Semi-quantum Key Agreement Protocol against Dishonest Third-party with Delegating Quantum Measuring

Yi-Hua Zhou
Beijing University of Technology
Yang Xu (18810526506@163.com)
Beijing University of Technology
Yu-Guang Yang
Beijing University of Technology
Wei-Min Shi
Beijing University of Technology
Ze-Song Chen
Beijing University of Technology

Research Article

Keywords: Semi-quantum protocol, Key agreement, GHZ-like state, Delegating quantum measuring, Single photon detection

Posted Date: April 14th, 2022

DOI: https://doi.org/10.21203/rs.3.rs-1539779/v1

Semi-quantum Key Agreement Protocol against Dishonest Third-party with Delegating Quantum Measuring

Yi-Hua Zhou[1,2], Yang Xu[1,2,*], Yu-Guang Yang[1,2], Wei-Min Shi[1,2], Ze-Song Chen[1,2]

[1] Faculty of Information Technology, Beijing University of Technology, Beijing 100124, China

[2] Beijing Key Laboratory of Trusted Computing, Beijing, 100124, China.

Abstract

In quantum cloud environment, most application protocols have the problems of using a lot of quantum resources, high communication costs, and inability to check the honesty of cloud server. Therefore, a semi-quantum key agreement protocol based on GHZ-like state with a dishonest delegated measuring center is proposed. In our protocol, the application system consists of a quantum cloud server which only needs to prepare GHZ-like states and distributes all the particles to other participants, a quantum measuring center which performs complicated quantum measurement, such as X-base measurement and Bell measurement, and many classical semi-quantum participants which perform key agreement. Our protocol has many advantages. First, our protocol removes the assumption of honest or semi-honest cloud server because the dishonesty of cloud sever can be checked by delegated measuring center and classical semi-quantum participants. Second, the dishonesty of measuring center can also be found by classical semi-quantum participants through joint measurement. Third, only classical semi-quantum participants can obtain random shared key even if quantum cloud server and measuring center are interested in shared keys. Fourth, a large number of participants may be semi-quantum users which saving a lot of quantum resources. Our protocol is especially suitable for applications such as a large number of classical users arbitrarily performing key agreement in a real cloud environment which only need fewer resources, being easy to implement, and controllable. Security analysis and efficiency analysis show that our protocol can not only effectively resist external and internal attacks, but also resist collusion attack, which is more efficient than similar protocols.

Keywords Semi-quantum protocol; Key agreement; GHZ-like state; Delegating quantum measuring; Single photon detection;

Statements and Declarations

The authors have no competing interests to declare that are relevant to the content of this article.

1 Introduction

In 1984, Bennett and Brassard [1] proposed the first quantum key distribution protocol (QKD), which allows two participants to safely share quantum keys by using the laws of quantum mechanics. Since then, quantum key distribution has spurred a number of theoretical and practical researches, and many related QKD protocols have been proposed [2-9]. However, the share key is generally determined unilaterally by a third party or one of the participants in these agreements. Other participants have no contribution to the key, which has many limitations in real-world applications and lacks fairness. Therefore, researchers proposed the Quantum Key Agreement Protocol (QKA). In QKA protocol, participants can fairly negotiate a share key through quantum channel, and each participant's contribution to the key is the same.

In 2004, Zhou et al. [10] proposed the first quantum key agreement protocol, which uses quantum teleportation to generate share keys. Later, Tsai and Hwang [11] pointed out that Zhou et al.'s protocol exists loopholes, and the share key can be determined unilaterally by one-party, which lacks fairness. Liu et al [12] also proposed that the QKA protocol may also be attacked by a man-in-the-middle, leading to information leakage. In 2010, Chong et al. [13] proposed a new QKA protocol based on the BB84

* Corresponding author. Email:18810526506@163.com;
Contributing authors: zhouyh@bjut.edu.cn; yangyang7357@bjut.edu.cn; shiweimin@bjut.edu.cn; zesongchen4ever@gmail.com

protocol and used delay measurement technology to ensure safety. In 2012, Shi et al. [14] proposed the first quantum multi-party key agreement with Bell state and Bell measurement, which expanded the participants of key agreement from two-party to multi-party. But Liu et al. [15] pointed out that in the Shi et al.'s protocol, the shared key can be determined independently by one-party. In 2014, Xu et al. [16] proposed a multi-party quantum key protocol based on GHZ states. The protocol only requires one quantum communication and measurement to obtain a shared key, and it has successfully expanded from two-party to multi-party. In order to improve the utilization of qubits, Shen et al. [17] proposed a quantum key agreement of high qubit efficiency based on four-qubit cluster state, and then more key agreement protocols were proposed [18-22].

However, all the above protocols assume that each participant is equipped with quantum generator and quantum memory. Considering the practical application situation, it is difficult to ensure that every participant can afford the expensive quantum equipment, so the semi-quantum protocol is proposed.

In 2007, Boyer et al. [23] proposed the first semi-quantum key distribution protocol, which firstly introduced the concept of "semi-quantum". In this protocol, he defined semi-quantum users as classical users with only partial quantum capabilities. In 2009, Boyer et al. [24] proposed another semi-quantum key distribution protocol, adding the function that the classical party can reorder the undisturbed qubits to ensure the robustness against attacks. Later, researchers proposed many new semi-quantum protocols based on this definition. In 2017, Liu et al. [25] proposed a multi-party semi-quantum key agreement with delegating quantum computation, which simplified the work of classical participants and entrusted all the complex quantum computing to the remote quantum center. However, in this protocol, each participant needs to communicate with the server for several times, so the steps are a little tedious. Shukla et al. [26] proposed four supplementary protocols for semi-quantum key agreement, controlled deterministic secure communication and dialogue. In 2019, Yan et al. [27] proposed semi-quantum key agreement and private comparison protocols using bell states, but these two protocols have low particle utilization and efficiency.

