Multipartite Quantum Key Agreement Over Collective Noise Channels

Volume 10, Number 1, February 2018

Binbin Cai
Gongde Guo
Song Lin
Huijuan Zuo
Chaohua Yu

DOI: 10.1109/JPHOT.2018.2797535
1943-0655 © 2018 IEEE
Abstract: In this paper, two classes of multipartite entangled states are constructed to resist against the collective-dephasing noise and collective-rotation noise, respectively. Based on it, two new multipartite quantum key agreement protocols over the collective noise are presented. In each protocol, only one user needs to prepare the multiparticle quantum entangled state. Then, the user keeps the first qubit, and distributes each two qubits of the state to other users. In this case, all users can perform the security test and derive the shared key from the measurement outcomes of the qubits in their hands. From the security analysis, it is evident that the presented protocols are secure against the inside attack and some common outside attacks.

Index Terms: Quantum cryptography, multipartite quantum key agreement, collective noise.

1. Introduction

In the last three decades, quantum cryptography has been developed vigorously and has become a hot topic. Different from the security of the classical cryptography which is mainly based on the assumption of computation complexity, the security of quantum cryptography relies on the quantum mechanics principles like no-cloning theorem and Heisenberg uncertainty principle which make it unconditionally secure. Hence, various research branches have been put forward in quantum cryptography, such as quantum key distribution (QKD) [1]–[5], quantum private query [6]–[9], quantum secret sharing (QSS) [10]–[16], quantum secure direct communication [17]–[19], and so on.

Quantum key agreement (QKA) [20]–[39] is also an important research issue of quantum cryptography. In contrast to QKD scheme in which one user distributes the prespecified key to other users, QKA protocols require that all users contribute to the generation of the shared key equally...
and any nontrivial subset of users cannot determine the shared key alone. Compared with QKD, QKA is clearly with more rigorous security requirements. Furthermore, the key agreement protocol also has a great many applications in the cryptographic field, like implementing perfect forward secrecy, providing the access control, providing the authentication and identification of users and so on [40]–[42]. The first QKA protocol was designed by Zhou et al. [20] in 2004. Based on the Bell states, two users utilize the means of quantum teleportation to agree on the shared key. In 2010, Chong et al. [21] proposed a new QKA protocol based on the well-known BB84 protocol [1]. In 2011, Chong et al. [22] found that Zhou et al. protocol is fragile to the participant attack, they showed that one user in this protocol can decide the shared key alone. Later on, not only some subtle two-party QKA protocols [23]–[27] have been designed, but it is generalized to the multipartite case. In 2013, based on EPR pairs and entanglement swapping, Shi et al. [28] gave out the first multipartite QKA protocol. Subsequently, Liu et al. [29] indicated that Shi et al. protocol is not secure since that one user in this protocol can fully determine the shared key without inducing errors. Besides, Liu et al. also proposed a new multipartite QKA protocol with single particles and single-particle measurement. However, the particle efficiency of Liu et al. protocol is unsatisfactory. By introducing another two additional unitary operations, Sun et al. [30] presented a “circle-type” QKA protocol to improve the particle efficiency of Liu et al. protocol. Regrettably, Huang et al. [31] pointed out that Sun et al. protocol exists defects in privacy and fairness which means the protocol is unfair. Recently, quite a few multipartite QKA protocols have been proposed, including Refs. [32]–[39].

Unfortunately, most of the existed QKA protocols all assume that the quantum channel is noiseless except the protocols of Refs. [23], [24], [27] which are immune to collective noise. However, these protocols only suit for two users. In this paper, we intend to design two multipartite QKA protocols which can resist against the collective-dephasing noise and collective-rotation noise, respectively. In each protocol, one user is selected randomly to prepare the entangled quantum state. Then, the user persists the first qubit and distributes each two qubits of the state to others. Afterwards, all users do the security test based on the interesting properties of the entangled state. At the end of the protocol, all users can get the shared key simultaneously by measuring on the remaining particles. Furthermore, the security analysis shows that the presented protocols are secure against some common attacks.

The rest of the paper is organized as follows. In the next section, some necessary preliminaries are introduced. In Section III, two multipartite QKA protocols are proposed. The security analysis of the protocols is given in Section IV. Then, some discussions are provided in Section V. Finally, a short conclusion is given in Section VI.

2. Preliminaries

Some essential preliminaries are provided in this section. There are three mutually nonorthogonal bases utilized in this paper, the X-basis is denoted as \( B_x = \{|+, -\rangle \} \), the Y-basis is indicated by \( B_y = \{|+y\rangle, \{-y\rangle \} \) and the computational basis is \( B_z = \{|0\rangle, |1\rangle \} \), where \( i = \sqrt{-1} \).

