Quantum anonymous ranking

Wei Huang,[1,2] Qiao-Yan Wen,[1] Bin Liu,[1] Qi Su,[1] Su-Juan Qin,[1] and Fei Gao[1,*]
[1]*State Key Laboratory of Networking and Switching Technology, Beijing University of Posts and Telecommunications, Beijing 100876, China*
[2]*State Key Laboratory of Integrated Services Networks, Xidian University, Xi'an, 710071, China*

(Received 21 November 2013; published 14 March 2014)

Anonymous ranking is a kind of privacy-preserving ranking whereby each of the involved participants can correctly and anonymously get the rankings of his data. It can be utilized to solve many practical problems, such as anonymously ranking the students' exam scores. We investigate the issue of how quantum mechanics can be of use in maintaining the anonymity of the participants in multiparty ranking and present a series of quantum anonymous multiparty, multidata ranking protocols. In each of these protocols, a participant can get the correct rankings of his data and nobody else can match the identity to his data. Furthermore, the security of these protocols with respect to different kinds of attacks is proved.

DOI: 10.1103/PhysRevA.89.032325 PACS number(s): 03.67.Dd, 03.65.Ud

I. INTRODUCTION

With the development of technology, the proliferation of the internet has triggered enormous demand for multiparty computation, in which people jointly conduct computation tasks based on the private inputs they each provide. In actual situations, these computations usually occur among partially trusted parties or even among competitors. Therefore, privacy naturally becomes a major concern of the people involved in these computations. The computation, which enables n ($n \geqslant 2$) participants to jointly compute a function based on their private inputs while at the same time keeping these inputs private, is referred to as secure multiparty computation (SMC) [1].

SMC is one of the most important subfields of cryptography and consists of many real-life applications such as Yao's millionaire problem [1], private database queries [2], anonymous voting (election) [3], and secret sharing [4]. Thus far, the privacy of the participants' inputs in all the practical SMC systems (e.g., electronic voting system) has relied on the public-key cryptography whose security is guaranteed by the assumptions of computational complexity. However, with the rapid development of quantum algorithms and quantum computing [5,6], these assumptions face more and more austere challenges. To solve this problem, many research groups have focused their attention on designing SMC protocols, which pursue information-theoretical security, based on the principles of quantum mechanics [7–22], including quantum secret sharing [7–9], quantum private database queries [10–13], quantum anonymous voting or surveying [14–17], and the quantum millionaire problem [18–22].

It is known that ranking is a fundamental problem in computer science and is one of the most common operations in data processing. In this paper, ranking refers to sequencing a set of non-negative integers with affiliation according to their numerical size. Concretely, the data set of the ranking is supposed to be a set of non-negative integers, each of which belongs to a specific participant. At the end of the ranking, each participant should know the positions of his numbers in the ascending (or descending) sequence of the ranked numbers. To achieve the ranking, the participants can make use of different strategies, such as comparing the numbers with each other. For instance, if n students desire to rank their physical test scores, they can make pairwise comparisons of their scores. To be specific, if a student has compared his score with each of the other $n-1$ students individually, he will know how many people score higher and lower than himself. Then he can get the position of his score in the ascending (or descending) ranking sequence of all the n scores. However, with the trend of the interactive lifestyle over internet, people are paying more and more attention to the protection of privacy. In this context, secure multiparty, multidata ranking (SMMR) [23–25] has become one of the promising approaches in SMC. Suppose there are n participants, P_1, $P_2, \dots,$ and P_n. Participant P_i has a data set $D_{P_i} = \{m_1^i, m_2^i, \dots, m_{k_i}^i\}$ for $1 \leqslant i \leqslant n$, where $D_{P_i} \subset \{1, 2, \dots, N\}$ and N is a natural number, which is larger than the maximum element in $D = D_{P_1} \cup D_{P_2} \cup \cdots \cup D_{P_n}$. The purpose of SMMR is to rank all the data in D following the rules given below.

(R1) *Correctness*. Every participant should correctly get the rankings of his data, i.e., the positions of his data in the ascending (or descending) ranking sequence of all the data in D.

(R2) *Anonymity*. For each of the participants, nobody else can obtain any useful information about the rankings of his data.

(R3) *Secrecy*. The values of each participant's data should be kept secret from all others.

It should be pointed out that if $n = 2$, no secure SMMR protocol exists since one participant can directly get the rankings of the other participant's data according to the rankings of his own data. Hence, the number of the participants involved in the ranking protocols in this paper is supposed to be larger than 2. When each of the n participants only has a single input, i.e., $k_1 = k_2 = \cdots = k_n = 1$, this ranking is referred to as secure multiparty, single-data ranking (SMSR). Obviously, SMSR is only a special case of SMMR.

Up to now, all the existing SMMR (or SMSR) protocols [23–25] are based on the computational complexity assumptions, which indicate that they cannot achieve information-theoretical security. More importantly, most of them are proposed in the semihonest model in which all the participants are assumed to be honest but curious [23–25]. However, in real life,

[*] gaofei_bupt@hotmail.com

ranking usually occurs among mutually untrusted participants; hence, the protocols designed under the semihonest model are impractical. For this reason, we wonder whether there exists a kind of privacy-preserving ranking that cannot only achieve information-theoretical security but also be of use in practical situations. Before answering this question, we should realize that the reason why most of the existing SMMR protocols are designed in the semihonest model is that it is difficult to design a SMMR protocol, which could simultaneously satisfy (R1)–(R3) without adding any additional assumption on the participants. Consequently, assuming all the participants to be semihonest was considered as a compromise in most of the previous protocols [23–25].

Actually, in many real-life situations, it is more desirable that the identity of the person who owns the data, rather than the data itself, be kept secret. In other words, anonymity of the participants in multiparty ranking is usually much more important than secrecy of the data in reality. In many practical cases, the primary concerns of the participants are correctness and anonymity. Hence, the participants do not care whether the values of the ranked data are public as long as no one can match the data with the identity of its owner. In some cases, the participants may even want the values of the ranked data to be public and hence they get the distribution of all the ranked data, which may be useful to them. For example, exam scores were not considered as students' private information at an early age. Therefore, each of the students in a group can get his or her ranking by disclosing his or her score publicly. However, in order to protect the students' self-esteem nowadays, it has become an international practice that the relationship between a student and his or her score should be kept secret. Thus, how a certain number of students can respectively get their rankings correctly under the premise of preserving anonymity has become an important problem. Another example arises when several competing companies within the same field want to make a ranking of the wages of all their employees in order to make each of the companies learn the level of its treatment among all these companies. However, no company wants to leak the relationship between it and the wages of its employees under this circumstance. Hence, the problem is that how each of the companies could correctly get the rankings of its employees' wages under the premise of preserving anonymity. Of course, there are still many examples like this in daily life, such as ranking the sales volume of a kind of product in several competing companies. Here we do not describe them in detail.

From the above examples, we can find that, in the real-life scenarios, a participant involved in privacy-preserving ranking usually does not care whether the values of his data can be known by others provided that nobody else could match the identity of him with his data. The primary concern of a participant is whether he can correctly and anonymously get the rankings of his data. As the anonymity of the participants occupies such an important position in privacy-preserving ranking in daily life, we devote ourselves to presenting a new quantum cryptographic primitive, the quantum anonymous multiparty, multidata ranking (QAMMR), which cannot only achieve information-theoretical security but also be consistent with the practical situations. The features that we want the QAMMR protocols to have are as follows.

(P1) *Correctness*. Each participant should correctly get the rankings of his data.

(P2) *Anonymity*. For each of the participants, nobody else can obtain any useful information about the rankings of his data.

(F3) *Untraceability*. Nobody can match the identity of a participant with his data except the participant himself.

(F4) *Security*. The protocol is secure against the quantum adversary whose actions are only limited by the laws of quantum mechanics.

Before proposing our protocols, we first introduce the basic idea of them. Concretely, suppose $D = D_{P_1} \cup D_{P_2} \cup \cdots \cup D_{P_n} = \{y_1, y_2, \dots, y_{|D|}\}$, where $y_1 < y_2 < \cdots < y_{|D|}$, and $|D|$ is the number of the elements contained in D. After the joint computation, if each of the n participants gets the value of $T^{y_i} = |D_{P_1}^{y_i}| + |D_{P_2}^{y_i}| + \cdots + |D_{P_n}^{y_i}|$ for $1 \leqslant i \leqslant |D|$, without leaking the information of which of the ranked data belongs to him (where $|D_{P_j}^{y_i}|$ represents the number of y_i contained in D_{P_j}, $1 \leqslant j \leqslant n$), they can respectively get the rankings of their data in ascending order (e.g., the ranking of the data y_i is $T^{y_1} + T^{y_2} + \cdots + T^{y_{i-1}} + 1$). Therefore, the task of the following part of this paper is to introduce several QAMMR protocols based on this idea.

The rest of this paper is organized as follows. In Sec. II, we present a protocol to achieve QAMMR in the semihonest model. Then two more practical QAMMR protocols, in which the participants need not be semihonest, are proposed in Sec. III. As in most of the previous quantum cryptographic protocols [7–21], the classical communication channels are assumed to be authenticated in this paper. In addition, the technique of "block transmission", which was proposed first by Long *et al.* [26], is employed to ensure the security of state transmission in our protocols. In block transmission, the quantum information carriers are ordered and transmitted in blocks, and the eavesdropping detection is also executed on the blocks. In Sec. IV, we demonstrate that all the presented protocols are secure. Then some useful discussions are given in Sec. V, and our conclusions are in Sec. VI.

