International Journal of Theoretical Physics (2019) 58:2834–2846
https://doi.org/10.1007/s10773-019-04167-8

High-Efficiency Three-Party Quantum Key Agreement Protocol with Quantum Dense Coding and Bell States

Wan-Ting He[1] · Jun Wang[1] · Tian-Tian Zhang[1] · Faris Alzahrani[2] · Aatef Hobiny[2] · Ahmed Alsaedi[2] · Tasawar Hayat[2,3] · Fu-Guo Deng[1,2]

Received: 5 December 2018 / Accepted: 24 May 2019 / Published online: 3 June 2019

Abstract

We propose a high-efficiency three-party quantum key agreement protocol, by utilizing two-photon polarization-entangled Bell states and a few single-photon polarization states as the information carriers, and we use the quantum dense coding method to improve its efficiency. In this protocol, each participant performs one of four unitary operations to encode their sub-secret key on the passing photons which contain two parts, the first quantum qubits of Bell states and a small number of single-photon states. At the end of this protocol, based on very little information announced by other, all participants involved can deduce the same final shared key simultaneously. We analyze the security and the efficiency of this protocol, showing that it has a high efficiency and can resist both outside attacks and inside attacks. As a consequence, our protocol is a secure and efficient three-party quantum key agreement protocol.

Keywords Quantum communication · Quantum key agreement · Three-party key agreement · Bell states · Single photons

1 Introduction

Quantum communication provides an unconditionally secure way for the transmission of information, by exploiting the principles in quantum mechanics. In recent decades, this field gains much attention of researchers all over the world. There are many important branches of quantum communication for different tasks, such as quantum key distribution (QKD) [1–3], quantum secure direct communication (QSDC) [4–12], quantum secret sharing (QSS) [13], and so on. QKD supplies a secure way for two remote legitimate parties to create a private

✉ Fu-Guo Deng
fgdeng@bnu.edu.cn

[1] Department of Physics, Applied Optics Beijing Area Major Laboratory, Beijing Normal University, Beijing, 100875, China

[2] NAAM-Research Group, Department of Mathematics, Faculty of Science, King Abdulaziz University, Jeddah, 21589, Saudi Arabia

[3] Department of Mathematics, Quaid-I-Azam University, 45320 Islamabad, 44000, Pakistan

key [1–3]. The parties in QKD can detect the eavesdropper, say Eve, if she monitors their quantum channel, by picking up a subset of their outcomes obtained with two nonorthogonal measuring bases to check eavesdropping. They can then discard the outcomes when they find Eve. Far different from QKD, QSDC gives an absolutely secure approach for two parties to transmit their secret message directly, without producing the private key in advance. The first QSDC scheme was proposed by Long and Liu [4] and it exploits the properties of Bell states and uses a block transmission technique in 2002. Subsequently, Deng, Long, and Liu [5] clarified the standard criterion for QSDC explicitly in 2003, and they proposed an important two-step QSDC protocol by using the Einstein-Podolsky-Rosen photon pair blocks . Recently, these two-step QSDC protocols [4, 5] were experimentally implemented by two groups [6, 7]. In 2004, Deng and Long [8] introduced the first QSDC protocol based on a sequence of single photons, called quantum one-time pad scheme which has been recently experimentally demonstrated by Hu et al. [9] in a noisy environment with frequency coding. In 2017, Wu et al. [10] proposed a high-capacity QSDC protocol with two-photon six-qubit hyperentangled states. QSS is used to share a secret key among some agents of a boss [13], in which the agents can reconstruct the secret if and only if they collaborate. QSS has a higher requirement than QKD because a potentially dishonest agent may injure the benefit of the boss. The inside attacks will increase largely the difficulty of the design of QSS schemes in practical applications.

Quantum key agreement (QKA)[14–36] is another interesting multiparty quantum communication. It is an extension of classical key agreement [37], by utilizing the principles of quantum mechanics, i.e., quantum no-cloning theorem, Heisenberg uncertainty principle, and the principle of quantum state superposition. Ways of generating the shared keys are different in QKA and QKD protocols. In a QKA protocol, a classical final shared key is derived by two (or more) parties as a function of information contributed by each of them [14], it is generated by all the participants together. But in a QKD protocol, a shared key is decided by one participant and distributed to others. A secure QKA protocol needs to satisfy four properties [15]: correctness, security, fairness, and privacy property. The correctness property requires that each participant should receive the correct secret key. The security property requires that outside eavesdroppers cannot obtain the shared key without being detected. The fairness property indicates that non-trivial subsets of the involved participants can determine the final shared key. And the privacy property requires that the sub-secret key of each participant should not be learned by any other [15]. Those properties make the QKA protocols more suitable for open insecure channels, and make it have the extensive application prospect in open network [16]. Also, they increase the difficulty of designing a secure QKA protocol. In 2004, Zhou et al. [17] proposed a QKA protocol which contains two users and utilizes the quantum teleportation technique. In 2010, Chong et al. [18] proposed a QKA protocol based on the BB84 protocol, utilizing a delayed measurement technique. Nevertheless, only two users are involved in the above protocols [17, 18]. In 2013, Shi et al. [19] presented a multi-party QKA (MQKA) protocol by using the entanglement swapping technique. In the same year, Liu et al. [20] pointed out that Shi et al.'s protocol is not a fair QKA protocol and then put forward another MQKA protocol with single particles. In 2014, a MQKA protocol using Bell state and Bell measurement was proposed by Shukla et al. [21]. In 2016, two MQKA protocol were proposed by Sun et al. with cluster state [22] and six-qubit states [23] respectively. In the same year, Liu et al. [14] calculated the previous MQKA protocols into three categories: the complete-graph-type MQKA protocols [16, 20], the circle-type MQKA protocols [15, 19, 21–24], and the tree-type MQKA protocol [25]. A circle-type protocol has a higher qubit efficiency than the complete-graph-type one. But in Ref. [25], they described an instructional mode of the attacks to the circle-type

MQKA protocols, and claimed that those previous MQKA protocol cannot resist the collusive participant attacks (or called inside attacks). In 2016, Huang et al. [26] proposed a QKA protocol in travelling-mode utilizing single photons and rotation operations. In 2017, Cai et al. [27] presented another MQKA protocol with rotation operations. Subsequently, Cao et al. [28] proposed a MQKA protocol based on quantum search algorithm. Recently, Huang et al. [29] put forward a MQKA protocol with collective detection and rotation operations. Up to now, many other different QKA protocols have been proposed [30–36].

