Multiparty quantum key agreement

Song Lin,[*] Xin Zhang, Gong-De Guo, Li-Li Wang, and Xiao-Fen Liu
College of Mathematics and Informatics, Fujian Normal University, Fuzhou 350007, China

(Received 23 January 2021; accepted 30 September 2021; published 25 October 2021)

In this paper, we discuss in some detail how multiparty quantum key agreement protocols must be carefully designed and present a collusion attack to illustrate this point. Then, a secure circle-type multiparty quantum key agreement with Bell states is proposed. Bell states are used as the information carriers and transmitted among the participants, who embed their secrets into the traveling particles via certain encoding operations. In this way, all participants simultaneously obtain the same agreement key, i.e., the sum of their secret inputs, at the end of the protocol. Here, quantum state discrimination is utilized to design the encoding operations, which ensures that the proposed protocol is correct and secure against the presented collusion attack. Furthermore, it is shown that the proposed protocol satisfies three conditions of a secure quantum key agreement protocol in theory. In addition, these encoding operations consist of some common single-qubit gates, the Hadamard operator and four Pauli operators, which makes the proposed protocol feasible using current technology.

DOI: 10.1103/PhysRevA.104.042421

I. INTRODUCTION

In 1984, Bennett and Brassard proposed the famous BB84 protocol [1], which perfectly achieves a key distribution task between two remote parties. Moreover, in contrast to the security of classical key distribution protocols that are based on the assumption of computational complexity, the security of the BB84 protocol relies on quantum-mechanics principles, which makes it unconditionally secure in theory. Subsequently, quantum key distribution (QKD) has attracted great attention, and progressed quickly in both theory and experiment [2]. In addition to key distribution, key agreement is another major method of key establishment [3] and plays a key role in the field of cryptography. In a key agreement protocol, two or more parties can agree on an identical key in such a way that both influence the key. As an important cryptographic primitive, key agreement is widely used in multiparty secure computing, access control, electronic auctions, and so on [4]. Similar to QKD, quantum key agreement (QKA) has been naturally proposed and has recently become a new research branch of quantum cryptography.

In 2004, Zhou *et al.* [5] proposed the first QKA protocol, in which two users utilize quantum teleportation to agree on a key. Afterward, based on entanglement swapping, Shi and Zhong [6] proposed the first multiparty QKA (MQKA) protocol in 2013. Unfortunately, these two protocols are insecure, as shown in Refs. [7,8]. This has greatly stimulated people's interest and enthusiasm in the study of this issue. Recently, a few subtle MQKA protocols [9–25] have been proposed, in which various properties of quantum mechanics are exploited. Based on the transmission structures of signal particles, these protocols are divided into three categories [26]: complete-graph-type [8], tree-type [9], and circle-type [10–25]. Compared with the former two types, circle-type MQKA (CMQKA) has higher efficiency and feasibility. Therefore, most of the existing MQKA protocols belong to the third type. However, in Ref. [26], it is shown that some CMQKA protocols are insecure because they are vulnerable against collusion attacks. Why are these protocols so fragile? One main reason is that QKA is not an alternative method in comparison with QKD, but solves another secure problem and has more rigorous security requirements. Unlike QKD, the participants do not trust each other since some of them can be dishonest in QKA. Thus, in addition to security against external eavesdroppers, the QKA protocol should be immune against participants' attacks. Especially, some dishonest participants may cooperate to predetermine the agreement key by themselves, and break the fairness condition, which has been mentioned in Refs. [24,25].

In this paper, we study this problem further and find two security flaws in some CMQKA protocols. To illustrate these flaws, a collusion attack is presented, which is more powerful than the attack proposed in Ref. [26]. Then, a multiparty quantum key agreement protocol is proposed, which is secure against the presented attack and certain common attacks under ideal conditions. Its security is ensured by some conclusions about quantum state discrimination [27]. Moreover, since only Bell states that are used as information carriers and some common single-qubit operations, the Hadamard operator and Pauli operators, are employed, the proposed protocol is more feasible with current technology.

The remainder of this paper is organized as follows: In Sec. II, we briefly review some notations related to this paper and multiparty quantum key agreement protocols. Then, a collusion attack by $m-1$ dishonest participants is described in Sec. III. Next, a multiparty quantum key agreement protocol with Bell states and the corresponding protocol analysis are presented in Secs. IV and V, respectively. Finally, a short conclusion is provided in Sec. VI.

[*] Corresponding author: lins95@gmail.com

2469-9926/2021/104(4)/042421(14)

II. PRELIMINARIES

A. Some notations

Let us start with describing some notations that are used in this paper. Bell states are the most common two-particle entangled states and usually utilized as the information carriers in some quantum cryptography protocols. For pairs of qubits, the four Bell states are defined as

$$|\psi(u,v)\rangle = \frac{1}{\sqrt{2}}|0\rangle|v\rangle + (-1)^u|1\rangle|v\oplus 1\rangle, \tag{1}$$

where $u, v \in \{0, 1\}$, and the symbol $\oplus$ denotes addition module 2. These four states form a basis MB_0 of a two-qubit system, and can be converted to each other by performing one of four Pauli operations:

$$\begin{aligned} U_{0,0} &= I = |0\rangle\langle 0| + |1\rangle\langle 1|, U_{0,1} = X = |0\rangle\langle 1| + |1\rangle\langle 0|,\\ U_{1,0} &= Z = |0\rangle\langle 0| - |1\rangle\langle 1|, U_{1,1} = iY = |0\rangle\langle 1| - |1\rangle\langle 0|. \end{aligned} \tag{2}$$

This process can be depicted as follows:

$$U_{x,y}\otimes I|\psi(u,v)\rangle = |\psi(u\oplus x, v\oplus y)\rangle, \tag{3}$$

where $x, y, u, v \in \{0, 1\}$. Moreover, the following equation holds: $U_{x,y}U_{x',y'} = (-1)^{yx'}U_{x\oplus x',y\oplus y'}$. Thus, four Pauli operators are used to construct the encoding operations in the proposed protocol.

Besides the above four single-qubit operators, the Hadamard operator is another important tool in the field of quantum information processing, and can be defined as follows:

$$H = \frac{1}{\sqrt{2}}(|0\rangle\langle 0| + |0\rangle\langle 1| + |1\rangle\langle 0| - |1\rangle\langle 1|). \tag{4}$$

When applying Hadamard operation on one particle of Bell states, we can get another basis of a two-qubit system, $MB_1 = \{|\Psi(u,v)\rangle = H\otimes I|\psi(u,v)\rangle\}$. As for the operators H and $U_{x,y}$, the following equation holds:

$$\begin{aligned} U_{0,0}H &= HU_{0,0}, U_{1,0}H = HU_{0,1},\\ U_{0,1}H &= HU_{1,0}, U_{1,1}H = -HU_{1,1}. \end{aligned} \tag{5}$$

Based on the above equation, the Hadamard operator acts as the obfuscation function in the proposed protocol. That is, the encoding operations consist of Hadamard operators H and four Pauli operators $U_{x,y}$. In Sec. V B, it is shown that these encoding operations cannot be distinguished by unambiguous discrimination [30] or minimum-error discrimination [27], which ensures the security of the proposed protocol.

B. Brief review of MQKA protocols

1. General CMQKA protocol

For a multiparty QKA protocol, there are m participants, P_i $(i = 0, 1, \ldots, m-1)$, who hold their own secret S_i. They want to agree on a common key K determined by these m secret inputs, $K = f(S_0, S_1, \ldots, S_{m-1})$ (e.g., $K = S_0 \oplus S_1 \oplus \cdots \oplus S_{m-1}$). This implies that these m participants contribute to the generation of the agreement key K equally. Moreover, unlike QKD, not all participants are honest in QKA. As a result, some dishonest participants may conspire to attack the protocol. The goal of these dishonest participants is to determine the agreement key by themselves, i.e., to undermine the fairness of the protocol. The basic idea of their collusion attack is to first eavesdrop the information about the secret inputs of the remaining honest participants, from which the agreement key may be derived before the end of the protocol. After that, they take advantage of the opportunity to participate in the protocol to execute their appropriate attack actions, by which the genuine agreement key is replaced with a fake key predetermined by these dishonest participants alone. Obviously, this kind of attack is more powerful than the external attack. Therefore, a secure quantum key agreement protocol should meet the following three conditions.

(C1) Correctness. At the end of the protocol, each participant gets the correct agreement key.

(C2) Security. No external eavesdropper can obtain any information about the agreement key without being detected.

(C3) Fairness. All participants equally influence the agreement key, that is, any nontrivial subset of the participants cannot determine the agreement key alone.

In addition, in most QKA protocols, the secret input of the participant is made up of random bits. Thus, after the protocol is successfully completed, it does not matter whether the input is obtained by other participants. Even if the protocol is aborted due to an attack, the participant can discard this input and restart the protocol with a new random bit string. On the other hand, for some classical KA protocols or QKA protocols with identity authentication [28,29], the input of the participant contains the information about his secret message (e.g., his master key). In this case, it is evident that his input should be always kept secret from other participants. Hence, for this kind of QKA protocols, the following privacy condition needs to be satisfied.

(C4) Privacy. The inputs of the participants can be kept secret.

The QKA protocols discussed in this paper are of the former type. That is, in these protocols, the inputs of participants are random bits and do not contain any private information. Therefore, when analyzing the securities of these protocols, we ignore the privacy requirement and focus on the first three conditions C1–C3.

Obviously, a key agreement task can be achieved by executing QKD multiple times. That is, each participant P_i utilizes a secure QKD protocol (e.g., BB84 protocol) to distribute his or her secret S_i to the other $m-1$ participants. In this way, each participant can directly deduce the key K from the received messages and his secret. This is the first type of MQKA protocol, i.e., complete-graph-type. Since all participants gain knowledge of these secret inputs, the privacy of these inputs cannot be ensured. Moreover, the particle efficiency is very low, and the quantum channels between any two of these participants should be established, which means that $m(m-1)/2$ quantum channels are required. All these factors make this type of protocol infeasible in a real environment.

The same is true of the second type. In a tree-type MQKA protocol, an m-particle entangled state is shared among m participants, who measure the particle in their hands and utilize the correlation of the measurement results to share an identical key. Obviously, when the number of participants is large, preparing an m-particle entangled state is still very difficult

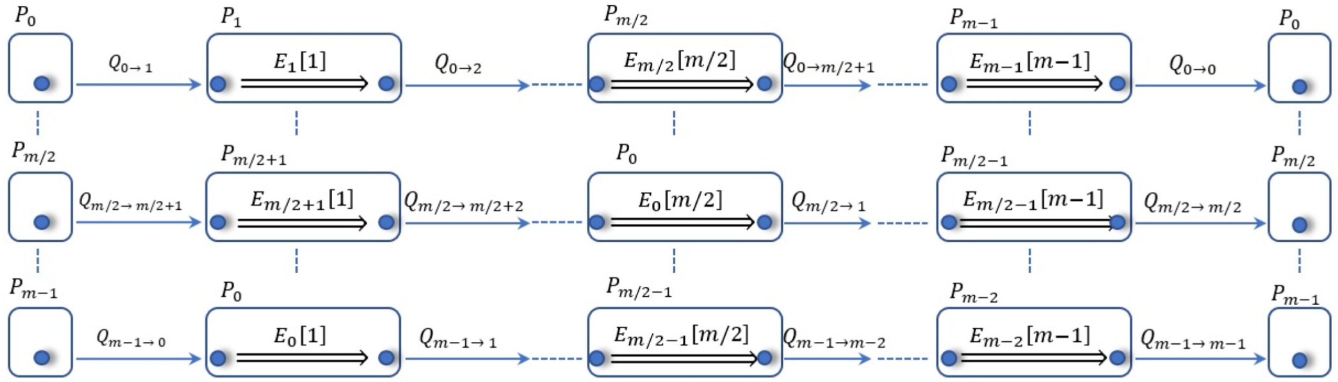

FIG. 1. A general particle transmission model of CMQKA protocols. In an m-party CMQKA protocol, the signal particle sequence $Q_{i\to i\oplus 1}$ prepared by P_i ($i = 0, 1, \dots, m-1$)is transmitted among the remaining $m-1$ participants, $P_{i\tilde{\oplus}1}, P_{i\tilde{\oplus}2}, \dots, P_{i\tilde{\oplus}(m-1)}$, who respectively encode their secret inputs by executing the operations, $E_{i\tilde{\oplus}1}[1], E_{i\tilde{\oplus}2}[2], \dots, E_{i\tilde{\oplus}(m-1)}[m-1]$), on the traveling particles. Finally, the particle sequence $Q_{i\to i}$ containing $m-1$ participants' secret inputs is sent back to P_i.

using current technology. This becomes a major obstacle in practical applications. Hence, from a practical perspective, the first two types of MQKA protocols are inefficient and infeasible. Therefore, most research focuses on the third type, i.e., circle-type MQKA.

In a CMQKA protocol, generally speaking, the signal particle sequences are transmitted among m participants (as shown in Fig. 1). To obtain a common agreement key K with a length of n, each participant P_i ($i = 0, 1, \dots, m-1$) prepares a random $n(1+\zeta)$-bit sequence S_i, where ζ is a factor that determines the size of the test sample and can be arbitrary in principle. The general procedure is described below.