II. QAMMR PROTOCOL IN THE SEMIHONEST MODEL

Herein we propose a QAMMR protocol in which n ($n \geqslant 3$) participants are involved. The participant P_i has a data set $D_{P_i} = \{m_1^i, m_2^i, \dots, m_{k_i}^i\}$, where $D_{P_i} \subset \{1, 2, \dots, N\}$, $1 \leqslant i \leqslant n$. That is to say, each participant may possess more than one datum, and different participants may own the same data. Similar to most of the classical SMMR protocols [23–25], all the participants in this protocol are assumed to be semihonest (honest but curious). That is, the participants always follow the procedure of the protocol, but they might try to steal the information from the record of the intermediate computations. Although this protocol is under semihonest assumption as most of the classical SMMR protocols, it is more secure than the classical ones since the security of it is guaranteed by laws of quantum mechanics. To achieve QAMMR by this protocol, a kind of two-particle d-level Bell state ($d \geqslant \sum_{i=1}^{n} k_i + 1$) is utilized [14,17,18]. One of the n participants should be responsible for preparing and measuring the entangled states. For simplicity, we assign this task to P_1. The specific steps of the protocol can be described as below (see also Fig. 1).

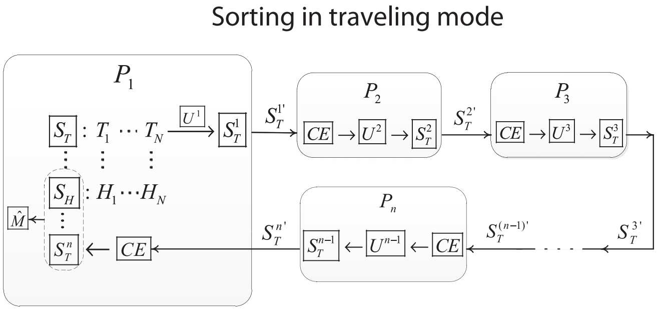

FIG. 1. Illustration of the proposed QAMMR protocol in the semihonest model, where CE is the eavesdropping check and U^i represents the encoding operation performed by P_i. The classical communications are omitted.

(i) P_1 prepares an ordered sequence of N two-qudit entangled pairs $[|\Phi\rangle_1, |\Phi\rangle_2, \ldots, |\Phi\rangle_N]$, where

$$|\Phi\rangle_i = \frac{1}{\sqrt{d}} \sum_{j=0}^{d-1} |j\rangle_{H_i} |j\rangle_{T_i}, \quad 1 \leqslant i \leqslant N. \tag{1}$$

Here the subscripts H and T represent two different qudits in one entangled pair and the subscript i $(i = 1,2,3,\ldots,N)$ indicates the order of the entangled pairs in this sequence. P_1 takes one qudit from each pair to form two ordered qudit sequences: $[H_1, H_2, \ldots, H_N]$ (denoted as S_H) and $[T_1, T_2, \ldots, T_N]$ (denoted as S_T).

(ii) P_1 encodes all his data (the data in D_{P_1}) on the corresponding qudits in S_T. Concretely, he performs the unitary operation U on the m_i^1th qudit in S_T, $i = 1,2,\ldots,k_1$, where

$$U = \sum_{j=0}^{d-1} \exp(i\theta j)|j\rangle\langle j|, \quad \theta = \frac{2\pi}{d}. \tag{2}$$

The effect of the operation U on state $|\Phi\rangle$ can be illustrated as

$$\begin{aligned} I^x \otimes U^x|\Phi\rangle &= I \otimes U^x|\Phi\rangle \\ &= \frac{1}{\sqrt{d}} \sum_{j=0}^{d-1} \exp(i\theta j x)|j\rangle_H |j\rangle_T, \end{aligned} \tag{3}$$

where U^x represents performing the operation U x times and I is the identity operation on the d-dimensional Hilbert space. After these operations, we denote the new sequence as $S_T^1 = [T_1^1, T_2^1, \ldots, T_N^1]$. Similar to [27], P_1 needs to prepare another δ states in $|\Phi\rangle$ for checking eavesdropping. Specifically, he inserts the first qudit of each of these states randomly in S_T^1 and preserves the remaining qudits (the second qudit of each of the states). After that, P_1 sends all the $N + \delta$ qudits (denoted as $S_T^{1'}$) to P_2.

(iii) After the reception of $S_T^{1'}$, P_2 requires P_1 to tell him the positions of the inserted decoy qudits. For each of the decoy qudits, P_2 measures it randomly in B_1 basis or B_2 basis, where

$$\begin{aligned} B_1 &= \{|j\rangle\}_{j=0}^{d-1}, \\ B_2 &= \left\{ \frac{1}{\sqrt{d}} \sum_{k=0}^{d-1} \exp(i\theta k j)|k\rangle \right\}_{j=0}^{d-1}. \end{aligned} \tag{4}$$

Then P_2 tells Alice which measuring basis he has chosen for each of the qudits and the corresponding outcome of his measurement. P_1 utilizes the same measuring basis as P_2 to measure each of the corresponding qudits in his hands and analyzes the security with P_2. If there exists no eavesdropping in the quantum channel, their outcomes should satisfy a deterministic correlation; i.e., their measurement outcomes should be the same (the sum of their measurement outcomes should be 0 modulo d) provided that B_1 basis (B_2 basis) is utilized. If any error exists, they abandon the protocol; otherwise, P_2 has securely received S_T^1. Then P_2 encodes the data in D_{P_2} on the corresponding qudits in S_T^1. Concretely, he performs the unitary operation U on the m_i^2th qudit in S_T^1, $i = 1,2,\ldots,k_2$. After these operations, we denote the new sequence as $S_T^2 = [T_1^2, T_2^2, \ldots, T_N^2]$. Before sending S_T^2 to the next participant, P_2 also makes use of δ states in $|\Phi\rangle$ to ensure the secure transmission of S_T^2, similar to what P_1 does in step (ii). Afterwards, he transmits all the $N + \delta$ qudits (denoted as $S_T^{2'}$) to P_3.

(iv) The rest of the n participants execute the procedures just like what the first two participants do one after another. Finally, the last participant P_n sends all the processed qudits (i.e., $S_T^{n'}$) back to P_1.

(v) Once receiving the sequence $S_T^{n'}$ sent from P_n, P_1 and P_n check eavesdropping with the decoy qudits. If no eavesdropping exists, P_1 has securely received S_T^n. Then he measures each of the entangled pairs in his hand, i.e., (H_i, T_i^n) for $1 \leqslant i \leqslant N$, with the operator $\hat{M}$, where

$$\begin{aligned} \hat{M} &= \sum_{t=0}^{d-1} t|M_t\rangle\langle M_t|, \\ |M_t\rangle &= \sum_{m=0}^{d-1} \exp(i\theta m t)|m\rangle|m\rangle, \\ \langle M_s|M_t\rangle &= \delta_{st}. \end{aligned} \tag{5}$$

The measurement outcome of the ith pair in his possession is recorded as T^i. Finally, he publicly announces all the values T^i for $1 \leqslant i \leqslant N$. According to the announced information, each of the n participants can get the rankings of his data anonymously. For example, P_i will know that the ranking of his data m_j^i $(1 \leqslant j \leqslant k_i)$ is $T^1 + T^2 + \cdots + T^{m_j^i - 1} + 1$, and nobody else knows that m_j^i belongs to him.

In this QAMMR protocol, before P_1 prepares the entangled states, each of the other $n - 1$ participants should publicly announce the number of his data, with which P_1 could determine the value of d. Besides, the participants in this protocol should set up the wavelength filter and the photon number splitter to prevent the Trojan-horse attack and the invisible-photon attack [28,29]. Obviously, this protocol can be employed to solve the two practical issues, i.e., ranking the students' exam scores and ranking of the wages of the employees in different companies, mentioned in Sec. I.

III. THE MORE PRACTICAL QAMMR PROTOCOLS

Thus far, we have proposed a quantum protocol to achieve anonymous multiparty ranking under the semihonest model. However, the assumption that all the participants involved in this kind of ranking protocols should be semihonest, is not reasonable since the participants are likely to be partially trusted parties or even competitors. In real life, one or more participants may want to get the rankings of another participant's data. Therefore, we desire to ease the restrictions on the participants in order to design a QAMMR protocol, which is more coincident with the actual situation.

A natural question which arises when designing a more practical protocol is whether we can remove all the restrictions on the participants, namely, whether there exists a secure QAMMR protocol that sets no limitation on the behavior of the participants. Unfortunately, it has been proved that any two-party classical deterministic function cannot be securely evaluated by using quantum means [30,31]. Of course, this conclusion is also applicable to the QAMMR protocols since these protocols can be viewed as two-party type. Take an n-party protocol, for example. If we take a participant as one party, then the remaining $n-1$ participants can be viewed as the other party if they cooperate with each other. Consequently, no secure QAMMR protocol can be presented without adding any additional assumption.

To achieve anonymous multiparty ranking with quantum methods, an additional party (denoted as Server) whose role is to help each of the participants anonymously get the rankings of his data, is introduced to the following protocols. The Server in our protocols is permitted to misbehave on his or her own but conspire with none of the participants. However, he or she is unable to match the identity of a participant with his data through active and passive attacks. Under the circumstances, the participants in our protocols no longer need limiting to be semihonest. In other words, to get the desirable information, a participant may not only misbehave on his own but also cooperate with some of the other participants.

Moreover, all the parties (including Server and the participants) in the protocols should be rational. Although the dishonest parties may utilize different attacking strategies to deduce the rankings of a participant's data, they will not disrupt the execution of the protocol by designed if they could obtain no useful information about the rankings of a certain participant. To be specific, each participant may provide fake inputs in the execution of the protocol. If one participant provides fake inputs during the executing of the protocol and then tries to get the rankings of his data with the outcome of the joint computation running with his fake inputs and other participants' true inputs, he will be the only one who can get the correct rankings of his own data. Nevertheless, even if a participant utilizes this strategy, he is unable to deduce the rankings of another participant's data. Obviously, it is the case that if two or more participants utilizes this strategy, no participant will get the the correct rankings of his data. Unfortunately, this situation is inevitable even when a trusted additional party is introduced to the protocol. Consequently, we assume that the first choice of a participant is to obtain the right rankings of his data. Only when the success probability is nonzero will he take the corresponding attacking strategies to obtain information about the rankings of another participant's data.