In this paper, we propose a secure and efficient three-party QKA protocol with Bell states, following partially the idea in previous studies [15, 24]. In our protocol, the idea of quantum dense coding is used [38]. Four unitary operations are used as encoding operations, which are performed by each participant on passing photons. The passing photons contains two parts, the first quantum qubits of Bell states and the single-photon states. Our protocol can prevent dishonest participants learning any useful information about other's sub-secret key. It can successfully resist both outside attacks and inside attacks. At the end of this protocol, all participants involved can deduce the final shared key simultaneously with very little information about the positions of those single photons announced by others. Moreover, by using the dense coding method, this protocol also prosesses a high efficiency.

2 High-Efficiency Three-Party QKA Protocol

In this QKA protocol, three participants, say Alice, Bob, and Charlie, cooperate to establish a final shared key. The two-photon polarization-entangled Bell states and some single-photon polarization states will be used in our protocol. Four Bell states can be expressed as:

$$\begin{aligned} \left|\phi^{\pm}\right\rangle &= \frac{1}{\sqrt{2}}\left(|00\rangle \pm |11\rangle\right), \\ \left|\psi^{\pm}\right\rangle &= \frac{1}{\sqrt{2}}\left(|01\rangle \pm |10\rangle\right), \end{aligned} \tag{1}$$

where $|0\rangle$ and $|1\rangle$ respectively present the horizontal and vertical polarization states of the single photon. They form a complete orthogonal basis, called Z basis. $|+\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)$ and $|-\rangle = \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)$ form another complete orthogonal basis, called X basis. We code the two-photon Bell state $\left|\phi^{+}\right\rangle$ as '00', $\left|\phi^{-}\right\rangle$ as '01', $\left|\psi^{+}\right\rangle$ as '10', $\left|\psi^{-}\right\rangle$ as '11'. Furthermore, we code the single-photon state $|0\rangle$ as '0', $|1\rangle$ as '1'.

In our protocol, according to the idea of quantum dense coding [38], we use four unitary operations $U_{00} = I$, $U_{01} = \sigma_z$, $U_{10} = \sigma_x$ and $U_{11} = i\sigma_y$ as the encoding operations. Here σ_z, σ_x, σ_y are the Pauli matrices. If we choose to perform one of those local unitary operations on the first quantum bit of the two-photon system in the state $\left|\phi^{\pm}\right\rangle$ or $\left|\psi^{\pm}\right\rangle$, the transformation of those Bell states can be summarized in Table 1. For single-photon states $|0\rangle$ and $|1\rangle$, their transformation by the those operations can be shown in Table 2.

We assume that the classic channel is authenticated in our protocol, and we utilize the block transmission technique, which was first proposed by Long et al. [4], to ensure the

Table 1 The transformation of four Bell states $\left|\psi^{\pm}\right\rangle$ and $\left|\phi^{\pm}\right\rangle$ by the unitary operations U_{00}, U_{01}, U_{10} and U_{11} performed on the first quantum bits

	$U_{00} \otimes I$	$U_{01} \otimes I$	$U_{10} \otimes I$	$U_{11} \otimes I$
$\left\|\phi^{\pm}\right\rangle$	$\left\|\phi^{\pm}\right\rangle$	$\left\|\phi^{\mp}\right\rangle$	$\left\|\psi^{\pm}\right\rangle$	$\left\|\psi^{\mp}\right\rangle$
$\left\|\psi^{\pm}\right\rangle$	$\left\|\psi^{\pm}\right\rangle$	$\left\|\psi^{\mp}\right\rangle$	$\left\|\phi^{\pm}\right\rangle$	$\left\|\phi^{\mp}\right\rangle$

Table 2 The transformation of two single-photon states $|0\rangle$ and $|1\rangle$ by the unitary operations U_{00}, U_{01}, U_{10} and U_{11}

	U_{00} (U_{01})	U_{10} (U_{11})
$\|0\rangle$	$\|0\rangle$	$\|1\rangle$
$\|1\rangle$	$\|1\rangle$	$\|0\rangle$

security of transmission. Three participants Alice, Bob and Charlie want to establish a final shared key K. Alice, Bob and Charlie first generate some random bit strings K_A, K_B and K_C as their secret bit strings (or called their sub-secret keys), which can be expressed as:

$$\begin{aligned} K_A &= (a_1, a_2, \ldots, a_n), \\ K_B &= (b_1, b_2, \ldots, b_n), \\ K_C &= (c_1, c_2, \ldots, c_n). \end{aligned} \tag{2}$$

Here a_i,b_i,$c_i \in$\{00,01,10,11\},$i = 1,2,\ldots n$. So the length of the each bit string is $2n$.

The illustration of our three-party QKA protocol are shown in Fig. 1. They can be described in detail as follows.

(Step 1) Alice (Bob, Charlie) prepares m two-photon systems S_A (S_B, S_C) in the maximally entangled state $|\phi^+\rangle$ and divides these particles into two ordered sequences, denoted as S_{A1} and S_{A2} (S_{B1} and S_{B2}, S_{C1} and S_{C2}), respectively. Note that, these particles in S_{A1} (S_{B1}, S_{C1}) are the first qubits of the systems in $|\phi^+\rangle$, and these particles in S_{A2} (S_{B2}, S_{C2}) are the second qubits of the systems in $|\phi^+\rangle$. Alice (Bob, Charlie) prepares kn single photons, which are randomly in the state $\{|0\rangle, |1\rangle, |+\rangle, |-\rangle\}$, as the decoy photons. Then, he (she) inserts randomly those decoy photons into the sequence S_{A1} (S_{B1}, S_{C1}) and sends the sequence to Bob (Charlie, Alice) through the quantum channel.

(Step 2) After confirming that Bob (Charlie, Alice) has received the sequence, Alice (Bob, Charlie) announces the positions of the decoy photons and the corresponding basis (Z basis or X basis) for the measurement on each decoy photon. Bob (Charlie, Alice) picks out and measures the decoy photons according to the announcement of Alice (Bob, Charlie). They compare the measurement results with the initial states of the decoy photons. If the error rate exceed the threshold, they abort the protocol; otherwise, they continue their quantum communication to the next step.