In order to solve the problem of lack of checking full-quantum participants' honesty, we propose a semi-quantum key agreement protocol based on GHZ-like state with delegating a dishonest quantum center Charlie to perform quantum measuring. On the premise of ensuring protocol security, communication cost is reduced. Compared with other protocols, our protocol does not need to limit the honesty of the controller, nor need to distribute the key between the controller and the participants in advance, saving quantum resources. The quantum cloud sever Trent provides quantum resources for semi-quantum participants, and the quantum center Charlie is responsible for performing quantum measuring. Finally, Charlie and semi-quantum participants only need to do one measurement to know the shared key.

The rest of the paper is organized as follows: In Section 2, we introduce some relevant theoretical knowledge. In Section 3, we describe the concrete steps of our protocol. Security analysis is described in Section 4. Efficiency analysis is given in Section 5. This paper is finally concluded in Section 6.

2 Preliminaries

2.1 GHZ-like State

The GHZ-like state we use are obtained by the Hadamard operation of the GHZ state. First of all, the three-particle GHZ state is the quantum resource widely used in quantum communication, which is generally expressed as:

$$|GHZ\rangle_{123} = \frac{1}{\sqrt{2}}(|000\rangle + |111\rangle)_{123} \quad (1)$$

Secondly, Hadamard operation is a commonly used quantum operation in quantum theory, which is generally described as:

$$H = \frac{\sqrt{2}}{2}\begin{bmatrix}1 & 1\\ 1 & -1\end{bmatrix}$$
$$= \frac{\sqrt{2}}{2}[(|0>+|1>)<0| + (|0>-|1>)<1|] \quad (2)$$

$$|+\rangle = \frac{\sqrt{2}}{2}(|0\rangle + |1\rangle, |-\rangle = \frac{\sqrt{2}}{2}(|0\rangle - |1\rangle) \quad (3)$$

Finally, the three-particle GHZ-like state can be obtained by operating the Hadamard gate on the GHZ state, expressed as:

$$\begin{aligned} |GHZ-like\rangle_{123} &= H_1H_2H_3|GHZ\rangle_{123} \\ &= \frac{\sqrt{2}}{2}(|++\rangle + |--\rangle)_{123} \\ &= \frac{1}{2}(|000\rangle + |011\rangle + |110\rangle + |101\rangle)_{123} \\ &= \frac{1}{2}[|0\rangle_1(|00\rangle_{23} + |11\rangle_{23}) + |1\rangle_1(|10\rangle_{23} + |01\rangle_{23})] \\ &= \frac{\sqrt{2}}{2}(|0\rangle_1|\phi^+\rangle_{23} + |1\rangle_1|\psi^+\rangle_{23}) \end{aligned} \quad (4)$$

The SQKA protocol designed in this paper is based on the GHZ-like state, which is described in Eq. (4). In the ideal situations, the measurement results of GHZ-like state states should meet **Table 1**. "0" represents the measurement result $\{|0\rangle\}$, and "1" represents the measurement result $\{|1\rangle\}$.

Table 1 Measuring results of three parties

Measuring base	Trent	Alice	Bob
Z	0	0	0
	0	1	1
	1	1	0
	1	0	1

In particular, if we measure the first particle with the Z-base and the second and third particles with the Bell basis, We can only get two corresponding results, namely $\{|0\rangle_1|\phi^+\rangle_{23}, |1\rangle_1|\psi^+\rangle_{23}\}$.

In this study, there are three types of participants, Trent, classical semi-quantum participants and Charlie. There are many classic parties, such as Alice, Bob and Bob1, etc. They can perform key agreement with any classic user with the help of the quantum server Trent. They are responsible for receiving quantum resources, measuring and resending, etc. Trent is an untrusted quantum cloud server, responsible for preparing quantum resources and distributing particles to Charlie, Alice and Bob. The GHZ-like states prepared by Trent are the basis of the key agreement. Charlie is a quantum center and is responsible for performing a series of quantum measurement operations. The roles of all parties are shown in **Figure 1**. The whole protocol consists of three stages: initial stage, entanglement detection stage and key measurement agreement stage. The third part introduces the concrete steps of these three stages in detail.