Herein, we present two practical QAMMR protocols under the above assumptions. One is based on the basic idea of multiparty quantum secret sharing (MQSS); the other is based on the technique of quantum key distribution (QKD).

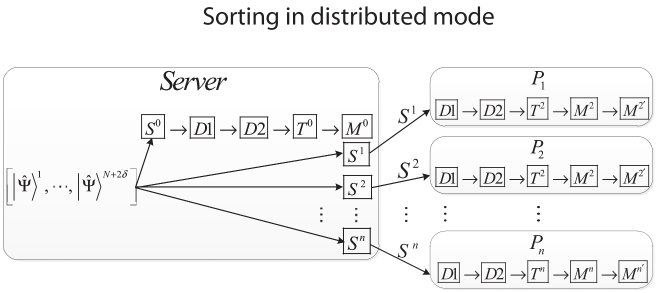

FIG. 2. Illustration of the more practical QSS-based QAMMR protocol, where the classical communications are omitted. $D1$ and $D2$ represent Detection 1 and Detection 2, respectively.

We also assume that n ($n \geqslant 3$) participants are involved in both of the protocols. Participant P_i has a data set $D_{P_i} = \{m_1^i, m_2^i, \ldots, m_{k_i}^i\}$, where $D_{P_i} \subset \{1,2,\ldots,N\}$, $1 \leqslant i \leqslant n$.

A. The QSS-based QAMMR protocol

Inspired by the idea in Ref. [32], let us first introduce a QAMMR protocol based on the d-level $(n+1)$-qudit Greenberger-Horne-Zeilinger (GHZ) states and the basic idea of MQSS. Different from the boss in MQSS who is assumed to be honest, the assumption of the Server in this protocol is more reasonable since he or she may try to steal the rankings of a participant's data with different kinds of attacks by himself or herself. Now, let us give an expatiation for this protocol as below (see also Fig. 2).

(a) Server prepares an ordered sequence of $N + \delta_1 + \delta_2$ GHZ states $[|\Psi\rangle^1, |\Psi\rangle^2, \ldots, |\Psi\rangle^{N+\delta_1+\delta_2}]$, where

$$|\Psi\rangle_{01\cdots n}^i = \frac{1}{\sqrt{d}} \sum_{j=0}^{d-1} |j\rangle_0^i |j\rangle_1^i \cdots |j\rangle_n^i. \tag{6}$$

Here the subscripts $0,1,2,\ldots,$ and n represent $n+1$ different qudits in a GHZ state and the superscripts i indicate the order of the GHZ states in this sequence, $1 \leqslant i \leqslant N + \delta_1 + \delta_2$, $d \geqslant \sum_{i=1}^n k_i + 1$. Then he or she performs a d-mode quantum discrete Fourier transform on each of the $n+1$ qudits in every GHZ state. The quantum discrete Fourier transform $\mathcal{F}$ is a unitary transformation of vector space of d-dimensional quantum systems that can be expressed in B_1 basis as

$$\mathcal{F}|j\rangle = \frac{1}{\sqrt{d}} \sum_{k=0}^{d-1} \exp\left(\frac{2\pi ijk}{d}\right) |k\rangle. \tag{7}$$

After these operations, the state $|\Psi\rangle$ is transformed into the form as

$$\begin{aligned}
|\widehat{\Psi}\rangle &= \mathcal{F} \otimes \mathcal{F} \otimes \cdots \otimes \mathcal{F}|\Psi\rangle \\
&= \frac{1}{\sqrt{d}} \sum_{j=0}^{d-1} \mathcal{F}|j\rangle_0 \otimes \mathcal{F}|j\rangle_1 \otimes \cdots \otimes \mathcal{F}|j\rangle_n \\
&= \frac{1}{\sqrt{d}} \sum_{j=0}^{d-1} \left\{ \left[\frac{1}{\sqrt{d}} \sum_{k_0=0}^{d-1} \exp\left(\frac{2\pi ijk_0}{d}\right) |k_0\rangle \right] \otimes \right.
\end{aligned}$$

$$
\begin{aligned}
&\cdots \otimes \left[\frac{1}{\sqrt{d}} \sum_{k_n=0}^{d-1} \exp\left(\frac{2\pi i j k_n}{d}\right) |k_n\rangle \right]\Bigg\} \\
&= d^{-\frac{1}{2}} \sum_{j=0}^{d-1} d^{-\frac{n+1}{2}} \sum_{k_0,\ldots,k_n} \exp\left[\frac{2\pi i j}{d}(k_0+ \right. \\
&\quad \left. \cdots + k_n)\right] |k_0\rangle \otimes \cdots \otimes |k_n\rangle \\
&= d^{-\frac{n}{2}} \sum_{K\equiv 0 (mod\ d)} |k_0\rangle|k_1\rangle \cdots |k_n\rangle, \qquad (8)
\end{aligned}
$$

where $K = k_0 + k_1 + \cdots + k_n$. After that, Server takes one qudit from each the entangled state $|\widehat{\Psi}\rangle^i$ ($i = 1,2,\ldots,N + \delta_1 + \delta_2$) to form $n + 1$ ordered qudit sequences: $[|\widehat{\Psi}\rangle_0^1,|\widehat{\Psi}\rangle_0^2,\ldots,|\widehat{\Psi}\rangle_0^{N+\delta_1+\delta_2}]$ (denoted as S^0), $[|\widehat{\Psi}\rangle_1^1,|\widehat{\Psi}\rangle_1^2,\ldots,|\widehat{\Psi}\rangle_1^{N+\delta_1+\delta_2}]$ (denoted as S^1), ..., $[|\widehat{\Psi}\rangle_n^1,|\widehat{\Psi}\rangle_n^2,\ldots,|\widehat{\Psi}\rangle_n^{N+\delta_1+\delta_2}]$ (denoted as S^n). Finally, he or she keeps qudit sequence S^0 and sends sequence S^i to P_i for $1 \leqslant i \leqslant n$, respectively.

(b) After receiving the qudit sequence sent from Server, the $n + 1$ parties (Server and the n participants) cooperate to execute the following two eavesdropping detections.

Detection 1. Server randomly chooses δ_1 qudits from S^0 and publishes the positions of the chosen qudits. For each of the chosen qudits, Server randomly chooses a basis (B_1 basis or B_2 basis) to measure it and requires the n participants to measure the corresponding qudits in their hands with the same basis. Then each of the participants announces his measurement outcome in a random order determined by Server. With the announced information, Server can check whether the measured qudits are in the state in Eq. (8), i.e., $|\widehat{\Psi}\rangle$. To be specific, if the $n + 1$ qudits are in $|\widehat{\Psi}\rangle$, the sum of the $n + 1$ measurement outcomes should be 0 modulo d (the $n + 1$ measurement outcomes should be the same), provided that B_1 basis (B_2 basis) is utilized. Once he or she finds any error in the process of this detection, he or she informs the others to discard their transmission and abort the protocol; otherwise, they continue to the next detection.

Detection 2. The n participants cooperate to choose δ_2 states randomly from the remaining $n + \delta_2$ states and process them as follows. P_i ($1 \leqslant i \leqslant n$) randomly chooses $\lfloor \frac{\delta_2}{n} \rfloor$ qudits from S^i and publishes the positions of the chosen qudits. For each of the chosen qudits, P_i randomly chooses a basis (B_1 basis or B_2 basis) and requires Server and the remaining $n - 1$ participants to measure the corresponding qudits in their possession with the same basis. After that, Server is required to announce his or her measurement outcome first. Then the $n - 1$ participants announce their measurement outcomes in a random order determined by P_i. By utilizing the detecting principle described in Detection 1, P_i can check whether the measured qudits are in $|\widehat{\Psi}\rangle$ with the announced information and his own measurement outcome. It should be noted that one of the participants should choose $\delta_2 - (n - 1)\lfloor \frac{\delta_2}{n} \rfloor$ qudits in his sequence for this detection in order to make sure that the total number of the states chosen by the n participants is δ_2. Without loss of generality, we assume the participant is P_n. If there exists any error in the process of this detection, they abort the protocol; otherwise, they continue to the next step.

(c) Once the $n + 1$ parties (Server and the n participants) confirm that there is no eavesdropping during the previous steps, they have securely shared an ordered sequence of N entangled states which are all in $|\widehat{\Psi}\rangle$, where the qudit sequence in Server's possession is denoted as W^0 and the qudit sequence of P_i is denoted as W^i for $1 \leqslant i \leqslant n$. Then each of the $n + 1$ parties measures the qudits in his or her sequence with B_1 basis and makes a record of the corresponding measurement outcomes. For example, the measurement outcome of the jth qudit in W^i is recorded as M_j^i for $1 \leqslant j \leqslant N$. Afterwards, each participant encodes his data on the N-dit classical string in his possession. Take P_i as an example: He encodes each data in D_{P_i} on the corresponding dit in M^i. Concretely, he replaces $M_{m_j^i}^i$ with $M_{m_j^i}^i + 1$ (mod d) for $1 \leqslant j \leqslant k_i$. After these encoding operations, the new classical string is denoted as $M^{i'}$. Finally, P_i publicly announces the string $M^{i'} = [M_1^{i'},M_2^{i'},\ldots,M_N^{i'}]$ for $1 \leqslant i \leqslant n$.