(G1) Each participant P_i ($i = 0, 1, \dots, m-1$) generates a signal particle sequence $Q_{i\to i\tilde{\oplus}1}$, where the symbol $\tilde{\oplus}$ denotes the addition module m. Here, the information carriers may be single-particle states (e.g., qubit [20,24] or qudit [23]) or entangled states (e.g., Bell states [10,11,16,18,21,22], Brown states [12,19], or cluster states [14,15]). Therefore, for simplicity, we assume that the signal particle is prepared in a certain initial state, $|\phi_i\rangle$. Then, he sends $Q_{i\to i\tilde{\oplus}1}$ to the next participant $P_{i\tilde{\oplus}1}$.

(G2) According to his secret $S_{i\tilde{\oplus}1}$, each participant $P_{i\tilde{\oplus}1}$ performs the encoding operation $E_{i\tilde{\oplus}1}[1]$ on the particle sequence $Q_{i\to i\tilde{\oplus}1}$, and obtains a new sequence $Q_{i\to i\tilde{\oplus}2}$. After that, he sends this new sequence to $P_{i\tilde{\oplus}2}$.

(G3) Similarly, the remaining $m-2$ participants $P_{i\tilde{\oplus}j}$ ($j = 2, 3, \dots, m-1$) respectively encode their secret messages $S_{i\tilde{\oplus}j}$ on sequence $Q_{i\to i\tilde{\oplus}j}$ by executing the encoding operation $E_{i\tilde{\oplus}j}[j]$ and send the encoded sequence $Q_{i\to i\tilde{\oplus}(j+1)}$ to the next participant $P_{i\tilde{\oplus}(j+1)}$.

(G4) After all participants receive the traveling particle sequences $Q_{i\to i}$, each participant P_i measures the signal particles that contain the secret messages of other $m-1$ participants. From the result and S_i, he can deduce $K_i = S_0 \oplus S_1 \oplus \cdots \oplus S_{m-1}$.

(G5) These participants choose ζn samples to execute the eavesdropping check process. The order of m participants is random. For simplicity, suppose these participants execute their respective eavesdropping check process orderly. Concretely, the first participant P_0 randomly selects $\lfloor \frac{\zeta n}{m} \rfloor$ positions from $n(1+\zeta)$ positions, and declares these chosen positions publicly. After that, he requires the other participants P_j ($j \neq 0$) to announce the corresponding part of K_js in these chosen positions. By comparing these messages with his own result K_0, P_0 determines whether or not eavesdropping exists. Just in the same way, participant P_i ($i = 1, 2, \dots, m-1$) randomly chooses $\lfloor \frac{\zeta n}{m} \rfloor$ samples from the remaining $n(1+\zeta) - i\lfloor \frac{\zeta n}{m} \rfloor$ positions. Then, he compares the $\lfloor \frac{\zeta n}{m} \rfloor$ bits of K_i in these chosen positions with the corresponding part of K_j declared by P_j ($j = 0, 1, \dots, m-1,\ \ j \neq i$). Obviously, in the ideal condition, these bits are identical if no eavesdropping exists. Hence, if the bits are equal, participant P_i accepts the remaining part of K_i (with a length of n) as a raw agreement key. Otherwise, this protocol is aborted.

From the above steps, it is not hard to see that only m quantum channels are required to achieve a CMQKA protocol among m participants. Moreover, except for the protocols with a third party, the signal particles are generally prepared by the participants. Instead of m-particle entangled states, single-particle or two-particle entangled states are usually used as the information carriers in CMQKA protocols. Obviously, these states are more easy to generate, which reduces the requirement for the quantum operation ability of the participants. Therefore, compared with the first two types of MQKA protocols, circle-type multiparty quantum key agreement is more feasible.

2. Liu's attack

However, in Ref. [26], Liu *et al.* concluded that some CMQKA protocols are insecure because they cannot satisfy the fairness requirement. To illustrate this, they designed a special collusion attack (Liu's attack), in which two dishonest participants at special positions, P_i and $P_{i\tilde{\oplus}m/2}$ (referred to as $\dot{P}_i$ and $\dot{P}_{i\tilde{\oplus}m/2}$), can determine the agreement key alone. Namely, they can forge a fake agreement key $\dot{K} \neq K$ beforehand and make other honest participants accept this fake key.

In Liu's attack, $\dot{P}_i$ ($\dot{P}_{i\tilde{\oplus}m/2}$) intercepts the particle sequence $Q_{i\to i\tilde{\oplus}m/2}$ ($Q_{i\tilde{\oplus}m/2\to i}$), which travels from $\dot{P}_i$ ($\dot{P}_{i\tilde{\oplus}m/2}$) to $\dot{P}_{i\tilde{\oplus}m/2}$ ($\dot{P}_i$), in the middle of the protocol. Then, he measures these particles that contain the secret message $T_1 = S_{i\tilde{\oplus}1} \oplus \cdots \oplus S_{i\tilde{\oplus}(m/2-1)}$ ($T_2 = S_{i\tilde{\oplus}(m/2+1)} \oplus \cdots \oplus S_{i\tilde{\oplus}(m-1)}$). Since the initial state $|\phi_i\rangle$ ($|\phi_{i\tilde{\oplus}m/2}\rangle$) is known to these two dishonest participants, they can deduce T_1 (T_2) from the measurement results, then obtain $K = S_i \oplus T_1 \oplus S_{i\oplus m/2} \oplus T_2$. After that, $\dot{P}_i$ ($\dot{P}_{i\oplus m/2}$) encodes a fake message $\dot{K} \oplus K \oplus S_i$ ($\dot{K} \oplus K \oplus S_{i\tilde{\oplus}m/2}$) on the sequences $Q_{i\tilde{\oplus}(m/2+1)\rightarrow i}$, $Q_{i\tilde{\oplus}(m/2+2)\rightarrow i}$, . . ., and $Q_{i\oplus(m-1)\rightarrow i}$ ($Q_{i\tilde{\oplus}1\rightarrow i\tilde{\oplus}m/2}$, $Q_{i\tilde{\oplus}2\rightarrow i\tilde{\oplus}m/2}$, . . ., and $Q_{i\tilde{\oplus}(m/2-1)\rightarrow i\tilde{\oplus}m/2}$). In step G4, by measuring their particles, all honest participants obtain a fake agreement key $\dot{K}$ that is predetermined by P_i and $P_{i\tilde{\oplus}m/2}$. Because the keys shared by all participants are the same, this attack introduces no errors in the eavesdropping check process of step G5. This fake agreement key $\dot{K}$ is accepted by all participants. Hence, the general CMQKA protocol cannot meet the fairness condition, and is insecure.

For example, in Ref. [18], Cao and Ma proposed a multiparty quantum key agreement protocol with Bell states (Cao's protocol). Each participant P_i ($i = 0, 1, \ldots, m-1$) has a secret input S_i (e.g., $S_0 = S_1 \cdots = S_{m-1} =$ "00"), and prepares a two-qubit entangled pair (q_i, r_i) that is randomly selected from four Bell states. Then, he holds particle r_i in his hands, and makes q_i orderly travel among the remaining $m - 1$ participants, i.e., $Q_{i\rightarrow i\oplus 1} = \{q_i\}$. Here, the signal particles are transmitted in the secure quantum channel that is ensured by decoy state method. When receiving the traveling particle, each participant performs one of four Pauli operations (e.g., $U_{0,0}$) according to his secret input. At last, the particle q_i that has been encoded by $m - 1$ participants $P_j (j \neq i)$ is sent back to P_i who applies Bell state measurements on two particles, q_i and r_i. In terms of the measurement result, the initial state and his own secret input, each participant P_i can obtain the agreement key, $K_i = S_0 \oplus S_1 \oplus \cdots \oplus S_{m-1}$ (e.g., "00"). However, it is vulnerable against Liu's attack, which is shown in Ref. [22].

Without loss of generality, we can assume that P_0 and $P_{m/2}$ are dishonest (referred to as $\dot{P}_0$ and $\dot{P}_{m/2}$). At the beginning of Cao's protocol, $\dot{P}_0$ and $\dot{P}_{m/2}$ prepare $|\psi(0, 0)\rangle_{q_0,r_0}$ and $|\psi(0, 0)\rangle_{q_{m/2},r_{m/2}}$. As shown in Fig. 1, the particle q_0 is transmitted from P_0 to P_0 via $P_1, \ldots, P_{m/2}, \ldots, P_{m-1}$, and $q_{m/2}$ is transmitted from $P_{m/2}$ to $P_{m/2}$ via $P_{m/2+1}, \ldots, P_0, \ldots, P_{m/2-1}$ at the same time. Therefore, when q_0 is received by $P_{m/2}$ from $P_{m/2-1}$, two dishonest participants can make Bell state measurements on (q_0, r_0), and deduce the sum of the secret inputs of $P_1, \ldots, P_{m/2-1}$, i.e., $T_1 = S_1 \oplus \cdots \oplus S_{m/2-1}$. Similarly, $\dot{P}_0$ and $\dot{P}_{m/2}$ obtain $T_2 = S_{m/2+1} \oplus \cdots \oplus S_{m-1}$ by measuring the particle pair ($q_{m/2}$, $r_{m/2}$). Obviously, from the values of T_1 and T_2, they can derive $K = T_1 \oplus T_2 \oplus S_0 \oplus S_{m/2} =$ "00" in the middle of Cao's protocol. Suppose the fake agreement key is $\dot{K} =$ "11." Therefore, instead of $U_{0,0}$, P_0 performs $U_{1,1}$ on the particles $q_{m/2-1}, \ldots, q_1$, that is, he encodes a fake message "11" on these particles. Similarly, $P_{m/2}$ also applies $U_{1,1}$ on the particles $q_{m-1}, \ldots, q_{m/2+1}$. At the end of the protocol, $\dot{K}$ is accepted by all participants, because they obtain the same values, $K_0 = K_1 = \cdots = K_{m-1} =$ "11," and no error occurs.

Recently, some subtle improved methods have been proposed to stand against Liu's attack. One [19,20] is to introduce a third party that helps participants fairly agree on a key. The third party is generally required to be trusted or semitrusted, which implies that this additional condition greatly limits the practical application of these improved protocols. A second method has been proposed by Wang *et al.* [21], which can achieve asymptotic security. In this protocol, to resist a t dishonest participants' collusion attack, all participants are divided into t groups, each of which performs a circle-type quantum key agreement protocol. Obviously, when one achieves security against the collusion attack by any number of dishonest participants, the protocol is changed to the complete-graph-type. In addition, a method has recently been adapted in designing the CMQKA protocol, in which the encoding operations for one participant on different particles are different. Namely, the operations, $E_i[1], E_i[2], \ldots,$ and $E_i[m-1]$, are not the same. In this way, three interesting groups of encoding operations are designed to achieve the key agreement task [22–24]. Moreover, these three protocols are secure against Liu's attack.

III. *m*-1 DISHONEST PARTICIPANTS' COLLUSION ATTACK

A. The proposed attack

Further study revealed two key leakages in these protocols, which may be the reason why these protocols are sensitive to collusion attacks. One is the encoding operation. In the CMQKA protocols, to achieve the same agreement key, each participant's encoding operations on different particle sequences are the same or related. That is, each participant performs his encoding operation $m - 1$ times, which may make some indistinguishable operations distinguishable. The other is the selection of the samples. In step G5, the samples are chosen by the participants, which will provide a chance for dishonest participants to cover up their attacks. Based on these two loopholes, quantum state discrimination is utilized to design a collusion attack that is more powerful than Liu's attack.

In the presented attack, only one participant, P_0, is honest, and the remaining $m - 1$ participants, $\dot{P}_i$ ($i = 1, 2, \ldots, m - 1$), are dishonest and conspire to attack. These $m - 1$ participants predetermine a fake key $\dot{K}$ and attempt to deceive P_0 into accepting this fake 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.

First, these $m - 1$ dishonest participants, i.e., $\dot{P}_i$ ($i \neq 0$), prepare $m - 1$ fake particles, each of which is in a state $|\Phi\rangle$, and orderly send them to P_0. Before the particle sequence $Q_{0\rightarrow 0}$ is sent back to P_0, these dishonest participants held $m - 1$ fake particles that have been encoded by P_0. Namely, these fake particles are in the state $E_0[1]|\Phi\rangle \otimes E_0[2]|\Phi\rangle \otimes \cdots \otimes E_0[m-1]|\Phi\rangle$. When P_0's encoding operation set is Ξ_0 (or Ξ_1) for his secret $S_0 = 0$ (or 1), these dishonest participants utilize a certain method to discriminate the following two sets of states:

$$\Delta_0 = \{E_0[1]|\Phi\rangle \otimes \cdots \otimes E_0[m-1]|\Phi\rangle \mid E_0[j] \in \Xi_0\},$$
$$\Delta_1 = \{E_0[1]|\Phi\rangle \otimes \cdots \otimes E_0[m-1]|\Phi\rangle \mid E_0[j] \in \Xi_1\}. \quad (6)$$

Suppose a deterministic or almost correct result is obtained with probability $1 - \rho$, and an uncertain one with probability ρ. In other words, there are approximately $n(1 + \zeta)(1 - \rho)$ deterministic results and $n(1 + \zeta)\rho$ uncertain results. Obviously if the result is deterministic or almost correct, it is easy for these dishonest participants to infer the corresponding bit of P_0's secret S_0. Based on the bits of S_0 and $\dot{K}$, they apply an appropriate operation on the corresponding particle of sequence $Q_{0\to 0}$ and transmit it to P_0. Otherwise, the particle is sent back to P_0 directly. In the eavesdropping check process, these $m-1$ dishonest participants select all or part of $n(1+\zeta)\rho$ uncertain results as the samples. In this way, they can reduce the error rate and cover up their attack actions. Evidently, when m is sufficiently large, the presented attack is valid because it cannot be detected in the eavesdropping check process.