2.1 Collective Noise

In reality, noise on quantum channel needs to be considered since it is evident that the travel particles interact with the external environment inevitably and then noises are introduced in. Herein, a significant assumption called collective noise [43]–[46] is presented. That is to say, the transformation is identical for each particle if all particles transmit through the noisy channel inside a time window that is shorter than the variation of decoherence. In general, the collective noise can be classified into two conventional kinds, i.e., the collective-dephasing noise and the collective-rotation noise. The alteration caused by the collective-dephasing noise is depicted as follows,

\[
U^0: |0\rangle \rightarrow |0\rangle, \quad |1\rangle \rightarrow e^{i\theta} |1\rangle.
\]
Then the transformation resulted in the collective-rotation noise is

\[ U^\sigma : |0\rangle \rightarrow \cos \sigma |0\rangle + \sin \sigma |1\rangle, \quad |1\rangle \rightarrow -\sin \sigma |0\rangle + \cos \sigma |1\rangle, \]  

where \( \theta \) and \( \sigma \) are the fluctuation factor of the noise with time.

### 2.2 Two Classes of Multiparticle Entangled States

It is known that the states from decoherence-free subspace (DFS) \([43],[47]\) are immune to collective decoherence. Based on this idea, two classes of multiparticle entangled states are constructed to repel the collective noise. To resist the collective-dephasing noise, the two level \((2m - 1)\)-particle state \( |\psi\rangle \) is defined as

\[ |\psi\rangle_{12\ldots(2m-1)} = \frac{1}{\sqrt{2}} |0\rangle_1 |\psi^+\rangle \otimes \cdots \otimes |\psi^+\rangle + \frac{1}{\sqrt{2}} |1\rangle_1 |\psi^-\rangle \otimes \cdots \otimes |\psi^-\rangle, \]  

where the subscript indicates the particle number and \( |\psi^\pm\rangle = \frac{1}{\sqrt{2}} (|01\rangle \pm |10\rangle) \). In order to negotiate a secret key, the encoding rule stated should be followed:

\[ \{ |0\rangle, |+\rangle, |01\rangle, |\psi^+\rangle : 0, |1\rangle, |\rangle, |10\rangle, |\psi^-\rangle : 1 \}. \]  

Based on (3), we can obtain

\[ \left( I_1 \otimes U_{23}^{\theta_1} \otimes \cdots \otimes U_{(2m-2)(2m-1)}^{\theta_{m-1}} \right) |\psi\rangle_{12\ldots(2m-1)} \]

\[ = \frac{1}{\sqrt{2}} |0\rangle \left( e^{i\theta_1} |\psi^+\rangle \otimes \cdots \otimes (e^{i\theta_{m-1}} |\psi^+\rangle \right) + \frac{1}{\sqrt{2}} |1\rangle \left( e^{i\theta_1} |\psi^-\rangle \otimes \cdots \otimes (e^{i\theta_{m-1}} |\psi^-\rangle \right)
\]

\[ = e^{i(\theta_1 + \theta_2 + \cdots + \theta_{m-1})} |\psi\rangle. \]  

Consequently, it is obvious that the \((2i)\) and \((2i + 1)\) qubits of the entangled state \( |\psi\rangle \) are invariant to the collective-dephasing noise channel if they are transmitted to a user inside a time window so that these two qubits go through the similar transformations, where \( i = 1, 2, \ldots, m - 1 \). Moreover, the entangled state \( |\psi\rangle \) has another representation,

\[ |\psi\rangle_{12\ldots(2m-1)} = \frac{1}{2^\frac{m-1}{2}} \left[ \sum_a \Gamma_a [(|10\rangle)^{2a} (|01\rangle)^{m-1-2a}] + \frac{1}{2^\frac{m-1}{2}} \sum_b \Gamma_b [(|10\rangle)^{2b+1} (|01\rangle)^{m-1-(2b+1)}] \right], \]  

where \((|v\rangle)^t = |v\rangle \otimes \cdots \otimes |v\rangle\), \( a = 0, 1, \ldots, \left\lfloor \frac{m-1}{2} \right\rfloor \), and \( b = 0, 1, \ldots, \left\lfloor \frac{m-1}{2} \right\rfloor \). Here \( \Gamma(S) \) indicates the set of all permutations of \( S \) and each two particles in the sequence \( S \) are taken as an ensemble. Therefore, we can obtain the following proposition according to (3) and (6).

**Proposition 1** A two level \((2m - 1)\)-particle quantum state is in the form of \( |\psi\rangle \) if and only if following two conditions are satisfied: (1) when the first particle is measured in the \( B_2 \) and the particles \((2i)\)\((2i + 1)\) are measured in the Bell state measurement, all of the \( m \) outcomes are the same (corresponding to the classical bit); (2) when the first particle is measured in the \( B_x \) and the particles \((2i)\)\((2i + 1)\) are measured in the \( B_z \) respectively, the sum of all outcomes modules 2 is equal to zero.