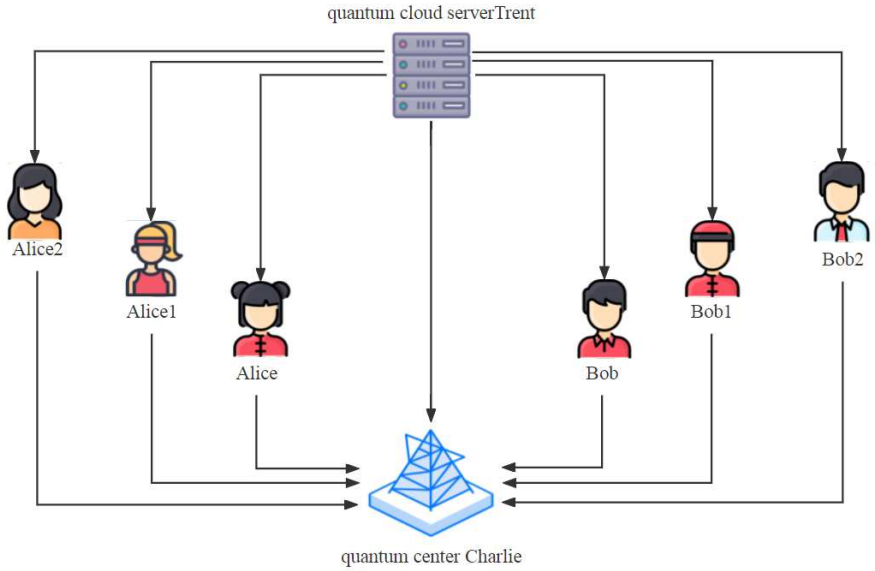

Figure 1 Schematic diagram of roles of all parties. Trent is a quantum cloud server that only has the function of preparing quantum resources. Alice, Alice1, Bob, and Bob1, etc. are all classical participants with only partial quantum functions and all classical functions. Charlie is the quantum center and only has the function of measuring

2.2 Semi-quantum Protocol

There are two kinds of participants in the semi-quantum key agreement protocol. One is quantum user, who can carry out all quantum operations, including the preparation, distribution and measurement of quantum particles with various measurement bases. The other is classical users, who have only partial quantum abilities including:

1. Preparing a particle in the classical basis Z= {|0⟩, |1⟩},
2. Measuring a particle in the classical basis Z,
3. Reordering particles via different delay lines,
4. Reflecting or sending the qubits without disturbance
5. Any other classic operations of a classic user

3 The Proposed Protocol

In practical applications, any classical participant can perform key negotiation with other participants, here we take Alice and Bob as examples. The specific steps of the agreement are as follows:

3.1 Initial Stage

Step 1: Quantum cloud server Trent prepares 2N GHZ-like states as described in Section 2, which is expressed as: {[$P_1(1), P_1(2), P_1(3)$], [$P_2(1), P_2(2), P_2(3)$], ... [$P_{2N}(1), P_{2N}(2), P_{2N}(3)$],}. Then, Trent divides the GHZ-like particles into three sequences, which are as follows:

S_1: [$P_1(1), P_2(1), \ldots, P_{2N}(1)$]

S_2: [$P_1(2), P_2(2), \ldots, P_{2N}(2)$]

S_3: [$P_1(3), P_2(3), \ldots, P_{2N}(3)$]

Trent randomly selects a certain number of single photons in the set of {|0⟩, |1⟩, |+⟩, |-⟩}, which is inserted into the sequences S_1, S_2 and S_3 as decoy photons. Then, Trent sends the sequences S_1, S_2 and S_3 to Charlie, Alice and Bob respectively.

Step 2: After confirming that everyone has received the corresponding sequence, Trent announces the

position of the decoy photons, and Alice and Bob reflect all the particles at the corresponding positions to Charlie. After Charlie has received the corresponding decoy photons sequence, Trent announces measurement base of all decoy photons. Charlie performs corresponding measurements on these photons and calculates the error rate. If the error rate is higher than a certain threshold, there may be an external eavesdropper, and Charlie will abort the agreement and restart from step 1. The entire initialization process is shown in **Figure 2**.

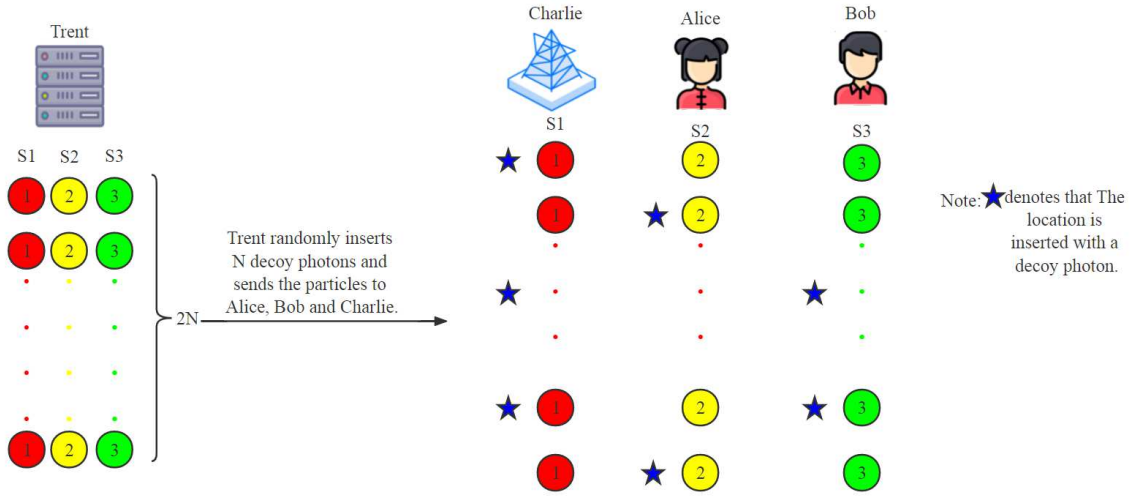

Figure 2 Process of the initialization stage.

3.2 Entanglement Detection Stage

Because of the limitation of Semi-quantum users, Alice and Bob can only measure with Z basis. In order to verify the honesty of the quantum cloud server, we introduce a dishonest quantum center Charlie to preform Bell-base measurement, Alice and Bob can ensure the security of the protocol through certain security checks.

