International Journal of Theoretical Physics (2022) 61: 60
https://doi.org/10.1007/s10773-022-05064-3

New Semi-Quantum Key Agreement Protocol Based on the χ-Type Entanglement States

Chao Liu[1] · Shan Cheng[2] · Huan-Huan Li[1] · Li-Hua Gong[1] · Hua-Ying Chen[3]

Received: 26 September 2021 / Accepted: 20 February 2022 / Published online: 9 March 2022

Abstract

A new two-party semi-quantum key agreement protocol is proposed with the four-particle χ-type entanglement states. In this protocol, the shared secret key is generated by using Bell measurement, Z-basis measurement, sequence replacement operations and unitary operations. The one-way semi-quantum key agreement protocol can resist the Trojan horse attack naturally and both participant attack and external one. Compared with other similar two-party quantum key agreement protocols, the presented protocol is relatively efficient since the random collapse of quantum entanglement states reduces the requirement on quantum operations, without involving the four-qubit joint measurements.

Keywords Semi-quantum key agreement protocol · χ-type entanglement state · Quantum cryptography · Quantum communication

1 Introduction

Since S Wiesner presented the seminal concept of quantum cryptography, it has made tremendous progress. As an important branch of quantum cryptography, quantum key agreement (QKA) has been studied widely in recent years. QKA protocol allows all legitimate parties to negotiate the shared key in a secure way. In other words, the final shared secret key is determined by all participants. In 2004, Zhou et al. invented the first original QKA protocol with quantum teleportation [1]. Tsai et al. thought that fairness should also be considered to

✉ Hua-Ying Chen
chenhuaying@ncu.edu.cn

Li-Hua Gong
lhgong@ncu.edu.cn

[1] Department of Electronic Information Engineering, Nanchang University, Nanchang 330031, China

[2] Department of Electrical Engineering, Jiangxi Vocational College of Mechanical & Electrical Technology, Nanchang 330013, China

[3] Department of Physics, Nanchang University, Nanchang 330031, China

exclude malicious participants in QKA and the key should not be controlled by a non-trivial subset of participants [2]. In 2010, based on quantum unitary transform and delay measurement techniques, Chong and Hwang investigated a two-party QKA protocol similar to BB84 [3]. In 2011, Chong et al. designed a quantum key agreement protocol with Bell states to improve quantum bit efficiency and allow Bob to verify the received quantum states [4]. Gao et al. designed a series of key agreement protocols under real channel with noises [5, 6]. Apparently, the QKA protocols in [1–6] only involve two parties and cannot meet the requirement of network communication involving multiple participants. In 2013, Shi and Zhong designed a multi-party QKA (MQKA) protocol based on Bell states and Bell measurement [7]. After analyzing the multiparty QKA protocol in [7], Liu et al. investigated a new multiparty QKA protocol with single particles to avoid participant attack [8]. Based on the QKA protocol in [8], Sun et al. improved the qubit efficiency with two additional quantum unitary operators [9]. In 2014, Shukla et al. proposed two quantum key agreement protocols with Bell state and Bell measurement, where the non-commutativity principle is not intrinsically necessary for unconditional security [10]. In 2016, Liu et al. classified the multi-party QKA protocols and pointed out most multi-party QKA protocols with circle-type are susceptible to the collusion attack by some participants [11]. Some existing MQKA protocols are very vulnerable to the collusion attack. Wang et al. studied the circular MQKA protocol, which can resist the cooperation of dishonest participants [12]. Furthermore, quantum key agreement has been extended to the conference case. In 2021, Zhao et al. put forward a conference key agreement protocol based on continuous-variable QKD, where any nontrivial subset of participants cannot determine the shared key alone [13]. Cao et al. proposed a quantum conference key agreement protocol with three users to inspire the coherent one-way and twin-field QKD protocols [14]. Li et al. analyzed the finite-key for quantum conference key agreement under asymmetric channels [15]. Hereafter, a number of QKA protocols have been put forward based on different quantum states [16–23]. Zhou et al. proposed a semi-quantum key distribution protocol with the four-particle cluster states, which owns higher time efficiency and qubit efficiency [16]. Gong et al. proposed a novel multi-party QKA protocol with G-like states and Bell states to counteract collusion attacks [17]. Based on locally indistinguishable orthogonal product states, Jiang et al. investigated a novel MQKA protocol [18]. Wang et al. put forward a circle-type MQKA protocol with Bell state to resist the collusion attack and other common external attacks [19]. Cai et al. presented an MQKA protocol with five-qubit Brown states and single-qubit measurements to resist common insider and outsider attacks [20]. Based on the four-qubit cluster states, Liu et al. provided a new MQKA protocol for higher efficiency [21]. Zhao et al. proposed a novel MQKA protocol based on entanglement swapping between Bell states and G-like states to ensure security and efficiency [22]. Abulkasim et al. discussed the security of a recently proposed multiparty key agreement protocol, which can remove the vulnerability from such circular-type key agreement protocols [23]. Lin et al. proposed a secure circle-type MQKA protocol with Bell states, which is secure against the collusion attack [24]. χ-type entanglement state, as a basic entanglement state, is different from the four-particle GHZ state [25] or W state. χ -type state with attractive properties has been used to realize different quantum communication tasks [26–28]. For example, Gao designed a QKD protocol with entanglement swapping of the χ-type entanglement states [26]. Yin et al. proposed a blind quantum signature scheme with the χ-type entanglement states [27]. He et al. came up with a QKA scheme with the χ-type entanglement states [28].

