Bell-state measurement on the corresponding particle pairs in p_C and $s_B^\dagger$, Charlie deduces that Alice's secret key and Bob's secret key are 0101 and 0111, respectively. Then Charlie further computes the final shared key $K = (0 \oplus 0 \oplus 1, 1 \oplus 1 \oplus 1, 0 \oplus 1 \oplus 0, 1 \oplus 1 \oplus 1) = 1111$. However, the key has been determined before the execution of the protocol, and Charlie cannot detect the attack.

The above analysis shows that Shukla et al.'s three-party QKA protocol [31] cannot achieve privacy and fairness properties. In the next, we will show there is another minor flaw in Shukla et al.'s two protocols; that is, eavesdroppers can flip any bit of the final key without introducing any error. We also take Shukla et al.'s three-party

QKA protocol as an example to show this flaw, and if an attacker performs U_1 or U_2 on each particle in q''_{A} $(q''_{\mathrm{B}}, q''_{\mathrm{C}})$ or r'_{A} $(r'_{\mathrm{B}}, r'_{\mathrm{C}})$, the state of each decoy photon pair does not change; however, the final states of the corresponding particle pairs in p_{A} $(p_{\mathrm{B}}, p_{\mathrm{C}})$ and s_{C} $(s_{\mathrm{A}}, s_{\mathrm{B}})$ may have been changed. In the end, when Alice (Bob, Charlie) performs Bell-state measurements on the corresponding particle pairs in p_{A} $(p_{\mathrm{B}}, p_{\mathrm{C}})$ and s_{C} $(s_{\mathrm{A}}, s_{\mathrm{B}})$, she/he may obtain a wrong final bit. However, there is not an effective eavesdropping checking strategy to prevent this kind of attacking.

4 Improvements to Shukla et al.'s QKA protocols

To avoid above security flaws we discussed in the above section, we propose following possible improvements to the protocols. In step 4 of Shukla et al.'s second protocol, after having performed I or X on the corresponding particle in q_{A} $(q_{\mathrm{B}}, q_{\mathrm{C}})$, Bob (Charlie, Alice) randomly chooses another additional unitary operation I or X to perform on the ith particle. In step 6, after having discarded all decoy photons, Charlie (Alice, Bob) still performs I or X on the ith particle in the received sequence if K^i_{C} $\left(K^i_{\mathrm{A}}, K^i_{\mathrm{B}}\right)$ is 0 or 1. In step 8, Alice (Bob, Charlie) first announces the details of the additional unitary operation. After having known the details of other two participants' additional unitary operation, Alice (Bob, Charlie) announces the coordinates of the message qubits. Alice (Bob, Charlie) rearranges the sequence and then performs same additional unitary operation on the ith particle according to Bob's (Charlie's, Alice's) announcements. Alice (Bob, Charlie) performs Bell-state measurement on the corresponding particle pairs in p_{A} $(p_{\mathrm{B}}, p_{\mathrm{C}})$ and s_{C} $(s_{\mathrm{A}}, s_{\mathrm{B}})$ to obtain exclusive OR values of the other two participants' secret keys. In the end of these two protocols, all participants randomly choose some bits from the generated key for a final eavesdropping checking, and they announce each bit in a random sequential order.

Now, we discuss the security of the improved protocols. The strategy of eavesdropping checking for external attack in our improved protocols is same as that in Shukla et al.'s second protocol. Shukla et al. have already discussed the unconditional security of this eavesdropping checking strategy. So we mainly focus on the fairness and privacy properties of the protocol. We first consider the fairness property. Without loss of generality, we also suppose that Alice and Bob are two dishonest participants. The success of their attack to Shukla et al.'s second protocol depends on following two facts. (1) Alice and Bob can deduce Charlie's unitary operations though measuring the particle pairs in which one particle has been performed unitary operation by Charlie in the end of step 5. (2) Bob can choose appropriate unitary operations to perform on the particles to offset the role of Charlie. In step 4 of our improved protocol, Charlie first performs I (X) on the particle in q_{B} according to his secret key; each EPR pair Bob prepared is in one of the following two states.