It is clear that \( |\psi\rangle \) can satisfy both the conditions in Proposition 1. Here we prove the sufficiency. On the one hand, to satisfy the condition (1) of Proposition 1 that all \( m \) outcomes of the state \( |\chi\rangle \) are the same, \( |\chi\rangle \) must be in the form

\[ |\chi\rangle_{12\ldots(2m-1)} = \alpha_1 |0\rangle |\psi^+\rangle \otimes \cdots \otimes |\psi^+\rangle + \beta_1 |1\rangle |\psi^-\rangle \otimes \cdots \otimes |\psi^-\rangle, \]  

where \( \alpha_1 \) and \( \beta_1 \) are the fluctuation factor of the noise with time.
where \( |\alpha|^2 + |\beta|^2 = 1 \). With a simple calculation, we can derive the following equation from (7),
\[
|\chi\rangle = \left| + \right\rangle \left[ \left( \frac{\alpha}{2^{\frac{1}{2}}} + \frac{\beta}{2^{\frac{1}{2}}} \right)|A_1\rangle + \left( \frac{\alpha}{2^{\frac{1}{2}}} - \frac{\beta}{2^{\frac{1}{2}}} \right)|B_1\rangle \right] + \left| - \right\rangle \left[ \left( \frac{\alpha}{2^{\frac{1}{2}}} + \frac{\beta}{2^{\frac{1}{2}}} \right)|B_1\rangle + \left( \frac{\alpha}{2^{\frac{1}{2}}} - \frac{\beta}{2^{\frac{1}{2}}} \right)|A_1\rangle \right]
\]  
(8)
where 
\[
|A_1\rangle = \sum_a \Gamma \left[ (|0\rangle)^{2a}(|01\rangle)^{m-1-2a} \right], \quad |B_1\rangle = \sum_b \Gamma \left[ (|10\rangle)^{2b+1}(|01\rangle)^{m-1-(2b+1)} \right].
\]  
(9)

On the other hand, to meet the condition (2) of Proposition 1, the following equation should be satisfied,
\[
\left\{ \begin{array}{l}
\left( \frac{\alpha_1}{2^{\frac{1}{2}}} - \frac{\beta_1}{2^{\frac{1}{2}}} \right)|B_1\rangle = 0 \\
\left( \frac{\alpha_1}{2^{\frac{1}{2}}} - \frac{\beta_1}{2^{\frac{1}{2}}} \right)|A_1\rangle = 0
\end{array} \right.
\]  
(10)

where 0 is denoted as a null vector. Based on (10), \( \alpha_1 = \beta_1 \) can be yielded directly. Thus, to satisfy normalization we have \( \alpha_1 = \beta_1 = \frac{1}{\sqrt{2}} \) with the global phase ignored. Then, we have
\[
|\chi\rangle_{12...2m-1} = \frac{1}{\sqrt{2}} [0] |\psi^+\rangle \otimes \cdots \otimes |\psi^+\rangle + \frac{1}{\sqrt{2}} [1] |\psi^-\rangle \otimes \cdots \otimes |\psi^-\rangle
\]  
= |\psi\rangle.
\]  
(11)

As of now, we have showed that if a two level \( (2m-1) \)-particle state satisfies both conditions (1) and (2) of Proposition 1, it must be |\psi\rangle.

Next, the quantum multiparticle entangled state against the collective-rotation noise is provided,
\[
|\xi\rangle_{12...2m-1} = \frac{1}{\sqrt{2}} [0] |\phi^+\rangle \otimes \cdots \otimes |\phi^+\rangle + \frac{1}{\sqrt{2}} [1] |\psi^-\rangle \otimes \cdots \otimes |\psi^-\rangle,
\]  
(12)

where \( |\phi^+\rangle = \frac{1}{\sqrt{2}} (|00\rangle + |11\rangle) \) and the phase factor \( \frac{1}{\sqrt{2^d}} \) lies on the number of users in protocol. The encoding rule here is depicted as,
\[
\left\{ \begin{array}{l}
|0\rangle, |+\rangle, |+y\rangle|y\rangle, |\phi^+\rangle : 0 \\
|1\rangle, |-\rangle, |-y\rangle|y\rangle, |\psi^-\rangle : 1
\end{array} \right.
\]  
(13)