Next, the securities for the CMQKA protocols under the presented attack are discussed. At first, for the protocols with the same encoding operations, there is only one operation in the set $\Xi_0 = \{\chi_0\}$ (or $\Xi_1 = \{\chi_1\}$), and the corresponding state is $\overbrace{\chi_0|\Phi\rangle \otimes \ldots \otimes \chi_0|\Phi\rangle}^{m-1}$ (or $\overbrace{\chi_1|\Phi\rangle \otimes \ldots \otimes \chi_1|\Phi\rangle}^{m-1}$). From the conclusions of Refs. [31,32], it can be directly deduced that these two operations can be infallibly discriminated as long as m is sufficiently large. This implies that all CMQKA protocols with the same encoding operations are insecure, because they are vulnerable against the presented attack.

Now, the case in which the encoding operations are different is considered. Since the operations cannot be perfectly discriminated, CMQKA protocols with different encoding operations are generally more secure than those with the same operations. However, except for perfect discrimination, there are two other common discrimination methods. One is unambiguous discrimination [30], which distinguishes them without error but leaves a nonzero probability for an inconclusive answer. The other is minimum-error discrimination [27], in which an inconclusive outcome is not allowed, and the probability of making an incorrect guess is minimized. For these two discriminations, there may exist a nonzero probability $1-\rho$ of obtaining a deterministic result or an almost correct one, which causes this type of protocol to be insecure. In the following section, to illustrate this more clearly, we take the protocol (Huang's protocol) presented in Ref. [22] as an example.

B. An example

To stand against Liu's attack, Huang *et al.* propose an improved multiparty quantum key agreement protocol with Bell states [22]. The signal particle transmission of Huang's protocol is similar to that of the general CMQKA protocol mentioned in Sec. II B 1. Specifically, in Huang's protocol, Bell states are used as the information carriers, and one particle of each Bell state travels among m participants. The general process of the agreement is reviewed briefly as follows.

(H1) Each participant P_i generates a random $n(1+\zeta)$-bit string that represents his secret, $S_i = \{s_i^1, s_i^2, \ldots, s_i^{n(1+\zeta)}\}$, and a sequence of $m-1$ $n(1+\zeta)$-bit strings, $B_i = \{B_i[1], B_i[2], \ldots,\ B_i[m-1] \ \mid\ B_i[k] = b_i^1[k], b_i^2[k], \ldots, b_i^{n(1+\zeta)}[k]\}$ (K_i and RH_i in the original protocol of Ref. [22]), where the subscript $i = 0, 1, \ldots, m-1$ indicates the ith participant and the superscript $j = 1, 2, \ldots, n(1+\zeta)$ indicates the jth bit of one participant's secret. Then, P_i prepares $n(1+\zeta)$ two-qubit entangle pairs, each of which is randomly in one of four states, $\{|BS_{00}\rangle = |\psi(0,0)\rangle,\ \ |BS_{01}\rangle = |\psi(1,0)\rangle,\ \ |DBS_{00}\rangle = \frac{1}{\sqrt{2}}(|\psi(0,0)\rangle - i|\psi(1,0)\rangle),\ |DBS_{01}\rangle = \frac{1}{\sqrt{2}}(|\psi(1,0)\rangle - i|\psi(0,0)\rangle)\}$. Finally, he takes two particles from each entangled pair to form two ordered particle sequences, and sends one particle sequence to the next participant.

(H2) In terms of two random bit sequences, S_i and R_i, each participant P_i performs his encoding operation $R_Z(\frac{\pi}{2})^{b_i^j[k]}Z^{s_i^j}$ on the jth traveling particle, where $R_Z(\frac{\pi}{2}) = \frac{1}{\sqrt{2}}I - \frac{1}{\sqrt{2}}iZ$. Then, he sends the particle sequence that contains his secret inputs to the next participant. This process continues until the particle sequence is sent back to P_i.

(H3) After all traveling particle sequences return to the hands of the participants who prepared them, each participant P_i declares the value of R_i. Based on these public messages, each participant P_i calculates a bit sequence $\hat{S}_i$ with a length of $n(1+\zeta)$ by measuring his entangled pairs. Obviously, when there are no attacks, the value for this secret sequence is $\hat{S}_i = \{\hat{s}_i^1, \hat{s}_i^2, \ldots, \hat{s}_i^{n(1+\zeta)} \mid \hat{s}_i^j = s_0^j \oplus s_1^j \oplus \cdots \oplus s_{m-1}^j\}$.

(H4) The eavesdropping check process is executed. Namely, each participant P_i randomly selects $\frac{n\zeta}{m}$ samples, and requires the other participants to announce their secret inputs. If the corresponding bit of his secret sequence $\hat{s}_i^j$ is inconsistent with the calculation of their secret inputs, he terminates the protocol. Otherwise, P_i accepts the remaining part of $\hat{S}_i$ as his raw agreement key.

It is not hard to see that the main improved method of Huang's protocol is the introduction of a controlling operation $R_Z(\frac{\pi}{2})$. In this way, the participants can encode the same bit 0 (1) on different traveling particles by applying one of two operations, I or $R_Z(\frac{\pi}{2})$ [Z or $R_Z(\frac{\pi}{2})Z$]. Namely, $\Xi_0 = \{I, R_Z(\frac{\pi}{2})\}$ and $\Xi_1 = \{Z, R_Z(\frac{\pi}{2})Z\}$. In the presented attack, according to the conclusion in Ref. [33], the maximally entangled states, Bell states, are used as the fake particles. Concretely, $m-1$ dishonest participants prepare $m-1$ two-particle pairs in the state $|\psi(0,0)\rangle$, and send one particle of each entangled pair to the honest participant P_0 in turn. After P_0 encodes his secret on this particle and sends it to the next participant, they intercept this particle. In this way, these $m-1$ dishonest participants have $m-1$ entangled pairs.

These particle pairs are in a set of states $\{|BS_{00}\rangle, |DBS_{00}\rangle = R_Z(\frac{\pi}{2})|\psi(0,0)\rangle\}$ or $\{|BS_{01}\rangle, |DBS_{01}\rangle = R_Z(\frac{\pi}{2})|\psi(1,0)\rangle\}$, which corresponds to P_0's secret bit $s_0^j = 0$ or 1. Obviously, these two sets of states cannot be discriminated unambiguously. However, the states can be discriminated with a minimum-error rate. From the well-known result [27] that to discriminate between two mixed states $\rho_0 = \frac{1}{2}(|BS_{00}\rangle\langle BS_{00}| + |DBS_{00}\rangle\langle DBS_{00}|)$ and $\rho_1 = \frac{1}{2}(|BS_{01}\rangle\langle BS_{01}| + |DBS_{01}\rangle\langle DBS_{01}|)$, the minimum-error probability attainable is derived to be $p_E = \frac{1}{2} - \frac{1}{2}||\frac{1}{2}(\rho_0 - \rho_1)|| = \frac{1}{2} - \frac{\sqrt{2}}{4} \approx 0.146 < 0.25$, where $||\Lambda|| = \mathrm{Tr}(\sqrt{\Lambda^\dagger\Lambda})$. Obviously, to achieve the minimum-error rate, a project measurement is performed in the basis, $\{\cos(\frac{\pi}{8})|BS_{00}\rangle + i\sin(\frac{\pi}{8})|BS_{01}\rangle,\ \ \sin(\frac{\pi}{8})|BS_{00}\rangle - i\cos(\frac{\pi}{8})|BS_{01}\rangle, |\psi(0,1)\rangle, |\psi(1,1)\rangle\}$.

For simplicity, we can adopt a direct method to distinguish these two mixed states, while the corresponding error rate is 0.25. That is, a Bell state measurement is

TABLE I. Four possible results and the corresponding probabilities.

η	0	1	2	3
Prob	0.015625	0.140625	0.421875	0.421875

applied on a two-qubit pair that is in one of four states $\{|BS_{00}\rangle, |DBS_{00}\rangle, |BS_{01}\rangle, |DBS_{01}\rangle\}$. When the measurement result is $|BS_{00}\rangle$ ($|BS_{01}\rangle$), we guess the particles are in the state ρ_0 (ρ_1), i.e., $S_0 = 0$ ($S_0 = 1$). Since $|DBS_{00}\rangle = \frac{1}{\sqrt{2}}(|BS_{00}\rangle + i|BS_{01}\rangle)$ and $|DBS_{01}\rangle = \frac{1}{\sqrt{2}}(|BS_{01}\rangle - i|BS_{00}\rangle)$, the error rate for such a guess is 0.25. This is not equal to 50%, which implies that one can obtain partial information about S_0 from the measurement result. In particular, when m is large enough, these $m-1$ dishonest participants can guess P_0's secret with a very small error rate. Moreover, they can further reduce the error rate by choosing some values as test samples.

Suppose $m = 5$, i.e., there is one honest participant P_0 and four dishonest participants, $\dot{P}_1$, $\dot{P}_2$, $\dot{P}_3$, and $\dot{P}_4$. The secret bits of P_0 and $m-1$ dishonest participants are S_0, S_1, ..., S_4, respectively. Therefore, the genuine agreement bit sequence is $K = S_0 \oplus S_1 \oplus \cdots \oplus S_4$, and the fake sequence is $\dot{K} = S_1 \oplus \cdots \oplus S_4$. In this case, these $m-1$ dishonest participants try to make P_0 accept the fake sequence as the agreement key, which requires that no error is introduced in the eavesdropping check. They can achieve this goal by executing the following special attack actions.

In step H2, for the jth position, these four dishonest participants prepare four entangled pairs in the initial state $|BS_{00}\rangle$, and send one particle of each entangled pair to P_0 in order. Meanwhile, they honestly encode their secret bits to the jth signal particle generated by P_0. Before $\dot{P}_4$ sends this particle back to P_0, these dishonest participants hold four entangled pairs, on which P_0 performed his encoding operations. They can apply Bell state measurements on the first three entangled pairs and keep the fourth pair untouched. When $S_0 = 0$ (or 1), there are η $|BS_{01}\rangle$ ($|BS_{00}\rangle$) among the three measurement results, where $\eta = 0, 1, 2, 3$. Through simple calculations, we can obtain the probabilities for η $|BS_{01}\rangle$ ($|BS_{00}\rangle$), which are listed in Table I.

Then, these dishonest participants can adopt a direct method to guess the value of s_0^j according to their results. Concretely, if $\eta \geqslant 2$, they think the value is zero, i.e., $\tilde{s}_0^j = 0$. If $\eta \leqslant 1$, $\tilde{s}_0^j = 1$. Finally, if $\tilde{s}_0^j$ is equal to 1, these dishonest participants think that the jth bit of K is not equal to that of $\dot{K}$, perform Z operation on P_0's signal particle, and send it to P_0. Otherwise, they send it back directly.

In step H3, P_0 measures his signal particle pairs to obtain his secret bit sequence $\hat{S}_i$. Obviously, when the guess is correct, the corresponding bit of $\hat{S}_i$ is equal to that of $\dot{K}$, i.e., $\hat{s}_i^j = \dot{k}_j$. Otherwise, $\hat{s}_i^j = \dot{k}_j \oplus 1$. In step H4, because the controlling sequence R_0 declared by P_0 is known to these dishonest participants, they can select a right basis to measure the untouched entangled pairs and deduce the value of s_0^j. After this, if $\tilde{s}_0^j \neq s_0^j$, these dishonest participants announce fake messages, the sum of which is equal to $\hat{s}_0^j$. Otherwise, i.e., the guess is right, they announce their secret inputs honestly. Obviously, in this way, the attack action cannot be found, because this announcement cannot introduce any errors.

Next, the success rate for these dishonest participants' predetermining the agreement key is discussed. It is evident that these dishonest participants can determine the key by themselves when they successfully guess the value of s_0^j in the attack. Thus, from Table I, the correct rate of the guess is $\text{Prob}(\eta = 3) + \text{Prob}(\eta = 2) = 0.843\,75$. In other words, the guess is wrong with a probability of $\text{Prob}(\eta = 1) + \text{Prob}(\eta = 0) = 0.15625$. In this case, P_0 acknowledges that the agreement key is k_j instead of k_j^*. However, these dishonest participants can select this bit as a test sample. Hence, when $\zeta > 0.2428$, the condition $\frac{\zeta\frac{(m-1)}{m}}{1+\zeta} > 0.156\,25$ is satisfied. Four dishonest participants are able to choose all bits in which they guessed wrong as the samples. In this way, the remaining bits for K, which are equal to that for $\dot{K}$, form the agreement key. Since no error is introduced in the eavesdropped check process, this fake agreement key is accepted by P_0.

To illustrate the attack more clearly, a case ($m = 5, n = 16, \zeta = 0.25$) is taken as an example. Supposing that P_0 has a secret $(1+\zeta)\times n = 20$-bit sequence, $S_0 =$ "11110011010010000100," four dishonest participants' fake bit sequence is $\dot{K} =$ "00000000000000000000." Therefore, the genuine sequence is $K = S_0 \oplus \dot{K} = S_0$. After measuring three entangled pairs that contain P_0 secret inputs, these dishonest participants obtain the result of the guess, $\tilde{S}_0 =$ "10110010010010010100." Here, because the error of the guess is 0.1563, we can assume that $0.1563 \times 20 \approx 3$ results (e.g., the second, eighth, and fifteenth bits) are incorrect. According to $\tilde{S}_0$ and $\dot{K}$, dishonest participants perform Z or I operation on P_0's signal particles. In step H3, P_0 obtains his bit sequence $\hat{S}_0 = S_0 \oplus \tilde{S}_0 =$ "01000001000000100000." After P_0 declares R_i, dishonest participants can deduce S_0 by measuring the untouched entangled pair. In terms of S_0 and $\tilde{S}_0$, they know the positions of three incorrect results. For $\zeta = 0.25$, each dishonest participant can choose $\frac{\zeta\times n}{m} \approx 1$ bit as his sample. Therefore, these three bits are able to be selected as the samples by four dishonest participants. At last, the remaining bit sequence "000000000000000" is accepted as the agreement key, which means that these dishonest participants successfully break the fairness of Huang's protocol.