Certainly, Bob (Charlie, Alice) should exploit the complex eavesdropping-checking process [39, 40] to prevent an eavesdropper, say Eve, to eavesdrop the quantum communication with Trojan horse attack in this step. As shown in Ref. [40], he should let each photon received pass through a filter with which only the wavelengths close to the operating one can be let in, which is used to filter out Eve's invisible photons and avoid the invisible photon eavesdropping scheme with which Eve utilizes the fact that the single-photon detector is only sensitive to the photons with a special wavelength. Moreover, Bob (Charlie, Alice) should use a photon number splitter (PNS: 50/50), which is used to divide each signal into two pieces for some of the decoy photons, to defeat the delay-photon Trojan horse attack [40].

(Step 3) Bob (Charlie, Alice) randomly inserts l single photons in the state $|0\rangle$ into S_{A1} (S_{B1}, S_{C1}) to form a new sequence S^1_{A1} (S^1_{B1}, S^1_{C1}). Note that, $m + l = n$, n is the half length of the secret bit strings, and l accounts for a very small percentage of

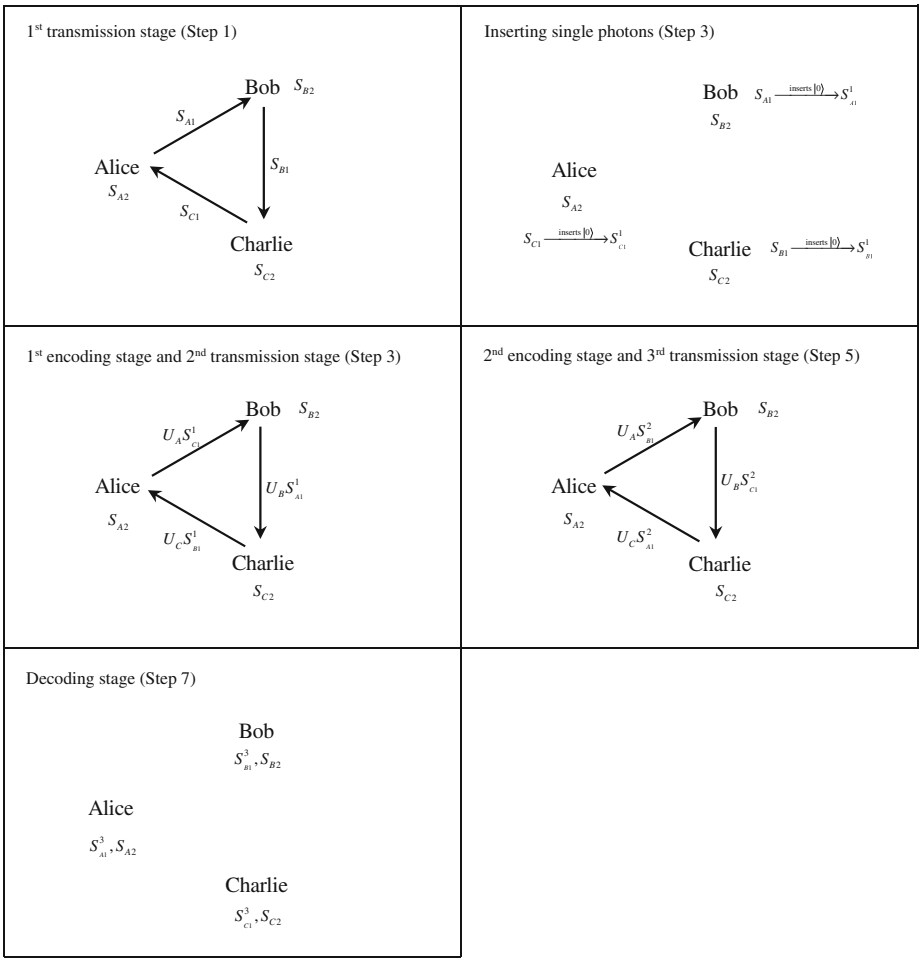

Fig. 1 The illustration of our three-party QKA protocol. U_A (U_B, U_C) denotes the unitary operations performed by Alice (Bob, Charlie) according to his (her) secret bit string K_A (K_B, K_C). The solid arrows present the sequence transmitted through the quantum channel with the block transmission technique [4].We ignore the eavesdropping check stages (Step 2, Step 4, Step 6) in this figure for conciseness

n. The purpose of inserting single photons here is to resist the possible attacks from dishonest participants. Then, he (she) performs the unitary operation U_{b_i} (U_{c_i}, U_{a_i}) on each photon in S^1_{A1} (S^1_{B1}, S^1_{C1}) according to his (her) secret bit string K_B (K_C, K_A). For instance, if b_i (c_i, a_i)= 00, Bob (Alice, Charlie) chooses U_{00} to perform on the i th photon of S^1_{A1} (S^1_{B1}, S^1_{C1}). After the local operations, we denote the new sequence as S^2_{A1} (S^2_{B1}, S^2_{C1}). Bob (Charlie, Alice) prepares kn decoy photons which are randomly in the state $\{|0\rangle, |1\rangle, |+\rangle, |-\rangle\}$, and inserts them into the sequence S^2_{A1} (S^2_{B1}, S^2_{C1}). Then, Bob (Charlie, Alice) sends the sequence to Charlie (Alice, Bob).

(Step 4) After confirming that Charlie (Alice, Bob) has received the sequence, they perform the second eavesdropping check. The checking method is same as that in Step 2. If the error rate exceeds the threshold, they abort the protocol; otherwise,

they continue the quantum communication to the next step. Also, Charlie (Alice, Bob) should exploit the complex eavesdropping-checking process [39, 40] to prevent Eve to eavesdrop the quantum communication with Trojan horse attack.

(Step 5) After picking out the decoy photons, Charlie (Alice, Bob) performs the unitary operation on each photon in S^2_{A1} (S^2_{B1}, S^2_{C1}) according to his (her) secret bit string K_C (K_A, K_B) and form a new sequence S^3_{A1} (S^3_{B1}, S^3_{C1}). The encoding method is same as that in Step 3. Then, Charlie (Alice, Bob) prepares kn decoy photons and inserts them into S^3_{A1} (S^3_{B1}, S^3_{C1}). After that, Charlie (Alice, Bob) sends it back to Alice (Bob, Charlie).