Then, the following equation can be yielded,
\[
(U_1 \otimes U_{23} \otimes \cdots \otimes U_{(2m-2)(2m-1)})|\xi\rangle_{12...2m-1}
\]  
\[= \frac{1}{\sqrt{2}} [0] \left( \frac{1}{\sqrt{2}} (|00\rangle + |11\rangle) \right) \otimes \cdots \otimes \left( \frac{1}{\sqrt{2}} (|00\rangle + |11\rangle) \right)
\]  
\[+ \frac{1}{\sqrt{2^d}} [1] \left( \frac{1}{\sqrt{2}} (|01\rangle - |10\rangle) \right) \otimes \cdots \otimes \left( \frac{1}{\sqrt{2}} (|01\rangle - |10\rangle) \right)
\]  
= |\xi\rangle.
\]  
(14)

As a result, it is clear that the \( 2i \) and \( 2i+1 \) qubits of the entangled state |\xi\rangle are immune to the collective-rotation noise channel if these two qubits are sent to a user in a short time. Furthermore, the entangled state |\xi\rangle can also be expressed in
\[
|\xi\rangle = \frac{1}{2^{\frac{1}{2}}} \left\{ |+\rangle \left( \sum_a \Gamma \left[ (|y\rangle|y\rangle)^{2a}(|y\rangle|y\rangle)^{m-1-2a} \right) \right\}
\]  
\[+ |-\rangle \left( \sum_b \Gamma \left[ (|y\rangle|y\rangle)^{2b+1}(|y\rangle|y\rangle)^{m-1-(2b+1)} \right) \right\}.
\]  
(15)

Again, there is another proposition we can get based on (12) and (15).
Proposition 2 A two level \((2m - 1)\)-particle quantum state is in the form of \(|\xi\rangle\) if and only if both of following two conditions are true: (1) when the first particle is measured in the \(B_x\) and the particles \((2i)(2i + 1)\) are measured in the Bell state measurement, all of the \(m\) outcomes are the same; (2) when the first particle is measured in the \(B_x\) and the particles \((2i)(2i + 1)\) are measured in the \(B_y\) respectively, the sum of all outcomes modules 2 is equal to zero (the proof of Proposition 2 is provided in Appendix).

2.3 The Defect of “tree-type” QKA Protocol and a Possible Solution

Before giving our protocols, let us discuss a defect that exists in the “tree-type” multipartite QKA protocol. In the light of the transmission structure of this type protocol, we can find that the last user who performs security test has a chance to control the protocol which also appears in the XWGQ protocol [33]. It is evident that the last user can measure all remaining particles first before announcing his test particles. Then, the last user can publish the coordinates of the test particles arbitrarily according to his desire and the measurement result. In this way, the last user can determine the shared key mostly without inducing errors. Hence, this defect makes the “tree-type” QKA protocol unfair.

Here, we study the issue and put forward a possible scheme. The detailed process of the scheme is stated below. First, all users agree on an one-way hash function \(h\) [48], where \(h\) can map data of arbitrary size to data of fixed size. Moreover, it is known that even one bit of the input of hash function is changed, the hash values will be very different. In calculation, it is almost impossible to find a same hash value with two different inputs. Then, every user announces the value of \(h(T)\), where \(T\) is the relative coordinates of test particles determined by the user. Undoubtedly, the relative coordinates of one user can be changed to the absolute coordinates after discarding test particles of previous users. By this means, the last user can only announce the correct coordinates of test particles he predetermined which avoids the above defect. Therefore, we can take hash function to check the honesty of the last user. Obviously, the XWGQ protocol may also be much secure by applying this one-way hash function technique.

3. Multipartite QKA Protocols

In this section, two multi-party QKA protocols against the collective-dephasing noise and the collective-rotation noise are proposed, respectively. Suppose that there are \(m\) users, \(P_0, P_1, \ldots, P_{m-1}\), who want to share a secure key. Here, all the quantum channels are public and all the classical channels are authenticated. In the presented protocols, one of the \(m\) users is chosen randomly to be the distributor. Without loss of generality, we assume \(P_0\) as the distributor. At first, we put forward the protocol against collective-dephasing noise. Achieving this security task is made up of following steps.

Step 1: All of \(m\) users negotiate a hash function \(h\), where \(h : \{0, 1\}^n \rightarrow \{0, 1\}^v\).

Step 2: \(P_0\) prepares \((n + m\delta)\) copies of quantum state \(|\phi\rangle\), where \(\delta\) is the security strength. For each quantum state \(|\phi\rangle\), \(P_0\) keeps qubit 1 in his hands as the ordered sequence \(S_0 = \{s_0^0, s_0^1, \ldots, s_0^{n+m\delta-1}\}\), and divides each qubits \((2i)\) and \((2i + 1)\) of each state \(|\phi\rangle\) to form the ordered sequence \(S_i = \{s_i^0, s_i^1, \ldots, s_i^{2(2i+m\delta-1)}, s_i^{2(2i+m\delta-1)+1}\}\).

