Quantum-secret-sharing scheme based on local distinguishability of orthogonal multiqudit entangled states

Jingtao Wang,[1] Lixiang Li,[1,*] Haipeng Peng,[1] and Yixian Yang[1,2]
[1]*Information Security Center, State Key Laboratory of Networking and Switching Technology, Beijing University of Posts and Telecommunications, Beijing 100876, China*
[2]*State Key Laboratory of Public Big Data, Guizhou 550025, China*
(Received 2 January 2017; published 13 February 2017)

In this study, we propose the concept of judgment space to investigate the quantum-secret-sharing scheme based on local distinguishability (called LOCC-QSS). Because of the proposing of this conception, the property of orthogonal mutiqudit entangled states under restricted local operation and classical communication (LOCC) can be described more clearly. According to these properties, we reveal that, in the previous (k,n)-threshold LOCC-QSS scheme, there are two required conditions for the selected quantum states to resist the unambiguous attack: (i) their k-level judgment spaces are orthogonal, and (ii) their $(k-1)$-level judgment spaces are equal. Practically, if $k < n$ (this is almost always true in the LOCC-QSS scheme), it is very difficult to satisfy the two conditions simultaneously. In the current study, we further establish a simple encoding method, which can concurrently ease the selection of quantum states and ensure the scheme's security, i.e., even if the $(k-1)$-level judgment spaces of the selected quantum states are not equal, these states can still be used for defeating the unambiguous attack. With this encoding method, we propose a more secure (k,n)-threshold LOCC-QSS scheme, and give two specific examples for illustration.

DOI: 10.1103/PhysRevA.95.022320

I. INTRODUCTION

Classical secret sharing (CSS) is an important branch of cryptography, which was invented independently by Shamir [1] and Blakely [2] in 1979. The (k,n)-threshold CSS can be described as follows: a secret is divided into n shares in such a way that any k or more sharers can reconstruct the secret while any $k-1$ or fewer ones cannot. It has been known that the security of most classical cryptosystems is based on the assumptions of computational complexity, which might be broken by the strong power of advanced algorithms such as quantum computation [3,4]. In addition, another main drawback of CSS schemes is that they are not perfectly secure from eavesdropper attack. Fortunately, all of these problems can be solved by the quantum cryptography [5]. In 1999, Hillery *et al.* [6] and Cleve *et al.* [7] simultaneously proposed the concept of quantum secret sharing (QSS), that is a secret sharing with quantum means. Subsequently, a number of QSS schemes were proposed in theoretical [8–14] and experimental [15–21] ways. In these QSS schemes, not only the classical secret can be shared but also the quantum secret.

The security requirements of the QSS scheme and the CSS scheme are the same. The difference between them is that the QSS scheme shares the (classical or quantum) secret via quantum states and can share quantum states directly. Although the QSS schemes have some advantages in defeating the eavesdropper attack, there are still some limitations in one way or another [8–11]. For example, the dealer needs to be involved in the step of revealing the secret, or the participants require the joint quantum measurement to reveal the secret. In order to deal with these restrictions, Rahaman *et al.* [22] demonstrated a simple and very efficient model for (k,n)-threshold quantum secret sharing based on only local quantum operations and classical communication (called an LOCC-QSS scheme). The main idea of LOCC-QSS scheme is that the dealer encodes his or her (classical) secret into several pairs of locally distinguishable orthogonal multipartite entangled states and distributes the particles according to the context, in such a way that only a sufficient number of cooperating parties can distinguish these pairs of orthogonal entangled states under LO and reconstruct the secret. In addition, the eigenvalue equations are adopted in this scheme for eavesdropping detection, in such a way that the external attack can be resisted perfectly.

According to the local distinguishability of GHZ sates and Dicke states, $(2,n)$-threshold and (k,n)-threshold LOCC-QSS $(k < n)$ were proposed in Ref. [22]. However, in the $(2,n)$-threshold LOCC-QSS, the two cooperating participants must come from different groups. In order to remove this restriction, Yang *et al.* [23] proposed a standard $(2,n)$-threshold LOCC-QSS scheme with a specified pair of orthogonal n-qudit entangled states. Moreover, they found that Rahaman *et al.*'s (k,n)-threshold LOCC-QSS schemes are ramp (or imperfect) schemes, i.e., there are some groups of cooperating participants less than k that can obtain partial information about the secret. In addition, for quantifying the information leakages, Yang *et al.* proposed two kinds of conspiracy attacks [23]: (i) No matter whether eavesdroppers obtain the shared secret or not, it is not allowed that they obtain a wrong shared secret and disturb the authorized groups to recover the shared secret. (ii) In order to obtain information about the shared secret as much as possible, it is allowed that eavesdroppers minimize the errors that occur in a state discrimination task and can disturb the authorized groups to recover the shared secret. The two eavesdropping probabilities of success are called unambiguous probability and guessing probability, respectively. From the definition of the two probabilities, in a perfect (k,n)-threshold LOCC-QSS scheme, the unambiguous probability is zero and the guessing probability is 1/2 for $k-1$ cooperating parties,

*li_lixiang2006@163.com

while both of them are 1 for the case of k cooperating parties. For convenience, we call the two kinds of conspiracy attacks unambiguous attack and guessing attack.

In the LOCC-QSS schemes, the emphasis is on the chosen of the pair of orthogonal entangled states, which will affect the efficiency and security of the schemes. For example, Yang *et al.* introduced a pair of generalized Bell states in a d-qudit system and designed a standard $(2,n)$-threshold LOCC-QSS scheme, which can resist the unambiguous attack and guessing attack. Therefore, a further study of the local distinguishability of a pair (or a set) of orthogonal multiqudit entangled states is necessary for designing more secure LOCC-QSS schemes. In addition, the two conspiracy attacks have different influence on the security of the scheme. The unambiguous attack is very terrible, because in this case those unauthorized parties can obtain partial correct information directly without being spotted. The guessing attack is inevitable, but it can be acceptable or can be reduced to a safe range by taking some measures. For example, there exists guessing probability in BB84 protocol [5], but the error correction and privacy amplification can be used to ensure the security. Thus, we focus on how to reduce the information leakages caused by unambiguous probability in this work.