(d) According to the strings announced by the n participants ($M^{i'}$, $1 \leqslant i \leqslant n$) and his own string M^0, Server calculates T^i for $1 \leqslant i \leqslant N$, where $T^i = M_i^0 + M_i^{1'} + \cdots + M_i^{n'}$ (mod d). Finally, he or she announces all the calculated values. Based on the announced information, each of the n participants can get the rankings of his data anonymously. For example, P_i will know that the ranking of his data m_j^i ($1 \leqslant j \leqslant k_i$) is $T^1 + T^2 + \cdots + T^{m_j^i - 1} + 1$, and nobody else knows that m_j^i is contained in D_{P_i}.

It is obvious that the qudits only travel once in the whole process of this protocol; hence, the proposed protocol is congenitally free from the Trojan-horse attack and the invisible-photon attack [28,29]. In this protocol, Server and the n participants first securely share an N-dit classical secret, i.e., $M^0 + M^1 + \cdots + M^n = \bar{0}$ (mod d), by utilizing d-level GHZ states, where $\bar{0}$ represents the zero string of length N and each of the subsecret strings (M^i, $i = 1,2,\ldots,n$) is a random N-dit string. Then they make use of the shared secret to rank their data anonymously by our method. Of course, this protocol can also be used to resolve both of the practical issues introduced in Sec. I. In addition, this protocol is more consistent with the actual situation since the n participants need not be semihonest.

B. The QKD-based QAMMR protocol

Now we propose another practical QAMMR protocol based on the technique of QKD. Different from the above QSS-based protocol which utilizes multipartite entangled states, this protocol can achieve anonymous multiparty ranking with single particles. The specific steps of the protocol can be described as below.

(A) Server distributes a random N-dit secret key to each of n participants as follows. To distribute a random N-dit string to P_i for $1 \leqslant i \leqslant n$, Server generates a random $2N$-dit string R^{P_i} and a random $2N$-bit string C^{P_i}, respectively, where the jth dit (bit) of R^{P_i} (C^{P_i}) is denoted as $R_j^{P_i}$ ($C_j^{P_i}$), $R_j^{P_i} \in \{0,1,\ldots,d-1\}$, $C_j^{P_i} \in \{0,1\}$ for $1 \leqslant j \leqslant 2N$, and $d \geqslant \sum_{i=1}^{n} k_i + 1$. According to the two random strings, Server prepares a sequence of $2N$ single qudits, which is denoted as L^i. Specifically, the jth qudit in L^i (denoted as

L^i_j) is $\Pi_{R^{P_i}_j C^{P_i}_j}$, where

$$\Pi_{m0} = |m\rangle,$$
$$\Pi_{m1} = \frac{1}{\sqrt{d}} \sum_{k=0}^{d-1} \exp\left(\frac{2\pi ikm}{d}\right) |k\rangle. \tag{9}$$

In other words, when $C^{P_i}_j$ is 0 (1), L^i_j should be prepared in $|m\rangle$ $[\frac{1}{\sqrt{d}}\sum_{k=0}^{d-1}\exp(\frac{2\pi ikm}{d})|k\rangle]$ provided that $R^{P_i}_j$ is m. After that, he or she sends L^i to P_i. Upon receiving L^i, P_i asks Server to announce string C^{P_i}. Then he measures each of the qudits in L^i according to C^{P_i}. Concretely, if $C^{P_i}_j$ is 0 (1), he measures L^i_j in B_1 basis (B_2 basis). With all the measurement outcomes, P_i gets a $2N$-dit string. Then he randomly chooses some dits in this string and requires Server to announce the corresponding values in R^{P_i} for checking eavesdropping. If the error rate exceeds a predetermined threshold, they abandon the protocol; otherwise, they can utilize information reconciliation and privacy amplification [33,34] to process the remaining dits and finally share an N-dit secret key, which is denoted as $K^{s,i} = [K^{s,i}_1, K^{s,i}_2, \ldots, K^{s,i}_N]$.

(B) P_i distributes a random N-dit secret key to P_{i+1} by utilizing the same method described in step (A) for $1 \leqslant i \leqslant n$, where $P_{n+1} = P_1$, and the secret key shared between P_i and P_{i+1} is denoted as $K^{i,i+1} = [K^{i,i+1}_1, K^{i,i+1}_2, \ldots, K^{i,i+1}_N]$. Then each of the n participants calculates an N-dit string as his subsecret string. For P_i, his subsecret string is V^i, where the jth dit of V^i is $V^i_j = d - K^{s,i}_j + d - K^{i-1,i}_j + K^{i,i+1}_j = 2d - K^{s,i}_j - K^{i-1,i}_j + K^{i,i+1}_j$ for $1 \leqslant j \leqslant N$.

(C) Then each of the n participants encodes his data on his subsecret string. Take P_i as an example: He encodes the data in D_{P_i} on the corresponding dits in V^i. Concretely, he replaces $V^i_{m^i_j}$ with $V^i_{m^i_j} + 1 \pmod{d}$ for $1 \leqslant j \leqslant k_i$. After the process of encoding, the new N-dit string is denoted as $V^{i'}$. Finally, P_i announces $V^{i'} = [V^{i'}_1, V^{i'}_2, \cdots, V^{i'}_N]$ for $1 \leqslant i \leqslant n$.

(D) Upon getting the n classical strings ($V^{i'}$, $i = 1,2,\ldots,n$) announced by the participants, Server calculates T^i with the received information for $1 \leqslant i \leqslant N$, where $T^i = \sum_{j=1}^n K^{s,j}_i + \sum_{j=1}^n V^{j'}_i$. Finally, he or she announces all the calculated values. Similar to the above two QAMMR protocols, each of the n participants can anonymously get the rankings of his data according to the announced information.

Similar to the QSS-based protocol, the qudits in the QKD-based protocol also travel only once in the whole process of this protocol; hence, this protocol is congenitally immune to the Trojan-horse attack and the invisible-photon attack [28,29]. Comparing the two practical QAMMR protocols proposed in this section, we can find that they have their respective advantages and disadvantages. The main advantage of the QKD-based protocol is that it does not require entanglement. However, the qubit efficiency of the QKD-based protocol is much lower than that of the QSS-based protocol. In addition, to achieve QAMMR, the participants in the QKD-based should be equipped with one more quantum apparatus, i.e., a qudit generating machine, than the ones in the QSS-based protocol.

IV. SECURITY ANALYSIS OF THE PROPOSED PROTOCOLS

It is known that two security models, the semihonest model and the malicious model, are generally considered in SMC protocols [35]. In the semihonest model (also called honest-but-curious model), the participants are assumed to follow the protocol but at the same time record all the intermediate information they have seen during its execution. In the malicious model, the participants may actively cheat and deviate from the the protocol; e.g., dishonest participants may try to learn information about the inputs of an honest participant. Hereafter, we first analyze the security of our protocol, which is designed under the semihonest model. Then we show that the protocols, in which the participants may be dishonest, are secure. Before proving the security of our protocols, we first give two theorems, which are respectively about the states $|\widehat{\Psi}\rangle$ and $|\Psi\rangle$, as follows.

Theorem 1. An $(n+1)$-qudit state is in the form of the state $|\widehat{\Psi}\rangle$, if and only if it satisfies both the following two conditions: (1) When each of its qudits is measured in B_1 basis, the sum of the $n+1$ measurement outcomes is 0 modulo d; (2) when each of its qudits is measured in B_2 basis, the $n+1$ measurement outcomes are the same.

The proof of Theorem 1 is shown in Appendix A. Apparently, the two states, $|\Psi\rangle$ and $|\widehat{\Psi}\rangle$, can be converted between each other with the unitary operations $\mathcal{F}^{\otimes(n+1)}$. In addition, the two measuring bases, B_1 basis and B_2 basis, can be converted between each other with the unitary operations $\mathcal{F}$. Thus, we can intuitively get a theorem about $|\Psi\rangle$ as below.

Theorem 2. An $(n+1)$-qudit state is in the form of the state $|\Psi\rangle$ if and only if it satisfies both of the following two conditions: (1′) When each of its qudits is measured in B_1 basis, the $n+1$ measurement outcomes are the same; (2′) when each of its qudits is measured in B_2 basis, the sum of the $n+1$ measurement outcomes is 0 modulo d.

A. Security of the proposed protocol in the semihonest model

For the proposed protocol in the semihonest model, the security includes two aspects. First, an external eavesdropper (Eve) could not get the rankings of a participant's data or match the identity of a participant with his data. Second, a participant can get no information about the rankings of another participant's data from the intermediate information he records during the execution of the protocol.

In this protocol, only one qudit of each the entangled states (T_i, $1 \leqslant i \leqslant N$) is transmitted among the n participants, and the qudits H_i ($i = 1,2,\ldots,N$) are always held by P_1. That is, no one but P_1 can get access to both of the qudits in $|\Phi\rangle_i$ ($1 \leqslant i \leqslant N$). However, in the whole procedure of the protocol, the density matrix of the traveling subsystem T_i is

$$\rho_{T_i} = \mathrm{tr}_{H_i}(|\Phi\rangle_{ii}\langle\Phi|) = \frac{1}{d}\sum_{j=0}^{d-1}|j\rangle\langle j| = \frac{I}{d}. \tag{10}$$

Obviously, ρ_{T_i} is invariant under the operation U; hence, no one can extract any useful information from T_i. Moreover, the particles in this protocol are transmitted with the technique of decoy qudits, which are in the manner of quantum data block [26]. In each of the traveling sequences ($S^{i'}_T$, $1 \leqslant i \leqslant n$), there exist some decoy qudits, the positions of which are just known by the sender. Since both the decoy qudits and the signal qudits (the qudits of the entangled states which are used to encode data) are in the maximally mixed state $\frac{I}{d}$ for Eve, she cannot distinguish the decoy qudits from the signal qudits. As a consequence, whatever kind of attack Eve utilizes, her eavesdropping actions will inevitably disturb some of the decoy qudits and hence introduce errors into the eavesdropping check according to Theorem 2. In other words, this protocol is secure against any external eavesdropping since Eve cannot get any valuable information but be found in the eavesdropping check if she eavesdrops in the transmission of $S_T^{i'}$, $1 \leqslant i \leqslant n$.