Step 3: Each user \(P_j\) \((j = 0, 1, \ldots, m - 1)\) generates a random string \(T_j = \{t_j^1, t_j^2, \ldots, t_j^{v-1}\}\) as the relative coordinates of test particles, where \(t_j^v\) \((v = 0, 1, \ldots, \delta - 1)\) ranges from 0 to \([n + \delta] \bmod \delta\). Then, \(P_j\) computes \(g_j = h(T_j)\) and announces the value of \(g_j\).

Step 4: \(P_0\) distributes the ordered sequence \(S_i\) to the user \(P_i\), respectively.

Step 5: After receiving the particle sequence, each user performs the security test. Start from \(P_0\), he measures each test particle of \(S_i^{\text{test}} = \{s_i^0, s_i^1, \ldots, s_i^{2v-1}\}\) in the \(B_z\) or \(B_x\) randomly. Then, he declares \(T_0\) and the corresponding measurement base.

Step 6: Each user \(P_i\) verifies whether \(h(T_0) = g_0\) is satisfied or not. If the verification is passed, they continue to the next step. Otherwise all users abandon the protocol.
Step 7: Each user $P_i$ measures the counterpart $S_{ij}^{\text{test}}$ in appropriate base, where $S_{ij}^{\text{test}} = \{s_0^{2^j}, s_1^{2^j}, \ldots, s_{2^j - 1}^{2^j}, s_0^{2^j+1}, s_1^{2^j+1}, \ldots, s_{2^j - 1}^{2^j+1}\}$. The detailed rule of the measurement is as follows: if $P_0$ measures the test particle $s_0^{2^j}$ in the $B_x$, $P_i$ needs to measure $s_0^{2^j}$ and $s_0^{2^j+1}$ in the Bell state measurement; if $P_0$ chooses $B_x$ as the measurement basis of $s_0^{2^j}$, $P_i$ is required to measure $s_0^{2^j}$ and $s_0^{2^j+1}$ in the $B_x$, respectively.

Step 8: After measurements, each user $P_i$ sends the measurement result $R_{ij}^{\text{test}}$ to $P_0$ in the order designed by $P_0$, where $R_{ij}^{\text{test}} = (t_0^j, t_1^j, \ldots, t_{2^j - 1}^j)$. If the measurement basis is $B_x$, $P_0$ is required to verify whether or not $r_0^j = t_0^j = \ldots = r_{m-1}^j$ is satisfied. If $P_0$ chooses $B_x$, he needs to check if $\sum_{j=0}^{m-1} r_j^j \mod 2 = 0$. If the test is failed, $P_0$ informs the other users to abort the protocol. Otherwise, they continue to the next step.

Step 9: Each user $P_i$ performs the security test as $P_0$ does from Steps (5) to (8). It is worth noting that if $P_i$ is the checker, the test sequence $P_i$ selects is $S_i^{\text{test}} = \{s_0^{2^i}, s_1^{2^i}, \ldots, s_{2^i - 1}^{2^i}, s_0^{2^i+1}, s_1^{2^i+1}, \ldots, s_{2^i - 1}^{2^i+1}\}$, where $t_0^i, t_1^i, \ldots, t_{2^j - 1}^i$ are even numbers now.

Step 10: If all security tests are passed, now $P_0$ has $n$ particles and $P_i$ has $2n$ particles left after discarding test particles, respectively. Then, $P_0$ measures each particle in the $B_x$ and $P_i$ measures each pair particles in the Bell state measurement, respectively. This will generate $n$ outcomes respectively which form the shared key $K = \{k_0, k_1, \ldots, k_{n-1}\}$.

The multipartite QKA protocol against collective-rotation noise is similar to the above protocol, except that

1. the quantum state $P_0$ prepared in Step 2 is $|\xi\rangle$;
2. if $P_0$ chooses $B_x$ as the measurement basis, $P_i$ is required to measure the counterpart in $B_y$ respectively in Step 7.

4. Security Analysis

In this section, we will prove that the presented protocols can resist against some common outside attacks and inside attack. Since the security analysis of the second protocol is similar to the first one, so we focus our analysis on the first protocol.

4.1 Outside Attack

We first analyse the outside attack. Roughly speaking, the common attacks the outside eavesdropper may employ are intercept-resend attack and entangle-measure attack. In the following, the security of the first protocol will be briefly discussed under these two common attacks.