Due to the high cost of quantum devices, the qubit efficiency of quantum communication protocol is expected to be improved as much as possible. Nevertheless, the participants in most of the aforementioned protocols possess full quantum abilities, which means expensive quantum facilities and resources involved. It is hard for some participants to afford these valuable quantum devices. To cope with this problem, Boyer et al. introduced the pioneering semi-quantum concept [29]. In 2017, Shukla et al. first proposed a semi-quantum key agreement (SQKA) protocol, controlled deterministic secure communication and quantum dialogue protocol [30]. In 2021, Yang et al. proposed a new one-round semi-quantum-honest SQKA scheme in MSTSA structure without entanglement [31]. Furthermore, most of the entanglement-based QKA protocols simply regarded the collapse of the entanglement state as a secret sequence and did not take advantage of the randomness collapse of the entanglement states. To enhance the qubit efficiency and reduce quantum operations involved, a new efficient semi-quantum key agreement protocol with the χ-type entanglement states is proposed.

The rest of this paper is organized as follows. In Section 2, χ-type entanglement state and basic notations are introduced. In Section 3, the proposed two-party SQKA protocol is described in detail. In Section 4, the protocol security is discussed. In Section 5, some typical two-party SQKA protocols and our protocol are compared. Finally, a brief conclusion is reached.

2 Preliminaries

For convenience, two unitary operations I and X are severally expressed as $I = |0\rangle\langle 0| + |1\rangle\langle 1|$ and $X = |0\rangle\langle 1| + |1\rangle\langle 0|$. Moreover, $\{|0\rangle, |1\rangle\}$ and $\{|+\rangle, |-\rangle\}$ belong to Z-basis and X-basis, respectively, where $|\pm\rangle = \frac{1}{\sqrt{2}}(|0\rangle \pm |1\rangle)$. Four Bell states $\left|\psi^{\pm}\right\rangle = \frac{1}{\sqrt{2}}(|01\rangle \pm |10\rangle)$ and $\left|\phi^{\pm}\right\rangle = \frac{1}{\sqrt{2}}(|00\rangle \pm |11\rangle)$ constitute a complete orthogonal basis. A four-qubit χ-type entanglement state is expressed as [26, 27].

$$\begin{aligned}|\chi^{00}\rangle_{1234} &= \frac{1}{2\sqrt{2}}\Big(|0000\rangle + |0011\rangle - |0101\rangle + |0110\rangle\Big)_{1234} \\ &+ \frac{1}{2\sqrt{2}}\Big(|1001\rangle + |1010\rangle + |1100\rangle - |1111\rangle\Big)_{1234} \\ &= \frac{1}{2}\Big(|\phi^{+}\rangle|00\rangle + |\phi^{-}\rangle|11\rangle - |\psi^{-}\rangle|01\rangle + |\psi^{+}\rangle|10\rangle\Big)_{1234},\end{aligned} \tag{1}$$

where subscripts 1, 2, 3 and 4 denote each particle of a four-qubit χ-type state in order. This state is utilized as a fundamental quantum resource in our SQKA protocol. If Alice performs the Bell measurement on Particles 1 and 2 while Bob performs $Z \otimes Z$-basis $\{|\ 00\rangle, |01\rangle, |10\rangle, |\ 11\rangle\}$ measurement on Particles 3 and 4, this four-particle χ-type entanglement state will collapse into the state $|\phi^{+}\rangle|00\rangle$, $|\phi^{-}\rangle|11\rangle$, $|\psi^{-}\rangle|01\rangle$ or $|\psi^{+}\rangle|10\rangle$ with equal probability. A hash function is depicted as

$$H : \{0,1\}^{L} \rightarrow \{0,1\}^{D}, \tag{2}$$

where L and D denote the length of the input message sequence and that of the output one, respectively. The hash function is helpful to detect the participant attack.

3 SQKA Protocol with the χ-Type Entanglement States

Suppose that two participants, namely Alice and Bob, prepare their respective random 4*N* bits secret key sequences K_A and K_B in advance,

$$K_A = K_{A_0} \| K_{A_1} \| K_{A_2} = k_A^1 k_A^2 \ldots k_A^{4N}, \tag{3}$$

$$K_B = K_{B_0} \| K_{B_1} \| K_{B_2} = k_B^1 k_B^2 \ldots k_B^{4N}, \tag{4}$$

where $k_A^i, k_B^i \in \{0, 1\}$ for $i = 1, 2, \ldots, 4N$, K_{A_j} and K_{B_j} are the sub-secret key sequences of K_A and K_B for $j = 0, 1, 2$, respectively. The symbol $\|$ represents the concatenation of secret key bits. Their secret key sequences are severally divided into *N* groups in order, where each group contains four bits of secret key and its number is defined as $g \in \{1, 2, \ldots, N\}$. Furthermore, they share a secret hash function *H* beforehand. The two participants intend to negotiate a final key K_F, i.e.,

$$K_F = k_{AB}^1 \| k_{A\oplus B}^1 k_{AB}^2 \| k_{A\oplus B}^2 \ldots k_{AB}^{4N} \| k_{A\oplus B}^{4N}, \tag{5}$$