$$
\begin{aligned}
(I\otimes I)\left|\psi^{+}\right\rangle_{p^i_{\mathrm{B}}q^i_{\mathrm{B}}} &= I\otimes I\frac{1}{\sqrt{2}}\left(|00\rangle+|11\rangle\right)_{p^i_{\mathrm{B}}q^i_{\mathrm{B}}} = \left(|00\rangle+|11\rangle\right)_{p^i_{\mathrm{B}}r^i_{\mathrm{C}}} = \left|\psi^{+}\right\rangle_{p^i_{\mathrm{B}}r^i_{\mathrm{C}}},\\
(I\otimes X)\left|\psi^{+}\right\rangle_{p^i_{\mathrm{B}}q^i_{\mathrm{B}}} &= I\otimes X\frac{1}{\sqrt{2}}\left(|00\rangle+|11\rangle\right)_{p^i_{\mathrm{B}}q^i_{\mathrm{B}}} = \left(|01\rangle+|10\rangle\right)_{p^i_{\mathrm{B}}r^i_{\mathrm{C}}} = \left|\phi^{+}\right\rangle_{p^i_{\mathrm{B}}r^i_{\mathrm{C}}}.
\end{aligned}
\tag{1}
$$

After having performed an additional unitary operation I or X on the ith particle, the above two EPR states will be changed as follows.

$$I \otimes X \left|\psi^{+}\right\rangle_{p_{\mathrm{B}}^{i} r_{\mathrm{C}}^{i}} = \left|\phi^{+}\right\rangle_{p_{\mathrm{B}}^{i} r_{\mathrm{C}}^{i}},$$
$$I \otimes X \left|\phi^{+}\right\rangle_{p_{\mathrm{B}}^{i} r_{\mathrm{C}}^{i}} = \left|\psi^{+}\right\rangle_{p_{\mathrm{B}}^{i} r_{\mathrm{C}}^{i}}. \quad (2)$$

In the end of step 5, Alice and Bob perform Bell-state measurement on the corresponding particles in p_{B} and r_{C}. If the measurement result Alice and Bob get is $\left|\psi^{+}\right\rangle$, through analyzing the above Eqs. (1–2), they can deduce that Charlie's first (additional) unitary operation may be I (I) or X (X), which means that the corresponding bit in Charlie's sub-key may be 0 or 1. If the measurement result Alice and Bob get is $\left|\phi^{+}\right\rangle$, they can deduce that Charlie's first (additional) unitary operation may be I (X) or X (I), which means that the corresponding bit in Charlie's secret key may be 0 or 1 too. We know that Charlie will not announce the details of the additional unitary operation until the protocol proceeds to step 8. So Alice and Bob cannot obtain Charlie's secret key in the end of step 5, in this situation, Alice and Bob cannot correctly choose appropriate unitary operations to perform on the particles to offset the role of Charlie in the generation of the final key in the step 6, and what Alice and Bob can do is to randomly guess Charlie's first (additional) unitary operation. The probability that non-trivial subset of the participants (Alice and Bob) can succeed in determining the shared key is $(1/2)^n$, and this probability will be exponentially close to 0 with the increase of n. So the protocol achieves fairness property.

In step 8, if each participant Alice (Bob, Charlie) first announces her/his coordinates of the message qubits and then announces the details of the additional unitary operation, Alice and Bob may launch attack as follows. Alice and Bob first perform Bell-state measurement on the corresponding photon pairs in s_{C} and q_{A}, they can deduce Charlie's second unitary operations according to the measurement result and Bob's first and additional unitary operations which have been performed on each particle in step 4, and then they can further deduce Bob's secret key. Then Alice can choose appropriate additional unitary operations to announce to offset the role of Charlie in the generation of the final key. However, we request that each participant Alice (Bob, Charlie) first announces the details of the additional unitary operation before she/he announces the coordinates of the message qubits in step 8, so the attack fails.

Now, let us consider the privacy property. As we adopt same unitary operations in step 4 and step 6, each participant Alice (Bob, Charlie) only can obtain the exclusive OR values of the other two participants' secret keys through performing Bell-state measurements on the corresponding particle pairs in p_{A} (p_{B}, p_{C}) and s_{C} (s_{A}, s_{B}); for example, if the measurement result the participant Alice gets is $\left|\psi^{+}\right\rangle$ ($\left|\phi^{+}\right\rangle$), Alice deduces that the exclusive OR value of the corresponding bits in Bob's secret key and Charlie's secret key is 0(1), where the bit 0 means that the corresponding bits in Bob's secret key and Charlie's secret key may be 0 (or 1) and 0 (or 1), respectively, the bit 1 means that the corresponding bits in Bob's secret key and Charlie's secret key may be 0 (or 1) and 1 (or 0), respectively, and the probability that Alice can succeed in deducing the corresponding bit in Bob's secret key or Charlie's secret key is only 50%. To the participant Bob or Charlie, we can get similar results. So the protocol achieves privacy property.