Step 3.1: Alice randomly selects N/2 particles from sequence S_2 and announces the positions of these particles. Then Bob also randomly selects N/2 particles from the remaining particles in sequence S_3 and announces the positions of these particles. In this way, Alice and Bob randomly select N particles in total.

Step 3.2: Alice and Bob prepare M single photons in the set of $\{|0\rangle, |1\rangle\}$ with Z basis respectively, which is randomly inserted into the N particles as decoy photons, forming two new sequences called E_1 and E_2. Alice and Bob save the location and initial state information of the decoy photons. Then, Alice and Bob send the sequences E_1 and E_2 to Charlie. (M is much smaller than N in mathematical theory)

Step 3.2: Charlie performs Bell-basis measurement on every pair of qubits he receives from Alice and Bob, and publishes the results. Also Charlie conducts Z-base measurement to the corresponding particles at the same positions in S_1 and announces measurement results at the same time.

Step 3.3: After Charlie publish their results, Alice and Bob announce the location and initial state information of the decoy photons.

According to the information announced by Alice and Bob, Bell-basis measurement can be divided into five scenarios: (a) One particle comes from sequence S_2 and the other one comes from decoy photons; (b) One particle comes from sequence S_3 and the other one comes from decoy photons;(c) The two particles come from sequences S_2 and S_3, respectively, but are not initially entangled;(d) Both particles come from decoy photons;(e) The two particles come from sequences S_2 and S_3, respectively, and they are initially entangled. In case (a)(b)(c), these particles can be viewed as single photons of unknown state, so the Bell-basis measurement results are irregular. For those qubits whose basis are different, a Bell-

basis measurement will yield any one of the four Bell-basis states, as shown in Eq. (5),

$$|+\rangle|0\rangle = \frac{1}{2}(|\phi^+\rangle + |\phi^-\rangle + |\psi^+\rangle + |\psi^-\rangle)$$

$$|+\rangle|1\rangle = \frac{1}{2}(|\phi^+\rangle - |\phi^-\rangle + |\psi^+\rangle + |\psi^-\rangle)$$

$$|-\rangle|0\rangle = \frac{1}{2}(|\phi^+\rangle + |\phi^-\rangle + |\psi^+\rangle - |\psi^-\rangle) \quad (5)$$

$$|-\rangle|1\rangle = \frac{1}{2}(-|\phi^+\rangle + |\phi^-\rangle + |\psi^+\rangle + |\psi^-\rangle)$$

$$|+\rangle|+\rangle = \frac{1}{\sqrt{2}}(|\phi^+\rangle + |\psi^+\rangle), |+\rangle|-\rangle = \frac{1}{\sqrt{2}}(|\phi^-\rangle - |\psi^-\rangle)$$

There are not useful for security check. In case (d), Because the decoy photons prepared by Alice and Bob are the identical basis, this security check is identical to that in the MDI-QKD. The decomposition of qubits with identical basis in terms of Bell-basis states are shown in Eq. (6).

$$|0\rangle|0\rangle = \frac{1}{\sqrt{2}}(|\phi^+\rangle + |\phi^-\rangle), |0\rangle|1\rangle = \frac{1}{\sqrt{2}}(|\psi^+\rangle + |\psi^-\rangle) \quad (6)$$

Ideally, a Bell-basis measurement can only obtain one of two Bell-basis states. Charlie's eavesdropping will have a 50% probability to obtain the other two Bell-basis states, hence increases the error rate. Alice and Bob can calculate the error rate from the measurement results. If the error rate is above a certain threshold, Charlie may be a dishonest quantum center. Alice and Bob will abort the protocol at this point and restart the protocol from step 1. In case (e), Alice and Bob will compare the results published by Charlie at the corresponding locations. Specifically, Charlie's Bell measurement is $|\phi^+\rangle$ when Z-base measurement result is 0. Charlie's Bell measurement is $|\psi^+\rangle$ when Z-base measurement result is 1. Alice and Bob calculate the error rate from the measurement results. If the error rate is above a certain threshold, Alice and Bob will abort the protocol. The entire process is shown in **Figure 3**.