4.1.1 Intercept-Resend Attack: Here, the intercept-resend attack is discussed. Suppose that Eve is an outside eavesdropper. From the process of the proposed protocol, it is obvious that Eve can only intercept the particles in Step 4. Without loss of generality, suppose that Eve intercepts arbitrary $2\mu$ particles she would like to in $S_i$. If $2\mu \leq 2n$, there is a chance that all $2\mu$ particles are not included in the test. So that Eve can get the value of $\mu$ bits of the shared key without inducing errors. In order to achieve her conspiracy, Eve may take the following methods. One is that Eve intercepts particles from $S_i$ directly. Then, the probability of that all $2\mu$ particles are not included in the test is

$$P_1 = \frac{(2n)!}{(2\mu)!} \cdot \frac{(2n + 2\mu + 1)!}{(2n + 2\mu)!}$$

$$= \frac{2n(2n - 1) \cdots (2n - 2\mu + 1)}{(2n + 2\mu + 1) \cdots (2n + 2\mu + 2\mu + 1)} = \prod_{c=2n}^{2n-2\mu+1} \frac{c}{c + 2\mu}$$

The other track is that Eve first cracks the hash function to obtain all correct coordinates of test particles. Then, the particles Eve intercepts must not be included in the test. Without loss of
generality, suppose the input of the hash function is $2^N$ bits and the output is $2^n$ bits (the value of $N$ is far greater than $n$). Thus, the probability of that Eve obtains the correct relative coordinates is $\frac{1}{2^N}$. Since the coordinates Eve gets are relative, the probability of that Eve acquires all correct absolute coordinates of test particles is

$$P_2 = \left(\frac{1}{2^{N-\eta}}\right)^m.$$  

(17)

However, both probabilities $P_1$ and $P_2$ are closing to 0 if we entail the security strength $\delta$ large enough. That is to say, the probability of the particles Eve intercepts contain test particles tends to 1, i.e., the particles Eve intercepts must include test particles with the help of the one-way hash function.

In this circumstance, Eve has to measure the particles she intercepts with the Bell state measurement. Then she generates fake particles to $P_i$ according to her measurements. In this case, the attack cannot be detected when the checker takes condition (1) to check for the security test. Nevertheless, the eavesdropping can be found by the checker when he verifies whether or not $\sum_{j=0}^{m-1} r_j \mod 2 = 0$ is satisfied. When the checker adopts $B_2$ to measure these intercepted particles, the measurement results must be random since the qubits that $P_i$ receives have no correlation with the qubits of others based on the quantum mechanics principles. By this means, $P_i$ has the probability $[1 - (3/4)^{1/2}]$ to detect the existence of Eve, where $\gamma$ is the number of intercepted particle-pairs that belong to the test. For example, the probability is 98.66% when $\gamma = 10$. Besides, the probability is approaching to 1 as the number $\gamma$ becomes larger. Thus, Eve cannot obtain the shared key without introducing any error in this case. Furthermore, it is worth noting that the security of our proposed “tree-type” protocols relies on the quantum mechanics principles rather than the hash function.

4.1.2 Entangle-Measure Attack: Now, let us analyze the entangle-measure attack. Entangle-measure attack is one kind of general attack, and is also an important means of the security analysis of quantum cryptography protocols [49]. In this attack, the eavesdropper Eve intercepts the transmitted particles and interacts these particles with ancillary particles by performing unitary operators. After that, Eve sends the travel particles to the original users. In the end, Eve measures the ancillary particles in her hands to obtain some information about the shared key.

Without loss of generality, suppose that Eve prepares one ancillary particle in the initial state $|\epsilon\rangle$. She first intercepts the travel particle sequence $S_i$ that $P_0$ sends in Step 4, and performs the unitary operation $U^E$ on the intercepted particles and $|\epsilon\rangle$. Then, Eve sends the operated particles to $P_i$. After receiving the particle sequence, $P_i$ tests and measures the particles he received. In this way, Eve tries to get the shared key from measuring the ancillary particle in her hands.

In this case, the two level $(2m-1)$-particle entangled state becomes into a two level $2m$-particle state

$$|\psi^{'}\rangle'_{12...2m} = \alpha_2|0\rangle|\psi^+\rangle \otimes \cdots \otimes |\psi^+\rangle|\epsilon_0\rangle + \beta_2|1\rangle|\psi^-\rangle \otimes \cdots \otimes |\psi^-\rangle|\epsilon_1\rangle,$$  

(18)

where $|\alpha_2|^2 + |\beta_2|^2 = 1$, $|\epsilon_0\rangle$ and $|\epsilon_1\rangle$ are pure states uniquely determined by $U^E$. From the (18), we can derive

$$|\psi^{'}\rangle = |+\rangle \left[ \frac{\alpha_2}{2^2}(|A_1\rangle + |B_1\rangle)|\epsilon_0\rangle + \frac{\beta_2}{2^2}(|A_1\rangle - |B_1\rangle)|\epsilon_1\rangle \right]$$

$$|+\rangle \left[ \frac{\alpha_2}{2^2}(|B_1\rangle + |A_1\rangle)|\epsilon_0\rangle + \frac{\beta_2}{2^2}(|B_1\rangle - |A_1\rangle)|\epsilon_1\rangle \right].$$  