In the current study we introduce the definition of judgment space for describing the local distinguishability of a pair of orthogonal entangled states in high-qudit systems. According to its properties, the conditions, which the quantum states should be satisfied for resisting the unambiguous attack, can be proposed. Especially, if there are three or more quantum states for local discrimination, the unambiguous attack would be divided into two cases. In order to resist these attacks, we present a very simple and efficient encoding method. Moreover, the construction of (k,n)-threshold LOCC-QSS schme based on local distinguishability of three orthogonal multiqudit entangled states is proposed, which can resist the unambiguous attack perfectly.

The rest of this paper is organized as follows. In Sec. II, we give the properties of the local distinguishability of orthogonal multiqudit entangled sates and propose an encoding method for resisting the unambiguous attack in Sec. III. The scheme of (k,n)-threshold LOCC-QSS and two examples are presented in Sec. IV, and Sec. V is our conclusion.

II. LOCAL DISTINGUISHABILITY OF MULTIQUDIT ENTANGLED STATES

The problem of local discrimination can be described as follows: a number of parties share a multipartite quantum state, which is chosen from a known set of orthogonal quantum states. Their goal is to determine which one is shared using LOCC. In this paper, the discussion of local distinguishability is under restricted local operations and classical communication (rLOCC) [24]. Here, rLOCC means that only a subset of the parties is allowed to communicate with each other. Now, we consider the local distinguishability of a pair of orthogonal multiqudit states.

Let $\{|0\rangle,|1\rangle,\ldots,|d-1\rangle\}$ be a standard orthonormal basis of a d-dimensional Hilbert space H. A multipartite qudit system can be denoted as $H^{\otimes n}$. Let $H^{\otimes k}$ and $H^{\otimes(n-k)}$ be two joint subspaces of $H^{\otimes n}$, and $\{|e_i^{(k)}\rangle\}$ and $\{|e_j^{(n-k)}\rangle\}$ are their standard orthonormal basis respectively. Suppose that $|\varphi_1\rangle$ and $|\varphi_2\rangle$ are a pair of n-qudit orthogonal entangled states, for a proper choice of basis, which can be written as

$$|\varphi_1\rangle = \sum_{i,j} a_{ij}|e_i^{(k)}\rangle|e_j^{(n-k)}\rangle,$$
$$|\varphi_2\rangle = \sum_{i,j} a'_{ij}|e_i^{(k)}\rangle|e_j^{(n-k)}\rangle, \quad (1)$$

where $\sum_{i,j}|a_{ij}|^2 = 1 = \sum_{i,j}|a'_{ij}|^2$, and $a_{ij}\cdot a'_{ij} = 0, \forall i,j$. Let us define two subspaces of the Hilbert space $H^{\otimes k}$, $S_1^{(k)} = \{|e_i^{(k)}\rangle, \text{if}\,\exists\, j, s.t. a_i j \neq 0\}$ and $S_2^{(k)} = \{|e_i^{(k)}\rangle, \text{if}\,\exists\, j, s.t.\, a'_i j \neq 0\}$, which are called the k-level judgment space of $|\varphi_1\rangle$ and $|\varphi_2\rangle$, respectively. Similarly, we can rewrite the $|\varphi_1\rangle$ and $|\varphi_2\rangle$ as the form of $(k-1,n-k+1)$-bipartite states, and define the corresponding $(k-1)$-level judgment space $S_1^{(k-1)}$ and $S_2^{(k-1)}$. Consequently, we have a Lemma as follows.

Lemma 1. Let $|\varphi_1\rangle$ and $|\varphi_2\rangle$ be a pair of orthogonal n-qudit symmetric entangled states, their judgment spaces have the following properties:

(i) if $S_1^{(k)} \perp S_2^{(k)}$, then $S_1^{(k+1)} \perp S_2^{(k+1)}$;
(ii) if $S_1^{(k)} = S_2^{(k)}$, then $S_1^{(k-1)} = S_2^{(k-1)}$;
(iii) if $S_1^{(k)} \subset S_2^{(k)}$, then $S_1^{(k-1)} \subseteq S_2^{(k-1)}$.

Proof. (i) For any $|e_{i_1}^{(k+1)}\rangle \in S_1^{(k+1)}$ and $|e_{i_2}^{(k+1)}\rangle \in S_2^{(k+1)}$, we have $|e_{i_1}^{(k+1)}\rangle = |e_{i_1}^{(k)}\rangle \otimes |l\rangle, |e_{i_2}^{(k+1)}\rangle = |e_{i_2}^{(k)}\rangle \otimes |m\rangle$, where $|e_{i_1}^{(k)}\rangle \in S_1^{(k)}, |e_{i_2}^{(k)}\rangle \in S_2^{(k)}$ and $|l\rangle,|m\rangle \in \{|0\rangle,|1\rangle,\cdots,|d-1\rangle\}$. Because $S_1^{(k)} \perp S_2^{(k)}$, we have $\langle e_{i_1}^{(k)}|e_{i_2}^{(k)}\rangle = 0$, for any $|e_{i_1}^{(k)}\rangle \in S_1^{(k)}$ and $|e_{i_2}^{(k)}\rangle \in S_2^{(k)}$. Therefore, $\langle e_{i_1}^{(k+1)}|e_{i_2}^{(k+1)}\rangle = \langle l| \otimes \langle e_{i_1}^{(k)}|e_{i_2}^{(k)}\rangle \otimes |m\rangle = 0$. Because of the arbitrary of $|e_{i_1}^{(k+1)}\rangle$ and $|e_{i_2}^{(k+1)}\rangle$, we have $S_1^{(k+1)} \perp S_2^{(k+1)}$.