(Step 6) After confirming that Alice (Bob, Charlie) has received the sequence, Alice, Bob and Charlie publicly announce the positions of the single-photon states that he (she) has inserted in Step 3 through the authenticated classic channel. In order to ensure the correctness of this protocol, Alice, Bob and Charlie randomly select a set of positions to check whether each participant has received the correct secret key at the end of this protocol. After that, they perform the third eavesdropping check. The checking method is same as that in Step 4. If the error rate exceeds the threshold, they abort the protocol; otherwise, they continue the quantum communication to the next step.

(Step 7) After picking out the decoy photons, the remaining photons form the sequence S^3_{A1} (S^3_{B1}, S^3_{C1}). Now, Alice (Bob, Charlie) has the sequences S^3_{A1} and S_{A2} (S^3_{B1} and S_{B2}, S^3_{C1} and S_{C2}). Note that the length of the sequence S_{A2} (S_{B2}, S_{C2}) is m, and the length of the sequence S^3_{A1} (S^3_{B1}, S^3_{C1}) is n. Then they come to the decoding stage. For these positions where the single-photon states have been inserted, Alice (Bob, Charlie) measures the photons from sequence S^3_{A1} (S^3_{B1}, S^3_{C1}) in Z basis, and records the bit string of the outcomes as M_a (M_b, M_c). For the other positions, Alice (Bob, Charlie) performs Bell measurement on the corresponding photon pairs from S^3_{A1} and S_{A2} (S^3_{B1} and S_{B2}, S^3_{C1} and S_{C2}), and records the bit string of the Bell state measurement results as M_A (M_B, M_C). Then, Alice (Bob, Charlie) computes $K'_A = M_A \parallel M_a$ ($K'_B = M_B \parallel M_b$, $K'_C = M_C \parallel M_c$), where $\parallel$ presents connecting two strings. After that, Alice (Bob, Charlie) picks out the same positions, as the single-photon state in S^3_{A1} (S^3_{B1}, S^3_{C1}), from the bit string K_A (K_B, K_C). He (She) keeps the first bits of the two bits and moves them to the end of bit sequence. After that, he (she) would get a new bit string K^*_A (K^*_B, K^*_C). Thus, the length of K^*_A (K^*_B, K^*_C) is same as K'_A (K'_B, K'_C). And it is easy to verify that $K^*_A \oplus K'_A = K^*_B \oplus K'_B = K^*_C \oplus K'_C$ according to Tables 1 and 2. Here $\oplus$ denotes the addition module 2.

Finally, for each participant, he (she) can get the same final shared key $K = K^*_A \oplus K'_A = K^*_B \oplus K'_B = K^*_C \oplus K'_C$. Then, they check whether the final shared key from those positions chosen in Step 6 is consistent. If not, they they abort the protocol.

3 Security Analysis

In this section, we analyze the security of our protocol. For QKA protocol, we not only need to consider the attacks from outside eavesdroppers, but also need to consider the inside attacks being done by dishonest participants. Hence, the security analysis of QKA protocols is more complex than that in QKD protocols.

3.1 Outside Attack

Suppose there is an eavesdropper Eve (not the legitimate participants) who wants to steal the final shared key without being detected by the legitimate participants. To achieve this goal, she must obtain participants' sub-secret key through some means. Eve mainly has these attack means: intercept-resend attack, measurement-resend attack, entangle-measure attack and Trojan horse attack. Therefore, if we want to demonstrate the security of our protocol against the outside attacks, we must prove that our protocol can resist all those four attack means. Without loss of generality, we take the situation that the sequence is generated by Alice, and sends to Bob and Charlie orderly for example to describe the security of our QKA protocol.

First, let us consider the intercept-resend attack. Eve intercepts the photons at the end of Step 1, Step 3 or Step 5, and replaces them with her own photons to get the sub-secret key of Bob or Charlie. But she cannot pass the eavesdropping check. Eve couldn't know the information of the decoy photons which are randomly in the state $\{|0\rangle, |1\rangle, |+\rangle, |-\rangle\}$. Therefore, the probability that she will be detected is $(1-\left(\frac{1}{2}\right)^{kn})$. If kn is large enough, Eve will be detected with the probability approaching to 100%.

Second, let us consider the measurement-resending attack. Eve intercepts the photons and measures them at the end of Step 1, Step 3 or Step 5, and then resends them to Bob or Charlie. However, Eve can't distinguish between the target photons and decoy photons before the eavesdropping check process. So She just randomly chooses the measurement bases. As a result, Eve introduces many errors in the eavesdropping stage and exposes herself. The probability that she exposes herself is $(1-\left(\frac{3}{4}\right)^{kn})$ which will approach to 100% when kn is large enough.

Now, let us come to the entangle-measuring attack. Eve intercepts the photons at the end of Step 1, Step 3 or Step 5, and employs a unitary operation on the ancillary photons $|E\rangle$ and the photons she captured.

Suppose the unitary operation is U_E, one can have the relations for the eavesdropping as follows:

$$\begin{aligned} U_E : |0\rangle|E\rangle \rightarrow \quad & |0\rangle|E_{00}\rangle + |1\rangle|E_{01}\rangle, \\ |1\rangle|E\rangle \rightarrow \quad & |0\rangle|E_{10}\rangle + |1\rangle|E_{11}\rangle. \end{aligned} \tag{3}$$