(19)

For satisfying the condition (2) of the security test, the following equation should be satisfied,

$$\left\{ \frac{\alpha_2}{2^2} |B_1\rangle|\epsilon_0\rangle - \frac{\beta_2}{2^2} |B_1\rangle|\epsilon_1\rangle = 0 \right. 
\left. \frac{\alpha_2}{2^2} |A_1\rangle|\epsilon_0\rangle - \frac{\beta_2}{2^2} |A_1\rangle|\epsilon_1\rangle = 0 \right. ;$$  

(20)
Hence, we can deduce
\[ \begin{align*}
\alpha_2 &= \beta_2 \\
|\varepsilon_0\rangle &= |\varepsilon_1\rangle
\end{align*} \]
which means that the initial particles and the ancillary particle are always product state. That is, Eve cannot get any useful information about the shared key from measuring the ancillary particle. Therefore, our protocol is secure against these two common outside attacks.

4.2 Inside Attack

Next, we consider the inside attack. It seems that \( P_0 \) is more special than other users since \( P_0 \) is the distributor of the protocol. Thus, we suppose that \( P_0 \) is a dishonest user who considers deciding the shared key alone. As the distributor, \( P_0 \) can prepare other quantum states to replace the appointed state to attain his evil. However, the sufficiency proved in Section II (Appendix) indicates that \( P_0 \) can only prepare and distribute the entangled state \( |\varphi\rangle \) \( (|\xi\rangle) \) to satisfy the conditions of Proposition 1 (Proposition 2). Hence, this does not work. Then, after all security tests, all users measure their remaining particles to obtain the shared key. At this point, the states in the hands of each user are intact. Now \( P_0 \) can only measure the remaining particles in his hands in \( B_z \) respectively. In this way, the measurement result of each qubit is randomly \( |0\rangle \) or \( |1\rangle \). In other words, \( P_0 \) has half probability to determine the value of every bit of the shared key to be 0 or 1. Therefore, \( P_0 \) cannot determine the shared key. There is no doubt that the other users cannot decide the shared key, too. Consequently, our protocol can resist against inside attack.

Moreover, since the proposed protocol can be regarded as the distribution of a genuine multipartite entangled state by an untrusted user \( P_0 \) in a quantum network, it is worth noting that there might exist some insecure devices in the process of distribution. Taking advantage of this loophole, dishonest users may achieve their conspiracy. Fortunately, a relevant quantum property deduced in Refs. [52]–[54] may be utilized to solve this problem. Namely, the steerability of \( P_0 \) over other users shows that the mutual dependence among them is more powerful than the imitation an unsteerable state can offer. Therefore, the multipartite steering may empower the security of QKA protocol more strongly even with some untrusted devices.

5. Discussions

Before giving a conclusion, the reasonable comparison of two kinds of protocol is discussed. In advance of the first QKA protocol [20], Chen et al. proposed a new protocol named quantum conference key protocol [51]. The goal of quantum conference key protocol is to share a common string of random number among all users except the eavesdropper Eve, which achieves the same purpose with QKA protocol. However, in contrast to quantum conference key protocol in which all users are in the same boat and they will always execute the protocol honestly, QKA protocol requires more rigorous security. In the QKA protocol, we need to consider the existence of dishonest users. Besides, dishonest users can collaborate to enforce their conspiracy, i.e., make all users share the common key which they predetermined alone. With the rigorous security requirements, QKA protocol can carry out another special tasks, like providing the access control, providing the authentication and identification of users and so on [41], [42].

Next, we focus on the efficiency of the proposed protocols. From Ref. [50], a natural definition of efficiency is \( E = \frac{i}{t + b} \), where \( i \) refers to the length of the final shared key, \( t \) and \( b \) denotes the number of the traveling qubits and bits respectively. However, the transmitted bits of both the proposed protocols and the XWGQ protocol are used to do security test. Besides, the extra transmitted bits may give some dishonest users more chance to carry out their conspiracy. Hence, the efficiency of these protocols is equal to the corresponding particle efficiency \( h = \frac{i}{t} \) which is defined in Ref. [30]. So, we obtain the efficiency of the presented protocols, \( \frac{n}{2(n+m)(m-1)} \). Furthermore, the comparison of two same category multipartite QKA protocols is shown in Table 1, which all belong to the “tree-type” QKA protocol. From Table 1, it is shown that the efficiency of the presented protocols is
TABLE 1
Comparison of Two Multipartite QKA Protocols

<table>
<thead>
<tr>
<th></th>
<th>Efficiency</th>
<th>Repel collective noise</th>
</tr>
</thead>
<tbody>
<tr>
<td>XWGQ protocol [33]</td>
<td>( \frac{(n+\delta)}{(n+m(n-1))} )</td>
<td>No</td>
</tr>
<tr>
<td>The proposed protocols</td>
<td>( \frac{n}{2(n+m(n-1))} )</td>
<td>Yes</td>
</tr>
</tbody>
</table>

approximately half of the XWGQ protocol, while the proposed protocols can resist against the collective noise.