Now we show that no one of the n participants can get the rankings of another participant's data from the intermediate information he records during the execution of the protocol. Take P_i $(2 \leqslant i \leqslant n)$ as an example, he cannot extract any useful information from the traveling qudits since each of them is in the maximal mixed state. Although P_1 can get both the two qudits of each of the N entangled states after P_n sends $S_T^{n'}$ back to him, he can only gets the value of T_i with these qudits for $1 \leqslant i \leqslant N$. However, he could get none of the useful information from T_i. For instance, if $T_i = 2$, he knows that one (or two) of the n participants has (have) data i, but he is unable to know the identity (identities) of him (them). Therefore, P_1 cannot get the rankings of another participant's data, either.

Finally, we consider two special kinds of attacking strategies for two-way quantum cryptographic protocols, i.e., Trojan-horse attack [28] and the invisible-photon attack [29]. In the two kinds of attacks, if Eve wants to extract the private input of P_i $(2 \leqslant i \leqslant n)$, she intercepts the traveling sequence $S_T^{(i-1)'}$ and inserts invisible qudits or fake qudits with a delay time. The inserted qudits cannot be detected by P_i since they do not click P_i's detector. After P_i encodes all his data on the corresponding qudits in S_T^{i-1} and sends $S_T^{i'}$ to P_{i+1}, Eve captures her fake qudits from the sequence, with which she can deduce information about P_i's private input. In fact, the participants can take the strategies in Refs. [28,29] to resist these attacks. For the sake of simplicity, we omit the description of the strategies here.

B. Security of the more practical protocols

In this part, we analyze the security of the QAMMR protocols proposed in Sec. III. According to the concrete steps of these protocols, if an attacker wants to get the rankings of a participant's data, he or she should get the specific values of the participant's private input (match the identity of this participant with his data). For clarity, we consider three possible cases. The first one is the attack from an external eavesdropper (Eve). The second case concerns a situation, in which one or more dishonest participants try to obtain the rankings of another participant's data. Finally, the attack from Server is discussed in the third case.

1. Security of the QSS-based QAMMR protocol

Outside attack. The signal qudits are transmitted only once during the whole procedure of this protocol. That is to say the transmission process in step (a) is the only chance for Eve to carry out her attacks. Therefore, if Eve wants to deduce the private input of P_i, she has to perform her actions on the qudits when they are transmitted from Server to the participants. Thus, she might be able to deduce the classical subsecret string of P_i (i.e., M^i, $1 \leqslant i \leqslant n$) and utilize it to extract the data of P_i in step (d). Apparently, if Eve can obtain M^i, she is able to get the data of P_i. For example, if $M_j^{i'} = M_j^i + s$ $(1 \leqslant j \leqslant N$, $1 \leqslant s \leqslant k_i)$, she knows that $j \in D_{P_i}$ and $|D_{P_i}^j| = s$.

Obviously, if Eve does not take active attacks, she is unable to deduce any useful information just according to the public information announced by the participants. However, no matter what kind of attack Eve utilizes, once she can get any valuable information about a participant's subsecret string, her eavesdropping actions will inevitably disturb part of the transmitted qudits, which indicates that the corresponding qudits shared by Server and the participants are no longer in $|\widehat{\Psi}\rangle$. According to Theorem 1, Eve's eavesdropping actions will unavoidably introduce errors into the eavesdropping detections in step (b), which will make the protocol aborted.

In addition, the participants will respectively encode their data on their classical subsecret strings only if they have affirmed that there is no eavesdropping in the transmission of S^i $(i = 1,2,\ldots,n)$, which indicates that the signal qudits transmitted in step (a) contains no information about the participants' private inputs. That is to say, the proposed protocol is robust against the attacks from Eve since she can get no useful information about the rankings of a participant's data but be found in the eavesdropping detections.

Participant attack. Actually, a dishonest participant has more power to attack a QAMMR scheme than an outside eavesdropper. On one hand, he can know partial information legally. On the other hand, he can cooperate with some of the other participants to cheat in the execution of the scheme. Hence, we now analyze the "participant attack", which emphasizes that the attacks from dishonest participants are generally more powerful and deserve more attention [37].

We consider the situation where l participants $(1 \leqslant l \leqslant n-1)$ cooperate to extract the private input of an honest participant. Without loss of generality, we assume that the l dishonest participants are $P_1, P_2, \ldots,$ and P_l, who want to deduce the subsecret string of an honest participant without being noticed. Since the qudits are transmitted only once in the whole protocol, it is natural that they should perform their attack during the transmission of S^i $(i = 1,2,\ldots,n)$ in step (a).

In Detection 1, Server randomly selects δ_1 states for checking eavesdropping. For each of the chosen states, the measuring basis is randomly chosen by Server from B_1 or B_2; also, the n participants are required to announce their measurement outcomes in a random order determined by Server. According to Theorem 1, once the dishonest participants cooperate to attack this scheme and acquire any useful information about an honest participant's subsecret string, they will unavoidably introduce errors into Detection 1 and make the protocol aborted. In other words, if the dishonest participants successfully pass Detection 1, they will get no useful information of an honest participant's subsecret string (see Appendix B for details). Therefore, to deduce the subsecret string of an honest participant, these dishonest participants can only utilize the qudit sequences in their own hands and the classical information announced in steps (c) and (d). However, this method is also useless. Intuitively, the subsecret strings possessed by the $n+1$ parties satisfy $M^0 + M^1 + \cdots + M^n = \bar{0}$ (mod d), which indicates that $M_j^1 + M_j^2 + \cdots + M_j^l = d - (M_j^0 + M_j^{l+1} + M_j^{l+2} + \cdots + M_j^n)$ for $1 \leqslant j \leqslant N$. Since M_j^0 is only known by Server, we can conclude that the l dishonest participants cannot get any one of the honest participants' subsecret strings. In other words, the dishonest participants are unable to extract the private input of an honest participant with their own subsecret strings.

Finally, we consider an extreme attack whereby l dishonest participants try to get the private input of an honest participant at the cost of leaking their own private inputs to each other. In this attack, each of the l participants honestly executes the protocol and privately informs the other $l-1$ cooperators of his input. After Server announces all the values of T_i for $1 \leqslant i \leqslant N$, they can deduce some information about an honest participant's private input with their private inputs and the announced information. Precisely speaking, by employing this strategy, the l participants can deduce the set that consists of the private inputs of the remaining $n-l$ honest participants.

It should be pointed out that this attack is a kind of trivial strategy that is usually not considered when designing certain kinds of SMC protocols, such as anonymous voting protocols, secure multiparty ranking protocols, and anonymous surveying (summation). In all these kinds of protocols, if $l = n-1$ (i.e., all the participants except one are dishonest), the dishonest participants can easily obtain the vote, ranking, or private data of the honest participant by utilizing this attack. Obviously, this is also the case with our protocol. However, in our protocol, when $1 \leqslant l \leqslant n-2$, the dishonest participants cannot deterministically deduce the private input of an honest participant. For simplicity, we assume that each of the n participants has only one datum. By employing the strategy in this circumstance, the l dishonest participants can only exactly extract the private input of an honest participant in the case that all the inputs of the $n-l$ honest participants are the same. Nevertheless, this case only happens with a negligible probability of $\frac{1}{N^{n-l-1}}$. That is to say, when $1 \leqslant l \leqslant n-2$, the l participants cannot exactly deduce the private input of an honest participant with a probability of $1 - \frac{1}{N^{n-l-1}}$, which will be exponentially close to 1 with the decrease of l.

Server's attack. Finally, we discuss the case where Server tries to steal the private input of a participant. In our protocol, Server is assumed to be a party who may misbehave on its own but will conspire with none of the participants.

To get a participant's private input, Server must get the subsecret string of the participant without introducing any error into the detections. It is apparent that if Server executes the protocol honestly, he can only deduce the sum of the participants' subsecret strings, i.e., $M^1 + M^2 + \cdots + M^n$ (mod d), with which he or she is unable to exactly extract the subsecret string of any participant. Therefore, the only way for him or her to get a participant's subsecret string is to send the participants fake qudits, which are not in the regulation state. For a simple example, if Server replaces $|\widehat{\Psi}\rangle$ with the $|1\rangle_0|1\rangle_1 \cdots |1\rangle_n$ and passes the detections in step (b), he or she will get all the n participants' subsecret strings with which he or she can deduce the private input of each participant in step (c).

However, in Detection 2, the participants randomly choose δ_2 samples from the shared states to test whether the states they have shared are in $|\widehat{\Psi}\rangle$. For each of the chosen states, they randomly choose one of the two conjugate bases, B_1 and B_2, for measuring its qudits and require Server to announce his measurement outcome first. According to Theorem 1, any kind of fake state prepared by Server for extracting participants' subsecret strings will introduce errors into Detection 2. In other words, if Server replaces $|\widehat{\Psi}\rangle$ with the states which can be used to extract M^i ($1 \leqslant i \leqslant n$), her or his action will inevitably be detected in Detection 2 and make the protocol aborted. Nevertheless, if he or she prepares and distributes the states as described in step (a), he or she can get no information about a participant' subsecret string. Therefore, the presented protocol is secure against the attacks from Server.