Here $|E_{00}\rangle$, $|E_{01}\rangle$, $|E_{10}\rangle$ and $|E_{11}\rangle$ are pure states determined by U_E. In this protocol, we use the decoy photons randomly in the state $\{|0\rangle, |1\rangle, |+\rangle, |-\rangle\}$ to prevent eavesdropping. At the end of Step 1, Step 3 or Step 5, if Eve use the entangle-measure attack, the states $|+\rangle$, $|-\rangle$ will have the relations:

$$\begin{aligned} U_E : |+\rangle|E\rangle \rightarrow \quad & \frac{1}{2}|+\rangle(|E_{00}\rangle + |E_{01}\rangle + |E_{10}\rangle + |E_{11}\rangle) \\ & + \frac{1}{2}|-\rangle(|E_{00}\rangle - |E_{01}\rangle + |E_{10}\rangle - |E_{11}\rangle), \\ |-\rangle|E\rangle \rightarrow \quad & \frac{1}{2}|+\rangle(|E_{00}\rangle + |E_{01}\rangle - |E_{10}\rangle - |E_{11}\rangle) \\ & + \frac{1}{2}|-\rangle(|E_{00}\rangle - |E_{01}\rangle - |E_{10}\rangle + |E_{11}\rangle). \end{aligned} \tag{4}$$

If Eve wants to introduce no error in the eavesdropping check in Step 2, Step 4 or Step 6, it must satisfy $|E_{01}\rangle = |E_{10}\rangle = 0$ and $|E_{00}\rangle = |E_{11}\rangle$. If not, the probability of Eve being detected is $(1-\left(\frac{1}{2}\right)^{kn})$.

And if Eve uses the entangle-measure attack to entangle the ancillary photons with the first qubits of $\left|\phi^{+}\right\rangle$, and then one will have the relations:

$$U_E : \left|\phi^{+}\right\rangle |E\rangle \rightarrow \quad \frac{1}{\sqrt{2}} \left(|00\rangle |E_{00}\rangle + |10\rangle |E_{01}\rangle + |01\rangle |E_{10}\rangle + |11\rangle |E_{11}\rangle\right). \quad (5)$$

Hence, if Eve wants to introduce no error (not be detected by the legitimate participants), we will have $U_E : \left|\phi^{+}\right\rangle |E\rangle \rightarrow \left|\phi^{+}\right\rangle |E_{00}\rangle$. Her ancillary photons and the encoded photons are in product states. She cannot get any useful information from measuring the ancillary photons. And we will come to the same conclusion when Eve entangles the ancillary photons with other Bell states or single-photon states. Thus we can say that Eve cannot obtain the sub-secret keys without being detected if she takes the entangle-measure attack.

Finally, our protocol may suffer from the Trojan attack, which take use of the invisible photons. The legitimate participants can use the wavelength quantum filters and PNSs to resist this attack [39, 40].

In conclusion, outside eavesdroppers can not obtain the shared key without being detected. According to the definitions in Ref. [15], our protocol can reach the security property of the QKA protocol.

3.2 Inside Attack

The inside attack can also be seen as a violation of the privacy and fairness property [15]. The inside attack is that one or more dishonest participants want to predetermine the final shared key without being detected. There are two cases, having only one dishonest participant, or having two dishonest participants. If this protocol is immune to two participants attack, it is surely immune to one participant attack. So we only need to consider the second situation. Suppose that Alice and Charlie are two dishonest participants, they want to conclude to determine the final shared key. In our protocol, the transmission route forms a circle. Choosing another two dishonest participants finally returns to the same situation.

Alice and Charlie must first get the sub-secret key of Bob K_B before the Step 6. Then they can choose a different unitary operations to preform on the photons and then send back to Bob, or they tell Bob a fake information about the positions of single photons to predetermine the final shared key. In this protocol, the only chance they can get K_B before Step 6 is measuring photons in the S_{A1}^2 which have been performed unitary operations by Bob and the photons in S_{A2} which has been preserved in their hands in the Step 5. But they do not know the positions of single photons which are randomly inserted by Bob, they cannot distinguish which two photons from sequence S_{A2} and S_{A1}^2 form an EPR pair. They cannot get any useful information of K_B to predetermine the final shared key. Thus, all participants involved can equally influence the final shared key. This protocol satisfies the fairness property. And we can see in this protocol, the sub-secret keys of each participant are kept secret during the protocol. Even two dishonest participants cannot get any useful information of the honest participant. Hence this protocol can reach the privacy property. Besides, in Step 6, each participant randomly selects a set of positions to check whether they can conclude the correct secret key at the end of the protocol, ensuring the correctness property of this protocol.

In reality, outside eavesdroppers or inside dishonest participants may hide their attack under the channel noises. The quantum bit error rate introduced by channel noise is about 2%–8.9% [27, 41–45]. But in our protocol, the error rate introduced by outside or inside attack is at least 25%. That is, our protocol will be immune to both the outside and inside

attacks. And it can reach the correctness, security, fairness, and privacy property which a secure QKA protocol need to satisfy.

4 Discussion and Summary

Now, we analyze the efficiency of our protocol, and show that the proposed protocol is efficient. According to the definition proposed by Cabello [46], the efficiency of the quantum protocol is:

$$\eta = \frac{c}{q+b}. \tag{6}$$

Here, c denotes the number of the secret bits (here in QKA protocol, c denotes the length of the classical final shared key), q refers to the number of qubits transmitted in the quantum channel, and b is the number of classical bits exchanged for decoding the message. In our protocol, comparing with n, l and kn are small quantities. So the efficiency of our protocol $\eta \approx \frac{2}{3}$. Comparing with previous QKA protocols under this definition of protocol efficiency, i.e. protocols with single photons [15, 20, 27, 29], protocols with Bell states [21, 24, 30], our protocol possess a higher efficiency in the three-party cases. This is because of dense-coding method which enables one qubit to carry two bits of information being used in the protocol. It should make sense that we use the method of inserting some single photons rather than using control strings and performing rotation operations [26, 27, 29] to prevent the inside attacks. With one encoding operation being performed, participant in those protocols can only encode one bit information on one photon while he can encode two bits in our protocol. In order to decode the message, participants in Ref. [26, 27, 29] need to exchange their control strings which are as long as the final shared key. While in our protocol, they only need to exchange very little information about the positions of those single photons. Thus, our protocol is easier to be implemented with less operations performed and less classical bits exchanged under this three-party condition.