6. Conclusion
The proposed protocols in this paper adopt the interesting properties of the multiparticle quantum entangled states to do the security test and agree on the shared key. In these protocols, only one user needs to take the quantum communication with other users. Furthermore, the representation of the entangled states shows that the presented protocols can be realized under the collective-dephasing noise channel and collective-rotation noise channel, respectively. At last, the security analysis implies that our protocols are secure against the inside attack and some common outside attacks.

In addition, although the schemes of QSS and MQKA are utilized to solve different secure tasks, these two kinds of protocols are concerned with multipartite users. Moreover, it is evident that the proof of unconditional security of multipartite quantum cryptography protocols is more difficult than two-party protocol (e.g. quantum key distribution). Recently, two partially device-independent QSS protocols have been proposed in Refs. [15], [16], which implies that unconditional secure entanglement-based continuous variable QSS has been achieved. Therefore, drawing ideas from the designing methods of some famous QSS protocols [10]–[13], [15], [16], we will try to design an unconditional secure MQKA protocol in the future. Besides that, it is also interesting to consider the practical implementation of QKA protocol. A work on this issue of QSS has been put forward [14], which will shed new light on designing a more feasible multipartite QKA protocol.

Appendix
In this section, we provide the proof of the Proposition 2.

Based on (12) and (15), it is evident that \(|\xi\rangle\) can meet both the conditions in Proposition 2. Now we prove the sufficiency. First, to satisfy the condition (1) of Proposition 2 that all \(m\) outcomes of the state \(|\omega\rangle\) are the same, \(|\omega\rangle\) must be in the form

\[
|\omega\rangle_{12...2m-1} = \alpha_3|0\rangle|\phi^+\rangle \otimes \cdots \otimes |\phi^+\rangle + \beta_3|1\rangle|\psi^+\rangle \otimes \cdots \otimes |\psi^+\rangle,
\]

where \(|\alpha_3|^2 + |\beta_3|^2 = 1\). Then we can derive the following equation from (22),

\[
|\omega\rangle = |+\rangle \left[ \left( \frac{\alpha_3}{2^\frac{m}{2}} + \frac{(i)^{m-1}\beta_3}{2^\frac{m}{2}} \right) |A_2\rangle + \left( \frac{\alpha_3}{2^\frac{m}{2}} - \frac{(i)^{m-1}\beta_3}{2^\frac{m}{2}} \right) |B_2\rangle \right]
+ |^{-}\rangle \left[ \left( \frac{\alpha_3}{2^\frac{m}{2}} + \frac{(i)^{m-1}\beta_3}{2^\frac{m}{2}} \right) |B_2\rangle + \left( \frac{\alpha_3}{2^\frac{m}{2}} - \frac{(i)^{m-1}\beta_3}{2^\frac{m}{2}} \right) |A_2\rangle \right].
\]

(23)
where
\[ |A_2\rangle = \sum_a \Gamma \left[ (| - y\rangle| + y\rangle)2^a (| + y\rangle| - y\rangle)2^{a-1} \right], \]
\[ |B_2\rangle = \sum_b \Gamma \left[ (| - y\rangle| + y\rangle)2b+1 (| + y\rangle| - y\rangle)2^{b+1} \right]. \]  
(24)

Next, to satisfy the condition (2) of Proposition 2, we can obtain
\[ \left\{ \begin{align*}
\left( \frac{\alpha_3}{2} - \left(\frac{\beta_3}{2} \right)^{m-1} \right) |B_2\rangle & = 0 \\
\left( \frac{\alpha_3}{2} - \left(\frac{\beta_3}{2} \right)^{m-1} \right) |A_2\rangle & = 0
\end{align*} \right. \]  
(25)

According to (25), \( \alpha_3 = (\frac{\beta_3}{2})^{m-1} \) can be derived. Therefore, to satisfy normalization we can get that \( \alpha_3 = \frac{1}{\sqrt{2}}, \beta_3 = \frac{1}{\sqrt{2}^{m-1}} \) with the global phase ignored. Then, we have \( |\omega\rangle = |\xi\rangle \). So far, we have proved that if a two level \((2m - 1)\)-particle state meets both conditions (1) and (2) of Proposition 2, it must be \( |\xi\rangle \).

References