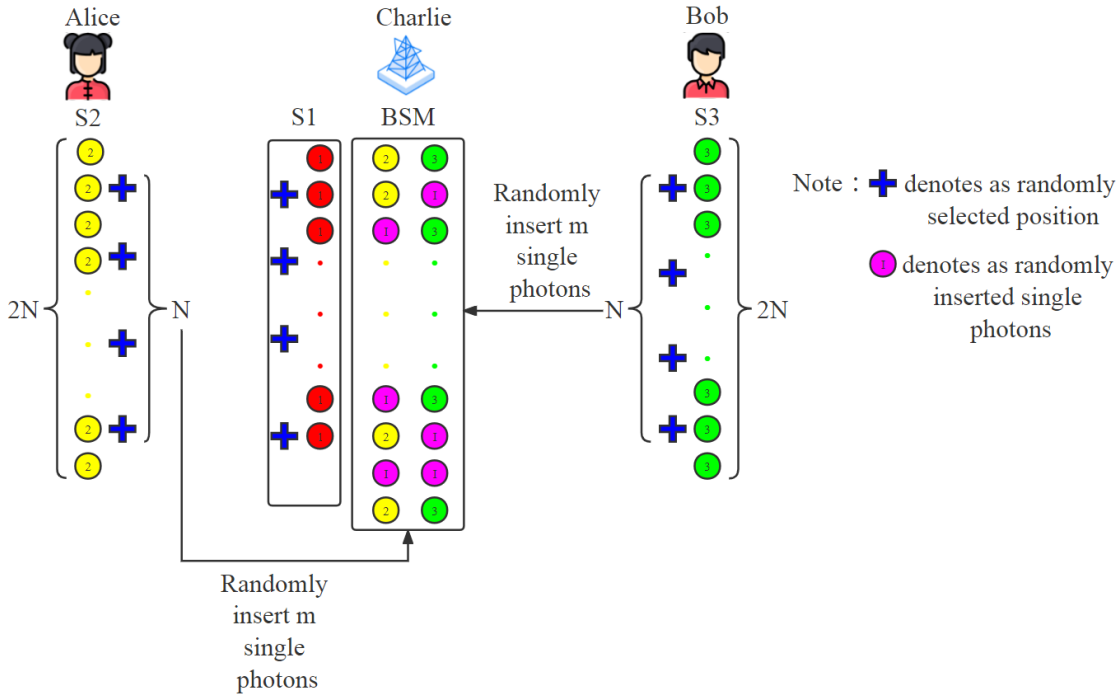

Figure 3 Process of the entanglement detection stage

3.3 Key Measurement Agreement Stage

Step 4: After passing the entanglement detection, Charlie, Alice and Bob make Z-base measurement of the remaining particles in their hands, and Charlie published the results.

Step 5: Alice (Bob) can calculate the result of Bob (Alice) according to Table 1 based on the result of her own measurement and the result published by Charlie. In this way, both parties know the other's measurement results, but Charlie does not. The reason is the randomness of the measurement result of the GHZ-like state. Even if Charlie knows his own measurement result and the various possible results in Table 1, he does not know the specific measurement values of Alice and Bob. Finally, the share key K_{AB} of Alice and Bob is based on Alice's measurement result.

For example, the measurement result published by Charlie is "1", and the actual measurement results of Alice and Bob are "0" and "1" in one measurement. Take Alice as an example. According to the result "1" published by Charlie and her own measurement result "0", she can deduce the measurement result of Bob as "1" according to Table 1. Similarly, Bob can also deduce the measurement result of Alice in the same way. Finally, the obtained one-bit agreement key is 0.

4 Security Analysis

4.1 External Attack

Three common methods of external attack are interception–resending, measuring–resending and entanglement–measurement. In interception–resending and measurement–resending attacks, since eavesdropper Eve cannot know the initial state and position of the decoy photons in advance, she can only choose a random measurement base for measurement. According to the principle of quantum collapse, Eve's random measurement will bring high error rate, so it will certainly be detected by three parties during the eavesdropping detection.

If Eve uses entanglement–measurement attacking method, she can entangle the intercepted particles from Trent with her own prepared particles, performing unitary operation on two particles. The most commonly used unitary operation is the CNOT operation. According to Heisenberg's uncertainty theorem and non-cloning theorem, it is impossible for Eve to obtain useful information without making mistakes. Although information can be obtained by entangling the auxiliary particle and the intercepted particle through unitary operation, it will affect the entanglement state of the original particle to some extent. If multiple unitary operations are performed, it will bring a high error rate which is easy to be detected. For example, if Eve introduces particles with the initial state $|0\rangle$ as auxiliary particles and uses the intercepted particles as control particles, Eve can conduct the CNOT operation with the auxiliary particles as target particles. The results are as follows:

$$CNOT|1\rangle|0\rangle_E = |1\rangle|1\rangle_E, CNOT|0\rangle|0\rangle_E = |0\rangle|0\rangle_E$$
$$CNOT|+\rangle|0\rangle_E = |0\rangle|0\rangle_E + |1\rangle|1\rangle_E = |+\rangle|+\rangle_E + |-\rangle|-\rangle_E$$
$$CNOT|-\rangle|0\rangle_E = |0\rangle|0\rangle_E - |1\rangle|1\rangle_E = |+\rangle|-\rangle_E + |-\rangle|+\rangle_E$$

It can be seen that when the control particles are $|0\rangle$ and $|1\rangle$, Eve can obtain particle information through CNOT operation without error. But for $|+\rangle$ and $|-\rangle$, there is a 50% probability that Eve will change the state of the control particle. Because Eve does not know the initial state and initial position of the decoy particles. She can only perform CNOT operations on particle sequence bit by bit, so the probability of Eve's attack being discovered is $1-\left(\frac{1}{2}\right)^D$, where D is the number of initial states $|+\rangle$ and $|-\rangle$ in the decoy photons. It can be seen that when the number of D becomes larger and larger, the probability of Eve being found tends to 1.

4.2 Internal Attack

(1) Participants' Attack

In the semi-quantum key agreement protocol (SQKA) proposed in this paper, the quantum cloud server Trent participates as a quantum producer. Trent prepares entangled particles and distributes them to everyone. The quantum center Charlie participates in entanglement detection and key measurement agreement stage. Compared with Eve, the internal eavesdropper Trent and Charlie have more advantage in acquiring information about entangled particles. Assuming that Charlie is a dishonest quantum center, he can access some quantum resources from the beginning and try to obtain the session key K_{AB} of Alice and Bob. In the key agreement stage, although Charlie knows the measurement results of his part of the particles and all possible results in Table 1, he cannot determine the measurement results of Alice and Bob. For example, the measurement results of Charlie, Alice and Bob are 011 respectively. At this time, according to Table 1, the measurement values of Alice and Bob should be the same. In order to obtain the correct key, Charlie can only select one randomly from {0,1} as the key, so that for each bit of the agreement key, the probability of Charlie getting the correct key is only 50%. For the N bits of the agreement key, the probability of Charlie getting the complete key is $\left(\frac{1}{2}\right)^N$. It can be seen that when the number of N becomes larger and larger, the probability of Trent getting the complete key tends to 0. Analysis of Trent is the same as analysis of Charlie.