where $k_{A\oplus B}^i = k_A^i \oplus k_B^i$ and $k_{AB}^i = c_g^i \left(k_A^i \times k_B^i\right) + \overline{c_g^i}\left(k_A^i + k_B^i\right)$ for $i = 1, 2, \ldots, 4N$. The symbols ⊕, × and + denote the addition module 2, the logical operations AND and OR, respectively. The subscript *g* in parameter c_g^i represents the group number of the secret key bit k_A^i (k_B^i). Parameter $\overline{c_g^i}$ is defined as the result of performing the logical operation NOT on c_g^i. Parameter c_g^i used to negotiate the key could be obtained due to the random collapse of quantum entanglement states. That's to say, if the *g*-th four-particle χ-type entanglement state collapses into $|\phi^+\rangle|00\rangle$ or $|\phi^-\rangle|11\rangle$, then c_g^i will be 0; otherwise, it will be 1. Thus, a binary sequence *C* could be obtained, $C = c_g^4 c_g^8 \ldots c_g^{4N}$, where $c_g^{4s} \in \{0, 1\}$ for $s = 1, 2, \ldots, N$. The specific description of the presented two-party SQKA protocol is as follows (Fig. 1).

Step. 1 Preparation and distribution of quantum entanglement states

Alice prepares *N* four-qubit χ-type entanglement states, and then she picks out the first two particles of each χ-type entanglement state to form Sequence S_A and the remaining two particles to yield Sequence S_B. Alice randomly selects and prepares enough decoy states in the four quantum states $\{|0\rangle, |1\rangle, |+\rangle, |-\rangle\}$, which are not completely orthogonal to each other. Then she randomly inserts them into Sequence S_B to construct a new Sequence S_B^*. Subsequently, Alice sends Sequence S_B^* over a quantum channel to Bob.

Step. 2 Eavesdropping detection

After Bob acknowledges the receipt of the sequence sent by Alice, Alice and Bob run the first round of eavesdropping detection. Alice first announces the locations of the decoy states and the measurement bases matching the decoy states via an authenticated classical communication channel. Subsequently, Bob randomly selects the decoy states belonging to the Z bases and sends the decoy states back to Alice without any interference with the information released by Alice. After Alice confirms that she received the decoy states sent by Bob, Bob announces

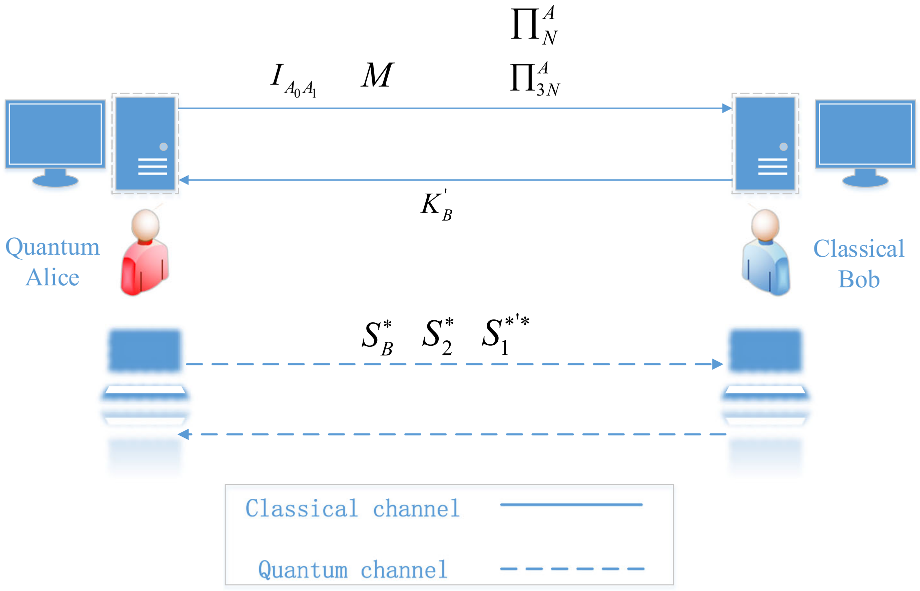

Fig. 1 Execution process of the SQKA protocol

the corresponding arrangement operation via the classical authentication channel. Alice measures the received decoy states accordingly and compares the corresponding measurement results with the initial decoy states. According to the error ratio of the decoy states randomly inserted into the sequence, the malicious eavesdropper in a quantum channel could be detected. If the error ratio of the decoy states is lower than the preset threshold, the key agreement protocol will continue. Otherwise, the key agreement protocol will be terminated. During eavesdropping detection, the preset threshold is determined by transmitting the quantum states in the quantum channel, which is not attacked by malicious eavesdropper. That is to say, only considering the effect of channel noise and the corresponding measurement errors on the transmission of quantum states will make the measurement results inconsistent with the initial states, and the corresponding average error ratio is calculated as a threshold after multiple tests.

Step. 3 Preliminary measurement

Bob first removes the decoy particles involved in the eavesdropping check and restores original Sequence S_B. Then, Alice (Bob) performs Bell basis ($Z \otimes Z$-basis) measurements on Sequence S_A (S_B) simultaneously. The measurement result of Sequence S_A (S_B) is encoded as the corresponding binary Sequence r_{A_0} (r_{B_0}) of length $2N$ according to the encoding rule shown in Table 1.