In the end of these two protocols, we require all participants randomly choose some bits from the generated key for a final eavesdropping checking, and it is obviously that the eavesdropper who wants to flip any bit of the final key will be detected by this final checking.

5 Conclusions

In summary, we show that Shukla et al.'s [31] three-party QKA protocol is not secure. Any participant in the protocol can directly obtain other two participants' secret keys. More seriously, two dishonest participants in the protocol can conclude to determine the shared key alone. Furthermore, we show that there is another flaw in their two protocols; that is, eavesdroppers can flip any bit of the final key without introducing any error. In the end, some possible improvements are proposed to avoid these flaws.

Acknowledgments The authors would like to thank the anonymous reviewers and editor for their comments that improved the quality of this paper. This work is supported by the National Science Foundation of China (Grant Nos. 61202448 and 61202352) and the National High-Tech Research and Development Program of China (Grant No. 2013AA014001).

References

1. Zhou, N., Zeng, G., Xiong, J.: Quantum key agreement protocol. Electron. Lett. **40**, 1149 (2004)
2. Diffie, W., Hellman, M.: New directions in cryptography. IEEE Trans. Inf. Theory **22**, 644–654 (1976)
3. Ingemarsson, I., Tang, D.T., Wong, C.K.: A conference key distribution system. IEEE Trans. Inf. Theory **28**, 714–719 (1982)
4. Burmester, M., Desmedt, Y.: A secure and efficient conference key distribution system. In: Advances in Cryptology-Eurocrypt'94, pp. 275–286. Springer, Berlin (1994)
5. Steiner, M., Tsudik, G., Waidner, M.: Key agreement in dynamic peer groups. IEEE Trans. Parallel Distrib. Syst. **11**, 769–780 (2000)
6. Bellare, M., Canetti, R., Krawczyk, H.: A modular approach to the design and analysis of authentication and key exchange protocols. In: Proceedings of the 30th Annual Symposium on the Theory of Computing, pp. 419–428. ACM, New York (1998)
7. Bellare, M., Pointcheval, D., Rogaway, P.: Authenticated key exchange secure against dictionary attacks. In: Advances in Cryptology-Eurocrypt'00, pp. 139–155. Springer, Berlin (2000)
8. Bellare, M., Rogaway, P.: Entity authentication and key distribution. In: Advances in Cryptology-Crypto'93, pp. 232-249. Springer, Berlin (1993)
9. Bellare, M., Rogaway, P.: Provably secure session key distribution-the three party case. In: Proceedings of the 27th Annual ACM Symposium on Theory of Computing, pp. 57–66. ACM, New York (1995)
10. Blake-Wilson, S., Johnson, D., Menezes, A.: Key agreement protocols and their security analysis. In: Proceedings of 6th IMA International Conference on Cryptography and Coding, pp. 30–45. Springer, Berlin (1997)
11. Kudla, C.: Paterson, K.G.: Modular security proofs for key agreement protocols. In: Advances in Cryptology-Asiacrypt'05, pp. 549–565. Springer, Berlin (2005)
12. Chong, S.K., Hwang, T.: Quantum key agreement protocol based on BB84. Opt. Commun. **283**, 1192 (2010)
13. Shi, R.H., Zhong, H.: Multi-party quantum key agreement with bell states and bell measurements. Quantum Inf. Process. **12**, 921 (2013)
14. Liu, B., Gao, F., Huang, W., Wen, Q.Y.: Multiparty quantum key agreement with single particles. Quantum Inf. Process. **12**, 1797 (2013)
15. Yin, X.R., Ma, W.P., Liu, W.Y.: Three-party quantum key agreement with two-photon entanglement. Int. J. Theor. Phys. **52**, 3915 (2013)