According to the classification standard described in Ref. [14], our protocol is a circle-type QKA protocol. And our protocol is not sensitive to collusive attacks (or called inside attacks) according to the above security analysis. Two-photon entangled states and single-photon states are used as the information carriers in our protocol, they can be prepared and controlled [47–51] even at a great distance. And photon states are also of great use in other fields, such as quantum computation [52–55] and quantum simulation [56, 57]. We utilize the Bell measurement to deduce the final secret key. Four polarization-entangled Bell states can be completely distinguished by the complete Bell state analysis method [58]. Hence, our protocol is feasible under the current technologies and it can be implemented in realistic devices. Certainly, in a practical application of this QKA protocol with a noisy environment, some useful methods should be exploited to depress the influence of noise, such as decoherence-free subspace [59–62], self-error-rejecting transmission [63–66], error correction with ancillary qubits [67], entanglement purification [68–83], and entanglement concentration [84–92].

In summary, we have proposed a three-party quantum key agreement protocol with Bell states and quantum dense-coding method. We have analyzed the security of our protocol, showing that it is immune to both outside and inside attacks. And it can achieve the the correctness, security, fairness, and privacy property at the same time. Further more, compared with other protocols under this three-party condition, it is also a high-efficiency protocol.

Acknowledgments This work is supported by the National Natural Science Foundation of China under Grant No. 11674033, No. 11474026, and No. 11505007.

References

1. Bennett, C.H., Brassard, G.: Quantum cryptography: public key distribution and coin tossing. In: Proceedings of the IEEE International Conference on Computers, Systems and Signal Processing, Bangalore, India, pp. 175–179. IEEE, New York (1984)
2. Ekert, A.K.: Quantum cryptography based on Bell's theorem. Phys. Rev. Lett. **67**, 661–663 (1991)
3. Bennett, C.H., Brassard, G., Mermin, N.D.: Quantum cryptography without Bell's theorem. Phys. Rev. Lett. **68**, 557 (1992)
4. Long, G.L., Liu, X.S.: Theoretically efficient high-capacity quantum-key-distribution scheme. Phys. Rev. A **65**, 032302 (2002)
5. Deng, F.G., Long, G.L., Liu, X.S.: Two-step quantum direct communication protocol using the Einstein-Podolsky-Rosen pair block. Phys. Rev. A **68**, 042317 (2003)
6. Zhang, W., Ding, D.S., Sheng, Y.B., Zhou, L., Shi, B.S., Guo, G.C.: Quantum secure direct communication with quantum memory. Phys. Rev. Lett. **118**, 220501 (2017)
7. Zhu, F., Zhang, W., Sheng, Y.B., Huang, Y.D.: Experimental long-distance quantum secure direct communication. Sci. Bull. **62**, 1519–1524 (2017)
8. Deng, F.G., Long, G.L.: Secure direct communication with a quantum one-time pad. Phys. Rev. A **69**, 052319 (2004)
9. Hu, J.Y., Yu, B., Jing, M.Y., Xiao, L.T., Jia, S.T., Qin, G.Q., Long, G.L.: Experimental quantum secure direct communication with single photons. Light: Sci. Appl. **5**, e16144 (2016)
10. Wu, F.Z., Yang, G.J., Wang, H.B., Xiong, J., Alzahrani, F., Hobiny, A., Deng, F.G.: High-capacity quantum secure direct communication with two-photon six-qubit hyperentangled states. Sci. China-Phys. Mech. Astron. **60**, 120313 (2017)
11. Chen, S.S., Zhou, L., Zhong, W., Sheng, Y.B.: Three-step three-party quantum secure direct communication. Sci. China-Phys. Mech. Astron. **61**, 090312 (2018)
12. Niu, P.H., Zhou, Z.R., Lin, Z.S., Sheng, Y.B., Yin, L.G., Long, G.L.: Measurement-device-independent quantum communication without encryption. Sci. Bull. **63**, 1345 (2018)
13. Hillery, M., Bužek, V., Berthiaume, A.: Quantum secret sharing. Phys. Rev. A **59**, 1829–1834 (1999)
14. Liu, B., Xiao, D., Jia, H.Y., Liu, R.Z.: Collusive attacks to "circle-type" multi-party quantum key agreement protocols. Quantum Inf. Process. **15**, 2113–2124 (2016)
15. 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**, 3411–3420 (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**, 649–663 (2014)
17. Zhou, N., Zeng, G., Xiong, J.: Quantum key agreement protocol. Electron. Lett. **40**, 1149–1150 (2004)
18. Chong, S.K., Hwang, T.: Quantum key agreement protocol based on BB84. Opt. Commun. **283**, 1192–1195 (2010)
19. Shi, R.H., Zhong, H.: Multi-party quantum key agreement with bell states and bell measurements. Quantum Inf. Process. **12**, 921–932 (2013)
20. Liu, B., Gao, F., Huang, W., Wen, Q.Y.: Multiparty quantum key agreement with single particles. Quantum Inf. Process. **12**, 1797–1805 (2013)
21. Shukla, C., Alam, N., Pathak, A.: Protocols of quantum key agreement solely using Bell states and Bell measurement. Quantum Inf. Process. **13**, 2391–2405 (2014)
22. Sun, Z.W., Yu, J.P., Wang, P.: Efficient multi-party quantum key agreement by cluster states. Quantum Inf. Process. **15**, 373–384 (2016)
23. Sun, Z.W., Zhang, C., Wang, P., Yu, J.P., Zhang, Y., Long, D.Y.: Multi-party quantum key agreement by an entangled six-qubit state. Int. J. Theor. Phys. **55**, 1920–1929 (2016)
24. Yin, X.R., Ma, W.P., Liu, W.Y.: Three-party quantum key agreement with two-photon entanglement. Int. J. Theor. Phys. **52**, 3915–3921 (2013)
25. Xu, G.B., Wen, Q.Y., Gao, F., Qin, S.J.: Novel multiparty quantum key agreement protocol with GHZ states. Quantum Inf. Process. **13**, 2587–2594 (2014)
26. Huang, W., Su, Q., Xu, B.J.: Improved multiparty quantum key agreement in travelling mode. Sci. China-Phys. Mech. Astron. **59**, 120311 (2016)
27. Cai, B.B., Guo, G.D., Lin, S.: Multi-party quantum key agreement without entanglement. Int. J. Theor. Phys. **56**, 1039 (2017)
28. Cao, H., Ma, W.P.: Multiparty quantum key agreement based on quantum search algorithm. Sci. Rep. **7**, 45046 (2017)
29. Huang, W., Su, Q., He, Y.H., Fan, F., Xu, B.J.: Efficient multiparty quantum key agreement with collective detection. Sci. Rep. **7**, 15264 (2017)