2. Security of the QKD-based QAMMR protocol

Outside attack. In this protocol, if Eve wants to get the rankings of P_i's data, she has to deduce P_i's subsecret string (i.e., V^i, $1 \leqslant i \leqslant n$). Then she can utilize V^i and $V^{i'}$ to extract the private inputs of P_i in step (C) and get the corresponding rankings. To deduce V^i, Eve should know the three classical strings, $K^{s,i}$, $K^{i,i+1}$, and $K^{i-1,i}$.

However, the distribution process for these strings can resist any kind of attack from Eve since it is equivalent to the BB84 QKD protocol [36], which has been proved to be unconditionally secure. Specifically, all the transmitted qudits in these protocol are randomly prepared in one of the states in the two conjugate bases, B_1 basis and B_2 basis. For Eve, each of the qudits is in a maximally mixed state. According to the Heisenberg uncertainty principle, it is impossible for her to discriminate these states perfectly. Consequently, no matter what kind of attack Eve utilizes, she will inevitably introduce errors and be found in the eavesdropping check, which indicates that our protocol is secure against the attacks from outside eavesdroppers.

Participant attack and Server's attack. First, we consider the circumstance in which an individual participant tries to eavesdrop the private inputs of P_i. As analyzed in the previous section, to get V^i, the dishonest participant should simultaneously get $K^{s,i}$, $K^{i,i+1}$, and $K^{i-1,i}$. However, it is an impossible task for him since he can get at most one of $K^{i,i+1}$ and $K^{i-1,i}$ only when he is P_{i-1} or P_{i+1}.

Then we consider the situation where more than one participant try to eavesdrop the private input of P_i. Obviously, the dishonest participants also cannot succeed since they are unable to get the string $K^{s,i}$ without being detected. Of course, since Server will not cooperates with any of the participants, no matter what kind of attack he or she utilizes, the case is the same with him as he or she cannot get $K^{i,i+1}$ or $K^{i-1,i}$ without being noticed.

As for the extreme attack in which the dishonest participants try to get the private input of P_i at the cost of leaking their own private inputs, the analysis is the same as that for the QSS-based protocol; hence, that is not covered again here. Until now, we have shown that this protocol is immune to the attacks from both dishonest participants and Server.

V. DISCUSSIONS

In all the proposed protocols, the private inputs of the participants are accurate to single digits. However, in some actual situations, the data of the participants may not be small, and it is unnecessary to rank the data accurately to single digits or tens since such small differences among the data are not concerned by the participants. Take the QSS-based protocol as an example: When it is utilized to rank the sales volume of a kind of product in several competing companies, we can use one state to represent a range of numbers. For instance, under the assumption that each state represents a range of 100 numbers, if the sales volume of company$_i$ is k, then company$_i$ adds 1 to the $(\lfloor\frac{k}{100}\rfloor+1)$th dit in M^i, i.e., $M^{i'}_{\lfloor\frac{k}{100}\rfloor+1} = M^i_{\lfloor\frac{k}{100}\rfloor+1} + 1$, where $1 \leqslant i \leqslant n$. In this condition, if the cap of the ranked sales volumes is 10 000, only 100 GHZ states ($N = 100$) would be enough to accomplish the task of ranking.

The next thing that we want to account for is the security levels of our two more practical QAMMR protocols. In each of the two protocols, Server is supposed to cooperate with none of the n participants since the protocol will be equivalent to a two-party one, which could not be secure [30,31], if Server cooperates with $n-1$ of the participants. Under this assumption, both of the protocols have been proved to be secure in the previous section.

However, under the assumption that Server is permitted to collaborate with part of the participants, the security level of the QSS-based protocol becomes different with that of the QKD-based one. Concretely, it is not hard to find that when the number of the dishonest participants who cooperate with Server is less than $n-1$, they could not obtain the subsecret string of any honest participant in the QSS-based protocol. Nevertheless, the situation is quite different with the QKD-based one. Obviously, if Server collaborates with P_{i-1} and P_{i+1}, they can easily get the subsecret string of P_i, where $1 \leqslant i \leqslant n$ and $P_{n+1} = P_0$. This situation happens because each participant in the QKD-based protocol only shares secret keys with Server and the two participants next to him, respectively. If every participant involved in the QKD-based protocol respectively shares a secret key with Sever and each of the other $n-1$ participants, the security level of this protocol will be the same as that of the QSS-based one. In other words, if every two of the $n+1$ parties involved in the QKD-based protocol share a secret key between each other, Server and the dishonest participants could not deduce the subsecret string of any honest participant if the number of the dishonest participants is less than $n-1$.

In addition, in our semihonest QAMMR protocol and QSS-based QAMMR protocol, which are presented with entangled states, if the qudits of the entangled states travel in a noisy channel, it seems that the entanglement may be threatened over a long distance. Under this circumstance, the quantum-repeater technique [38,39], containing the entanglement purification and teleportation, can be used to keep the reliably shared entanglement.

VI. CONCLUSIONS

In summary, this paper represents an attempt to address the issue of anonymous multiparty ranking in quantum domain. It proposes three secure protocols to achieve QAMMR. By utilizing these protocols, each of the participants can correctly and anonymously get the rankings of his data. That is to say, except the participant himself, no one can get the rankings of his data. Similar to most of the previous classical SMC protocols, the first of our protocols is proposed in the semihonest model. Then we present two more practical QAMMR protocols, in which the participants need not be semihonest, based on the basic idea of MQSS and the technique of QKD, respectively.

There are several merits of our protocols. First, the proposed protocols are of realistic significance since anonymous ranking can be employed to solve many practical problems, such as anonymously ranking the students' exam scores, anonymously ranking the wages of the employees in different companies, and anonymously ranking the sales volume of a kind of product in different companies. Second, compared with almost all the existing secure multiparty ranking protocols that are based on the assumptions of computational complexity, our protocols are more secure since they are secure against the adversary with quantum computation ability. Third, both of the practical QAMMR protocols are congenitally free from the Trojan-horse attack and the invisible-photon attack since the quantum states need transmitting only once in each of the two protocols. In addition, not all the parties involved in the QSS-based protocol are required to have full quantum power. In fact, to achieve the anonymous ranking with the help of the Server by this protocol, the n participants need not have the ability to generate quantum states or perform unitary operations, only the abilities to perform single-qudit measurements and store qudits are enough. That is to say, this protocol may be easier to be widely applied over the quantum network in the future because of its convenience and low expense for the users. Moreover, different from the QSS-based protocol, the QKD-based protocol can achieve the purpose of QAMMR without the aid of quantum entanglement, which indicates that it may have an advantage in implementation.

To execute the QSS-based protocol, Server should be equipped with the devices for preparing the d-level $(n+1)$-particle GHZ state, which can be remotely prepared by using only one d-level two-particle entangled state and n d-level CNOT operations [40]. Meanwhile, he or she should also be equipped with the devices for performing quantum Fourier transform. The participants involved in this protocol should be equipped with the devices for single-qudit measurements, i.e., measuring the received qudits in B_1 basis or B_2 basis. Besides, Sever and all the participants should also have the quantum memory apparatus for storing qudits [41]. To execute the QKD-based protocol, Server and the participants should be capable of generating the d-level single particle. For example, they could utilize the method in Ref. [42] to prepare spatial qudits with a single phase-only spatial light modulator. Meanwhile, Server and the participants need also be equipped with the devices for measuring and storing single qudits [41]. In addition, since both the QSS-based protocol and the QKD-based protocol employ the technique of "block transmission" [26], in order to transmit the ordered qudit block to the receiver, the sender could employ the similar circuits composed of optical delays and switches in Refs. [27,43] to adjust the qudits in the transmitted sequence.

In each of the three proposed protocols, with the information of T_i $(i = 1,2,\ldots,N)$ which is announced by Server, every participant not only gets the rankings of his data anonymously, but also gets the values of the ranked data and hence obtains the distribution of the all the n participants' data. Actually, this feature that each participant will get the distribution of all the ranked data while ranking his data can also be viewed as an advantage of our protocols in many real-life cases. For example, when ranking the scores (wages) of the students (employees) in different schools (companies), each of the schools (companies) may also want to know the distribution of all the ranked data since it may be useful for their work. In such circumstances, the distribution of the ranked data need not be considered as a secret and hence everyone can obtain it. However, in some other cases, this distribution may become one of the private attributes which should be obtained by none of the participants. Therefore, how to design quantum SMMR protocols in which each of the participants can only get the rankings of his own data, especially the ones in the malicious model, still remains an open problem.

ACKNOWLEDGMENTS

This work is supported by NSFC (Grants No. 61272057, No. 61170270, No. 61100203, No. 61003286, No. 61121061), NCET (Grant No. NCET-10-0260), SRFDP (Grant No. 2009000 5110010), CPSF (Grant No. 2013M530561), Beijing Natural Science Foundation (Grants No. 4112040 and No. 4122054), the Fundamental Research Funds for the Central Universities (Grant No. 2011YB01), BUPT Excellent Ph.D. Students Foundation (Grant No. CX201334), and Beijing Higher Education Young Elite Teacher Project (Grants No. YETP0475 and No. YETP0477).

APPENDIX A: PROOF OF THEOREM 1

According to Eq. (8), it is easy to verify that $|\widehat{\Psi}\rangle$ can satisfy both the two conditions in Theorem 1. Now we prove that if an $(n+1)$-qudit state satisfies both the two conditions, it must be $|\widehat{\Psi}\rangle$.