(2) Collusion Attack

Assuming that Trent and Charlie conspire to eavesdrop on the shared key. Here, these dishonest participants have unlimited computing power and private communication the technology of which is only limited by the laws of quantum mechanics. The detailed attack strategy is described as follows.

The GHZ-like state states prepared by Trent is not entangled, which is a series of individual $|000\rangle$, $|011\rangle$, $|110\rangle$, $|101\rangle$ states. Trent records the serial number of each group of quantum states and shares with Charlie. If Alice and Bob do not randomly insert single photons during the entanglement detection stage, Trent can pass the security check with the help of Charlie. Specifically, Charlie can publish his Z-base measurement results first, then Charlie can change his published Bell-base measurement results to meet Equation 4, without being discovered by Alice and Bob, even if Charlie does not perform the Bell-base measurement. Finally, Charlie publishes the measurement results of his own particles in S_1. According to the particle number, Trent and Charlie can know the measurement results of Alice and Bob and achieve the shared key. However, Trent and Charlie's collusion attack will not succeed when Alice and Bob randomly insert single photons. The proof is as follows.

Theorem 1 *Without knowing the location of the single photons inserted by Alice and Bob, Charlie's announcing the measurement result dishonestly will be discovered with a non-trivial probability.*

Proof

In our protocol, Charlie is required to announce the measurement result in step (3.2), before Alice and Bob announce the position and initial state information of the single photons in step (3.3). Therefore, Charlie cannot delay their announcement until they learn the position information. Alice(Bob) Inserts m single photons into n particles. There are a total of $2^m \sum_{i=1}^{m} A_{n+1}^{i}$ results. In other words, for sequences E_1 and E_2, there are $2^m \sum_{i=1}^{m} A_{n+1}^{i}$ different outcomes for each sequence. When Charlie doesn't know the specific location information of these decoy particles, for each pair of photon measurements, they can be any of case (a), (b), (c), (d), (e). Even if Charlie intercepts a certain number of photons and

conducts Z-base measurement privately, there is no measurement on {00,11,01,10} that can help him identify decoy photons, Because the GHZ-like state and the single photon have similar results in the Z-base measurement. If Charlie wants to publish his measurements based on the Z-base measurement results, he must be discovered in step (3.3). Specifically, since the sequences E1 and E2 are inserted with m single photons, Charlie must have published m more Bell-base measurement results than Z-base measurement results. Since Charlie doesn't know the exact location of the single photon, He needs to select n of the (m+n) results to match Z-base measurement results, so he has C_{n+m}^{m} options. Each selection method will introduce certain errors, that is, the probability that the measurement results of n GHZ state photons and m single photons are all selected correctly is $\frac{1}{C_{n+m}^{n}}[\left(\frac{1}{2}\right)^{n} * \left(\frac{1}{4}\right)^{m}]$. So, the probability that Charlie is detected as cheating is $1-\frac{1}{C_{n+m}^{n}}[\left(\frac{1}{2}\right)^{n} * \left(\frac{1}{4}\right)^{m}]$. Although m is much smaller than n, when n is large enough, the probability of Charlie passing the security check tends to 0. In this case, if he announces a result opposite to what is obtained in his measurement (or announces a random result without actually performing the measurement) as the state of $|\phi^{+}\rangle$, He must be detected by Alice and Bob in step(3.3).

The above theorem guarantees that the performance of the measurement devices in the protocol is checkable, so that Alice and Bob can arrive at the same raw key correctly. In summary, our protocol can resist Internal Attacks.

4.3 Further security discussion

(1) Trojan horse attack

Trojan Horse attack is a physical attack that uses the physical characteristics and special devices of photons to obtain photon states. This attack mainly exists in two-way communication protocols. In our scheme, the five quantum information flows are: $\text{Trent} \rightarrow \text{Alice} \rightarrow \text{Charlie}$; $\text{Trent} \rightarrow \text{Bob} \rightarrow \text{Charlie}$; $\text{Trent} \rightarrow \text{Charlie}$; $\text{Alice} \rightarrow \text{Charlie}$; $\text{Bob} \rightarrow \text{Charlie}$. One-way quantum communication protocol refers to only one party transfers the quantum information flow to the other, and no returned information. Therefore, our protocol is a one-way quantum communication protocol and Trojan horse attack will be naturally resisted in this protocol.

(2) Man-in-the-middle attack

Key agreement may also suffer from man-in-the-middle attacks, that is, Eve pretends to be a third party or a participant in the negotiation process to obtain the negotiation key. Generally, Eve can take two attack methods: One is measuring the intercepted particles and preparing a false photon sequence to send to Alice and Bob. However, due to the characteristics of quantum resources, Eve cannot know in advance the positions of particles which are to make X-base measurement in the eavesdropping detection of step 2 in advance. So there will be a large error rate, and the attack will definitely be detected. The other one is replay attack, that is, Eve prepares a new GHZ-like state and sends it to Alice and Bob. However, due to the non-reproducibility of quantum resource, the particles of Trent and the particles of A and B are not entangled, so the result of the measurement does not meet Table 1, so it will definitely be detected. In summary, the man-in-the-middle attack is invalid for our protocol.