IV. THE PROPOSED CMQKA PROTOCOL

In this section, a CMQKA protocol with Bell states is proposed, in which quantum state discrimination and hash function are utilized to plug up the two loopholes mentioned in the above section. Here, the hash function is required to be preimage resistant, that is, it is difficult to find an input that maps to a certain hash value. For the sake of clarity, let us start with a specific three-party (i.e., $m = 3$) case, in which three participants P_0, P_1, and P_2 respectively hold three random bit strings, $S_0 =$ "000110," $S_1 =$ "101011," and $S_2 =$ "100110." These three bit strings represent their secret inputs.

TABLE II. The classical sequences in the three-party protocol.

	S_i	A_i	B_i	C_i	H_i
P_0	000110	001101,011011	010100,010110	001011,011101	0010
P_1	101011	110101,111010	010110,011001	011110,010001	1010
P_2	100110	100101,011011	001101,101001	000011,111101	1001

By the following steps, they can agree on a common key, $K = S_0 \oplus S_1 \oplus S_2$.

In the initialization phase, each participant P_0 (P_1, P_2) first generates two random 12-bit strings, $A_0 = \{A_0[1], A_0[2] \mid A_0[1] = \text{“001101,”}\ A_0[2] = \text{“011011”}\}$ and $B_0 = \{B_0[1], B_0[2] \mid B_0[1] = \text{“010100,”}\ B_0[2] = \text{“010110”}\}$ (A_1 and B_1, A_2 and B_2). From S_0 and A_0 (S_1 and A_1, S_2 and A_2), he can deduce $C_0 = \{C_0[1], C_0[2] \mid C_0[1] = S_0 \oplus A_0[1] = \text{“001011,”}\ C_0[2] = S_0 \oplus A_0[2] = \text{“011101”}\}$ (C_1, C_2). Meanwhile, they agree on a hash function $h : \{0, 1\}^{12} \to \{0, 1\}^4$, and obtain the hash value of B_0 (B_1, B_2), $H_0 = h(B_0) = \text{“0010”}$ (H_1, H_2). Obviously, this hash function cannot be preimage resistant, because the hash value is too short, only 4 bits. Generally speaking, for a hash function to be preimage resistant, the minimum length of the output is 80 bits. Therefore, this is just an example, where we need to adopt a preimage-resistant hash function, e.g., SHA or MD5, in the practical application of the presented protocol.

The concrete values of these classical bit sequences are listed in Table II. After that, three hash values are declared by these participants publicly. In addition, each participant P_0 (P_1, P_2) prepares six Bell states as the signal particles, which are all in the initial state $|\psi(0, 0)\rangle$, and obtains two ordered qubit sequences, $Q_{0\to1}$ and R_0 ($Q_{1\to2}$ and R_1, $Q_{2\to0}$ and R_2).

In the encoding phase, three signal particle sequences, $Q_{0\to1}$, $Q_{1\to2}$, and $Q_{2\to0}$, are transmitted among three participants who perform the encoding operation on these particles. For example, P_0 holds R_0 in his hands and sends $Q_{0\to1}$ to P_1 first. After receiving $Q_{0\to1}$, P_1 encodes the messages, $A_1[1]$, $B_1[1]$, and $C_1[1]$, on the traveling particles. Concretely, if the jth bit of $B_1[1]$ is 0 (or 1), P_1 performs the operation I (or H) on the jth qubit of $Q_{0\to1}$, $j = 1, 2, \ldots, 6$. Then, in terms of the values of $A_1[1]$ and $C_1[1]$, he performs one of four Pauli operations on the corresponding particle, i.e., “xy” $\mapsto U_{x,y}$. Therefore, after the encoding operations $U_{1,0} \otimes U_{1,1}H \otimes U_{0,1} \otimes U_{1,1}H \otimes U_{0,1}H \otimes U_{1,0}$, these six two-qubit entangled pairs are in the state $|\psi(1, 0)\rangle|\Psi(1, 1)\rangle|\psi(0, 1)\rangle|\Psi(1, 1)\rangle|\Psi(1, 0)\rangle|\psi(1, 0)\rangle$. The encoded particle sequence that is named as $Q_{0\to2}$ is sent from P_1 to P_2. Similarly, P_2 encodes his messages, $A_2[2]$, $B_2[2]$, and $C_2[2]$, by applying the operation $U_{0,1}H \otimes U_{1,1} \otimes U_{1,1}H \otimes U_{0,1} \otimes U_{1,0} \otimes U_{1,1}H$ on $Q_{0\to2}$, and sends the encoded sequence $Q_{0\to0}$ back to P_0. The concrete states of three particle sequences are listed in Table III.

In the decoding phase, three participants respectively announce the values of B_0, B_1, and B_2, after acknowledging that three sequences, $Q_{0\to0}$, $Q_{1\to1}$, and $Q_{2\to2}$, are received by them. If $H_0 \neq h(B_0)$, $H_1 \neq h(B_1)$ or $H_2 \neq h(B_2)$, they abort the protocol. Otherwise, in terms of these public messages, P_0 (P_1, P_2) performs I or H operation on the corresponding particle of $Q_{0\to0}$ ($Q_{1\to1}$, $Q_{2\to2}$), and then makes Bell state measurements on the particles of sequences R_0 and $Q_{0\to0}$ (R_1 and $Q_{1\to1}$, R_2 and $Q_{2\to2}$). From the measurement results and his secret messages, three participants can deduce a six-bit sequence $\hat{S}_0$, $\hat{S}_1$, and $\hat{S}_2$, respectively. For example, based on $B_1[1] \oplus B_2[2] = \text{“111111,”}$ P_0 applies the operation $H \otimes H \otimes H \otimes H \otimes H \otimes H$ on six particles of $Q_{0\to0}$. Then, according to the measurement result $|\psi(0, 0)\rangle|\psi(0, 0)\rangle|\psi(1, 0)\rangle|\psi(0, 1)\rangle|\psi(1, 1)\rangle|\psi(0, 1)\rangle$, he deduces that the sum of P_1's secret input and P_2 's is “001101,” where $|\psi(0, 0)\rangle, |\psi(1, 1)\rangle \mapsto$ “0” and $|\psi(0, 1)\rangle, |\psi(1, 0)\rangle \mapsto$ “1.” By adding his own secret input S_0, P_0 obtains $\hat{S}_0$=“001011.” In the same way, the other two participants respectively get $\hat{S}_1$ and $\hat{S}_2$. Obviously, if there is no eavesdropping, $\hat{S}_1$=$\hat{S}_2$=$\hat{S}_0$.

In the eavesdropping check phase, three participants calculate a six-bit sequence $D = B_0[1] \oplus B_0[2] \oplus B_1[1] \oplus B_1[2] \oplus B_2[1] \oplus B_2[2] = \text{“101001.”}$ In accordance with D, the second, fourth, and fifth positions are chosen as the samples, where the corresponding bit of D is “0.” Therefore, $\hat{S}_0$ is divided into two sequences, $T_0 = \text{“001”}$ and $K_0 = \text{“011”}$ (the remainder), the lengths of which are 3, i.e., $n_1 = n_2 = 3$. Meanwhile, since $D \in \{0, 1\}^6$ can be represented as a number, $41 = 2^5 + 2^3 + 1$, they can obtain $\delta = D \mod n_1 = 2$. Thus, P_0 announces the third bit of T_0, i.e., $T_0' = \text{“1.”}$ Similarly, P_1 and P_2 respectively declare the first bit of T_1 and the second bit of T_2, i.e., $T_1' = \text{“0”}$ and T_2'=“0.” A new sequence $T' = \text{“001”}$ is formed by these three public messages. Participant P_0 (P_1, P_2) can detect the eavesdropping by comparing T' with T_0 (T_1, T_2). If $T_0 = T_1 = T_2 = T'$, three participants accept the

TABLE III. The change of the states of three signal particle sequences during the encoding phase of the three-party protocol.

P_0	$P_1 : Q_{0\to1} \xrightarrow{(A_1[1],B_1[1],C_1[1])} Q_{0\to2}$	$P_2 : Q_{0\to2} \xrightarrow{(A_2[2],B_2[2],C_2[2])} Q_{0\to0}$
$Q_{0\to1}R_0 : \otimes_{j=1}^{6}\|\psi(0, 0)\rangle$	$\|\psi(1, 0)\rangle\|\Psi(1, 1)\rangle\|\psi(0, 1)\rangle\|\Psi(1, 1)\rangle\|\Psi(1, 0)\rangle\|\psi(1, 0)\rangle$	$\|\Psi(0, 0)\rangle\|\Psi(0, 0)\rangle\|\Psi(1, 0)\rangle\|\Psi(0, 1)\rangle\|\Psi(1, 1)\rangle\|\Psi(0, 1)\rangle$
P_1	$P_2 : Q_{1\to2} \xrightarrow{(A_2[1],B_2[1],C_2[1])} Q_{1\to0}$	$P_0 : Q_{1\to0} \xrightarrow{(A_0[2],B_0[2],C_0[2])} Q_{1\to1}$
$Q_{1\to2}R_1 : \otimes_{j=1}^{6}\|\psi(0, 0)\rangle$	$\|\psi(1, 0)\rangle\|\psi(0, 0)\rangle\|\Psi(0, 0)\rangle\|\Psi(0, 1)\rangle\|\psi(0, 1)\rangle\|\Psi(1, 1)\rangle$	$\|\psi(1, 0)\rangle\|\Psi(1, 1)\rangle\|\Psi(1, 1)\rangle\|\psi(0, 0)\rangle\|\Psi(0, 0)\rangle\|\Psi(0, 0)\rangle$
P_2	$P_0 : Q_{2\to0} \xrightarrow{(A_0[1],B_0[1],C_0[1])} Q_{2\to1}$	$P_1 : Q_{2\to1} \xrightarrow{(A_1[2],B_1[2],C_1[2])} Q_{2\to2}$
$Q_{2\to0}R_2 : \otimes_{j=1}^{6}\|\psi(0, 0)\rangle$	$\|\psi(0, 0)\rangle\|\Psi(0, 0)\rangle\|\psi(1, 1)\rangle\|\Psi(0, 1)\rangle\|\psi(0, 1)\rangle\|\psi(1, 1)\rangle$	$\|\psi(1, 0)\rangle\|\psi(1, 1)\rangle\|\Psi(1, 0)\rangle\|\Psi(0, 1)\rangle\|\psi(1, 1)\rangle\|\Psi(0, 1)\rangle$

remainder of the bits as the raw agreement key, i.e., $K = K_0 = K_1 = K_2 =$ "011," and achieve the key agreement task successfully.

Here, it is evident that the positions of the samples are determined by the value of D, which is the sum of B_is. Since the hash value $H_i = h(B_i)$ is announced during the initialization phase, the participant is not free to declare the value of B_i in the decoding phase. This implies that the dishonest participant cannot cover up his attack action by selecting the uncertain results as the samples. In addition, since the hash function is a many-to-one mapping, one cannot derive a unique correct B_i from the hash value $h(B_i)$, even if he has unlimited computing power. For the encoding operations, we will prove in the next section that these operations cannot be distinguished by unambiguous discrimination and minimum-error discrimination. Therefore, in the proposed protocol, the two security loopholes mentioned in Sec. III have been overcome through quantum state discrimination and the classical hash function. Moreover, the above three-party protocol can be directly generalized to the multiparty case, as described below.

Suppose there are m parties, P_i $(i = 0, 1, \ldots, m-1)$, who hold their own secret n-bit strings $S_i = \{s_i^1, s_i^2, \ldots, s_i^n\}$, respectively. After executing the following steps, these participants obtain an agreement key K with a length of approximately $\frac{n}{2}$.

Step (1) Each participant P_i $(i = 0, 1, \ldots, m-1)$ generates two sequences of $m-1$ random n-bit strings, A_i=$\{A_i[1], A_i[2], \ldots, A_i[m-1] \mid A_i[k] = a_i^1[k] \ldots a_i^n[k], a_i^j[k] \in \{0, 1\}\}$ and $B_i = \{B_i[1], B_i[2], \ldots, B_i[m-1] \mid B_i[k] = b_i^1[k] \ldots b_i^n[k], b_i^j[k] \in \{0, 1\}\}$. Then, according to S_i and A_i, he can obtain a sequence of $m-1$ n-bit strings $C_i = \{C_i[1], C_i[2], \ldots, C_i[m-1] \mid C_i[k] = c_i^1[k] \ldots c_i^n[k], c_i^j[k] \in \{0, 1\}\}$, where

$$c_i^j[k] = a_i^j[k] \oplus s_i^j, \tag{7}$$

and $k = 1, 2, \ldots, m-1$, $j = 1, 2, \ldots, n$. In addition, these m participants agree on a preimage-resistant hash function $h : \{0, 1\}^* \to \{0, 1\}^w$. Finally, P_i keeps his strings A_i, B_i, and C_i secret and declares the hash value, $H_i = h(B_i)$, publicly. Note that, since the function h is preimage resistant, it is impossible to derive the input B_i from its hash value H_i.