(ii) For any $|e_{i_1}^{(k)}\rangle \in S_1^{(k)}$, there exists a j_1 such that $a_{i_1 j_1} \neq 0$. Since $a_{i_1 j_1}|e_{i_1}^{(k)}\rangle|e_{j_1}^{(n-k)}\rangle = a_{i_1 j_1}|e_i^{(k-1)}\rangle \otimes |l\rangle \otimes |e_j^{(n-k)}\rangle = a_{i_1 j_1}|e_{i'_1}^{(k-1)}\rangle|e_{j'_1}^{(n-k+1)}\rangle$, then there exists a j'_1 such that $a_{i'_1 j'_1} = a_{i_1 j_1} \neq 0$. According to the definition of the judgment space, we have $|e_{i'_1}^{(k-1)}\rangle \in S_1^{(k-1)}$. Therefore, the $(k-1)$-level judgment space of $|\varphi_1\rangle$ can be written as $S_1^{(k-1)} = \{\text{Tr}_k(|e_i^{(k)}\rangle), \text{if}\,|e_i^{(k)}\rangle \in S_1^{(k)}\}$, where Tr_k is tracing over the kth particle. Similarly, the $(k-1)$-level judgment space of $|\varphi_2\rangle$ is $S_2^{(k-1)} = \{\text{Tr}_k(|e_i^{(k)}\rangle), \text{if}\,|e_i^{(k)}\rangle \in S_2^{(k)}\}$. Therefore, if $S_1^{(k)} = S_2^{(k)}$, then $S_1^{(k-1)} = S_2^{(k-1)}$.

(iii) It has been shown that $S_1^{(k-1)} = \{\text{Tr}_k(|e_i^{(k)}\rangle), \text{if}\,|e_i^{(k)}\rangle \in S_1^{(k)}\}$. Because $S_1^{(k)} \subset S_2^{(k)}$, $S_1^{(k-1)} \subseteq \{\text{Tr}_k(|e_i^{(k)}\rangle), \text{if}\,|e_i^{(k)}\rangle \in S_2^{(k)}\} = S_2^{(k-1)}$. This completes the proof. ■

Theorem 1. Let $|\varphi_1\rangle$ and $|\varphi_2\rangle$ be a pair of orthogonal n-qudit symmetric entangled states. If their k-level judgment spaces are orthogonal, then they can always be unambiguously distinguished by no less than k cooperating participants under LOCC.

Proof. If there are k participants, let all of them measure their own particle in the computational basis $\{|j\rangle\}_{j=0}^{d-1}$ locally. Assume that their measurement result is $|e_i^{(k)}\rangle$. Without loss of generality, taking k measurement results randomly, and their tensor product can be written as a quantum state $|e_i^{(k)}\rangle$. Since

$S_1^{(k)} \perp S_2^{(k)}$, then their intersection is empty. That is to say, $|e_i^{(k)}\rangle$ only belongs to one of the judgment spaces $S_1^{(k)}$ and $S_2^{(k)}$. If $|e_i^{(k)}\rangle \in S_1^{(k)}$, then the shared state is $|\varphi_1\rangle$. Otherwise, the shared state is $|\varphi_2\rangle$. Similarly, according to the Lemma 1(i), the theorem still holds when there are more than k participants. ■

Corollary 1. Let $|\varphi_0\rangle, |\varphi_1\rangle, \ldots, |\varphi_{n-1}\rangle$ be a set of n-qudit orthogonal symmetric entangled states. If their k-level judgment spaces are orthogonal, then they can always be unambiguously distinguished by no less than k cooperating participants under LOCC.

Theorem 2. Let $|\varphi_1\rangle$ and $|\varphi_2\rangle$ be a pair of orthogonal n-qudit symmetric entangled states. If their $(k-1)$-level judgment spaces are equal, they cannot be unambiguously distinguished by less than k cooperating participants under LOCC.

Proof. We consider that the number of the cooperating participants is less than k. For the case of $k-1$, since $S_1^{(k-1)} = S_2^{(k-1)}$, then their measurement result $|e_i^{(k-1)}\rangle$ belongs to both $S_1^{(k-1)}$ and $S_2^{(k-1)}$. Therefore, $k-1$ cooperating participants cannot unambiguously distinguish the shared states under LOCC. According to the Lemma 1(ii), the theorem works in the case of less than $k-1$. ■

Corollary 2. Let $|\varphi_0\rangle, |\varphi_1\rangle, \ldots, |\varphi_{n-1}\rangle$ be a set of orthogonal n-qudit symmetric entangled states. If their $(k-1)$-level judgment spaces are equal, they cannot be unambiguously distinguished by less than k cooperating participants under LOCC.

According to the Theorem 1 and Theorem 2, a (k,n)-threshold LOCC-QSS scheme can be designed by a pair (or a set) of orthogonal orthogonal n-qudit symmetric entangled states, when their judgment spaces satisfy the conditions $S_1^{(k)} \perp S_2^{(k)}, S_1^{(k-1)} = S_2^{(k-1)}$. Here, when the number of cooperating participants is no less than k, the unambiguous probability is 1. Otherwise, the unambiguous probability is zero. It is easy to satisfy one of the conditions, while it is difficult to meet the two conditions at the same time. Next, we consider how to weaken these conditions.

Theorem 3. Let $|\varphi_0\rangle, |\varphi_1\rangle, |\varphi_2\rangle$ be a set of orthogonal n-qudit symmetric entangled states. If their $(k-1)$-level judgment spaces satisfy the conditions

$$\begin{aligned} S_0^{(k-1)} &\subseteq S_1^{(k-1)} \cup S_2^{(k-1)}, \\ S_1^{(k-1)} &\subseteq S_0^{(k-1)} \cup S_2^{(k-1)}, \\ S_2^{(k-1)} &\subseteq S_0^{(k-1)} \cup S_1^{(k-1)}, \end{aligned} \tag{2}$$

then they cannot be unambiguously distinguished by less than k cooperating participants under LOCC.

Proof. Without loss of generality, let $k-1$ participants measure their own particle in the computational basis $\{|j\rangle\}_{j=0}^{d-1}$ locally. Assume that their measurement result is $|e_i^{(k-1)}\rangle$, which belongs to $S_0^{(k-1)}$. Since $S_0^{(k-1)} \subseteq S_1^{(k-1)} \cup S_2^{(k-1)}$, then $|e_i^{(k-1)}\rangle$ belongs to at least two groups simultaneously. Therefore, the $k-1$ cooperating participants cannot unambiguously distinguish the shared states under LOCC. Similarly, when the measurement result belongs to $S_1^{(k-1)}$ or $S_2^{(k-1)}$, we can get the same conclusion. According to the Lemma 1(iii), the theorem still holds when the number of participants is less than $k-1$. ■

Corollary 3. Let $|\varphi_0\rangle, |\varphi_1\rangle, \ldots, |\varphi_{n-1}\rangle$ be a set of orthogonal n-qudit symmetric entangled states. If their $(k-1)$-level judgment spaces satisfy the condition $S_j^{(k-1)} \subseteq \cup_{i=0, i\neq j}^{n-1} S_i^{(k-1)}, j = 0,1,\ldots,n-1$, they cannot be unambiguously distinguished by less than k cooperating participants under LOCC.