Let us suppose that $|\Theta\rangle$ is an $(n+1)$-qudit state that can satisfy both condition (1) and condition (2). On one hand, as $|\Theta\rangle$ satisfies condition (1), it should be in the subspace spanned by

$$M = \left\{ |k_0 k_1 \cdots k_n\rangle \Big| \sum_{i=0}^{n} k_i \xlongequal{mod\ d} 0,\ k_i \in N,\ k_i < d \right\}. \tag{A1}$$

It is easy to find that the number of the states contained in M is d^n. Without loss of generality, we denoted the d^n states as $|K_1\rangle, |K_2\rangle, \ldots, |K_{d^n}\rangle$, respectively. In other words, if $|\Theta\rangle$ satisfies condition (1), we have

$$|\Theta\rangle = \sum_{i=1}^{d^n} \lambda_i |K_i\rangle, \tag{A2}$$

where $\sum_{i=1}^{d^n} |\lambda_i|^2{=}1$. On the other hand, since $|\Theta\rangle$ satisfies condition (2), it should be in the subspace spanned by

$$N = \{K'_j | K'_j = \mathcal{F}^{\otimes(n+1)} |j\rangle_0 |j\rangle_1 \cdots |j\rangle_n\}_{j=0}^{d-1}, \tag{A3}$$

where the subscripts $0,1,\ldots,$ and n represent $n+1$ different qudits in $|\Theta\rangle$. In other words, if $|\Theta\rangle$ satisfies condition (2), we have

$$|\Theta\rangle = \sum_{j=0}^{d-1} \lambda'_j K'_j, \tag{A4}$$

where $\sum_{j=0}^{d-1} |\lambda'_j|^2 = 1$. Obviously,

$$\begin{aligned}
|\Theta\rangle &= \sum_{j=0}^{d-1} \lambda'_j K'_j = \sum_{j=0}^{d-1} \lambda'_j \mathcal{F}^{\otimes(n+1)} |j\rangle_0 |j\rangle_1 \cdots |j\rangle_n \\
&= \sum_{j=0}^{d-1} \lambda'_j \left\{ \left[\frac{1}{\sqrt{d}} \sum_{k_0=0}^{d-1} \exp\left(\frac{2\pi i j k_0}{d}\right) |k_0\rangle \right] \otimes \cdots \otimes \left[\frac{1}{\sqrt{d}} \sum_{k_n=0}^{d-1} \exp\left(\frac{2\pi i j k_n}{d}\right) |k_n\rangle \right] \right\} \\
&= d^{-\frac{n+1}{2}} \sum_{j=0}^{d-1} \lambda'_j \sum_{k_0,\ldots,k_n} \exp\left[\frac{2\pi i j}{d}(k_0 + \cdots + k_n)\right] |k_0\rangle \otimes \cdots \otimes |k_n\rangle \\
&= d^{-\frac{n+1}{2}} \sum_{j=0}^{d-1} \lambda'_j \left\{ \sum_{\sum_{i=0}^{n} k_i = 0 (mod\ d)} \exp\left[\frac{2\pi i j}{d}(k_0 + \cdots + k_n)\right] |k_0\rangle \cdots |k_n\rangle \right. \\
&\quad \left. + \sum_{\sum_{i=0}^{n} k'_i \neq 0 (mod\ d)} \exp\left[\frac{2\pi i j}{d}(k'_0 + \cdots + k'_n)\right] |k'_0\rangle \cdots |k'_n\rangle \right\}.
\end{aligned} \tag{A5}$$

According to Eqs. (A2) and (A5), we have

$$\sum_{j=0}^{d-1} \lambda'_j \sum_{\sum_{i=0}^{n} k'_i \neq 0 (mod\ d)} \exp\left[\frac{2\pi i j}{d}(k'_0 + \cdots + k'_n)\right] |k'_0\rangle \cdots |k'_n\rangle = 0, \tag{A6}$$

which indicates that

$$|\Theta\rangle = \sum_{i=1}^{d^n} \lambda_i |K_i\rangle = d^{-\frac{n-1}{2}} \sum_{j=0}^{d-1} \lambda'_j \sum_{i=1}^{d^n} |K_i\rangle. \quad \text{(A7)}$$

Hence, we can derive from Eq. (A7) that

$$\lambda_1 = \lambda_2 = \cdots = \lambda_{d^n} = d^{-\frac{n-1}{2}} \sum_{j=0}^{d-1} \lambda'_j. \quad \text{(A8)}$$

In addition, since $\sum_{i=1}^{d^n} |\lambda_i|^2 = \sum_{j=0}^{d-1} |\lambda'_j|^2 = 1$, we can get that

$$\sum_{j=0}^{d-1} \lambda'_j = d^{-\frac{1}{2}}, \quad \lambda_1 = \lambda_2 = \cdots = \lambda_{d^n} = d^{-\frac{n}{2}}, \quad \text{(A9)}$$

which indicates that

$$|\Theta\rangle = d^{-\frac{n}{2}} \sum_{\sum_{i=0}^{n} k_i = 0 (mod\ d)} |k_0\rangle \cdots |k_n\rangle = |\widehat{\Psi}\rangle. \quad \text{(A10)}$$

So far, we have showed that if an $(n+1)$-qudit state satisfies both condition (1) and condition (2), it must be $|\widehat{\Psi}\rangle$. That is to say, we have proved Theorem 1.

APPENDIX B: IF THE DISHONEST PARTICIPANTS SUCCESSFULLY PASS DETECTION 1, THEY WILL GET NO USEFUL INFORMATION OF AN HONEST PARTICIPANT'S SUBSECRET STRING

Before demonstrating this point, we first introduce an equivalent version of steps (a) and (b).

According to Theorem 2 and the relationship between $|\Psi\rangle$ and $|\widehat{\Psi}\rangle$, the first two steps of the QSS-based protocol, step (a) and step (b), are completely equivalent to the following version.

(a$'$) Instead of transforming $|\Psi\rangle^i$ into $|\widehat{\Psi}\rangle^i$ with Fourier transform and then sharing $|\widehat{\Psi}\rangle^i$ with the n participants, Server directly share $|\Psi\rangle^i$ with the n participants utilizing the same method as that used for sharing $|\widehat{\Psi}\rangle^i$ in step (a) for $1 \leqslant i \leqslant N + \delta_1 + \delta_2$.

(b$'$) After all the participants receives their qudit sequences sent from Server, respectively, they begin to check eavesdropping by testing whether their shared states are in $|\Psi\rangle$. The detecting process, which also contains two detections (denoted as Detection 1$'$ and Detection 2$'$), is essentially the same as those in step (b). The only difference is that the $n+1$ parties should check whether the states they have shared are in $|\Psi\rangle$ according to Theorem 2 instead of checking whether the states they have shared are in $|\widehat{\Psi}\rangle$ according to Theorem 1. That is, if there is no eavesdropping, the $n+1$ measurement outcomes should be the same (the sum of the $n+1$ measurement outcomes should be 0 modulo d) provided that B_1 basis (B_2 basis) is utilized in both of the detections. Once they confirm that there is no eavesdropping during the transmission in step (a$'$), each of the $n+1$ parties performs $\mathcal{F}$ on every qudit in his or her possession. After that, the $n+1$ parties have securely shared a sequence of N states which are all in $|\widehat{\Psi}\rangle$.

The purpose of both steps (a) and (b) and steps (a$'$) and (b$'$) is to securely share a sequence of N states, which are all in $|\widehat{\Psi}\rangle$, among the $n+1$ parties. The vital difference between them is that only Server should be equipped with the devices for performing quantum Fourier transform in steps (a) and (b), while all the $n+1$ parties should be equipped with such devices in steps (a$'$) and (b$'$). In order to reduce the implementation cost for the participants in our protocol, we make use of steps (a) and (b) to share $|\widehat{\Psi}\rangle$ among the $n+1$ parties. Even so, the security of steps (a) and (b) is equivalent to that of steps (a$'$) and (b$'$). Hence, we now prove that, under the premise of introducing no errors into Detection 1$'$ and Detection 2$'$, the l dishonest participants cannot get any useful information about the subsecret string of an honest participant in steps (a$'$) and (b$'$) as follows.

In step (a$'$), Server prepares an ordered sequence of $N + \delta_1 + \delta_2$ GHZ states $[|\Psi\rangle^1, |\Psi\rangle^2, \ldots, |\Psi\rangle^{N+\delta_1+\delta_2}]$, where

$$\begin{aligned} |\Psi\rangle^i_{01\ldots n} &= \frac{1}{\sqrt{d}} \sum_{j=0}^{d-1} |j\rangle^i_0 |j\rangle^i_1 \cdots |j\rangle^i_n \\ &= \frac{1}{\sqrt{d}} \sum_{j=0}^{d-1} |j\rangle^i_0 |j\rangle^i_{l+1} \cdots |j\rangle^i_n |j\rangle^i_1 \cdots |j\rangle^i_l. \quad \text{(B1)} \end{aligned}$$

In the distribution of these states, the l dishonest participants may attack each of the states and then try to extract information about the subsecret string of an honest participant with the qudits transmitted to them and some other auxiliary qudits prepared by themselves. Take $|\Psi\rangle^i$ as an example. The dishonest participants first prepare s ancilla qudits in $|0\rangle_E^{\otimes s}$, where s is a parameter determined according to their attacking strategy. Initially, the state $|\Psi\rangle^i$ and the ancilla qudits compose a composite system as

$$|\Psi^1\rangle^i = \frac{1}{\sqrt{d}} \sum_{j=0}^{d-1} |j\rangle^i_0 |j\rangle^i_{l+1} \cdots |j\rangle^i_n |j\rangle^i_1 \cdots |j\rangle^i_l |0\rangle_E^{\otimes s}. \quad \text{(B2)}$$