Step. 4 Qubit sequence transmission

Sequence S_A is divided into two subsequences, where the first qubit and the second qubits in each χ-type entanglement state constitute subsequences S_1 and S_2, respectively. Similar to

Table 1 Encoding rule

Measurement result	Binary encoding
$\|00\rangle$ or $\|\phi^-\rangle$	00
$\|01\rangle$ or $\|\psi^+\rangle$	01
$\|10\rangle$ or $\|\psi^-\rangle$	10
$\|11\rangle$ or $\|\phi^+\rangle$	11
$\|0\rangle$	0
$\|1\rangle$	1

Step. 1, Alice obtains a new Sequence S_2^* with the decoy-state method. Subsequently, Alice transmits Sequence S_2^* to Bob. Like Step. 2, after confirming that Bob has received Sequence S_2^* sent from Alice, they execute the second round of eavesdropping detection. If the quantum channel is secure, they will proceed to the next step. Otherwise, the protocol will be terminated.

Step. 5 Classical basis measurement

Bob first extracts the decoy particles used to detect eavesdropping and restores Sequence S_2. Alice (Bob) performs the classical basis (Z-basis) measurements on the quantum states in Sequence S_1 (S_2). According to the coding rule shown in Table 1, the measurement result of Sequence S_1 (S_2) is encoded as the corresponding binary Sequence r_{A1} (r_{B1}) of length N.

Step. 6 Encoding operation

Alice first implements the quantum unitary operations on the remaining Sequence S_1 according to her secret key K_{A_2} to obtain a new sequence S_1^*. If K_{A2}^i is equal to 0, Alice performs the unitary operation I on the i-th particle in Sequence S_1; Otherwise, Alice performs the unitary operation X. Besides, she selects a permutation operator $\prod_N^A$ to rearrange Sequence S_1^* to acquire a new Sequence $S_1^{*'}$ before inserting decoy particles. Similarly, Alice acquires a new Sequence $S_1^{*'*}$ with the decoy-state method. Subsequently, Alice sends $S_1^{*'*}$ to Bob. Similarly, after Bob confirms the receipt of Sequence $S_1^{*'*}$ sent by Alice, two participants perform the third round of eavesdropping check. If the qubit transmission is insecure, the protocol will be aborted. Otherwise, they will proceed to the next step.

Step. 7 Generation of the final secret key

Similar to Step. 5, Bob first discards the decoy particles and performs Z-basis measurement on Sequence $S_1{*'}$. The measurement result of Sequence $S_1{*'}$ is encoded as binary bit Sequence r_{B_2} of length N. The encoding rule is same as that in Step. 5. Bob calculates Sequence $K_B^{'} = K_B \oplus r_B$, where $r_B = r_{B_0} \| r_{B_1} \| r_{B_2}$. Meanwhile, Alice could obtain Sequence $K_A^{'}$, where $K_A^{'} = K_{A_0A_1}^{'} \| K_{A_2}^{'}$, Sequence $K_{A_0A_1}^{'} = (K_{A_0} \| K_{A_1}) \oplus (r_{A_0} \| r_{A_1})$ and Sequence $K_{A_2}^{'} = K_{A_2} \oplus C$. She rearranges Sequence $K_{A_0A_1}^{'}$ to obtain a new sequence $I_{A_0A_1}$ with a random permutation operator $\prod_{3N}^{A}$. The first d bits in Sequence $K_{A}^{'}$ are defined as $K_{A}^{'d}$. Furthermore, Alice needs to compute a key check value M defined as $M = H\left(K_{A}^{'}\right) \oplus K_{A}^{'d}$, where $H\left(K_{A}^{'}\right)$ represents the hash value of $K_{A}^{'}$ and suppose its corresponding number of bits is d. With the classical authenticated communication channel, Alice first sends $I_{A_0A_1}$ and M to Bob. Next, Bob sends $K_{B}^{'}$ to Alice in a same way. Subsequently, Alice announces the random permutation operators $\prod_{3N}^{A}$ and $\prod_{N}^{A}$. Hence, Alice and Bob negotiate the final shared key K_F.

4 Security Analysis

In general, participant attacks and outsider attacks should be taken into account.

4.1 Participant Attack

Participant attack refers to the malicious participants in the SQKA protocol attempt to control the final agreement key independently without being detected.

Assuming that Alice is a malicious participant and she attempts to control the ultimate shared secret key independently. In this case, she needs to crack the secret key of Bob before sending the relevant key information. Nevertheless, before publishing $K_{B}^{'}$ to Alice, Bob receives the key check value M and the result of $I_{A_0A_1}$ rearranged with the permutation operator $\prod_{3N}^{A}$. That's to say, if Alice tries to control the shared secret key sequence, she only changes the predetermined permutation operators $\prod_{3N}^{A}$ and $\prod_{N}^{A}$ after Bob publishes Sequence $K_{B}^{'}$. However, Bob could detect Alice's malicious attack with the key check value, including the hash value $H\left(K_{A}^{'}\right)$ published previously. For the hash function, given a deterministic input x and its hash value $H(x)$, it is hard to find another input value x' different from x to satisfy the condition such that $H(x) = H(x')$. Thus, Bob could recalculate $H^{'}\left(K_{A}^{'}\right)$ and compare it with that published by Alice. Therefore, the malicious participant Alice could not perform the participant attack successfully.