Step (2) Each participant P_i prepares n two-qubit entangled pairs and obtains two ordered particle sequences, $Q_{i\to i\tilde{\oplus}1} = \{q_i^1, q_i^2, \ldots, q_i^n\}$ and $R_i = \{r_i^1, r_i^2, \ldots, r_i^n\}$. Each two-qubit pair (q_i^j, r_i^j) is in an initial state $|\psi(0, 0)\rangle$. After that, P_i holds particle sequence R_i in his hands and sends $Q_{i\to i\tilde{\oplus}1}$ to the next participant $P_{i\tilde{\oplus}1}$.

Step (3) After receiving the signal particle sequence $Q_{i\to i\tilde{\oplus}1}$, participant $P_{i\tilde{\oplus}1}$ $(i = 0, 1, \ldots, m-1)$ executes his encoding operation based on his strings $A_{i\tilde{\oplus}1}[1]$, $B_{i\tilde{\oplus}1}[1]$, and $C_{i\tilde{\oplus}1}[1]$. Concretely, for the jth particle of sequence $Q_{i\to i\tilde{\oplus}1}$, he performs the local unitary operation $U_{a_i^j[1], c_i^j[1]} H^{b_i^j[1]}$ on particle q_i^j. In this way, he obtains a new particle sequence $Q_{i\to i\tilde{\oplus}2}$ that contains his secret messages $A_{i\tilde{\oplus}1}[1]$, $B_{i\tilde{\oplus}1}[1]$, and $C_{i\tilde{\oplus}1}[1]$. Finally, he sends $Q_{i\to i\tilde{\oplus}2}$ to participant $P_{i\tilde{\oplus}2}$

Step $(l+2)$ $(l = 2, 3, \ldots, m-1)$: In the same way as step 3, participant $P_{i\tilde{\oplus}l}$ $(i = 0, 1, \ldots, m-1)$ encodes his secret messages $A_{i\tilde{\oplus}l}[l]$, $B_{i\tilde{\oplus}l}[l]$, and $C_{i\tilde{\oplus}l}[l]$ on the sequence $Q_{i\to i\tilde{\oplus}l}$, which is transmitted from the previous participant $P_{i\tilde{\oplus}(l-1)}$. After that, he sends the encoded sequence $Q_{i\to i\tilde{\oplus}(l+1)}$ to participant $P_{i\tilde{\oplus}(l+1)}$.

Step $(m+2)$: When he receives the particle sequence $Q_{i\to i}$, participant P_i $(i = 0, 1, \ldots, m-1)$ sends the acknowledgment to the other participants. After all participants hold the traveling particles generated by themselves, they announce the secret messages B_i in random order. Then, each participant P_i takes advantage of the irreversibility of the hash function h to verify the correctness of B_j $(j \neq i)$ for the other $m-1$ participants. If $h(B_i) \neq H_i$, all participants think that there exist some dishonest participants and abort the protocol. Otherwise, they are assured that B_i is genuine and continue the protocol.

Step $(m+3)$: Each participant P_i $(i = 0, 1, \ldots, m-1)$ holds two participle sequences $Q_{i\to i}$ and R_i. In terms of the public messages $B_{i\tilde{\oplus}k}[k]$ $(k = 1, 2, \ldots, m-1)$, he performs the operation H or I on the traveling particles. Concretely, if $b^j_{i\tilde{\oplus}1}[1] \oplus b^j_{i\tilde{\oplus}2}[2] \oplus \cdots \oplus b^j_{i\tilde{\oplus}(m-1)}[m-1] = 1$, he applies H on the particle q_i^j. Otherwise, he does nothing, i.e., the operation I is chosen. After that, P_i performs Bell state measurements on each two-particle pair and obtains the result $|\psi(u_i^j, v_i^j)\rangle$. In accordance with these n measurement results, he is able to deduce $\hat{S}_i = \{\hat{s}_i^1, \hat{s}_i^2, \ldots, \hat{s}_i^n\}$, where $\hat{s}_i^j = u_i^j \oplus v_i^j \oplus s_i^j$.

Step $(m+4)$: All participants execute the eavesdropping check process. In this process, each participant P_i calculates the sum of B_i and obtains a bit sequence D with a length of n, i.e., $D = \{d_1, d_2, \ldots, d_n \mid d_j = \oplus_{i=0}^{m-1} B_i[j]\}$. If the value of d_j is equal to zero, the corresponding bit $\hat{s}_i^j$ is selected as a sample. In this way, P_i divides the sequence $\hat{S}_i$ into two ordered bit sequences with a length of approximately $\frac{n}{2}$, the sample sequence $T_i = \{t_i^1, t_i^2, \ldots, t_i^{n_1}\}$ and the information sequence $K_i = \{k_i^1, k_i^2, \ldots, k_i^{n_2}\}$, where $n_1 \approx n_2 \approx \frac{n}{2}$ and $n_1 + n_2 = n$. Next, in terms of D, P_i calculates $\delta = (d_1 \times 2^{n-1} + d_2 \times 2^{n-2} + \cdots + d_n \times 2^0) \mod n_1$ and declares part of T_i, $T_i' = \{t_i^{(\delta+i) \mod n_1}, t_i^{(\delta+i+m) \mod n_1}, \ldots, t_i^{(\delta+i+\lfloor n_1/m \rfloor \times m) \mod n_1}\}$. Finally, based on these public messages, all participants obtain a new n_1-bit sequence T', which consists of m T_i's. Each participant can compare this bit sequence with their own T_i. Obviously, if $\hat{S}_1 = \hat{S}_2 = \cdots = \hat{S}_{m-1}$, then all T_i are equal to T'. In this case, all participants accept $K = K_0 = K_1 = \cdots = K_{m-1}$ as the raw agreement key. Otherwise, the protocol is abandoned.

V. PROTOCOL ANALYSIS

In the proposed protocol, since the secret input of the participant is a random bit string, there is no need to discuss the privacy of the protocol. Therefore, in this section, we focus on the first three conditions, and show that the proposed protocol is correct, fair, and secure in theory.

A. Correctness

For a key agreement protocol, it is correct, which means that all participants must eventually get the same key. It is easy for CMQKA protocols with the same encoding operations to satisfy this condition. However, in the proposed protocol, the encoding operations, which are performed by a participant on the different signal particles at the same order, are different. Thus, the correction of the proposed protocol should be considered. In the following, it is shown that the keys obtained by all participants are equal.

Without loss of generality, the jth agreement key is taken as an example. That is, we discuss whether or not the following equation holds:

$$\hat{s}_0^j = \hat{s}_1^j = \cdots = \hat{s}_{m-1}^j. \tag{8}$$

In this case, the corresponding value of each participant P_i's secret bit strings S_i $(i = 0, 1, \ldots, m-1)$ is s_i^j; those of classical messages A_i, B_i, and C_i are $\{a_i^j[1], a_i^j[2], \ldots, a_i^j[m-1]\}$, $\{b_i^j[1], b_i^j[2], \ldots, b_i^j[m-1]\}$, and $\{c_i^j[1], c_i^j[2], \ldots, c_i^j[m-1]\}$, respectively. So, according to Eq. (7), we have

$$a_i^j[1] \oplus c_i^j[1] = \cdots = a_i^j[m-1] \oplus c_i^j[m-1] = s_i^j. \tag{9}$$

In the protocol, in order to obtain $\hat{s}_0^j$, P_0 generates a two-particle pair $(q_0^j,\ r_0^j)$ in the initial state $|\psi(0,0)\rangle$. After that, the remaining participants P_i $(i = 1, 2, \ldots, m-1)$ orderly perform their encoding operations, $U_{a_1^j[1],c_1^j[1]}H^{b_1^j[1]}$, $U_{a_2^j[2],c_2^j[2]}H^{b_2^j[2]}, \ldots, U_{a_{m-1}^j[m-1],c_{m-1}^j[m-1]}H^{b_{m-1}^j[m-1]}$ on the traveling particle q_0^j. Thus, in step $(m+3)$, this entangled pair is in the state

$$\begin{aligned} |\psi(u_0, v_0)\rangle = {} & H^{\oplus_{l=1}^{m-1} b_l^j[l]} U_{a_{m-1}^j[m-1],c_{m-1}^j[m-1]} \\ & H^{b_{m-1}^j[m-1]} \ldots U_{a_1^j[1],c_1^j[1]} H^{b_1^j[1]} |\psi(0,0)\rangle. \end{aligned} \tag{10}$$

From Eq. (5), we can obtain

$$U_{x,y}H^z = (-1)^{xy} H^{\hat{z}} U_{\hat{x},\hat{y}}, \tag{11}$$

where

$$\hat{z} = z, \quad \hat{x} = \bar{z} \cdot x \oplus z \cdot y, \quad \hat{y} = \bar{z} \cdot y \oplus z \cdot y, \tag{12}$$

and $\bar{z} = z \oplus 1$. From Eqs. (10) and (11), the following equation can be derived:

$$\begin{aligned} |\psi(u_0, v_0)\rangle = {} & (-1)^{\oplus_{l=1}^{m-1}(a_l^j[l] \oplus c_l^j[l])} U_{\hat{a}_{m-1}^j[m-1],\hat{c}_{m-1}^j[m-1]} \\ & \ldots U_{\hat{a}_1^j[1],\hat{c}_1^j[1]} |\psi(0,0)\rangle, \end{aligned} \tag{13}$$

where

$$\begin{aligned} \hat{a}_k^j[k] &= \overline{(\oplus_{l=1}^k b_l^j[l])} a_k^j[k] \oplus (\oplus_{l=1}^k b_l^j[l]) c_k^j[k], \\ \hat{c}_k^j[k] &= \overline{(\oplus_{l=1}^k b_l^j[l])} c_k^j[k] \oplus (\oplus_{l=1}^k b_l^j[l]) a_k^j[k], \end{aligned} \tag{14}$$

and $k = 1, 2, \ldots, m-1$. In terms of Eqs. (3) and (13), we get

$$u_0 = \oplus_{l=1}^{m-1} \hat{a}_l^j[l], \ \ v_0 = \oplus_{l=1}^{m-1} \hat{c}_l^j[l]. \tag{15}$$

So, after measuring the Bell state $|\psi(u_0, v_0)\rangle$, P_0 obtains his agreement key $\hat{s}_0^j$, where

$$\hat{s}_0^j = u_0 \oplus v_0 \oplus s_0^j = s_0^j \oplus s_1^j \oplus \cdots \oplus s_{m-1}^j. \tag{16}$$

Similarly, for the other $m-1$ entangled pairs, (q_i^j, r_i^j) $(i = 1, 2, \ldots, m-1)$, they are in the state $\otimes_{i=1}^{m-1} |\psi(u_i, v_i)\rangle$, after the encoding operations. Here,

$$\begin{aligned} |\psi(u_i, v_i)\rangle = {} & H^{\oplus_{l=1}^{m-1} b_{i\tilde{\oplus} l}^j[l]} U_{a_{i\tilde{\oplus}(m-1)}^j[m-1],c_{i\tilde{\oplus}(m-1)}^j[m-1]} \\ & H^{b_{i\tilde{\oplus}(m-1)}^j[m-1]} \ldots U_{a_i^j[1],c_i^j[1]} H^{b_i^j[1]} |\psi(0,0)\rangle. \end{aligned} \tag{17}$$

In the same way, the following equation is attained:

$$\hat{s}_i^j = u_i \oplus v_i \oplus s_i^j = s_0^j \oplus s_1^j \oplus \cdots \oplus s_{m-1}^j. \tag{18}$$

From Eqs. (16) and (18), it is shown that all participants receive the same agreement key, i.e., Eq. (8) holds. Therefore, the proposed protocol is correct.

B. Fairness

In this section, the security of the proposed protocol in the $m-1$ dishonest participants' collusion attack is analyzed. In the attack, we can assume that P_0 is honest, and the remaining dishonest participants $\dot{P}_i$ $(i = 1, 2, \ldots, m-1)$ conspire to attack the presented protocol. Their purpose is to determine the agreement key by themselves, and succeed in cheating P_0 to accept this fake key.

For the jth bit of the agreement key k^j, these dishonest participants $\dot{P}_i$ want to replace the key $k^j = s_0^j \oplus s_1^j \oplus \ldots s_{m-1}^j$ with a fake key $\dot{k}^j = s_1^j \oplus s_2^j \oplus \ldots s_{m-1}^j$, without introducing any error. Namely, they should make P_0 accept this fake key, i.e., $\hat{s}_0^j = \dot{k}^j$. In step $(m+3)$, P_0 calculates the value of $\hat{s}_0^j$ by measuring the entangled pair $(q_0^j,\ r_0^j)$. Since the particle r_0^j is always in P_0's hands, participants $\dot{P}_i$ should execute their attack action on particle q_0^j before it is sent back to P_0. On the other hand, if these dishonest participants obtain the value of s_0^j, they can apply an appropriate operation on q_0^j, which makes $\hat{s}_0^j = \dot{k}^j$. Concretely, if $s_0^j = 1$, the operation X (or Z) is executed; otherwise, there is no action. Therefore, the key point of this attack is whether the dishonest participants eavesdrop the value of s_0^j before the sequence $Q_{0\to 0}$ is sent from P_{m-1} to P_0 in step $(m+1)$.