30. Chong, S.K., Tsai, C.W., Hwang, T.: Improvement on "Quantum key agreement protocol with maximally entangled state". Int. J. Theor. Phys. **50**, 1793–1802 (2011)
31. Huang, W., Wen, Q.Y., Liu, B., Su, Q., Gao, F.: Cryptanalysis of a multi-party quantum key agreement protocol with single particles. Quantum Inf. Process. **13**, 1651–1657 (2014)
32. Huang, W., Su, Q., Wu, X., Li, Y.B., Sun, Y.: Quantum key agreement against collective decoherence. Int. J. Theor. Phys. **53**, 2891–2901 (2014)
33. Shen, D.S., Ma, W.P., Wang, L.L.: Two-party quantum key agreement with four-qubit cluster states. Quantum Inf. Process. **13**, 2313–2324 (2014)
34. He, Y.F., Ma, W.P.: Quantum key agreement protocols with four-qubit cluster states. Quantum Inf. Process. **14**, 3483–3498 (2015)
35. Zhu, Z.C., Hu, A.Q., Fu, A.M.: Participant attack on three-party quantum key agreement with two-photon entanglement. Int. J. Theor. Phys. **55**, 55–61 (2016)
36. He, Y.F., Ma, W.P.: Two-party quantum key agreement based on four-particle GHZ states. Int. J. Theor. Phys. **14**, 1650007 (2016)
37. Diffie, W., Hellman, M.: New directions in cryptography. IEEE Trans. Inf. Theory **22**(6), 644 (1976)
38. Bennett, C.H., Wiesner, S.J.: Communication via one- and two-particle operators on Einstein-Podolsky-Rosen states. Phys. Rev. Lett. **69**, 2881 (1992)
39. Deng, F.G., Li, X.H., Zhou, H.Y., Zhang, Z.: Improving the security of multiparty quantum secret sharing against Trojan horse attack. Phys. Rev. A **72**, 044302 (2005)
40. Li, X.H., Deng, F.G., Zhou, H.Y.: Improving the security of secure direct communication based on the secret transmitting order of particles. Phys. Rev. A **74**, 054302 (2006)
41. Jennewein, T., Simon, C., Weihs, G., Weinfurter, H., Zeilinger, A.: Quantum cryptography with entangled photons. Phys. Rev. Lett. **84**, 4729–4732 (2000)
42. Stucki, D., Gisin, N., Guinnard, O., Ribordy, G., Zbinden, H.: Quantum key distribution over 67 km with a plug and play system. New J. Phys. **4**, 41 (2002)
43. Hughes, R.J., Nordholt, J.E., Derkacs, D., Peterson, C.G.: Practical free-space quantum key distribution over 10 km in daylight and at night. New. J. Phys. **4**, 43 (2002)
44. Beveratos, A., Brouri, R., Gacoin, T., Villing, A., Poizat, J.P., Grangier, P.: Single photon quantum cryptography. Phys. Rev. Lett. **89**, 187901 (2002)
45. Gobby, C., Yuan, Z.L., Shields, A.J.: Quantum key distribution over 122 km of standard telecom fiber. Appl. Phys. Lett. **84**, 3762–3764 (2004)
46. Cabello, A.: Quantum key distribution in the Holevo limit. Phys. Rev. Lett. **85**, 5635 (2000)
47. Yu, R.F., Lin, Y.J., Zhou, P.: Joint remote preparation of arbitrary two- and three-photon state with linear-optical elements. Quantum Inf. Process. **15**, 4785 (2016)
48. Lin, J.Y., He, J.G., Gao, Y.C., Li, X.M., Zhou, P.: Controlled remote implementation of an arbitrary single-qubit operation with partially entangled quantum channel. Int. J. Theor. Phys. **56**, 1085 (2017)
49. Zhou, P., Jiao, X.F., Lv, S.X.: Parallel remote state preparation of arbitrary single-qubit states via linear-optical elements by using hyperentangled Bell states as the quantum channel. Quantum Inf. Process. **17**, 298 (2018)
50. Lv, S.X., Zhao, Z.W., Zhou, P.: Joint remote control of an arbitrary single-qubit state by using a multiparticle entangled state as the quantum channel. Quantum Inf. Process. **17**, 8 (2018)
51. Lv, S.X., Zhao, Z.W., Zhou, P.: Multiparty-controlled joint remote preparation of an arbitrary m-qudit state with d-dimensional Greenberger- Horne- Zeilinger states. Int. J. Theor. Phys. **57**, 148 (2018)
52. Shor, P.W.: In: Proceedings of the 35th Symposium on the Foundations of Computer Science, vol. 124. IEEE, New York (1994)
53. Sheng, Y.B., Zhou, L.: Blind quantum computation with a noise channel. Phys. Rev. A **98**, 052343 (2018)
54. Song, X.K., Ai, Q., Qiu, J., Deng, F.G.: Physically feasible three-level transitionless quantum driving with multiple Schrodinger dynamics. Phys. Rev. A **93**, 052324 (2016)
55. Sheng, Y.B., Zhou, L.: Distributed secure quantum machine learning. Sci. Bull. **62**, 1025 (2017)
56. Buluta, I., Nori, F.: Quantum simulators. Science **326**, 108–111 (2009)
57. Wang, B.X., Tao, M.J., Ai, Q.: Efficient quantum simulation of photosynthetic light harvesting. npj. Quantum Inf. **4**, 52 (2018)
58. Kim, Y.H., Kulik, S.P., Shih, Y.: Quantum teleportation of a polarization state with a complete bell state measurement. Phys. Rev. Lett. **86**, 1370–1373 (2001)
59. Walton, Z.D., Abouraddy, A.F., Sergienko, A.V., Saleh, B.E.A., Teich, M.C.: Decoherence-free subspaces in quantum key distribution. Phys. Rev. Lett. **91**, 087901 (2003)
60. Li, X.H., Deng, F.G., Zhou, H.Y.: Efficient quantum key distribution over a collective noise channel. Phys. Rev. A **78**, 022321 (2008)
61. Deng, F.G., Li, X.H., Li, T.: Quantum error rejection and fault tolerant quantum communication. Acta Phys. Sin. **67**, 130301 (2018)