Suppose that Bob is a malicious participant. It is similar to the case of malicious participant Alice. Only after Bob announces Sequence $K_{B}^{'}$ containing his secret key sequence K_B to Alice, could he acquire the permutation operators $\prod_{3N}^{A}$ and $\prod_{N}^{A}$. Hence, Bob cannot control the final shared key independently either.

4.2 Outsider Attack

The disclosure of $K_{B}^{'}$ does not influence the confidentiality of the secret key K_B if r_B is kept secret. Similarly, the confidentiality of the secret key $K_{A_0} \| K_{A_1}$ is insusceptible to the disclosure of $I_{A_0A_1}$. Furthermore, the publication of the key check value M does not affect the privacy of Sequence $K_{A}^{'}$. Even if Eve acquires Sequence $K_{A}^{'}$, she could not obtain Sequence K_A, since the corresponding measurement results of the χ-type entanglement states are unknown for her. Thus, Eve has to eavesdrop on the measurement result of partial particles belonging to the χ-type entanglement states to obtain the final shared key. The common attack types of QKD include intercept-send attack, measure-replay attack, entangle-measure attack, Trojan horse attack, and so on.

4.2.1 Trojan Horse Attacks

Since each photon can only be transmitted in quantum channel once, the presented SQKA protocol is congenitally free from two kinds of Trojan horse attacks. In other words, the invisible photon eavesdropping (IPE) Trojan attack and the delayed photon Trojan attack are ineffective for this protocol.

4.2.2 Measure-Resend Attack

Supposed that Eve performs the measure-resend attack on the particles in Sequences S_B^*, S_2^* and $S_1^{*'*}$, respectively. However, before the first round of eavesdropping check, Eve does not know the positions and the corresponding measurement bases of the decoy particles. If Eve performs $Z \otimes Z$-basis measurements on the two unmatched particles, then the correct measurement result of Sequence S_B will not be obtained. If Eve measures a decoy particle with a wrong measurement basis, then the eavesdropping action will be detected with the probability of 0.5 in the first round of eavesdropping check averagely. Obviously, if Eve chooses the correct measurement basis, she will pass the eavesdropping check. Statistically, the probability of Eve passing the eavesdropping check is 0.75 for each decoy particle. If the quantum channel is secure after the first round of eavesdropping detection, it indicates that Eve has no idea of the information of Bell states in Sequence S_A. The security analyses of the second and the third rounds of eavesdropping detection are similar to that of the first round of eavesdropping detection. Eve does not either have the knowledge about the collapsed results of the Bell states in Step 5, since the protocol is implemented step by step. In other words, she is unaware of the measurement results of Sequence S_2 and the initial states of Sequence S_1. In Step 6, Eve could not derive the sub-secret key Sequence K_{A_2} by directly measuring Sequence $S_1^{*'*}$ either. Therefore, Eve could not obtain any useful information about Sequences K_A and K_B. Furthermore, the improper measurement of Eve will influence the decoy states in Sequences S_B^*, S_2^* and $S_1^{*'*}$, respectively. Therefore the eavesdropping detection could find this kind of attacks with the probability of $1 - 0.75^m$, where m is the number of decoy particles. If m is large enough, the detection probability of the measure-resend attack will approach 1. Hence, the introduced SQKA protocol could resist the measure-resend attack.

4.2.3 Intercept-Resend Attack

The intercept-resend attack means that Eve intercepts the qubit sequences sent by Alice and prepares the corresponding fake sequences to be sent to Bob. Moreover, with the relevant information published by Alice and Bob, Eve measures the intercepted particles in Sequences S_B, S_2 and S_1 correspondingly after the SQKA protocol is implemented. Similar to the security analysis on the measure-resend attack, Eve does not know the locations and the measurement bases of the decoy states in Sequences S_B^*, S_2^* and $S_1^{*'*}$. Because of the fake sequence, Eve could only pass the eavesdropping detection with the probability of 0.5 for each decoy particle averagely. Consequently, the intercept-resend attack will be detected with the probability of $1 - 0.5^m$ during eavesdropping detection. Therefore, Eve could not successfully perform the intercept-resend attack either and obtain the information about the shared secret key.

4.2.4 Entangle-Measure Attack

If Eve wants to execute the entangle-measure attack, she needs to perform the entanglement operation U on the prepared ancillary particles in a state $|E\rangle$ and the target particles sent by Alice. After performing the entanglement operations, Eve resends the particles to Bob immediately. Afterward, when the protocol is finished, Eve performs suitable measurements on the ancillary particles to deduce information about the shared key. At different phases of the protocol, she could intercept and perform the same entanglement operations on three types of particles in different states, including decoy states, χ-type states and Bell states. Nevertheless, Eve is unaware of the positions of the decoy photons, thus she will perform the same entanglement operation U on the decoy particles before each round of eavesdropping detection. Then the four decoy states will become entangled with the ancillary particles to constitute four two-particle entanglement states, respectively.