Through careful analyses, it can be found that if $S_0^{(k-1)} = S_1^{(k-1)} = \ldots = S_{n-1}^{(k-1)}$, then $S_j^{(k-1)} \subseteq \cup_{i=1, i\neq j}^{n-1} S_i^{(k-1)}$, $j = 0,1,\ldots,n-1$. That is to say, Corollary 2 is just a special case of Corollary 3. Therefore, according to the Corollary 3, the conditions for designing a (k,n)-threshold LOCC-QSS scheme can be reduced. We can find more qualified entangled states to design the scheme.

III. ENCODING METHOD AND ITS COMPLETENESS

Although the conditions have been reduced, that will cause another problem. When these $(k-1)$-level judgment spaces are not equal to each other, there exists $k-1$ cooperating parties who can determine at least one state that is not the shared state. For example, in the Theorem 3, assume that $S_0^{(k-1)}$ is not a subset of $S_1^{(k-1)}$. There exists at least one state $|e_i^{(k-1)}\rangle$, which belongs to $S_0^{(k-1)}$ and not to $S_1^{(k-1)}$. Meanwhile, since $S_0^{(k-1)} \subseteq S_1^{(k-1)} \cup S_2^{(k-1)}$, we have that $|e_i^{(k-1)}\rangle$ belongs to $S_2^{(k-1)}$. Therefore, if the $k-1$ party's measurement result is $|e_i^{(k-1)}\rangle$, they cannot unambiguously determine whether the shared state is $|\varphi_0\rangle$ or $|\varphi_2\rangle$, but they can determine that the shared state is not $|\varphi_1\rangle$. A general encoding method is: $|\varphi_0\rangle \to 0, |\varphi_1\rangle \to 1, |\varphi_2\rangle \to 2$. If we use the three quantum states in Theorem 3 for information communication, then $k-1$ or less of the cooperating participants can unambiguously narrow the range of secret space. Therefore, the unambiguous attack can be divided into two types: the first class and the second class, as follows.

(i) The first class of unambiguous attack: the cooperating participants can correctly determine the data information from the secret set.

(ii) The second class of unambiguous attack: the cooperating participants can correctly determine which one is not in the secret set.

According to the previous analysis, it can be indicated that a (k,n)-threshold LOCC-QSS scheme can resist the two classes of unambiguous attack if and only if the $(k-1)$-level judgment spaces of the selected set of orthogonal entangled states are equal. Therefore, in order to reduce the conditions and resist the unambiguous attack, an alternate encoding method is needed. In this paper, we propose a simple encoding method for the case of three quantum states as follows.

Encoding method. Let $\{|\varphi_0\rangle, |\varphi_1\rangle, |\varphi_2\rangle\}$ be a set of quantum states, $\{0,1,2\}$ be a set of data information, the mapping between the two sets is:

$$\begin{aligned} |\varphi_i\rangle|\varphi_{i\oplus 1}\rangle &\to 0, \\ |\varphi_i\rangle|\varphi_i\rangle &\to 1, \\ |\varphi_i\rangle|\varphi_{i\ominus 1}\rangle &\to 2, \end{aligned} \tag{3}$$

where $i \in \{0,1,2\}$, $\oplus$ and $\ominus$ denote modulo-3 addition and modulo-3 subtraction, respectively.

Consequently, the k-level judgment space of 0 can be denoted as $U_0^{(k)} = \bigcup_{i=0}^{2}(S_i^{(k)} S_{i\oplus 1}^{(k)})$. Similarly, $U_1^{(k)} = \bigcup_{i=0}^{2}(S_i^{(k)} S_i^{(k)})$, $U_2^{(k)} = \bigcup_{i=0}^{2}(S_{i\ominus 1}^{(k)} S_i^{(k)})$. Under this encoding method, each of the cooperating participants needs to measure two particles for determining a unit of data. It should be noted that the two measures are independent. In order to evaluate the completeness of our encoding method, we give a definition.

Definition 1. Let $\{0,1,\ldots,n-1\}$ be a set of data information. A encoding method is k-level complete, if all of the k-level judgment spaces of each data element are equal, i.e. $U_0^{(k)} = U_1^{(k)} = \cdots = U_{n-1}^{(k)}$.

Therefore, according to the Definition 1, the encoding method should be $(k-1)$-level complete for designing a (k,n)-threshold LOCC-QSS scheme, which can resist the unambiguous attack. Now, we consider the case of where the number of quantum states is three.

Theorem 4. Let {0, 1, 2} be a set of data information, which is encoded into the set of quantum states in the Theorem 3, then the encoding method is $(k-1)$-level complete, i.e., $U_0^{(k)} = U_1^{(k)} = U_2^{(k)}$.

Proof. Assume that n participants share two n-qudit quantum states $|\varphi_{?_1}\rangle, |\varphi_{?_2}\rangle$, which are chosen from $\{|\varphi_0\rangle, |\varphi_1\rangle, |\varphi_2\rangle\}$ in Theorem 3, independently. Let

$$\begin{aligned} I_0^{(k-1)} &= S_1^{(k-1)} \cap S_2^{(k-1)}, \\ I_1^{(k-1)} &= S_0^{(k-1)} \cap S_2^{(k-1)}, \\ I_2^{(k-1)} &= S_0^{(k-1)} \cap S_1^{(k-1)}, \end{aligned} \tag{4}$$

then according to the Eq. (2), we have

$$\begin{aligned} S_0^{(k-1)} &= I_1^{(k-1)} \cup I_2^{(k-1)}, \\ S_1^{(k-1)} &= I_0^{(k-1)} \cup I_2^{(k-1)}, \\ S_2^{(k-1)} &= I_0^{(k-1)} \cup I_1^{(k-1)}. \end{aligned} \tag{5}$$

