SCIENTIFIC REPORTS

OPEN

# Quantum secret sharing via local operations and classical communication

Received: 07 July 2015
Accepted: 22 October 2015
Published: 20 November 2015

Ying-Hui Yang[1,2], Fei Gao[1], Xia Wu[1], Su-Juan Qin[1], Hui-Juan Zuo[3] & Qiao-Yan Wen[1]

**We investigate the distinguishability of orthogonal multipartite entangled states in *d*-qudit system by *restricted local operations and classical communication*. According to these properties, we propose a standard (2, *n*)-threshold quantum secret sharing scheme (called LOCC-QSS scheme), which solves the open question in [Rahaman *et al.*, Phys. Rev. A, 91, 022330 (2015)]. On the other hand, we find that all the existing (*k*, *n*)-threshold LOCC-QSS schemes are imperfect (or "ramp"), i.e., unauthorized groups can obtain some information about the shared secret. Furthermore, we present a (3, 4)-threshold LOCC-QSS scheme which is close to perfect.**

Quantum secret sharing (QSS) is an important branch of quantum cryptography, which was simultaneously proposed by Hillery *et al.*[1] and Cleve *et al.*[2]. It allows a secret to be shared among many participants in such a way that only the authorized groups can reconstruct it. In a (*k*, *n*)-threshold QSS scheme, the dealer distributes a shared secret among *n* participants, and any group of *k* or more participants can collaboratively recover the shared secret, however, no group of fewer than *k* participants can.

During the past two decades, many interesting QSS schemes[1–11] were proposed (for an incomplete list). Recently, Rahaman *et al.* concentrated on the implementation of classical secret sharing by quantum means, and first introduced the theory of local distinguishability of quantum states to the design of QSS scheme[12]. A novel, simple and efficient model of QSS scheme was presented, where the participants only used local quantum operations and classical communication (LOCC), in other words, any joint quantum operations were not required. This QSS model is called LOCC-QSS model. According to the model, a series of (*k*, *n*)-threshold LOCC-QSS schemes were proposed in ref. [12]. The designs of them are based on the local distinguishability of orthogonal multipartite quantum states. That is, some pairs of locally distinguishable orthogonal multipartite entangled states which represent the encoded secret can be collaboratively distinguished by a sufficient number of participants using LOCC, but cannot be distinguished by any fewer than the threshold *k* participants.

The topic of LOCC-QSS is very interesting, meanwhile, it brings us some valuable study points. First, (2, *n*)-threshold LOCC-QSS scheme in ref. [12] is a nonstandard QSS scheme since it needs a strictly restricted condition, i.e., the two cooperating participants must come from two disjoint groups. A natural question how to design a standard (2, *n*)-threshold LOCC-QSS scheme is an open question. Second, all the existing (*k*, *n*)-threshold LOCC-QSS schemes are *ramp* (or "imperfect") QSS schemes, i.e., there exist some information leakages in these schemes. How to quantify the information leakages and design a (*k*, *n*)-threshold LOCC-QSS scheme of less information leakages or even a *perfect* (*k*, *n*)-threshold LOCC-QSS scheme is also an interesting topic.

In this paper, we revolve around above study points to research and try to solve them. On the one hand, we study the properties of orthogonal multipartite entangled states in *d*-qudit system. What's more, a standard (2, *n*)-threshold LOCC-QSS scheme is presented, i.e., there is no any restricted condition

[1]State Key Laboratory of Networking and Switching Technology, Beijing University of Posts and Telecommunications, Beijing, 100876, China. [2]School of Mathematics and Information Science, Henan Polytechnic University, Jiaozuo, 454000, China. [3]Mathematics and Information Science College, Hebei Normal University, Shijiazhuang, 050024, China. Correspondence and requests for materials should be addressed to F.G. (email: gaofei_bupt@hotmail.com)

for the two cooperating participants. On the other hand, we find that all the existing $(k, n)$-threshold LOCC-QSS schemes are ramp schemes, i.e., unauthorized groups can obtain some information about the shared secret. Then a near-perfect (3, 4)-threshold LOCC-QSS scheme is proposed.