$$U|0\rangle|E\rangle = a|0\rangle|e_0\rangle + b|1\rangle|e_1\rangle, \tag{6}$$

$$U|1\rangle|E\rangle = c|0\rangle|e_2\rangle + d|1\rangle|e_3\rangle, \tag{7}$$

$$\begin{aligned} U|+\rangle|E\rangle &= \frac{1}{\sqrt{2}}\Big(a|0\rangle|e_0\rangle + b|1\rangle|e_1\rangle + c|0\rangle|e_2\rangle + d|1\rangle|e_3\rangle\Big) \\ &= \frac{1}{2}|+\rangle\Big(a|e_0\rangle + b|e_1\rangle + c|e_2\rangle + d|e_3\rangle\Big) \\ &+ \frac{1}{2}|-\rangle\Big(a|e_0\rangle - b|e_1\rangle + c|e_2\rangle - d|e_3\rangle\Big), \end{aligned} \tag{8}$$

$$\begin{aligned} U|-\rangle|E\rangle &= \frac{1}{\sqrt{2}}\Big(a|0\rangle|e_0\rangle + b|1\rangle|e_1\rangle - c|0\rangle|e_2\rangle - d|1\rangle|e_3\rangle\Big) \\ &= \frac{1}{2}|+\rangle\Big(a|e_0\rangle + b|e_1\rangle - c|e_2\rangle - d|e_3\rangle\Big) \\ &+ \frac{1}{2}|-\rangle\Big(a|e_0\rangle - b|e_1\rangle - c|e_2\rangle + d|e_3\rangle\Big), \end{aligned} \tag{9}$$

where $|e_0\rangle$, $|e_1\rangle$, $|e_2\rangle$ and $|e_3\rangle$ are pure states uniquely determined by U and the coefficients satisfy the conditions such that $|a|^2 + |b|^2 = 1$ and $|c|^2 + |d|^2 = 1$.

If Eve wants to pass the eavesdropping detection methods in Steps 2, 4 and 6, the states of these decoy particles should remain unchanged after Eve performs the entanglement operation U. Thus, the conditions such that $b = c = 0$ and $a|e_0\rangle = d|e_3\rangle$ should be satisfied. That is to say, Eve cannot distinguish the auxiliary particles in states $|e_0\rangle$ and $|e_3\rangle$. As a result, she cannot acquire any useful information about the target particles. Suppose that $a|e_0\rangle = d|e_3\rangle = |e\rangle$, Eqs. (6)–(9) could be rewritten respectively as

$$\begin{cases} U|0\rangle|E\rangle = |0\rangle|e\rangle \\ U|1\rangle|E\rangle = |1\rangle|e\rangle \\ U|+\rangle|E\rangle = |+\rangle|e\rangle \\ U|-\rangle|E\rangle = |-\rangle|e\rangle \end{cases}. \tag{10}$$

Similarly, suppose that Eve also performs the entanglement operation U on the particles in the χ-type states. By taking Particle 4 in the χ-type entanglement state as an example, the four-qubit χ-type state entangled with the ancillary particle will become a five-particle entanglement state, i.e.,

$$\begin{aligned} U|\chi^{00}\rangle_{1234}|E\rangle = & \frac{1}{2}\Big(|\phi^+\rangle|0\rangle + |\psi^+\rangle|1\rangle\Big)_{123}\Big(a|0\rangle_4|e_0\rangle + b|1\rangle_4|e_1\rangle\Big) \\ & +\frac{1}{2}\Big(|\phi^-\rangle|1\rangle - |\psi^-\rangle|0\rangle\Big)_{123}\Big(c|0\rangle_4|e_2\rangle + d|1\rangle_4|e_3\rangle\Big). \end{aligned} \tag{11}$$

Eq. (11) also meets the same condition. It can also be reduced as

$$\begin{aligned} U|\chi^{00}\rangle_{1234}|E\rangle & = \frac{1}{2}\Big(|\phi^+\rangle|00\rangle + |\phi^-\rangle|11\rangle - |\psi^-\rangle|01\rangle + |\psi^+\rangle|10\rangle\Big)_{1234}|e\rangle \\ & = |\chi^{00}\rangle_{1234}|e\rangle. \end{aligned} \tag{12}$$

It could be seen that the collapsed result of the χ-type entanglement state is independent of the measurement result of the ancillary particle. Furthermore, Eve also executes the entangle-measure attack on the particles of Bell state before the second round of eavesdropping detection. Likewise, by considering the second particle in Bell state $|\psi^+\rangle$, the Bell state will become entangled with the ancillary particle to compose a three-qubit entanglement state, i.e.,

$$\begin{aligned} U|\psi^+\rangle_{12}|E\rangle = & \frac{1}{\sqrt{2}}\Big(|0\rangle_1\Big(c|0\rangle_2|e_2\rangle + d|1\rangle_2|e_3\rangle\Big)\Big) \\ & +\frac{1}{\sqrt{2}}\Big(|1\rangle_1\Big(a|0\rangle_2|e_0\rangle + b|1\rangle_2|e_1\rangle\Big)\Big), \end{aligned} \tag{13}$$

where subscripts 1 and 2 denote the first particle and the second one in Bell states, respectively. Apparently, Eq. (13) should satisfy the conditions such that $b = c = 0$ and $a|e_0\rangle = d|e_3\rangle$, and it could be simplified equivalently as

$$U|\psi^+\rangle_{12}|E\rangle = \frac{1}{\sqrt{2}}\left(d|0\rangle_1|1\rangle_2|e_3\rangle + a|1\rangle_1|0\rangle_2|e_0\rangle\right) = |\psi^+\rangle_{12}|e\rangle. \tag{14}$$

It is clear that Bell state is irrelevant to the auxiliary state $|E\rangle$. Thus, Eve could not derive useful information about the measurement results of Sequences S_B, S_2 and $S_1^{*'}$ by only measuring her ancillary particles. Obviously, even if two participants publish Sequences $I_{A_0A_1}$ and $K_B^{'}$, Eve does not know the information about the final shared secret keys either. On the contrary, if the entanglement operation U does not meet the above conditions such that $a|e_0\rangle \neq d|e_3\rangle$, the decoy particles $|+\rangle$ and $|-\rangle$ will be disturbed according to Eqs. (8) and (9). It is apparent that her entangle-measure attack will also be found during eavesdropping detection. Therefore, the presented protocol could also resist the entangle-measure attack.