The $(k-1)$-level judgment space of the data 0 can be rewritten as

$$\begin{aligned} U_0^{(k-1)} &= \bigcup_{i=0}^{2} \left(S_i^{(k-1)} S_{i\oplus 1}^{(k-1)}\right) \\ &= \bigcup_{i=0}^{2} \left[\left(I_{i\ominus 1}^{(k-1)} \cup I_{i\oplus 1}^{(k-1)}\right) \otimes \left(I_i^{(k-1)} \cup I_{i\ominus 1}^{(k-1)}\right)\right] \\ &= \bigcup_{i=0}^{2} \left[\left(I_{i\ominus 1}^{(k-1)} \otimes I_i^{(k-1)}\right) \cup \left(I_{i\ominus 1}^{(k-1)} \otimes I_{i\ominus 1}^{(k-1)}\right)\right. \\ &\quad \left. \cup \left(I_{i\oplus 1}^{(k-1)} \otimes I_i^{(k-1)}\right) \cup \left(I_{i\oplus 1}^{(k-1)} \otimes I_{i\ominus 1}^{(k-1)}\right)\right] \\ &= \bigcup_{i=0}^{2} \bigcup_{j=0}^{2} \left(I_i^{(k-1)} I_j^{(k-1)}\right). \end{aligned} \tag{6}$$

Similarly, we can calculate the $U_1^{(k-1)}$ and $U_2^{(k-1)}$. Then, we have $U_0^{(k-1)} = U_1^{(k-1)} = U_2^{(k-1)} = \bigcup_{i=0}^{2} \bigcup_{j=0}^{2} (I_i^{(k-1)} I_j^{(k-1)})$. The Theorem 4 is proved completely. ■

IV. AN IMPROVEMENT OF (k,n)-THRESHOLD LOCC-QSS SCHEME

In a perfect (k,n)-threshold QSS scheme, $k-1$ cooperating participants cannot obtain any information about the secret. There are two kinds of eavesdropping probabilities of success in the (k,n)-threshold LOCC-QSS scheme, i.e., unambiguous probability and guessing probability [23]. Therefore, it is difficult to design such a scheme without any information leakage. However, according to our previous analysis, we can propose a (k,n)-threshold LOCC-QSS scheme, where the unambiguous probability is zero if the number of the cooperating participants is less than k. This means that the scheme can resist the unambiguous attack. Since the basic model of LOCC-QSS in Ref. [22] is very simple and efficient, we still use it in this paper.

Step 1 (preparation). The dealer Alice prepares a large number (say $L > n$) of states chosen randomly from a set of orthogonal n-qudit ($n = d$) symmetric entangled states $\{|\varphi_0\rangle, |\varphi_1\rangle, |\varphi_2\rangle\}$. For the set of states, their k-level judgment spaces should be orthogonal, and their $(k-1)$-level judgment spaces should satisfy the conditions in Theorem 3. Let us denote the prepared states by $|S(a,b_t)\rangle$ to keep details of each prepared state in each run. Here, $|S(a,b_t)\rangle$ represents that Alice prepared a state a at time $t(= 1,2,\ldots,L)$, and the position of all n qudits in the state are recorded as $b_t(= 1_t, 2_t, \ldots, n_t)$.

Step 2 (distribution). Alice prepares a different sequence, at random, $r_i = \Pi_i(1,2,3,\ldots,L)$, for each Bob_i, and sends the i_tth qudit ($i = 1,2,\ldots,n; t = 1,2,\ldots,L$) to Bob_i according to the r_i sequence order, where Π_i is an arbitrary permutation of the sequence $(1,2,3,\ldots,L)$. No one has the information about Π_i except for Alice. After receiving their associated sequence of qudits, all of the receivers share L n-qudit entangled states $|S[a,r(b_t)]\rangle$. Here, $r(b_t) = [\Pi_1(t), \Pi_2(t), \ldots, \Pi_n(t)]$.

Step 3 (measurement). After all of the receivers confirm the receipt of all their L qudits, Alice randomly chooses some run, say $\{t_s\}_{s=1}^{u} (\subset \{1,2,\ldots,L\})$, and also computes n arbitrarily chosen permutations, p_i of $\{1,2,\ldots,u\}$, only known to herself. She then prepares the list $C_i = \{[\sigma_i(t_{p_i(s)}), \Pi_i(t_{p_i(s)})]\}_{s=1}^{u}$ for Bob_i (for $i = 1,2,\ldots,n$) and sends it to him. For convenience, we denote the n-tuple observable as $O_{t_s} \in \{O\}$.

After receiving the list C_i, Bob_i measures his $\Pi_i(t_{p_i(s)})$th qubit in the $\sigma_i(t_{p_i(s)})$ basis and sends the measurement outcome $v_i(t_{p_i(s)})$ to Alice.

It should be noted that each of the prepared states is the eigenstate of at least one element of $\{O\}$. This means that there exists at least one $O_{t_s} \in \{O\}$, which satisfies the following eigenvalue relation:

$$O_{t_s} |S[a,r(b_{t_{p(s)}})]\rangle = \lambda(a,t_s) |S[a,r(b_{t_{p(s)}})]\rangle, \tag{7}$$

where $\lambda(a,t_s)$ is an eigenvalue and $r(b_{t_{p(s)}}) = [\Pi_1(t_{p_1(s)}), \Pi_2(t_{p_2(s)}), \ldots, \Pi_n(t_{p_n(s)})]$. Therefore, the product of all individual local out comes $v_i(t_{p_i(s)})$ for the observable O_{t_s} must be equal to the corresponding eigenvalue for the state $|S[a,r(b_{t_{p(s)}})]\rangle$ i.e., $\lambda(a,t_s) = \prod_{i=1}^{n} v_i(t_{p_i(s)})$.

In this step, Alice does still not give the information of Π_i to Bob_i. The list C_i only contain the measurement basis for each selected qudits. This means that Bob_i still does not know which n qudits come from the same entangled state. Therefore, the eavesdropper has the same problem.