16. Huang, W., Wen, Q.Y., Liu, B., Gao, F., Sun, Y.: Quantum key agreement with EPR pairs and single-particle measurements. Quantum Inf. Process. **13**, 649 (2014)
17. Huang, W., Su, Q., Wu, X., Li, Y.B., Sun, Y.: Quantum key agreement against collective decoherence. Int. J. Theor. Phys. **53**, 2891 (2014)
18. Xu, G.B., Wen, Q.Y., Gao, F., Qin, S.J.: Novel multiparty quantum key agreement protocol with GHZ states. Quantum Inf. Process. **13**, 2587 (2014)
19. Gao, F., Qin, S.J., Guo, F.Z., Wen, Q.Y.: Cryptanalysis of the arbitrated quantum signature protocols. Phys. Rev. A **84**, 022344 (2011)
20. Zhang, Y.S., Li, C.F., Guo, G.C.: Comment on "quantum key distribution without alternative measurements" [Phys. Rev. A 61, 052312 (2000)]. Phys. Rev. A **63**, 036301 (2001)
21. Wójcik, A.: Eavesdropping on the "ping-pong" quantum communication protocol. Phys. Rev. Lett. **90**, 157901 (2003)
22. Cai, Q.Y.: The "ping-pong" protocol can be attacked without eavesdropping. Phys. Rev. Lett. **91**, 109801 (2003)
23. Deng, F.G., Li, X.H., Zhou, H.Y., Zhang, Z.J.: Improving the security of multiparty quantum secret sharing against Trojan horse attack. Phys. Rev. A **72**, 044302 (2005)
24. Gao, F., Qin, S.J., Wen, Q.Y., Zhu, F.C.: A simple participant attack on the brádler-dušek protocol. Quantum Inf. Comput. **7**, 329 (2007)
25. Qin, S.J., Gao, F., Wen, Q.Y., Zhu, F.C.: Cryptanalysis of the Hillery–Bužek–Berthiaume quantum secret-sharing protocol. Phys. Rev. A **76**, 062324 (2007)
26. Gao, F., Wen, Q.Y., Zhu, F.C.: Comment on: "quantum exam" [Phys. Lett. A 350 (2006) 174]. Phys. Lett. A **360**, 748 (2007)
27. Gao, F., Guo, F.Z., Wen, Q.Y., Zhu, F.C.: Comment on "experimental demonstration of a quantum protocol for Byzantine agreement and Liar detection". Phys. Rev. Lett. **101**, 208901 (2008)
28. Song, T.T., Zhang, J., Gao, F., Wen, Q.Y., Zhu, F.C.: Participant attack on quantum secret sharing based on entanglement swapping. Chin. Phys. B **18**, 1333 (2009)
29. Gao, F., Qin, S.J., Wen, Q.Y., Zhu, F.C.: Cryptanalysis of multiparty controlled quantum secure direct communication using Greenberger–Horne–Zeilinger state. Opt. Commun. **283**, 192 (2010)
30. Guo, F.Z., Qin, S.J., Gao, F., Lin, S., Wen, Q.Y., Zhu, F.C.: Participant attack on a kind of MQSS schemes based on entanglement swapping. Eur. Phys. J. D **56**, 445 (2010)
31. Shukla, C., Alam, N., Pathak, A.: Protocols of quantum key agreement solely using Bell states and Bell measurement. Quantum Inf. Process. **13**, 2391 (2014)
32. Sun, Z.W., Zhang, C., Wang, B.H., Li, Q., Long, D.Y.: Improvements on "multiparty quantum key agreement with single particles". Quantum Inf. Process. **12**, 3411 (2013)
33. Bennett, C.H., Brassard, G.: Quantum cryptography: Public key distribution and coin tossing. In: Proceedings of IEEE International Conference on Computers, Systems and Signal Processing, pp. 175-179. IEEE, New York (1984) [Bennett, C.H., Brassard, G.: Quantum cryptography: Public key distribution and coin tossing. Theor. Comput. Sci. **560**, 7 (2014)]
34. Gottesman, D., Lo, H.K.: Proof of security of quantum key distribution with two-way classical communications. IEEE Trans. Inf. Theory **49**, 457–475 (2003)
35. Shukla, C., Pathak, A., Srikanth, R.: Beyond the Goldenberg–Vaidman protocol: secure and efficient quantum communication using arbitrary, orthogonal, multi-particle quantum states. Int. J. Quantum Inf. **10**, 1241009 (2012)
36. Yadav, P., Srikanth, R., Pathak, A.: Two-step orthogonal-state-based protocol of quantum secure direct communication with the help of order-rearrangement technique. Quantum Inf. Process. **13**, 2731 (2014)