Table 2 Comparisons among some typical two-party QKA protocols and our protocol

Protocol	QR	QC	NQO	QE (%)
[4]	Single photon	One-way	SPM	16.67
[5]	Cluster state	Two-way	SPUO+FPOM	26.67
[7]	EPR pair	One-way	BM	33.33
[10]	EPR pair	Two-way	SPUO+BM	14.29
[18]	χ-type state	One-way	SPM+BM+SPUO	36.36
[37]	EPR pair	One-way	SPM	16.67
[34]	Cluster state	Two-way	SPUO+FPOM	33.33
[35]	Cluster state	One-way	SPUO + FPOM	30.77
[36]	GHZ state	One-way	SPM+BM+SPUO+CNOT	36.36
Ours	χ-type state	One-way	SPM+BM+SPUO	42.11

QR (quantum resource), NQO (necessary quantum operation), QC (quantum communication), QE (qubit efficiency), SPUO (single-particle unitary operation), SPM (single-particle measurement), FPOM (four-particle orthogonal measurement), CNOT (controlled-NOT) and BM (Bell measurement).

5 Comparison

As described in [32], the qubit efficiency of the QKA protocol can be defined as $\eta = \frac{C}{B+Q}$, where C is the length of the final key, Q is the number of qubits used, and B is the number of classical bits used to generate the final key. To implement the protocol, Alice needs to publish her Sequence $I_{A_0}\ A_1$ (3Nbits), including the sub-secret key sequence and her permutation operators $\prod_{3N}^{A}$ and $\prod_{N}^{A}$. At the same time, Bob also needs to declare his sub-secret key sequence $K_B^{'}$ (4N bits). Therefore, the qubit efficiency [32] of our QKA protocol is $\frac{8}{15+4m/n}$, where n ($N = n$) denotes the number of the χ-type entanglement states employed in the SQKA protocol and 4m denotes the total number of decoy photons in all transmitted quantum sequence. If $m = n$, η will be up to 42.11%. The comparison results among several two-party QKA protocols [4, 7, 10, 33–36] and the presented protocol are compiled in Table 2. The qubit efficiency of our QKA protocol is the highest among these protocols. The qubit efficiency of the protocol in [10] is the lowest. The qubit efficiencies of the protocols in [18, 36] are calculated similarly. The protocols in [5, 10, 34] are two-way communication. Due to the two-way communication transmission, it is necessary to check the Trojan horse attack. Trojan horse attack is a major threat to the two-way communication protocols. Different from the previous QKA protocols [33–36] based on the four-particle entanglement states, our protocol requires single-particle measurements and Bell measurements rather than the four-qubit joint measurements to decode the private key of participants.

6 Conclusion

Based on the properties of the four-qubit χ-type entanglement states, a new two-party semi-quantum key agreement protocol is introduced. It is shown that the proposed semi-quantum key agreement protocol could resist both outsider attack and participant attack. Compared with the existing QKA protocols based on the four-qubit entanglement states, our protocol has a qubit efficiency up to 42.11% due to the random collapse of quantum entanglement state. Furthermore, it is unnecessary for the proposed protocol to involve the four-qubit joint measurements. On the premise of ensuring security, the designed semi-quantum key agreement protocol enhances the qubit efficiency and reduces the consumption of quantum resources.

Acknowledgments This work is supported by the National Natural Science Foundation of China (Grant Nos. 61871205 and 62161025).

Code Availability None.

Data Availability None.

Declarations

Conflict of Interest There are no Conflicts of Interest or Competing.