Step 4 (detection). For each selected run t_s, Alice checks whether or not the product of local results of each measurement satisfies the eigenvalue relations $\lambda(a,t_s)=\prod_{i=1}^{n} v_i(t_{p_i}(s))$. Because the eavesdropper does not have any information about the sequence of qudits, he or she cannot create a measurement outcome to satisfy all of the relations.

Therefore, by analyzing the measurement results and associated measurement settings, Alice can easily detect the eavesdropper. If there is one, she aborts the scheme and starts again with a new set of resources.

Step 5 (reconstruction). If no eavesdropper is detected, Alice announces, to the respective parties, all qubit positions of two unmeasured states $|S[a,r(b_{t_1})]\rangle$ and $|S[a,r(b_{t_2})]\rangle$. Alice selects the two quantum states according to her (classical) secret a (= 0, 1, or 2). The mapping between classical bit value and quantum states is fixed with our encoding method and is securely communicated from Alice to all Bobs in advance. If Alice's secret is more than one bit, then she reveals the qubit positions of a sequence of unmeasured states $|S[a,r(b_t)]\rangle$.

To discuss the scheme in detail including the choice of states in Step 1, the measurements in Step 3 and Step 4, and the ability of resisting the unambiguous attack for different threshold scenarios, here we give two examples as follows.

A. (3, 4)-threshold LOCC-QSS scheme

Step 1. Alice prepares the states, each chosen at random from the set of quantum states as follows:

$$|\varphi_0\rangle=\frac{1}{\sqrt{4}}\sum_{j=0}^{3}|jjjj\rangle,$$
$$|\varphi_1\rangle=\frac{1}{\sqrt{24}}\sum_{P_i\in P}P_i(|0123\rangle), \tag{8}$$
$$|\varphi_2\rangle=\frac{1}{\sqrt{36}}\sum_{P_i\in P}\sum_{k,j=0;k>j}^{3}P_i(|jjkk\rangle).$$

Step 3. If $|S[a,r(b_{t_{p(s)}})]\rangle=|\varphi_0\rangle or|\varphi_1\rangle$, Alice chooses randomly the same measurement settings [i.e., $\sigma_1(t_{p_1(s)})=\sigma_2(t_{p_2(s)})=\sigma_3(t_{p_3(s)})=\sigma_4(t_{p_4(s)})$] from $\{X,Z,Z^2\}$ for all Bobs$_i$ for the run $t_{p_i(s)}$, whereas for $|\varphi_1\rangle$, Alice chooses from $\{X,Z^2\}$. Here, X and Z are the generalized Pauli operators in d-dimensional Hilbert space,

$$X=\sum_{j=0}^{d-1}|j+1\rangle\langle j|,$$
$$Z=\sum_{j=0}^{d-1}\omega^j|j\rangle\langle j|, \tag{9}$$

where $\omega=e^{2\pi\mathbb{I}/d}$, '+' is performed modulo d. In this scheme, $d=n=4$. Therefore, the set $\{O\}$ can be given as $\{O\}=\{X^{\otimes 4},Z^{\otimes 4},(Z^2)^{\otimes 4}\}$. It should be noted that there is a mistake in Ref. [23], i.e., the definition of generalized Pauli operators should not have the coefficient $1/\sqrt{d}$ before the summation notation.

Step 4. If $|S[a,r(b_{t_{p(s)}})]\rangle=|\varphi_0\rangle$, then

$$\lambda(a,t_s)=+1,\quad \forall\, O_{t_s}\in\{O\}, \tag{10}$$

if $|S[a,r(b_{t_{p(s)}})]\rangle=|\varphi_1\rangle$, then

$$\lambda(a,t_s)=\begin{cases}-1, & \text{if } O_{t_s}=Z^{\otimes 4}\\ +1, & \text{if } O_{t_s}=X^{\otimes 4}\text{or}\,(Z^2)^{\otimes 4}\end{cases} \tag{11}$$

and if $|S[a,r(b_{t_{p(s)}})]\rangle=|\varphi_2\rangle$, then

$$\lambda(a,t_s)=+1,\quad \text{if } O_{t_s}=X^{\otimes 4}\,\text{or}\,(Z^2)^{\otimes 4}. \tag{12}$$

Now, let us prove that this scheme is a (3, 4)-threshold LOCC-QSS. The three-level judgment spaces of the set of quantum states can be given as follows:

$$S_0^{(3)}=\{|jjj\rangle; j=0,\ldots,3\},$$
$$S_1^{(3)}=\{|ijk\rangle; i\neq j\neq k,i,j,k=0,\ldots,3\},$$
$$S_2^{(3)}=\{P_i(|jjk\rangle); P_i\in P, j\neq k,j,k=0,\ldots,3\}. \tag{13}$$

The three judgment spaces are orthogonal. Therefore, according to the Corollary 1, three cooperating participants can always exactly distinguish the prepared states. In the Step 5, they can recover the shared secret with their measurement results and the encoding method in advance.

The two-level judgment spaces of the set of quantum states are

$$S_0^{(2)}=\{|jj\rangle; j=0,\ldots,3\},$$
$$S_1^{(2)}=\{|jk\rangle; j\neq k,j,k=0,\ldots,3\},$$
$$S_2^{(2)}=\{|jk\rangle; j,k=0,\ldots,3\}. \tag{14}$$

Let $|jk\rangle$ be an arbitrary element of the $S_2^{(2)}$. We have that if $j=k$, then $|jk\rangle\in S_0^{(2)}$; if $j\neq k$, then $|jk\rangle\in S_1^{(2)}$. Therefore, $S_2^{(2)}\subseteq S_0^{(2)}\bigcup S_1^{(2)}$. Similarly, we have $S_0^{(2)}\subseteq S_1^{(2)}\bigcup S_2^{(2)}$, $S_1^{(2)}\subseteq S_0^{(2)}\bigcup S_2^{(2)}$. Therefore, the $(k-1)$-level judgment spaces of the set of quantum states satisfy the Eq. (2). With our encoding method, any two cooperating participants cannot distinguish the shared states completely, i.e., the unambiguous probability is zero. Hence, the (3,4)-threshold LOCC-QSS scheme can resist the unambiguous attack.