62. Song, X.K., Zhang, H., Ai, Q., Qiu, J., Deng, F.G.: Shortcuts to adiabatic holonomic quantum computation in decoherence-free subspace with transitionless quantum driving algorithm. New J. Phys. **18**, 023001 (2016)
63. Kalamidas, D.: Single-photon quantum error rejection and correction with linear optics. Phys. Lett. A **343**, 331–335 (2005)
64. Li, X.H., Deng, F.G., Zhou, H.Y.: Faithful qubit transmission against collective noise without ancillary qubits. Appl. Phys. Lett. **91**, 144101 (2007)
65. Li, T., Wang, G.Y., Deng, F.G., Long, G.L.: Deterministic error correction for nonlocal spatial-polarization hyperentanglement. Sci. Rep. **6**, 20677 (2016)
66. Jiang, Y.X., Guo, P.L., Gao, C.Y., Wang, H.B., Alzahrani, F., Hobiny, A., Deng, F.G.: Self-error-rejecting photonic qubit transmission in polarization-spatial modes with linear optical elements. Sci. China-Phys. Mech. Astron. **60**, 120312 (2017)
67. Yamamoto, T., Shimamura, J., Ödemir, S.K., Koashi, M., Imoto, N.: Faithful qubit distribution assisted by one additional qubit against collective noise. Phys. Rev. Lett. **95**, 040503 (2005)
68. Bennett, C.H., Brassard, G., Popescu, S., Schumacher, B., Smolin, J.A., Wootters, W.K.: Purification of noisy entanglement and faithful teleportation via noisy channels. Phys. Rev. Lett. **76**, 722 (1996)
69. Pan, J.W., Simon, C., Brukner, C., Zeilinger, A.: Entanglement purification for quantum communication. Nature **410**, 1067–1070 (2001)
70. Sheng, Y.B., Deng, F.G., Zhou, H.Y.: Efficient polarization-entanglement purification based on parametric down-conversion sources with cross-Kerr nonlinearity. Phys. Rev. A **77**, 042308 (2008)
71. Sheng, Y.B., Deng, F.G.: Deterministic entanglement purification and complete nonlocal Bell-state analysis with hyperentanglement. Phys. Rev. A **81**, 032307 (2010)
72. Sheng, Y.B., Deng, F.G.: One-step deterministic polarization entanglement purification using spatial entanglement. Phys. Rev. A **82**, 044305 (2010)
73. Li, X.H.: Deterministic polarization-entanglement purification using spatial entanglement. Phys. Rev. A **82**, 044304 (2010)
74. Deng, F.G.: One-step error correction for multipartite polarization entanglement. Phys. Rev. A **83**, 062316 (2011)
75. Sheng, Y.B., Zhou, L., Long, G.L.: Hybrid entanglement purification for quantum repeaters. Phys. Rev. A **88**, 022302 (2013)
76. Sheng, Y.B., Zhou, L.: Deterministic polarization entanglement purification using time-bin entanglement. Laser Phys. Lett. **11**, 085203 (2014)
77. Ren, B.C., Du, F.F., Deng, F.G.: Two-step hyperentanglement purification with the quantum-state-joining method. Phys. Rev. A **90**, 052309 (2014)
78. Wang, G.Y., Liu, Q., Deng, F.G.: Hyperentanglement purification for two-photon six-qubit quantum systems. Phys. Rev. A **94**, 032319 (2016)
79. Zhou, L., Sheng, Y.B.: Purification of logic-qubit entanglement. Sci. Rep. **6**, 28813 (2016)
80. Zhou, L., Sheng, Y.B.: Polarization entanglement purification for concatenated Greenberger-Horne-Zeilinger state. Ann. Phys. **10**, 385 (2017)
81. Deng, F.G., Ren, B.C., Li, X.H.: Quantum hyperentanglement and its applications in quantum information processing. Sci. Bull. **62**, 46 (2017)
82. Liu, Z.C., Hong, J.S., Guo, J.J., Li, T., Ai, Q., Alsaedi, A., Hayat, T., Deng, F.G.: Entanglement purification of nonlocal quantum-dot-confined electrons assisted by double-sided optical microcavities. Ann. Phys. (Berlin) **530**, 1800029 (2018)
83. Wang, G.Y., Li, T., Ai, Q., Alsaedi, A., Hayat, T., Deng, F.G.: Faithful entanglement purification for high-capacity quantum communication with two-photon four-qubit systems. Phys. Rev. Appl. **10**, 054058 (2018)
84. Bennett, C.H., Bernstein, H.J., Popescu, S., Schumacher, B.: Concentrating partial entanglement by local operations. Phys. Rev. A **53**, 2046 (1996)
85. Sheng, Y.B., Deng, F.G., Zhou, H.Y.: Nonlocal entanglement concentration scheme for partially entangled multipartite systems with nonlinear optics. Phys. Rev. A **77**, 062325 (2008)
86. Sheng, Y.B., Zhou, L., Zhao, S.M., Zheng, B.Y.: Efficient single-photon-assisted entanglement concentration for partially entangled photon pairs. Phys. Rev. A **85**, 012307 (2012)
87. Deng, F.G.: Optimal nonlocal multipartite entanglement concentration based on projection measurements. Phys. Rev. A **85**, 022311 (2012)
88. Sheng, Y.B., Zhou, L., Zhao, S.M.: Efficient two-step entanglement concentration for arbitrary W states. Phys. Rev. A **85**, 042302 (2012)
89. Ren, B.C., Du, F.F., Deng, F.G.: Hyperentanglement concentration for two-photon four-qubit systems with linear optics. Phys. Rev. A **88**, 012302 (2013)

90. Ren, B.C., Long, G.L.: General hyperentanglement concentration for photon systems assisted by quantum dot spins inside optical microcavities. Opt. Express **22**, 6547–6561 (2014)
91. Li, X.H., Ghose, S.: Hyperentanglement concentration for time-bin and polarization hyperentangled photons. Phys. Rev. A **91**, 062302 (2015)
92. Liu, J., Zhou, L., Zhong, W., Sheng, Y.B.: Logic Bell state concentration with parity check measurement. Front. Phys. **14**, 21601 (2019)