References

1. Zhou, N., Zeng, G., Xiong, J.: Quantum key agreement protocol. Electron. Lett. **40**(18), 1149–1150 (2004)
2. Tsai, C.W., Hwang, T.: On Quantum Key Agreement Protocol. Technical Report, CS-I-E, NCKU, Taiwan (2009)
3. Chong, S.K., Hwang, T.: Quantum key agreement protocol based on BB84. Opt. Commun. **283**(6), 1192–1195 (2010)
4. Chong, S.K., Tsai, C.W., Hwang, T.: Improvement on "quantum key agreement protocol with maximally entangled states". Int. J. Theor. Phys. **50**(6), 1793–1802 (2011)
5. Gao, H., Chen, X.G., Qian, S.R.: Two-party quantum key agreement protocols under collective noise channel. Quantum Inf. Process. **17**(6), 140 (2018)
6. Yang, Y.G., Gao, S., Li, D., Zhou, Y.H., Shi, W.M.: Two-party quantum key agreement over a collective noisy channel. Quantum Inf. Process. **18**(3), 74 (2019)
7. Shi, R.H., Zhong, H.: Multi-party quantum key agreement with bell states and bell measurements. Quantum Inf. Process. **12**(2), 921–932 (2013)
8. Liu, B., Gao, F., Huang, W., Wen, Q.Y.: Multiparty quantum key agreement with single particles. Quantum Inf. Process. **12**(4), 1797–1805 (2013)
9. Sun, Z., Zhang, C., Wang, B., Li, Q., Long, D.: Improvements on "multiparty quantum key agreement with single particles". Quantum Inf. Process. **12**(11), 3411–3420 (2013)
10. Shukla, C., Alam, N., Pathak, A.: Protocols of quantum key agreement solely using bell states and bell measurement. Quantum Inf. Process. **13**(11), 2391–2405 (2014)
11. 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**(5), 2113–2124 (2016)
12. Wang, P., Sun, Z.W., Sun, X.Q.: Multi-party quantum key agreement protocol secure against collusion attacks. Quantum Inf. Process. **16**(7), 170 (2017)
13. Zhao, W., Shi, R., Feng, Y., Ruan, X.: Conference key agreement based on continuous-variable quantum key distribution. Laser Phys. Lett. **18**(7), 075205 (2021)
14. Cao, X.Y., Gu, J., Lu, Y.S., Yin, H.L., Chen, Z.B.: Coherent one-way quantum conference key agreement based on twin field. New J. Phys. **23**(4), 043002 (2021)
15. Li, Z., Cao, X.Y., Li, C.L., Weng, C.X., Gu, J., Yin, H.L., Chen, Z.B.: Finite-key analysis for quantum conference key agreement with asymmetric channels. Quantum Sci. Technol. **6**(4), 045019 (2021)
16. Zhou, N.R., Zhu, K.N., Zou, X.F.: Multi-party semi-quantum key distribution protocol with four-particle cluster states. Ann. Phys.-Berlin. **531**(8), 1800520 (2019)
17. Min, S.Q., Chen, H.Y., Gong, L.H.: Novel multi-party quantum key agreement protocol with G-like states and bell states. Int. J. Theor. Phys. **57**(6), 1811–1822 (2018)
18. Jiang, D., Xu, G.B.: Multiparty quantum key agreement protocol based on locally indistinguishable orthogonal product states. Quantum Inf. Process. **17**(7), 180 (2018)
19. Wang, S.S., Xu, G.B., Liang, X.Q., Wu, Y.L.: Quantum key agreement with bell states and cluster states under collective noise channels. Quantum Inf. Process. **18**(6), 190 (2019)

20. Cai, T., Jiang, M., Cao, G.: Multi-party quantum key agreement with five-qubit Brown states. Quantum Inf. Process. **17**(5), 103 (2018)
21. Liu, H.N., Liang, X.Q., Jiang, D.H., Xu, G.B., Zheng, W.M.: Multi-party quantum key agreement with four-qubit cluster states. Quantum Inf. Process. **18**(8), 242 (2019)
22. Zhao, X.Q., Zhou, N.R., Chen, H.Y., Gong, L.H.: Multiparty quantum key agreement protocol with entanglement swapping. Int. J. Theor. Phys. **58**(2), 436–450 (2019)
23. Abulkasim, H., Mashatan, A., Ghose, S.: Secure multiparty quantum key agreement against collusive attacks. Sci. Rep. **11**(1), 1–8 (2021)
24. Lin, S., Zhang, X., Guo, G.D., Wang, L.L., Liu, X.F.: Multiparty quantum key agreement. Phys. Rev. A. **104**(4), 042421 (2021)
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**(12), 2587–2594 (2014)
26. Gao, G.: Quantum key distribution using a χ-type state. Int. J. Theor. Phys. **49**(8), 1870–1877 (2010)
27. Yin, X.R., Ma, W.P., Liu, W.Y.: A blind quantum signature scheme with χ-type entangled states. Int. J. Theor. Phys. **51**(2), 455–461 (2012)
28. He, Y.F., Ma, W.P.: Two-party quantum key agreement against collective noise. Quantum Inf. Process. **15**(12), 5023–5035 (2016)
29. Boyer, M., Kenigsberg, D., Mor, T.: Quantum key distribution with classical bob [J]. Phys. Rev. Lett. **99**(14), 140501 (2007)
30. Shukla, C., Thapliyal, K., Pathak, A.: Semi-quantum communication: protocols for key agreement, controlled secure direct communication and dialogue. Quantum Inf. Process. **16**(12), 295 (2017)
31. Yang, J., Li, Z., Wu, J., Zhu, H.: One-round semi-quantum-honest key agreement scheme in MSTSA structure without entanglement. Quantum Inf. Process. **20**(5), 1–17 (2021)
32. Cabello, A.: Quantum key distribution in the Holevo limit. Phys. Rev. Lett. **85**(26), 5635–5638 (2000)
33. He, Y.F., Ma, W.P.: Quantum key agreement protocols with four-qubit cluster states. Quantum Inf. Process. **14**(9), 3483–3498 (2015)
34. Shen, D.S., Ma, W.P., Wang, L.L.: Two-party quantum key agreement with four-qubit cluster states. Quantum Inf. Process. **13**(10), 2313–2324 (2014)
35. Yang, Y.G., Li, B.R., Kang, S.Y., Chen, X.B., Zhou, Y.H., Shi, W.M.: New quantum key agreement protocols based on cluster states. Quantum Inf. Process. **18**(3), 77 (2019)
36. He, Y.F., Ma, W.P.: Two-party quantum key agreement based on four-particle GHZ states. Int. J. Quantum Inf. **14**(01), 1650007 (2016)
37. 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**(3), 649–663 (2014)