According to the procedure of the proposed protocol, only one possible chance may be utilized to obtain s_0^j. That is steps 3 to $(m+1)$, in which P_0 encodes s_0^j on the traveling particles. In this case, the encoding operation is applied by P_0 $(m-1)$ times, which is the same as the general CMQKA protocol in Sec. II B. Hence, similar to the analysis in Sec. III, the key point is changed to discriminate two sets of states, Δ_0 and Δ_1, where $\Xi_0 = \{U_{0,0}, U_{0,0}H, U_{1,1}, U_{1,1}H\}$ and $\Xi_1 = \{U_{0,1}, U_{0,1}H, U_{1,0}, U_{1,0}H\}$.

First, unambiguous discrimination is considered. Without loss of generality, we can assume that dishonest participants prepare m fake particles that are in the initial state:

$$\begin{aligned} |\Phi\rangle = {} & \sum_{\mu_1,\mu_2,\ldots,\mu_{m-1}=0,1} |\mu_1\rangle_{f_1} |\mu_2\rangle_{f_2} \ldots |\mu_{m-1}\rangle_{f_{m-1}} \\ & |\xi_{\mu_1,\mu_2,\ldots,\mu_{m-1}}\rangle_{f_m}. \end{aligned} \tag{19}$$

In step $(i+1)$ $(i = 1, 2, \ldots, m-1)$, $\dot{P}_{m-1}$ sends a fake particle f_i to P_0, instead of the signal particle q_{m-i}^j. When P_0 performs his encoding operation $E_0[i] = U_{a_0^j[i],c_0^j[i]} H^{b_0^j[i]}$ and sends particle f_i to $\dot{P}_1$ in step $(i+2)$, $\dot{P}_1$ intercepts this fake particle. The above action is repeated $m-1$ times. At the end of step $(m+1)$, the dishonest participants hold all fake particles, which is in the state $\otimes_{i=1}^{m-1} E_0[i] \otimes I|\Phi\rangle_{f_1,f_2,\ldots,f_m}$. They try their best to eavesdrop the value of s_0^j by performing a certain positive operator-valued measurement on these fake particles. So, the key of this attack is changed to distinguish two sets of quantum states, $\Gamma_0 = \{\otimes_{i=1}^{m-1} E_0[i] \otimes I|\Phi\rangle \mid E_0[i] \in \Xi_0\}$ and $\Gamma_1 = \{\otimes_{i=1}^{m-1} E_0[i] \otimes I|\Phi\rangle \mid E_0[i] \in \Xi_1\}$. However, since $H = \frac{1}{\sqrt{2}}(X+Z)$, a state $|\gamma\rangle = H \otimes H \otimes \cdots \otimes H \otimes I|\Phi\rangle \in \Gamma_0$ can be written as

$$
\begin{aligned}
|\gamma\rangle &= \left(\frac{1}{\sqrt{2}}\right)^{m-1} (X+Z) \otimes \cdots \otimes (X+Z) \otimes I|\Phi\rangle \\
&= \left(\frac{1}{\sqrt{2}}\right)^{m-1} \sum_{E_0[1],\ldots,E_0[m-1]=X,Z} \left(\otimes_{i=1}^{m-1} E_0[i] \otimes I|\Phi\rangle \right). \quad (20)
\end{aligned}
$$

From the above equation, it is directly derived that the state $|\gamma\rangle \in \Gamma_0$ can be linearly generated by the states of set Γ_1. Similarly, because $iY = \frac{1}{\sqrt{2}}(ZH - XH)$, $I = \frac{1}{\sqrt{2}}(ZH + XH)$, and $iYH = \frac{1}{\sqrt{2}}(Z - X)$, any state from the set Γ_0 is a linear combination of the states of Γ_1, and vice versa. Hence, two sets Γ_0 and Γ_1 are linearly dependent. According to Theorem 2 of Ref. [34], we can conclude that these two sets cannot be unambiguously discriminated.

In the following, the case in which minimum-error discrimination is adopted is discussed. First, the dishonest participants perform a simple attack that is similar to the attack depicted in Sec. III B. That is, they prepare $m-1$ two-particle entangled pairs in the state

$$
\left|\omega_{00}^{(1)}\right\rangle = |0\rangle_{e_1}|\varphi_0\rangle_{e_2} + |1\rangle_{e_1}|\varphi_1\rangle_{e_2}, \quad (21)
$$

where $\langle\varphi_0|\varphi_0\rangle + \langle\varphi_1|\varphi_1\rangle = 1$. Then, $\dot{P}_{m-1}$ sends the fake particle e_1 to P_0. After this particle containing the information about P_0's encoding operation is sent from P_0 to $\dot{P}_1$, $\dot{P}_1$ intercepts particle e_1 and performs a certain minimum-error discrimination. Concretely, if $s_0^j = 0$, the particle pair is in one of four states $\{|\omega_{0\nu_1}^{(1)}\rangle = U_{\nu_1^1,\nu_1^1} H^{\nu_1^2} |\omega_{00}^{(1)}\rangle \mid \nu_1 = \nu_1^1 \times 2 + \nu_1^2,\ \nu_1^1, \nu_1^2 \in \{0, 1\}\}$, where

$$
\begin{aligned}
|\omega_{01}^{(1)}\rangle &= \frac{1}{\sqrt{2}}[(|0\rangle + |1\rangle)|\varphi_0\rangle + (|0\rangle - |1\rangle)|\varphi_1\rangle], \\
|\omega_{02}^{(1)}\rangle &= (-|1\rangle|\varphi_0\rangle + |0\rangle|\varphi_1\rangle), \\
|\omega_{03}^{(1)}\rangle &= \frac{1}{\sqrt{2}}[(|0\rangle + |1\rangle)|\varphi_1\rangle - (|0\rangle - |1\rangle)|\varphi_0\rangle]. \quad (22)
\end{aligned}
$$

Because the encoding operation is selected from Ξ_0 (Ξ_1) randomly, the two-particle entangled pair is in a mixed state, $\rho_0^{(1)} = \frac{1}{4}(\sum_{\nu_1=0}^{3} |\omega_{0\nu_1}^{(1)}\rangle\langle\omega_{0\nu_1}^{(1)}|)$. Similarly, when $s_0^j = 1$, the set is $\{|\omega_{1\nu_1}^{(1)}\rangle = U_{\nu_1^1,\overline{\nu_1^1}} H^{\nu_1^2} |\omega_{00}^{(1)}\rangle \mid \nu_1 = \nu_1^1 \times 2 + \nu_1^2,\ \nu_1^1, \nu_1^2 \in \{0, 1\}\}$, where

$$
\begin{aligned}
\left|\omega_{10}^{(1)}\right\rangle &= (|1\rangle|\varphi_0\rangle + |0\rangle|\varphi_1\rangle), \\
\left|\omega_{11}^{(1)}\right\rangle &= \frac{1}{\sqrt{2}}[(|0\rangle + |1\rangle)|\varphi_0\rangle - (|0\rangle - |1\rangle)|\varphi_1\rangle], \\
\left|\omega_{12}^{(1)}\right\rangle &= (|0\rangle|\varphi_0\rangle - |1\rangle|\varphi_1\rangle), \\
\left|\omega_{13}^{(1)}\right\rangle &= \frac{1}{\sqrt{2}}[(|0\rangle - |1\rangle)|\varphi_0\rangle + (|0\rangle + |1\rangle)|\varphi_1\rangle]. \quad (23)
\end{aligned}
$$

The corresponding mixed state is $\rho_1^{(1)} = \frac{1}{4}(\sum_{\nu_1=0}^{3} |\omega_{1\nu_1}^{(1)}\rangle\langle\omega_{1\nu_1}^{(1)}|)$. From Eqs. (22) and (23), the following equations can be deduced:

$$
\begin{aligned}
\rho_0^{(1)} = \rho_1^{(1)} = \frac{1}{4}\Big(&\left|\kappa_0^{(1)}\right\rangle\!\left\langle\kappa_0^{(1)}\right| + \left|\kappa_1^{(1)}\right\rangle\!\left\langle\kappa_1^{(1)}\right| \\
&+ \left|\kappa_2^{(1)}\right\rangle\!\left\langle\kappa_2^{(1)}\right| + \left|\kappa_3^{(1)}\right\rangle\!\left\langle\kappa_3^{(1)}\right|\Big) \quad (24)
\end{aligned}
$$

where

$$
\left|\kappa_{\nu_1}^{(1)}\right\rangle = U_{\nu_1^1,\nu_1^2}\left|\omega_{00}^{(1)}\right\rangle. \quad (25)
$$

Based on the conclusion of Ref. [27], we have the minimum-error probability of distinguishing these two mixed states, $p_E = 1/2$, which means that the discrimination is the same as a random guess.

Further, we consider a more general attack, in which $m-1$ dishonest participants prepare a m-particle entangled state, $|\omega_{00\ldots0}^{(m-1)}\rangle = |\Phi\rangle$. Then, similar to the attack with unambiguous discrimination, $\dot{P}_{m-1}$ orderly sends $m-1$ fake particles, f_1, f_2, …, and f_{m-1}, to P_0. Thus, after P_0 performs $m-1$ encoding operations, the whole system is in one of 4^{m-1} states $\Gamma_0 = \{|\omega_{0\nu_1\nu_2\ldots\nu_{m-1}}^{(m-1)}\rangle\}$ ($\Gamma_1 = \{|\omega_{1\nu_1\nu_2\ldots\nu_{m-1}}^{(m-1)}\rangle\}$) if $s_0^j = 0\,(1)$. Here, the states $|\omega_{0\nu_1\nu_2\ldots\nu_{m-1}}^{(m-1)}\rangle$ and $|\omega_{1\nu_1\nu_2\ldots\nu_{m-1}}^{(m-1)}\rangle$ are depicted as follows:

$$
\begin{aligned}
\left|\omega_{0\nu_1\nu_2\ldots\nu_{m-1}}^{(m-1)}\right\rangle = {}& U_{\nu_1^1,\nu_1^1} H^{\nu_1^2} \otimes U_{\nu_2^1,\nu_2^1} H^{\nu_2^2} \otimes \cdots \\
& \otimes U_{\nu_{m-1}^1,\nu_{m-1}^1} H^{\nu_{m-1}^2} |\omega_{00\ldots0}^{(m-1)}\rangle, \\
\left|\omega_{1\nu_1\nu_2\ldots\nu_{m-1}}^{(m-1)}\right\rangle = {}& U_{\nu_1^1,\overline{\nu_1^1}} H^{\nu_1^2} \otimes U_{\nu_2^1,\overline{\nu_2^1}} H^{\nu_2^2} \otimes \cdots \\
& \otimes U_{\nu_{m-1}^1,\overline{\nu_{m-1}^1}} H^{\nu_{m-1}^2} |\omega_{00\ldots0}^{(m-1)}\rangle. \quad (26)
\end{aligned}
$$

Thus, the corresponding two mixed states are

$$
\begin{aligned}
\rho_0^{(m-1)} &= \frac{1}{4^{m-1}} \sum_{\nu_1,\nu_2,\ldots,\nu_{m-1}=0}^{3} \left|\omega_{0\nu_1\nu_2\ldots\nu_{m-1}}^{(m-1)}\right\rangle\!\left\langle\omega_{0\nu_1\nu_2\ldots\nu_{m-1}}^{(m-1)}\right|, \\
\rho_1^{(m-1)} &= \frac{1}{4^{m-1}} \sum_{\nu_1,\nu_2,\ldots,\nu_{m-1}=0}^{3} \left|\omega_{1\nu_1\nu_2\ldots\nu_{m-1}}^{(m-1)}\right\rangle\!\left\langle\omega_{1\nu_1\nu_2\ldots\nu_{m-1}}^{(m-1)}\right|. \quad (27)
\end{aligned}
$$

By simple calculations, we get

$$
\begin{aligned}
\rho_0^{(m-1)} &= \rho_1^{(m-1)} \\
&= \left(\frac{1}{4}\right)^{m-1} \sum_{\nu_1,\nu_2,\cdots,\nu_{m-1}=0}^{3} \left|\kappa_{\nu_1\nu_2\cdots\nu_{m-1}}^{(m-1)}\right\rangle\!\left\langle\kappa_{\nu_1\nu_2\cdots\nu_{m-1}}^{(m-1)}\right| \quad (28)
\end{aligned}
$$

where

$$
\begin{aligned}
\left|\kappa_{\nu_1\nu_2\cdots\nu_{m-1}}^{(m-1)}\right\rangle = {}& U_{\nu_1^1,\nu_1^2} \otimes U_{\nu_2^1,\nu_2^2} \otimes \cdots \\
& \otimes U_{\nu_{m-1}^1,\nu_{m-1}^2} \left|\omega_{00\cdots0}^{(m-1)}\right\rangle. \quad (29)
\end{aligned}
$$

Because these two mixed states are the same, it is obviously impossible to discriminate them.

From the above analysis, it is shown that no one is able to obtain the value of s_0^j by performing unambiguous discrimination or minimum-error discrimination. For completeness, the case in which these dishonest participants cooperate to attack the proposed protocol after P_0 received $Q_{0\rightarrow 0}$ in step $(m+2)$ is discussed briefly. Before he declares his secret message B_0, P_0 should receive the traveling particle sequence $Q_{0\rightarrow 0}$. That is, when they obtain the value of B_0, these dishonest participants cannot operate the particles in $Q_{0\rightarrow 0}$ that are in P_0's site. In this case, the only attack action performed by these dishonest participants is to announce the fake secret messages, $B_1, B_2, \ldots, B_{m-1}$, which is similar to the attack mentioned in Ref. [22]. Therefore, when P_0 performs H or I operation on each particle pair in step $(m+3)$, half of them use the wrong operation and half use the right one. When the operation is wrong, the measurement result is also incorrect. This means that the error rate is approximately 50%. Hence, this attack is inevitably detected by P_0 because the probability that it successfully passes the eavesdropping check process is $(\frac{1}{2})^{\lfloor \frac{\zeta n}{m} \rfloor} \approx 0$.