When the jth qudit of $|\Psi\rangle^i$ (i.e., $|\Psi\rangle^i_j$) is transmitted from Server to the P_j in step (a$'$) for $1 \leqslant j \leqslant n$, the dishonest participants can cooperate to perform their desirable unitary operation U_E on the n transmitted qudits and the s ancilla qudits. After the operation, the state of the composite system will be converted from $|\Psi^1\rangle^i$ into

$$|\Psi^2\rangle^i = I \otimes U_E |\Psi^1\rangle^i. \quad \text{(B3)}$$

Although the dishonest participants can choose any unitary operation as U_E in their favor, they do not want to introduce any error into Detection 1$'$. In this detection, Server randomly chooses B_1 or B_2 and requires the n participants to measure the corresponding qudits in their hands with the chosen basis. To avoid introducing any error under the condition that B_1 basis is chosen, the measurement outcomes of the honest participants and Server should be the same, which indicates that $|\Psi^2\rangle^i$ should be in the form of

$$|\Psi^2\rangle^i = \frac{1}{\sqrt{d}} \sum_{j=0}^{d-1} |j\rangle^i_0 |j\rangle^i_{l+1} \cdots |j\rangle^i_n |\Upsilon(j)\rangle, \quad \text{(B4)}$$

where $|\Upsilon(j)\rangle$ represents the $l+s$ qudits controlled by the dishonest participants after being performed U_E. As their eavesdropping actions are not detected in Detection 1$'$ (here we suppose that they also pass Detection 2$'$), the honest participants and Server will perform $\mathcal{F}$ on each of the qudits in their hands following step (b′). After these operations, the state of $|\Psi^2\rangle^i$ will be transformed into

$$\begin{aligned}|\Psi^3\rangle^i &= \frac{1}{\sqrt{d}}\sum_{j=0}^{d-1}\left\{\left[\frac{1}{\sqrt{d}}\sum_{k_0=0}^{d-1}\exp\left(\frac{2\pi ijk_0}{d}\right)|k_0\rangle\right]\otimes\cdots\otimes\left[\frac{1}{\sqrt{d}}\sum_{k_{l+1}=0}^{d-1}\exp\left(\frac{2\pi ijk_{l+1}}{d}\right)|k_{l+1}\rangle\right]\otimes\cdots\right.\\ &\quad\left.\otimes\left[\frac{1}{\sqrt{d}}\sum_{k_n=0}^{d-1}\exp\left(\frac{2\pi ijk_n}{d}\right)|k_n\rangle\right]\otimes|\Upsilon(j)\rangle\right\}\\ &= d^{-\frac{n-l+2}{2}}\sum_{j=0}^{d-1}\sum_{k_0,k_{l+1},\ldots,k_n}\exp\left[\frac{2\pi ij}{d}(k_0+k_{l+1}+\cdots+k_n)\right]|k_0\rangle|k_{l+1}\rangle\cdots|k_n\rangle\otimes|\Upsilon(j)\rangle\\ &= d^{-\frac{n-l+2}{2}}\sum_{k_0,k_{l+1},\ldots,k_n}|k_0\rangle|k_{l+1}\rangle\cdots|k_n\rangle\sum_{j=0}^{d-1}|\Upsilon(j)\rangle\exp\left[\frac{2\pi ij}{d}(k_0+k_{l+1}+\cdots+k_n)\right]. \qquad \text{(B5)}\end{aligned}$$

In step (c), Server and each of the honest participants will measure the qudit in his or her hand with B_1 basis and record the measurement outcome as one dit of his or her subsecret string. According to Eq. (B5), we can conclude that if the dishonest participants do not introduce any error in Detection (1′) and Detection (2′), they can at most get the value of $k_0+\sum_{i=l+1}^{n}k_i$, no matter what kind of strategy they utilize. Since Server will conspire with none of the participants, $\sum_{i=l+1}^{n}k_i$ is random for the dishonest participants, which indicates that they can deduce no useful information about the subsecret string of an honest participant.

Thus far, we have proved that the dishonest participants cannot get the subsecret string of an honest participant without being detected if they eavesdrop in step (a).

[1] A. C. Yao, in *Proceedings of the 23rd Annual IEEE Symposium on Foundations of Computer Science* (IEEE, Chicago, 1982), p. 160.

[2] B. Chor, O. Goldreich, E. Kushilevitz, and M. Sudan, J. ACM. **45**, 965 (1998); C. Cachin, S. Micali, and M. Stadler, in *Advances in Cryptology-EUROCRYPT99* (Springer-Verlag, Berlin, 1999); C. Gentry and Z. Ramzan, in *Proc. 32nd ICALP* (Springer-Verlag, Berlin, 2005), pp. 803–815; S. Yekhanin, Technical Report ECCC TR06-127, 2006.

[3] J. C. Benaloh and D. Tuinstra, in *Proceedings of the 26th ACM Symposium on the Theory of Computing (STOC)*, edited by F. T. Leighton (ACM Press, New York, 1994), p. 544.

[4] A. Shamir, Commun. ACM **22**, 612 (1979).

[5] P. W. Shor, in *Proceedings of 35th Annual IEEE Symposium on Foundations of Computer Science* (IEEE, Los Alamitos, 1994), pp. 124–134.

[6] L. K. Grover, in *Proceedings of 28th Annual ACM Symposium on the Theory of Computing* (ACM Press, Philadelphia, 1996), pp. 212–219.

[7] L. Xiao, G. L. Long, F. G. Deng, and J. W. Pan, Phys. Rev. A **69**, 052307 (2004).

[8] F. G. Deng, H. Y. Zhou, and G. L. Long, Phys. Lett. A **337**, 329 (2005).

[9] Z. J. Zhang, Y. Li, and Z. X. Man, Phys. Rev. A **71**, 044301 (2005).

[10] V. Giovannetti, S. Lloyd, and L. Maccone, Phys. Rev. Lett. **100**, 230502 (2008).

[11] M. Jakobi, C. Simon, N. Gisin, J. D. Bancal, C. Branciard, N. Walenta, and H. Zbinden, Phys. Rev. A **83**, 022301 (2011).

[12] L. Olejnik, Phys. Rev. A **84**, 022313 (2011).

[13] F. Gao, B. Liu, Q. Y. Wen, and H. Chen, Opt. Express **20**, 17411 (2012).

[14] J. A. Vaccaro, J. Spring, and A. Chefles, Phys. Rev. A **75**, 012333 (2007).

[15] M. Bonanome, V. Bužek, M. Hillery, and M. Ziman, Phys. Rev. A **84**, 022331 (2011).

[16] L. Jiang, G. Q. He, D. Nie, J. Xiong, and G. H. Zeng, Phys. Rev. A **85**, 042309 (2012).

[17] Y. Li and G. H. Zeng, Opt. Rev. **15**, 219 (2008).

[18] H. Y. Jia, Q. Y. Wen, T. T. Song, and F. Gao, Opt. Commun. **284**, 545 (2011).

[19] Y. G. Yang and Q. Y. Wen, J. Phys. A **42**, 055305 (2009).

[20] S. Lin, Y. Sun, X. F. Liu, and Z. Q. Yao, Quantum Inf. Process. **12**, 559 (2013).

[21] W. Liu, Y. B. Liu, and Z. T. Jiang, Opt. Commun. **284**, 3160 (2011).

[22] H. Y. Tseng, J. Lin, and T. Hwang, Quantum Inf. Process. **11**, 373 (2012).

[23] W. Liu, S. S. Luo, Y. B. Wang, and Z. T. Jiang, in *Proceedings of the 4th International Joint Conference on Computational Sciences and Optimization* (CSO, Yunnan, 2011), pp. 272–275.

[24] K. V. Jónsson, G. Kreitz, and M. Uddin, in *Proceedings of the 9th International Conference on Applied Cryptography and Network Security* (ACNS, Malaga, 2011).

[25] W. Liu, S. S. Luo, and P. Chen, in *Proceedings of the 8th ACIS International Conference on Software Engineering, Artificial Intelligence, Networking, and Parallel/Distributed Computing* (SNPD, Qingdao, 2007), pp. 727–732.

[26] G. L. Long and X. S. Liu, Phys. Rev. A **65**, 032302 (2002).

[27] F. G. Deng, G. L. Long, and X. S. Liu, Phys. Rev. A **68**, 042317 (2003).

[28] X. H. Li, F. G. Deng, and H. Y. Zhou, Phys. Rev. A **74**, 054302 (2006).

[29] Q. Y. Cai, Phys. Lett. A **351**, 23 (2006).

[30] H. K. Luo, Phys. Rev. A **56**, 1154 (1997).

[31] H. Buhrman, M. Christandl, and C. Schaffner, Phys. Rev. Lett. **109**, 160501 (2012).

[32] S. Dolev, I. Pitowsky, and B. Tamir, arXiv:quant-ph/0602087v2.

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

[34] D. Deutsch, A. Ekert, R. Jozsa, C. Macchiavello, S. Popescu, and A. Sanpera, Phys. Rev. Lett. **77**, 2818 (1996).

[35] G. Brassard, A. Broadbent, J. Fitzsimons, S. Gambs, and A. Tapp, in *Proceedings of Asiacrypt 2007* (Springer, Berlin, 2007), pp. 460–473.

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

[37] F. Gao, S. J. Qin, and Q. Y. Wen, Quantum Inf. Comput. **7**, 329 (2007).

[38] Z. B. Chen, B. Zhao, Y. A. Chen, J. Schmiedmayer, and J. W. Pan, Phys. Rev. A **76**, 022329 (2007).

[39] Y. B. Sheng, L. Zhou, and G. L. Long, Phys. Rev. A **88**, 022302 (2013).

[40] Y. Xia, J. Song, and H. S. Song, J. Mod. Opt. **55**, 1723 (2008).

[41] D.-S. Ding, Z.-Y. Zhou, B.-S. Shi, and G.-C. Guo, Nat. Commun. **4**, 2527 (2013).

[42] M. A. Solís-Prosser, A. Arias, J. J. M. Varga, L. Rebón, S. Ledesma, C. Iemmi, and L. Neves, Opt. Lett. **38**, 4762 (2013).

[43] F. G. Deng and G. L. Long, Phys. Rev. A **69**, 052319 (2004).