B. (5, 6)-threshold LOCC-QSS scheme

Step 1. Alice prepares the states, the desired set of quantum states are in the Eq. (15)

$$|\varphi_0\rangle=\frac{1}{\sqrt{1800}}\sum_{P_i\in P}\sum_{j,k,l=0;l>k>j}^{5}P_i(|jjkkll\rangle),$$
$$|\varphi_1\rangle=\frac{1}{\sqrt{1020}}\left[\sum_{P_i\in P}P_i(|012345\rangle)+\sum_{P_i\in P}\sum_{k,j=0;k>j}^{5}P_i(|jjjkkk\rangle)\right]$$
$$|\varphi_2\rangle=\frac{1}{\sqrt{1800}}\sum_{P_i\in P}\sum_{k,j=0;m>l>k>j}^{5}P_i(|jjjklm\rangle). \tag{15}$$

Step 3. Alice chooses randomly the same measurement settings from $\{X,Z^2\}$, $\{X,Z^3\}$, and X when $|S[a,r(b_{t_{p(s)}})]\rangle$ is $|\varphi_0\rangle$,

$|\varphi_1\rangle$ or $|\varphi_2\rangle$, respectively. Here, X and Z are the generalized Pauli operators in d-dimensional Hilbert space, and $d = n = 6$. Therefore, the set $\{O\}$ is $\{O\} = \{X^{\otimes 6}, (Z^2)^{\otimes 6}, (Z^3)^{\otimes 6}\}$.

Step 3. If $|S[a, r(b_{t_{p(s)}})]\rangle = |\varphi_0\rangle$, then

$$\lambda(a, t_s) = +1, \quad \text{if } O_{t_s} = X^{\otimes 6} \text{or} (Z^3)^{\otimes 6} \tag{16}$$

if $|S[a, r(b_{t_{p(s)}})]\rangle = |\varphi_1\rangle$, then

$$\lambda(a, t_s) = +1, \quad \text{if } O_{t_s} = X^{\otimes 6} \text{or} (Z^2)^{\otimes 6} \tag{17}$$

and if $|S[a, r(b_{t_{p(s)}})]\rangle = |\varphi_2\rangle$, then

$$\lambda(a, t_s) = +1, \quad \text{if } O_{t_s} = X^{\otimes 6}. \tag{18}$$

Now, let us prove that this scheme is a (5, 6)-threshold LOCC-QSS. The five-level judgment spaces of the set of quantum states can be given as follows:

$$\begin{aligned}
S_0^{(5)} &= \{P_i(|jjkkl\rangle);\ P_i \in P, l > k > j, j, k, l = 0, \ldots, 5\},\\
S_1^{(5)} &= \{P_i(|jjjkk\rangle) \text{ or } P_i(|jklmn\rangle);\\
&\qquad P_i \in P, n > m > l > k > j, j, k, l, m, n = 0, \ldots, 5\},\\
S_2^{(5)} &= \{P_i(|jjjkl\rangle) \text{ or } P_i(|jjklm\rangle);\\
&\qquad P_i \in P, m > l > k > j, j, k, l, m = 0, \ldots, 5\}.
\end{aligned} \tag{19}$$

The three judgment spaces are orthogonal. Therefore, according to the Corollary 1, three cooperating participants can always exactly distinguish the prepared states. In the Step 5, they can recover the shared secret with their measurement results and the encoding method in advance.

The four-level judgment spaces of the set of quantum states are

$$\begin{aligned}
S_0^{(4)} &= \{P_i(|jjkk\rangle) \text{ or } P_i(|jjkl\rangle);\\
&\qquad P_i \in P, l > k > j, j, k, l = 0, \ldots, 5\},\\
S_1^{(4)} &= \{P_i(|jjjk\rangle), P_i(|jjkk\rangle) \text{ or } P_i(|jklm\rangle);\\
&\qquad P_i \in P, m > l > k > j, j, k, l, m = 0, \ldots, 5\},\\
S_2^{(4)} &= \{P_i(|jjjk\rangle), P_i(|jjkl\rangle) \text{ or } P_i(|jklm\rangle);\\
&\qquad P_i \in P, m > l > k > j, j, k, l, m = 0, \ldots, 5\}.
\end{aligned} \tag{20}$$

It is obvious that $S_0^{(4)} \subseteq S_1^{(4)} \bigcup S_2^{(4)}$, $S_1^{(4)} \subseteq S_0^{(4)} \bigcup S_2^{(4)}$, $S_2^{(4)} \subseteq S_0^{(4)} \bigcup S_1^{(4)}$. Therefore, according to the previous analysis, the (5, 6)-threshold LOCC-QSS scheme can resist the unambiguous attack, i.e., the unambiguous probability is zero when the number of cooperating participants is less than 5.

In the Ref. [23], Yang *et al.* introduced two parameters k_1, k_2 into (k,n)-threshold LOCC-QSS scheme, denoted as (k_1, k_2, k, n), to describe the information leakages. If $k_2 = k$, then the scheme can resist the unambiguous attack; if $k_1 = k$, then the scheme can resist the guessing attack. For perfect LOCC-QSS scheme, it has $k_1 = k_2 = k$. Therefore, according to Yang *et al.*'s definition, the (k,n)-threshold LOCC-QSS scheme in this current study can be denoted as (k_1, k, k, n), since our QSS scheme can resist the unambiguous attack. In addition, the guessing probability formula $p = \frac{1}{2}(1 + tr|q_2\rho_2 - q_1\rho_1|)$ [25] indicates that the $(k-1)$-level reduced density matrix of each unit data should be equal for resisting the guessing attack. Moreover, we can find that the two examples in this paper can be denoted as (2, 3, 3, 4)-threshold and (2, 5, 5, 6)-threshold.