## Results

**Local distinguishability of quantum states in high dimension system.** The paradigm of local distinguishability can be described as follows. Suppose some parties shared a multipartite quantum state which is secretly chosen from a known set of orthogonal quantum states. Their aim is to identify the unknown quantum state perfectly using local operations and classical communication. Numerous interesting results have been reported[13–25]. Now we discuss the distinguishability about a pair of orthogonal multipartite entangled states by *restricted local operations and classical communication* (rLOCC). Here, rLOCC means only a subset of parties is allowed to communicate with each other[12].

Let $\{|0\rangle, |1\rangle, \cdots, |d-1\rangle\}$ be a standard orthonormal basis of a $d$-dimensional Hilbert space. Consider the following two orthogonal state $|\psi_1\rangle, |\psi_2\rangle$, which can act as generalized Bell states in $d$-qudit system.

$$\begin{aligned} |\psi_1\rangle &= \frac{1}{\sqrt{d}}\sum_{j=0}^{d-1}|jjj\cdots j\rangle, \\ |\psi_2\rangle &= \frac{1}{\sqrt{d}}\sum_{j=0}^{d-1}|j, j+1, j+2,\cdots, j+d-1\rangle, \end{aligned} \tag{1}$$

where "+" is performed modulo $d$. For $d=2$, the two states are known as Bell states. Now we show that the two states in Eq.(1) have the following properties.

Theorem 1. *Two orthogonal entangled states $|\psi_1\rangle, |\psi_2\rangle$ in Eq.(1) can always be exactly distinguished by no less than two cooperating participants using LOCC. But they cannot be distinguished by only one participant.*

*Proof.* On the one hand, according to the forms of the two states, it is easy to obtain a distinguishable protocol. All the cooperating participants (no less than two) measure their own particle in the computational basis $\{|j\rangle\}_{j=0}^{d-1}$ locally. If they have precisely the same results, then the shared state is $|\psi_1\rangle$. Otherwise, if they have completely different results, the state is $|\psi_2\rangle$.

On the other hand, for the two states, it is straightforward to calculate that any single particle reduced density matrices are $I/d$, where $I$ is the identity operator in $d$-dimensional system. It means that only one participant cannot obtain any information from his own particle. That is, the two states cannot be distinguished by only one participant.

Now we recall the notion of stabilizer state. The generalized Pauli operators in $d$-dimensional Hilbert space are

$$\begin{aligned} X &= \frac{1}{\sqrt{d}}\sum_{j=0}^{d-1}|j+1\rangle\langle j|, \\ Z &= \frac{1}{\sqrt{d}}\sum_{j=0}^{d-1}\omega^j|j\rangle\langle j|, \end{aligned} \tag{2}$$

where $\omega = e^{2\pi i/d}$. A stabilizer state $|\psi\rangle$ is a state of an $n$-qudit system that is the simultaneous eigenvector, with eigenvalues 1, of a subgroup of $d^n$ commuting elements of the Pauli group which does not contain multiples of the identity other than the identity itself. We call this subgroup as the stabilizer $G$ of $|\psi\rangle$[26]. When $d$ is prime, $G$ can always be generated by $n$ suitably chosen group elements $g_j$, where the order of each $g_j$ is $d$. $\{g_j\}_{j=1}^n$ is called a set of generators. When $d$ is not prime, one might need more than $n$ generators in some cases.

In $d$-qudit system, $d$ is a prime. Let us define two sets of quantum operations

$$\begin{aligned} \mathcal{S}_1 &= \{g_1, g_1g_2, g_1g_3, \cdots, g_1g_d\}, \\ \mathcal{S}_2 &= \{g_1, \omega^{d-1}g_1g_2, \omega^{d-2}g_1g_3, \cdots, \omega g_1g_d\}, \end{aligned} \tag{3}$$

where

$$\begin{aligned} g_1 &= X\otimes X\otimes X\otimes\cdots\otimes X, \\ g_2 &= Z^{d-1}\otimes Z\otimes I\otimes\cdots\otimes I, \\ g_3 &= Z^{d-1}\otimes I\otimes Z\otimes\cdots\otimes I, \\ &\vdots \\ g_d &= Z^{d-1}\otimes I\otimes I\otimes\cdots\otimes Z. \end{aligned}$$

According to the definition of stabilizer, we can easily obtain the following lemma.