5 Efficiency Analysis and Comparison

5.1 Efficiency Analysis

Now let's discuss the efficiency of our protocol. According to [31], the reference index of efficiency can

be defined as the following two parameters:

$$\eta_1 = \frac{c}{q+b} \tag{7}$$

$$\eta_2 = \frac{\mathrm{c}}{q} \tag{8}$$

Eq. (7) can be used to represent the efficiency of the quantum communication protocol, and Eq. (8) represents the qubit efficiency. In the formula, c represents the shared key bits generated by the protocol, q represents the total quantum bits utilized in the protocol, and b represents the classical bits used for decoding (excluding the classical bits used for eavesdropping detection). In our protocol, firstly we generate 2N three-particle GHZ-like state, so, 6N qubits are required. The generated decoy photon bits are generally the same as the final share key bits, that is, we need N qubits quantum resources. In the phase of entanglement detection, Alice and Bob prepare 2m single photons. Because M is much smaller than N, compared to N, the proportion is significantly smaller of number of decoy photons which are used for entanglement detection and it can be neglected theoretically. Therefore, q=6N+N=7N, the final share key is obtained from the measurement results published by Charlie, so, b=N. The share key for negotiation is N bits, so c=N. Therefore:

$$\eta_1 = \frac{c}{q+b} = \frac{n}{7n+n} = \frac{1}{8} = 12.5\%$$

$$\eta_2 = \frac{\mathrm{c}}{q} = \frac{n}{7n} = 14.3\%$$

5.2 Comparisons

We have selected three different types of key negotiation protocols for comparison with our protocol, and the results are shown in Table 2:

Table 2 Comparison among related protocols

Protocols	$\eta_1(\%)$	$\eta_2(\%)$	Semi-quantum	Controlling party
Ref. [26]	6.7	8.3	Yes	Yes
Ref. [22]	8.3	11.1	No	Yes
Ref. [25]	10	12.5	Yes	No
our protocol	12.5	14.3	Yes	Yes

According to the data in the table, we can see that the efficiency of our protocol is the highest when there is a third party and semi-quantum agreement function is realized. Under the condition of three-particle entangled resources, our protocol does not require the third party to distribute the key with the classical party in advance, which is much better than the protocol [22] in terms of scheme steps and quantum resources. In addition, our proposed protocol simplifies the work of the quantum cloud, where the cloud Trent is only responsible for generating and distributing quantum resources. All measurements are entrusted to the Quantum Center. To sum up, our protocol simplifies steps on the premise of ensuring security, and maintains efficiency at a relatively high level, which has certain practical application value.

6 Conclusion

In this paper, we propose a semi-quantum key agreement protocol based on three-particle GHZ-like state.

In the whole protocol, Trent, the quantum cloud sever, is only responsible for preparing and distributing quantum resources. Quantum center Charlie is responsible for checking Trent's honesty, which is only responsible for measuring the corresponding particles. After the three-party eavesdropping detection and entanglement detection, the key agreement stage is entered. After the three-party measurement, Charlie announces his measurement results, and Alice and Bob can obtain the share key, but Trent and Charlie cannot know the session key. Compared with the existing QKA, the efficiency of our protocol is feasible, and it does not need to carry out three-party key distribution in advance, saving quantum resources. The result of detailed analysis shows it holds good security against external attacks, internal attacks and collusion attacks. In addition, since the powerful quantum device is expensive and scarce, it is suitable for applications such as a large number of classic users arbitrarily conducting key negotiation in a real cloud environment. Specifically, in a multi-user cloud environment, only the server Trent needs to have the ability to prepare quantum resources, while the complicated quantum measurement, such as X-base measurement and Bell measurement, will be delegated to the quantum center. That is, with more participants, our protocol saves quantum resources more than other protocols. In the future, we will further explore the extended applications of three-particle entangled states in other quantum fields, such as quantum secret sharing, key distribution, and quantum trusted computing.

Acknowledgments

This work was supported by the National Natural Science Foundation of China under grant No. 62071015.

References

1. Bennett, C. H. and 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, 175–179 (1984) https://doi.org/10.1016/j.tcs.2014.05.025
2. Ekert, A.K. : Quantum cryptography based on Bell's theorem. Phys. Rev. Lett.67, 6 6 1–663 (1991) https://doi.org/10.1103/PhysRevLett.67.661
3. Bennett, C.H.: Quantum cryptography using any two nonorthogonal states. Phys. Rev. Lett.68, 3 1 2 1–3124 (1992) https://doi.org/10.1103/PhysRevLett.68.3121
4. Grosshans, F., V an Assche, G., Wenger, J., Brouri, R., Cerf, N.J., Grangier, P .: Quantum key distribution using gaussian-modulated coherent states. Nature.421, 2 3 8–241 (2003) https://doi.org/10.1038/nature01289
5. Wang, T.Y ., Wen, Q.Y ., Chen, X.B.: Cryptanalysis and improvement of a multi-user quantum key distribution protocol. Opt. Commun.283(24), 5261–5263 (2010) https://doi.org/10.1016/j.optcom.2010.07.022
6. Lo, H.K., Curty, M., Qi, B.: Measurement-device-independent quantum key distribution. Phys. Rev. Lett. 108, 130503 (2012) https://doi.org/10.1103/PhysRevLett.108.130503
7. Pathak, A.: Elements of Quantum Computation and Quantum Communication. CRC Press, Boca Raton(2013)
8. Salas, P .J.: Security of plug-and-play QKD arrangements with finite resources. Quantum Inf. Comput.13(9–10), 861–879 (2013) https://doi.org/10.1088/1674-1137/37/9/093101
9. Xu, G., Chen, X.B., Dou, Z., Y ang, Y .X., Li, Z.: A novel protocol for multiparty quantum key management. Quantum Inf. Process.14(8), 2959–2980 (2015) https://doi.org/10.1007/s11128-015-1021-1
10. Zhou, N., Zeng, G., Xiong, J.: Quantum key agreement protocol. Electron. Lett.40(18), 1149–1150 (2004) https://doi.org/10.1049/el:20045183
11. Tsai, C.W., Hwang, T.: On Quantum Key Agreement Protocol. Technical Report C-S-I-E, NCKU,