C. Security

Suppose Eve is an external eavesdropper who attempts to eavesdrop on the agreement key. Since $k^j = s_0^j \oplus s_1^j \oplus \cdots \oplus s_{m-1}^j$, Eve can generally use two methods to obtain the value of k^j. One is that Eve tries to eavesdrop each value of s_0^j and then calculates the sum of these m values. However, similar to some multiparty quantum cryptography protocols (e.g., quantum secret sharing), the participants take part in the protocol and are more powerful than Eve in the proposed protocol. Therefore, like the dishonest participants, Eve is also unable to eavesdrop s_i^j from the analysis of the above section.

The other method involves directly eavesdropping on the value of k^j. This is the same case as the participant who does not know the secrets of the other participants but gets the agreement key. Without loss of generality, we take the particle pair (q_0^j, r_0^j) as an example. In the proposed protocol, Eve has no access to the particle r_0^j that is always held by P_0; thus, all her attack actions are restricted to the particle q_0^j, which is transmitted among the participants. Moreover, no matter what these encoding operations are, this traveling particle is always in the maximal mix state $\rho = \frac{1}{2}(|0\rangle\langle 0| + |1\rangle\langle 1|)$. Thus, Eve cannot obtain any information about k^j only from the traveling particle. To see this in a sufficient way, we will consider two possible cases, in which Eve may execute two common attacks: intercept-resend attack and entangle-ancilla attack.

In the intercept-resend attack, Eve intercepts the traveling particle q_0^j and replaces it with a fake particle q_e. Here, the fake particle pair (q_e, r_e) is prepared in an initial state $|\psi(0,0)\rangle$. After all participants execute their encoding operations on the fake particle, Eve can measure it to obtain the value of k^j if and only if she knows the secret message B_i. However, these messages are announced by the participants in step $(m+2)$ after all traveling particle sequences $Q_{i\rightarrow i}$ are received by the participants P_i $(i = 0, 1, \ldots, m-1)$. Hence, Eve should transmit the intercepted particle q_0^j to participant P_0. Meanwhile, the secret messages are still unknown to her. Therefore, Eve has to randomly choose one basis from MB_0 and MB_1 to measure the fake particle pair. Then, in terms of the measurement result, Eve performs the corresponding operation on particle q_0^j and sends it back to P_0. Obviously, the probability that Eve selects a wrong measurement basis is approximately 50%, which means that this attack will introduce an error rate of 25%. Hence, this attack can be easily detected in the eavesdropping check process.

Another more general attack is an entangle-ancilla attack. The general idea of this attack is described as follows. First, Eve prepares two ancillary particles, g_1 and g_2, in the initial states, $|0\rangle_{g_1}$ and $|0\rangle_{g_2}$. In step 2, when the signal particle q_0^j is transmitted from P_0 to P_1, Eve entangles the first ancilla g_1 with q_0^j, and then sends q_0^j to P_1. Next, particle q_0^j travels among these participants. When the signal particle is sent back to P_0 in step $(m+1)$, Eve intercepts this particle and makes the second ancilla g_2 interact unitarily with particle q_0^j. At the end of the protocol, Eve tries to eavesdrop k^j by measuring two ancillary particles. In the following, we will show that Eve cannot reveal any information about k^j under the condition that no error occurs.

Here, we can write the most general operations, G_1 and G_2, which Eve could apply to the signal particle and two ancillary particles, as follows:

$$\begin{aligned} G_1:\ |0\rangle_{q_0^j}|0\rangle_{g_1} &\rightarrow |0\rangle_{q_0^j}|\varepsilon_{00}\rangle_{g_1} + |1\rangle_{q_0^j}|\varepsilon_{01}\rangle_{g_1},\\ |1\rangle_{q_0^j}|0\rangle_{g_1} &\rightarrow |0\rangle_{q_0^j}|\varepsilon_{10}\rangle_{g_1} + |1\rangle_{q_0^j}|\varepsilon_{11}\rangle_{g_1}, \end{aligned} \tag{30}$$

$$\begin{aligned} G_2:\ |0\rangle_{q_0^j}|0\rangle_{g_2} &\rightarrow |0\rangle_{q_0^j}|\tau_{00}\rangle_{g_2} + |1\rangle_{q_0^j}|\tau_{01}\rangle_{g_2},\\ |1\rangle_{q_0^j}|0\rangle_{g_2} &\rightarrow |0\rangle_{q_0^j}|\tau_{10}\rangle_{g_2} + |1\rangle_{q_0^j}|\tau_{11}\rangle_{g_2}, \end{aligned} \tag{31}$$

where the states $|\varepsilon_{ij}\rangle$ and $|\tau_{ij}\rangle$ are pure ancilla states uniquely determined by G_1 and G_2. The following conditions can be derived from the unitary features of these two operations:

$$\begin{aligned} \langle\varepsilon_{00}|\varepsilon_{10}\rangle + \langle\varepsilon_{01}|\varepsilon_{11}\rangle = 0,\ \langle\tau_{00}|\tau_{10}\rangle + \langle\tau_{01}|\tau_{11}\rangle = 0,\\ \langle\varepsilon_{00}|\varepsilon_{00}\rangle + \langle\varepsilon_{01}|\varepsilon_{01}\rangle = \langle\varepsilon_{10}|\varepsilon_{10}\rangle + \langle\varepsilon_{11}|\varepsilon_{11}\rangle = 1,\\ \langle\tau_{00}|\tau_{00}\rangle + \langle\tau_{01}|\tau_{01}\rangle = \langle\tau_{10}|\tau_{10}\rangle + \langle\tau_{11}|\tau_{11}\rangle = 1. \end{aligned} \tag{32}$$

In the entangle-ancilla attack, the signal particle pair and two ancillary particles are in an initial state, $|\alpha^0\rangle_{r_0^j q_0^j g_1 g_2} = |\psi(0,0)\rangle_{r_0^j q_0^j}|0\rangle_{g_1}|0\rangle_{g_2}$. After the first unitary interaction between particles q_0^j and g_1, the whole system is in the state

$$\begin{aligned} |\alpha^1\rangle_{r_0^j q_0^j g_1 g_2} &= I \otimes G_1 \otimes I |\alpha^0\rangle_{r_0^j q_0^j g_1 g_2}\\ &= \frac{1}{\sqrt{2}}(|00\varepsilon_{00}0\rangle + |01\varepsilon_{01}0\rangle + |10\varepsilon_{10}0\rangle\\ &\quad + |11\varepsilon_{11}0\rangle)_{r_0^j q_0^j g_1 g_2}. \end{aligned} \tag{33}$$

From Eq. (5), we can derive that the encoding operations of these participants can be represented by one of eight unitary operators, $\Xi_0 \cup \Xi_1$. Namely, after all participants encode their secrets on particle q_0^j, the four particles are in the state

$$\left|\alpha^2_{i'j'k'}\right\rangle_{r_0^j q_0^j g_1 g_2} = I \otimes U_{j',k'} H^{i'} \otimes I \otimes I |\alpha^1\rangle_{r_0^j q_0^j g_1 g_2}, \tag{34}$$

where $i', j', k' \in \{0, 1\}$. Then, Eve entangles the second ancilla g_2 with q_0^j, and the state $|\alpha^2_{i'j'k'}\rangle_{r_0^j q_0^j g_1 g_2}$ is changed to

$$\left|\alpha^3_{i'j'k'}\right\rangle_{r_0^j q_0^j g_1 g_2} = I \otimes I \otimes G_2 \left|\alpha^2_{i'j'k'}\right\rangle_{r_0^j g_1 q_0^j g_2}. \tag{35}$$

In step $(m+3)$, P_0 performs operation H or I on the signal particle q_0^j based on the public messages. So, the whole quantum system is in one of eight states:

$$|\theta_{i'j'k'}\rangle_{r_0^j q_0^j g_1 g_2} = I \otimes H^{i'} \otimes I \otimes I \left|\alpha^3_{i'j'k'}\right\rangle_{r_0^j q_0^j g_1 g_2}. \tag{36}$$

At last, Eve may eavesdrop k^j from two ancillary particles in her hands. That is, she tries to use the difference between two mix states,

$$\varrho_0 = \frac{1}{4}\sum_{i'=0}^{1}\left[\mathrm{tr}_{r_0^j q_0^j}(|\theta_{i'00}\rangle\langle\theta_{i'00}|) + \mathrm{tr}_{r_0^j q_0^j}(|\theta_{i'11}\rangle\langle\theta_{i'11}|)\right],$$

$$\varrho_1 = \frac{1}{4}\sum_{i'=0}^{1}\left[\mathrm{tr}_{r_0^j q_0^j}(|\theta_{i'01}\rangle\langle\theta_{i'01}|) + \mathrm{tr}_{r_0^j q_0^j}(|\theta_{i'10}\rangle\langle\theta_{i'10}|)\right], \tag{37}$$

to obtain information about $k^j = j' \oplus k'$, where $\mathrm{Tr}_{r_0^j q_0^j}$ is the partial trace over the signal particle pair (r_0^j, q_0^j).

Through simple calculations, we can rewrite eight states $|\theta_{i'j'k'}\rangle$ of Eq. (36) as

$$\begin{aligned}
|\theta_{000}\rangle &= \frac{1}{\sqrt{2}}\sum_{j',k'=0}^{1} |j'k'\rangle|\beta_{j'00k'}\rangle,\ |\theta_{001}\rangle = \frac{1}{\sqrt{2}}\sum_{j',k'=0}^{1} |j'k'\rangle|\beta_{j'10k'}\rangle,\\
|\theta_{010}\rangle &= \frac{1}{\sqrt{2}}\sum_{j',k'=0}^{1} |j'k'\rangle|\beta_{j'01k'}\rangle,\ |\theta_{011}\rangle = \frac{1}{\sqrt{2}}\sum_{j',k'=0}^{1} |j'k'\rangle|\beta_{j'11k'}\rangle,\\
|\theta_{100}\rangle &= \frac{1}{2\sqrt{2}}\sum_{j'=0}^{1}\{|0j'\rangle[|\beta_{0010}\rangle + |\beta_{0100}\rangle + (-1)^{j'}(|\beta_{0011}\rangle + |\beta_{0101}\rangle)] + |1j'\rangle[|\beta_{1010}\rangle + |\beta_{1100}\rangle + (-1)^{j'}(|\beta_{1011}\rangle + |\beta_{1101}\rangle)]\},\\
|\theta_{101}\rangle &= \frac{1}{2\sqrt{2}}\sum_{j'=0}^{1}\{|0j'\rangle[|\beta_{0110}\rangle + |\beta_{0000}\rangle + (-1)^{j'}(|\beta_{0111}\rangle + |\beta_{0001}\rangle)] + |1j'\rangle[|\beta_{1110}\rangle + |\beta_{1000}\rangle + (-1)^{j'}(|\beta_{1111}\rangle + |\beta_{1001}\rangle)]\},\\
|\theta_{110}\rangle &= \frac{1}{2\sqrt{2}}\sum_{j'=0}^{1}\{|0j'\rangle[|\beta_{0000}\rangle - |\beta_{0110}\rangle + (-1)^{j'}(|\beta_{0001}\rangle - |\beta_{0111}\rangle)] + |1j'\rangle[|\beta_{1000}\rangle - |\beta_{1110}\rangle + (-1)^{j'}(|\beta_{1001}\rangle - |\beta_{1111}\rangle)]\},\\
|\theta_{111}\rangle &= \frac{-1}{2\sqrt{2}}\sum_{j'=0}^{1}\{|0j'\rangle[|\beta_{0100}\rangle - |\beta_{0010}\rangle + (-1)^{j'}(|\beta_{0101}\rangle - |\beta_{0011}\rangle)] + |1j'\rangle[|\beta_{1100}\rangle - |\beta_{1010}\rangle + (-1)^{j'}(|\beta_{1101}\rangle - |\beta_{1011}\rangle)]\},
\end{aligned} \tag{38}$$

where

$$|\beta_{i'j'k'l'}\rangle = |\varepsilon_{i'0}\rangle|\tau_{j'l'}\rangle + (-1)^{k'}|\varepsilon_{i'0}\rangle|\tau_{\overline{j'}l'}\rangle. \tag{39}$$

In the eavesdropping check process, P_0 makes a Bell state measurement on the particle pair (r_0^j, q_0^j). Thus, in order for there to be no error, the states $|\theta_{i'j'k'}\rangle$ should satisfy the following conditions:

$$\begin{aligned}
\langle\psi(0,0)|\theta_{i'01}\rangle &= \langle\psi(0,0)|\theta_{i'10}\rangle = 0,\\
\langle\psi(1,1)|\theta_{i'01}\rangle &= \langle\psi(1,1)|\theta_{i'10}\rangle = 0,\\
\langle\psi(0,1)|\theta_{i'00}\rangle &= \langle\psi(0,1)|\theta_{i'11}\rangle = 0,\\
\langle\psi(1,0)|\theta_{i'00}\rangle &= \langle\psi(1,0)|\theta_{i'11}\rangle = 0.
\end{aligned} \tag{40}$$