Lemma 1. *The elements of $\mathcal{S}_i$ in Eq.(3) constitute the generators set of the stabilizer of the state $|\psi_i\rangle$, $i=1, 2$.*

It is easy to see that quantum state $|\psi_2\rangle$ is the unique eigenstate of all the elements of $\mathcal{S}_1$ with eigenvalues $\omega^j$ ($j=0, \cdots, d-1$). So we have the following theorem.

Theorem 2. *If an unknown state $|\psi_?\rangle$ satisfy: $O_i|\psi_?\rangle = \lambda_i|\psi_?\rangle$, $\forall\ O_i \in \mathcal{S}_1$. Then*

(1) eigenvalues $\lambda_i=1$ if and only if $|\psi_?\rangle = |\psi_1\rangle$, $i=1, \cdots, d$;

(2) eigenvalues $\lambda_i=\omega^{i-1}$ if and only if $|\psi_?\rangle = |\psi_2\rangle$, $i = 1, \cdots, d$.

Note that whether $d$ is a prime or not, the two states $|\psi_1\rangle$, $|\psi_2\rangle$ are both the eigenstates of all the elements of $\mathcal{S}_1$. However, Theorem 2 holds only when $d$ is a prime. It means that both of the two states can be uniquely determined by the set $\mathcal{S}_1$ according to eigenvalues. If $d$ is not a prime, they may not be uniquely determined by the set $\mathcal{S}_1$ according to eigenvalues.

Theorem 3. *Two orthogonal entangled states in Eq. (4) can always be exactly distinguished by no less than three cooperating participants using LOCC. However, they cannot be deterministically distinguished by any two or fewer participants by LOCC.*

$$
\begin{aligned}
|\varphi_1\rangle &= \frac{1}{\sqrt{28}}\left[\sum_{j=0}^{3}|jjjj\rangle + \sum_{P_i\in P} P_i(|0123\rangle)\right],\\
|\varphi_2\rangle &= \frac{1}{\sqrt{36}}\sum_{P_i\in P}\sum_{k,j=0;k>j}^{3} P_i(|jjkk\rangle),
\end{aligned}
\tag{4}
$$

where $P$ is the set of all possible distinct permutations.

*Proof.* All the cooperating participants (no less than three) measure their own particle in the computational basis $\{|j\rangle\}_{j=0}^{d-1}$ locally. If they have precisely the same results or completely different results, then the shared state is $|\varphi_1\rangle$. Otherwise, if there exist two participants who have the same results, but their results are different from the other participants' results, then the shared state is $|\varphi_2\rangle$.

On the other hand, for the two states, it is straightforward to calculate that any one participant have the same reduced density matrix $I/d$, where $I$ is the identity operator in $d$-dimensional system. It means that only one participant cannot obtain any information from his own particle. All the bipartite reduced density matrices of $|\varphi_1\rangle$ are same because of the symmetry of $|\varphi_1\rangle$, so are that of $|\varphi_2\rangle$. Employing the probability formula of the minimum-error state discrimination $p = \frac{1}{2}(1 + tr|q_2\rho_2 - q_1\rho_1|)$[27], where $q_1$, $q_2$ are a priori probabilities and $\rho_1$, $\rho_2$ are two states, we can calculate that the probability with which any two participants can distinguish the states is 0.5536. It means that two participants cannot perfectly distinguish the two states even if they use joint quantum operations. So the two states cannot be exactly distinguished by any two participants by LOCC. That completes the proof.