V. CONCLUSION

The original (k,n)-threshold LOCC-QSS scheme [22] proposed a novel idea for designing a QSS scheme based on the local distinguishability of orthogonal multipartite entangled states. It can defeat the external attack perfectly, but cannot defeat the conspiracy attack, i.e., unambiguous attack and guessing attack. Yang *et al.* have quantified the information leakages, but didn't reveal the type of quantum states that can be chosen for defeating these attacks. In this current study, we investigate the local distinguishability of a pair of orthogonal multiqudit entangled states and extend it to a set. To resist the unambiguous attack, we should choose the quantum states whose $(k-1)$-level judgment spaces are equal. However, these types of quantum states are very difficult to be found when $k < n$. In the current study, we propose a very simple and efficient encoding method, and the completeness of that is proved in detail. With our encoding method, to resist the unambiguous attack, the selected three quantum states just need to satisfy the inclusion relation in Eq. (2). Moreover, combined with the original LOCC-QSS scheme, we state our scheme in detail and present a (3,4)-threshold and a (5,6)-threshold LOCC-QSS schemes as our examples. In our scheme the participants need to measure two particles for determining a unit secret data, but the security of the schemes has been improved greatly. Therefore, the increased cost is acceptable. Although the guessing attack was still not 100% resisted, the study of local distinguishability in the current study helps us to to better understand the type of quantum states suitable for designing a (k,n)-threshold LOCC-QSS scheme and it may move the QSS study one step forward.

ACKNOWLEDGMENTS

Supported by the National Natural Science Foundation of China (Grants No. 61472045 and No. 61573067), the National Key Research and Development Program (Grants No. 2016YFB0800602 and No. 2016YFB0800604), the Beijing City Board of Education Science and Technology Key Project (Grant No. KZ201510015015), the Beijing City Board of Education Science and Technology Project (Grant No. KM201510015009), and BUPT Excellent Ph.D. Students Foundation (Grant No. CX2015206).

[1] A. Shamir, How to share a secret, Commun. ACM **22**, 612 (1979).

[2] G. R. Blakely, Safeguarding cryptographic keys, in *Proceedings of the 1979 AFIPS National Computer Conference, New Jersey, 1979* (AFIPS, Montvale, 1979), pp. 313–317.

[3] P. W. Shor, Algorithms for quantum computation: Discrete logarithms and factoring, in *Proc. 35th Annu. Symp. Foundations Comput. Sci.* (Santa Fe, New Mexico, 1994), pp. 124–134.

[4] L. K. Grover, A fast quantum mechanical algorithm for database search, in *Proc. 28th Annu. ACM Symp. Theory Comput.* (ACM Press, New York, 1996), pp. 212–219.

[5] C. H. Bennett and G. Brassard, Quantum Cryptography: Public Key Distribution and Coin Tossing, in *IEEE Int. Conf. Comput., Syst. Signal* (Bangalore, 1984), pp. 175–179.
[6] M. Hillery, V. Buzek, and A. Berthiaume, Quantum secret sharing, Phys. Rev. A **59**, 1829 (1999).
[7] R. Cleve, D. Gottesman, and H. K. Lo, How to Share a Quantum Secret, Phys. Rev. Lett. **83**, 648 (1999).
[8] S. K. Singh and R. Srikanth, Generalized quantum secret sharing, Phys. Rev. A **71**, 012328 (2005).
[9] Z.-J. Zhang, Y. Li, and Z.-X. Man, Multiparty quantum secret sharing, Phys. Rev. A **71**, 044301 (2005).
[10] B. Fortescue and G. Gour, Reducing the quantum communication cost of quantum secret sharing, IEEE Trans. Inf. Theor. **58**, 6659 (2012).
[11] V. Gheorghiu and B. C. Sanders, Accessing quantum secrets via local operations and classical communication, Phys. Rev. A **88**, 022340 (2013).
[12] H. Pilaram and T. Eghlidos, An efficient lattice based multi-stage secret sharing scheme, IEEE Trans. Depend. Secure Comput. **14**, 2 (2017).
[13] A. Tavakoli, I. Herbauts, M. Zukowski, and M. Bourennane, Secret sharing with a single d-level quantum system, Phys. Rev. A **92**, 030302(R) (2015).
[14] V. Karimipour and M. Asoudeh, Quantum secret sharing and random hopping: Using single states instead of entanglement, Phys. Rev. A **92**, 030301(R) (2015).
[15] W. Tittel, H. Zbinden, and N. Gisin, Experimental demonstration of quantum secret sharing, Phys. Rev. A **63**, 042301 (2001).
[16] C. Schmid, P. Trojek, M. Bourennane, C. Kurtsiefer, M. Zukowski, and H. Weinfurter, Experimental Single Qubit Quantum Secret Sharing, Phys. Rev. Lett. **95**, 230505 (2005).
[17] Y. A. Chen, A. N. Zhang, Z. Zhao, X. Q. Zhou, C. Y. Lu, C. Z. Peng, T. Yang, and J. W. Pan, Experimental Quantum Secret Sharing and Third-Man Quantum Cryptography, Phys. Rev. Lett. **95**, 200502 (2005).
[18] A. M. Lance, T. Symul, W. P. Bowen, B. C. Sanders, and P. K. Lam, Tripartite Quantum State Sharing, Phys. Rev. Lett. **92**, 177903 (2004).
[19] A. M. Lance, T. Symul, W. P. Bowen, B. C. Sanders, T. Tyc, T. C. Ralph, and P. K. Lam, Continuous-variable quantum-state sharing via quantum disentanglement, Phys. Rev. A **71**, 033814 (2005).
[20] B. A. Bell *et al.*, Experimental demonstration of a graph state quantum error-correction code, Nat. Commun. **5**, 3658 (2014).
[21] H. Lu, Z. Zhang, L. K. Chen, Z. D. Li, C. Liu, L. Li, N. L. Liu, X. Ma, Y. A. Chen, and J. W. Pan, Secret Sharing of a Quantum State, Phys. Rev. Lett. **117**, 030501 (2016).
[22] R. Rahaman and M. G. Parker, Quantum scheme for secret sharing based on local distinguishability, Phys. Rev. A **91**, 022330 (2015).
[23] Y. H. Yang *et al.*, Quantum secret sharing via local operations and classical communication, Sci. Rep. **5**, 16967 (2015).
[24] S. Bandyopadhyay, S. Ghosh, and G. Kar, LOCC distinguishability of unilaterally transformable quantum states, New J. Phys. **13**, 123013 (2011).
[25] J. Bae and L. C. Kwek, Quantum state discrimination and its applications, J. Phys. A: Math. Theor. **48**, 083001 (2015).