From Eqs. (38) and (40), the following equation can be derived:

$$\begin{aligned}
|\beta_{0000}\rangle - |\beta_{1001}\rangle &= |\beta_{0001}\rangle + |\beta_{1000}\rangle = \mathbf{0},\\
|\beta_{0100}\rangle + |\beta_{1101}\rangle &= |\beta_{0101}\rangle + |\beta_{1100}\rangle = \mathbf{0},\\
|\beta_{0010}\rangle + |\beta_{1011}\rangle &= |\beta_{0011}\rangle - |\beta_{1010}\rangle = \mathbf{0},\\
|\beta_{0110}\rangle - |\beta_{1111}\rangle &= |\beta_{0111}\rangle + |\beta_{1110}\rangle = \mathbf{0},
\end{aligned} \tag{41}$$

where $\mathbf{0}$ is denoted as a null vector. Based on Eqs. (32), (39), and (41), we obtain the following two constraints:

$$\begin{aligned}
|\varepsilon_{00}\rangle &= |\varepsilon_{11}\rangle, |\varepsilon_{01}\rangle = -|\varepsilon_{10}\rangle,\\
|\tau_{00}\rangle &= |\tau_{11}\rangle, |\tau_{01}\rangle = -|\tau_{10}\rangle,
\end{aligned} \tag{42}$$

or,

$$\begin{aligned}
|\varepsilon_{00}\rangle &= -|\varepsilon_{11}\rangle, |\varepsilon_{01}\rangle = |\varepsilon_{10}\rangle,\\
|\tau_{00}\rangle &= -|\tau_{11}\rangle, |\tau_{01}\rangle = |\tau_{10}\rangle.
\end{aligned} \tag{43}$$

When the condition (42) is satisfied, the following equation can be deduced from Eq. (38):

$$\begin{aligned}
|\theta_{000}\rangle &= |\psi(0,0)\rangle|\beta_{0000}\rangle + |\psi(1,1)\rangle|\beta_{0001}\rangle,\\
|\theta_{001}\rangle &= -|\psi(1,0)\rangle|\beta_{0011}\rangle + |\psi(0,1)\rangle|\beta_{0010}\rangle,\\
|\theta_{010}\rangle &= |\psi(1,0)\rangle|\beta_{0010}\rangle + |\psi(0,1)\rangle|\beta_{0011}\rangle,\\
|\theta_{011}\rangle &= -|\psi(0,0)\rangle|\beta_{0001}\rangle + |\psi(1,1)\rangle|\beta_{0000}\rangle,\\
|\theta_{100}\rangle &= |\psi(0,0)\rangle|\beta_{0010}\rangle - |\psi(1,1)\rangle|\beta_{0011}\rangle,\\
|\theta_{101}\rangle &= |\psi(1,0)\rangle|\beta_{0000}\rangle - |\psi(0,1)\rangle|\beta_{0001}\rangle,\\
|\theta_{110}\rangle &= |\psi(1,0)\rangle|\beta_{0001}\rangle + |\psi(0,1)\rangle|\beta_{0000}\rangle,\\
|\theta_{111}\rangle &= -|\psi(0,0)\rangle|\beta_{0011}\rangle + |\psi(1,1)\rangle|\beta_{0010}\rangle.
\end{aligned} \tag{44}$$

Based on Eqs. (37) and (44), we get

$$\varrho_0 = \varrho_1 = \frac{1}{2}\sum_{j',k'=0}^{1} |\beta_{00j'k'}\rangle\langle\beta_{00j'k'}|. \tag{45}$$

As for the condition (43), the same conclusion is drawn, i.e., Eq. (45) still holds. This implies that Eve cannot obtain any information about k^j under the condition that no errors are introduced during the eavesdropping check process. Hence, the proposed protocol is secure against the entangle-ancilla attack.

VI. CONCLUSION

Before presenting our conclusion, we briefly discuss the hash function used in the protocol. From the above security analysis, it is shown that the presented protocol is secure in theory when the hash function is preimage resistant. With the development of quantum computing, some classical hash functions will be compromised by some advanced quantum algorithms. Thus, the presented protocol with classical hash functions is only computationally secure. To achieve perfect security, replacing the classical hash function with the quantum hash function [35,36] is an effective solution. In other words, the presented protocol with quantum hash functions is secure, because it is still preimage resistant under the condition of quantum computing. However, it is easier to perform a classical hash function than the quantum counterpart using current technology. As said in Ref. [2], infinite security will demand infinite cost, which means zero practical interest. Hence, in the following, the security of the presented protocol with classical hash functions is analyzed briefly.

In the protocol with classical hash functions, the preimage-resistant condition cannot be satisfied. Namely, one can calculate some possible preimages from a hash value. It may provide $m-1$ dishonest participants a chance to attack the protocol. However, in the protocol, the honest participant P_0 deduces the agreement key from his measurement results of particle sequence $Q_{0\to 0}$, which is received before announcing B_0 in step $(m+2)$. Thus, in order to make P_0 accept a fake key (e.g., $\dot{K}$ = "00 . . . 0"), $m-1$ dishonest participants should perform an appropriate operation on $Q_{0\to 0}$ before sending it back to P_0. This operation is determined by the values of the fake key and P_0's secret input. However, before step $(m+2)$, the value of B_0 is only known to P_0. Since the hash function is a many-to-one mapping, one cannot derive a unique correct B_0 from the hash value $h(B_0)$. Especially for the balanced hash function, these dishonest participants have to choose randomly a measurement basis and eavesdrop P_0's input by measuring the signal particles. Thus, there are some positions, at which their guess about P_0's input is wrong. That is, some bits of P_0's measurement results are not what the dishonest participants want. In this case, $m-1$ dishonest participants should calculate many preimages, from which $m-1$ appropriate fake $\dot{B}_i$s ($\dot{B}_1$, $\dot{B}_2$, . . . , $\dot{B}_{m-1}$) are selected to satisfy two conditions. One is that P_0's measurement basis determined by $\oplus_{i=1}^{m-1}\dot{B}_i[i]$ should be correct. Namely, in order to introduce no errors, P_0's measurement results are not random. On the other hand, to make P_0's agreement key equal to $\dot{K}$, these positions, at which the guess about P_0's input is wrong, should be selected as the samples. Therefore, the other condition is that the bit value of $\oplus_{i=1}^{m-1}\dot{B}_i \oplus B_0$ at these positions must be zero. Obviously, getting these appropriate $\dot{B}_i$s will take a lot of time and has a probability of failure, i.e., there are no $m-1$ fake $\dot{B}_i$s that meet these two conditions. However, in step $(m+2)$, these dishonest participants are required to declare their $\dot{B}_i$s after P_0 announces the value of B_0. Obviously, they have not much time to compute these $m-1$ $\dot{B}_i$s from the hash values H_is. Consequently, even if the classical hash function is broken by quantum computing, it is quite difficult for the dishonest participants to successfully cheat the honest participant to accept a fake key. In other words, the presented protocol with some balanced classical hash functions (e.g., SHA or MD5) can be used to achieve key agreement tasks in most practical implementation scenarios, though it is only computationally secure. In addition, since the agreement key is raw, the classical postprocessing process may reduce the leaked information to zero. Similar to that for QKD, a rigorous analysis is required, which will be considered in our future works.

In this paper, the design and analysis of a secure multiparty quantum key agreement protocol, which is another main key establishment method in addition to quantum key distribution, is studied, especially for the circle-type MQKA. According to the fairness requirements of this kind of protocol, through analysis of some existing protocols, two possible security loopholes are found. Based on these loopholes, quantum state discrimination is utilized to present a collusion attack by $m-1$ dishonest participants. To resist this attack, a circle-type multiparty quantum key agreement protocol with Bell states is proposed. In this protocol, a set of quantum encoding operations is designed by using the Hadamard operator and four Pauli operators. Since these encoding operations cannot be discriminated by unambiguous discrimination or minimum-error discrimination, the proposed protocol is secure against the presented $m-1$ dishonest participants' collusion attack. Furthermore, it is shown that the proposed protocol is secure against some common external and internal attacks. Additionally, the implementation of the protocol only requires the preparation and measurement of Bell states and some common single-qubit gates, thus the protocol is feasible using current technology. Since the implementation of the protocol is inevitably affected by noise, the threshold value for the error rate should be provided before implementing it. However, in this paper, no exact threshold value is given, which is also the case for many multiparty quantum cryptography protocols and becomes an open problem. Combined with quantum state discrimination, we will study this problem in the future.

ACKNOWLEDGMENTS

We are very grateful to two anonymous reviewers for their constructive comments that have greatly helped to improve the quality of this paper. This work was supported by National Natural Science Foundation of China (Grants No. 61772134, No. 61976053, and No. 62171131), Fujian Province Natural Science Foundation (Grant No. 2018J01776), and Program for New Century Excellent Talents in Fujian Province University.

[1] C. H. Bennett and G. Brassard, in *Proceedings of the IEEE International Conference on Computers, Systems, and Signal Processing* (IEEE, New York, 1984), p. 175.

[2] N. Gisin, G. Ribordy, W. Tittel, and H. Zbinden, Rev. Mod. Phys. **74**, 145 (2002).

[3] J. Pieprzyk, T. Hardjono, and J. Seberry, *Key Establishment Protocols* (Springer-Verlag, Berlin, 2003).

[4] M. Steiner, G. Tsudik, and M. Waidner, IEEE Trans. Parallel Distrib. Syst. **11**, 769 (2000).

[5] N. Zhou, G. Zeng, and J. Xiong, Electron. Lett. **40**, 1149 (2004).

[6] R. H. Shi and H. Zhong, Quantum Inf. Process. **12**, 921 (2013).

[7] S. K. Chong, C. W. Tsai, and T. Hwang, Int. J. Theor. Phys. **50**, 1793 (2011).

[8] B. Liu, F. Gao, W. Huang, and Q. Y. Wen, Quantum Inf. Process. **12**, 1797 (2013).

[9] G. B. Xu, Q. Y. Wen, F. Gao, and S. J. Qin, Quantum Inf. Process. **13**, 2587 (2014).

[10] B. B. Cai, G. D. Guo, and S. Lin, Mod. Phys. Lett. B **31**, 1750102 (2017).

[11] W. J. Liu, Z. Y. Chen, S. Ji, H. B. Wang, and J. Zhang, Int. J. Theor. Phys. **56**, 3164 (2017).

[12] T. Cai, M. Jiang, and G. Cao, Quantum Inf. Process. **17**, 103 (2018).

[13] B. B. Cai, G. D. Guo, S. Lin, H. J. Zuo, and C. H. Yu, IEEE Photonics J. **10**, 7600211 (2018).

[14] S. S. Wang, D. H. Jiang, G. B. Xu, Y. H. Zhang, and X. Q. Liang, Quantum Inf. Process. **18**, 190 (2019).

[15] H. N. Liu, X. Q. Liang, D. H. Jiang, G. B. Xu, and W. M. Zheng, Quantum Inf. Process. **18**, 242 (2019).

[16] Y. G. Yang, B. R. Li, D. Li, Y. H. Zhou, and W. M. Shi, Quantum Inf. Process. **18**, 322 (2019).

[17] Y. H. Zhou, J. Zhang, W. M. Shi, Y. G. Yang, and M. F. Wang, Mod. Phys. Lett. B **34**, 2050083 (2020).

[18] H. Cao and W. Ma, Quantum Inf. Process. **17**, 219 (2018).

[19] A. Elhadad, S. Abbas, H. Abulkasim, and S. Hamad, Comput. Commun. **159**, 155 (2020).

[20] Z. Sun, R. Cheng, C. Wu, and C. Zhang, Sci. Rep. **9**, 17177 (2019).

[21] P. Wang, Z. Sun, and X. Sun, Quantum Inf. Process. **16**, 170 (2017).

[22] W. C. Huang, Y. K. Yang, D. Jiang, and L. J. Chen, Sci. Rep. **9**, 16421 (2019).

[23] Z. W. Sun, C. H. Wu, S. G. Zheng, and C. Zhang, IEEE Access **7**, 102377 (2019).

[24] W. Huang, Q. Su, B. Liu, Y.-H. He, F. Fan, and B.-J. Xu, Sci. Rep. **7**, 15264 (2017).

[25] W. Huang, Q. Y. Wen, B. Liu, Q. Su, and F. Gao, Quantum Inf. Process. **13**, 1651 (2014).

[26] B. Liu, D. Xiao, H. W. Jia, and R. Z. Liu, Quantum Inf. Process. **15**, 2113 (2016).

[27] C. W. Helstrom, *Quantum Detection and Estimation Theory* (Academic, New York, 1976).

[28] H. Zhu, L. Wang, and Y. Zhang, Quantum Inf. Process. **19**, 381 (2020).

[29] R. H. Shi, B. Liu, and M. W. Zhang, Int. J. Theor. Phys. **60**, 227 (2021).

[30] A. Chefles and S. M. Barnett, Phys. Lett. A **250**, 223 (1998).

[31] A. Acin, Phys. Rev. Lett. **87**, 177901 (2001).

[32] R. Duan, Y. Feng, and M. Ying, Phys. Rev. Lett. **103**, 210501 (2009).

[33] G. M. D'Ariano, P. Lo Presti, and M. G. A. Paris, Phys. Rev. Lett. **87**, 270404 (2001).

[34] S. Y. Zhang and M. S. Ying, Phys. Rev. A **65**, 062322 (2002).

[35] D. Li, J. Zhang, F. Z. Guo, W. Huang, Q. Y. Wen, and H. Chen, Quantum Inf. Process. **12**, 1501 (2013).

[36] Y. G. Yang, P. Xu, R. Yang, Y. H. Zhou, and W. M. Shi, Sci. Rep. **6**, 19788 (2016).