Taiwan(2009)
12. Liu, S.L., Zheng, D., Chen, K.F.: Analysis of information leakage in quantum key agreement. J. Shanghai Jiaotong Univ. (Sci.).E-11(2), 219–223 (2006) https://doi.org/10.1007/s002540100348
13. Chong, S.K., Hwang, T.: Quantum key agreement protocol based on BB84. Opt. Commun.283(6), 1192–1195 (2010) https://doi.org/10.1016/j.optcom.2009.11.007
14. Shi, R.H., Zhong, H.: Multi-party quantum key agreement with bell states and bell measurements. Quantum Inf. Process12, 921–932 (2013) https://doi.org/10.1007/s11128-012-0443-2
15. Liu, B., Gao, F., Huang, W., Wen, Q.-Y .: Multiparty quantum key agreement with single particles. Quantum Inf. Process12, 1797–1805 (2013) https://doi.org/10.1007/s11128-012-0492-6
16. Xu, G.-B., Wen, Q.-Y., Gao, F., Qin, S.-J.: Novel multiparty quantum key agreement protocol with GHZ states[J]. Quantum Inf. Process.13(12), 2587–2594 (2014) https://doi.org/10.1007/s11128-014-0816-9
17. Shen, D.S., Ma, W.P ., Wang, L.L.: Two-party quantum key agreement with four-qubit cluster states. Quantum Inf. Process13, 2313–2324 (2014) https://doi.org/10.1007/s11128-014-0785-z
18. Sun, Z.W., Y u, J.P ., Wang, P .: Efficient multi-party quantum key agreement by cluster states. Quantum Inf. Process15, 373–384 (2016) https://doi.org/10.1007/s11128-015-1155-1
19. He, Y .F., Ma, W.P .: Two-party quantum key agreement based on four-particle GHZ states. Int. J. Theor.Phys.14, 1650007 (2016) https://doi.org/10.1142/S0219749916500076
20. He, Y .F., Ma, W.P .: Two-party quantum key agreement with five-particle entangled states. Int. J. Quantum Inf.15, 1750018 (2017) https://doi.org/10.1142/S0219749917500186
21. Gu, J., Hwang, T.: Improvement of "Novel multiparty quantum key agreement protocol with GHZ states". Int. J. Theor. Phys.56, 3108–3116 (2017) https://doi.org/10.1007/s10773-017-3478-4
22. Zhu H , Wang C , Li Z . Semi-Honest Three-Party Mutual Authentication Quantum Key Agreement Protocol Based on GHZ-Like State[J]. International Journal of Theoretical Physics, 2021(18): https://doi.org/1-11. 10.1007/s10773-020-04692-x
23. Boyer, M., Kenigsberg, D., Mor, T.: Quantum key distribution with classical bob. Phys. Rev. Lett. 99(14),140501 (2007) https://doi.org/10.1103/PhysRevLett.99.140501
24. Boyer, M., Gelles, R., Kenigsberg, D., Mor, T.: Semiquantum key distribution. Phys. Rev. A. 79(3), 032341(2009) https://doi.org/10.1103/PhysRevA.79.032341
25. W.J. Liu, Z.Y. Chen, S. Ji, H.B. Wang, J. Zhang, Multi-party semi-quantum key agreement with delegating quantum computation. Int. J. Theor. Phys. 56, 3164–74 (2017) https://doi.org/10.1007/s10773-017-3484-6
26. C. Shukla, K. Thapliyal, A. Pathak, Semi-quantum communication: protocols for key agreement, controlled secure direct communication and dialogue, Quantum Inf. Process. 16 (2017) https://doi.org/295. 10.1007/s11128-017-1736-2
27. Yan, L.L., Zhang, S.B., Chang, Y., Sheng, Z.W., Yang, F.: Mutual semi-quantum key agreement protocol using Bell states. Mod. Phys. Lett. A. 34, (2019) https://doi.org/10.1142/S0217732319502948
28. Cai, Q.Y .: Eavesdropping on the two-way quantum communication protocols with invisible photons. Phys. Lett. A. 351(1–2), 23–25 (2006) https://doi.org/10.1016/j.physleta.2005.10.050
29. 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(5), 054302 (2006) https://doi.org/10.1103/PhysRevA.74.054302
30. 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(4), 044302 (2005) https://doi.org/10.1103/PhysRevA.72.044302

31. Cabello, A.: Quantum key distribution in the Holevo limit. Phys. Rev. Lett. 85, 5633–5638 (2000) https://doi.org/10.1103/PhysRevLett.85.5635