**LOCC-QSS.** Suppose the sender Alice wants to share a key between $n$ separated participants $\text{Bob}_1$, $\text{Bob}_2$, …, $\text{Bob}_n$. Only no less than $k$ participants can collaboratively recover the shared secret. That is, a ($k$, $n$)-threshold QSS should be designed. Here, we still adopt the basic model of LOCC-QSS in ref. [12] since the basic model is very simple and efficient. For readability, we still use the same notations.

**The standard (2, *n*)-threshold LOCC-QSS scheme.** *Step 1.* Alice first prepares a large number (say $L>n$) of states chosen randomly from a specified pair of orthogonal $n$-qudit ($n=d$) entangled states in Eq.(1) according to her requirement. Let us denote the prepared states by $|S(a, b_t)\rangle$ to keep details of each prepared state in each run (run $t$ is associated with the prepared state $|S(a, b_t)\rangle$ at time $t$). Here, $a$ represents the state randomly chosen from a pair of orthogonal states, that Alice prepares at time $t\,(=1, 2, \ldots, L)$, where $b_t = (1_t, 2_t, \ldots, n_t)$ represents the positions of all $n$ qudits of a prepared state $|S(a, b_t)\rangle$ at time $t$, i.e., the position of $i$th qudit of a prepared state $a$ at time $t$ is denoted by $i_t (i = 1, 2, \ldots, n)$.

*Step 2.* Alice prepares at random, a different sequence, $r_i = \Pi_i(1, 2, \ldots, L)$ for each $\text{Bob}_i$, and sends the $i_t$th qudit ($i=1, 2, \ldots, n$; $t=1, 2, \ldots, L$) to $\text{Bob}_i$ according to the $r_i$ sequence order, where $\Pi_i$ is an arbitrary permutation of the sequence (1, 2, …, $L$). No one has the information about $\Pi_i$ except for Alice. After receiving their associated sequence of qudits, all of the receivers now 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.* Alice now randomly selects 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, …, $u$}, only known to herself. She then prepares list $C_i = \{\sigma_i(t_{p_i(s)}), \Pi_i(t_{p_i(s)})\}_{s=1}^{u}$ for $\text{Bob}_i$ (for $i=1, 2, \ldots, n$) and sends it to him. After receiving the list $C_i$, $\text{Bob}_i$ measures his $\Pi_i(t_{p_i(s)})$th qudit in the $\sigma_i(t_{p_i(s)})$ basis and sends the measurement outcome $v_i\left(t_{p_i(s)}\right)$ to Alice.

Here Alice choose randomly elements of the set $\mathcal{S}_1$ in Eq.(3) to determine $\mathrm{Bob}_i$'s measurement basis. Now we interpret it. First, for the set $\mathcal{S}_1$, both $|\psi_1\rangle$ and $|\psi_2\rangle$ are the eigenstates of the elements of $\mathcal{S}_1$. They have the following relation

$$O_{t_s}|S[a, r(b_{t_{p(s)}})]\rangle = \lambda(a, t_s)|S[a, r(b_{t_{p(s)}})]\rangle, \forall O_{t_s} \in \mathcal{S}_1, \tag{5}$$

where eigenvalue $\lambda(a, t_s) \in \{\omega^j\}_{j=0}^{n-1}$ and $r(b_{t_{p(s)}}) = [\Pi_1(t_{p_1(s)}), \Pi_1(t_{p_1(s)}), \ldots, \Pi_n(t_{p_n(s)})]$. Therefore, all the product of all the local measurement results $v_j(t_{p_j(s)})$ for $O_{t_s}$ must be equal to the corresponding eigenvalue, i.e., $\lambda(a, t_s) = \Pi_{j=1}^n v_j(t_{p_j(s)})$. It should be noted that the generalized Pauli operators $X$ and $Z$ are not Hermite, so $X$, $Z$ and $O_{t_s}$ cannot act as observables. However, they are unitary operators. Since the relation between unitary operator $U$ and Hermite operator $H$ is $U = \exp(iH)$, and they have the same eigenstates. While the above measurement can always be completed using Hermite operator $H$ as observables. For simplicity, roughly speaking, one can use the eigenstates of $U$ as measurement basis to complete projective measurement, and measurement results can be denoted by eigenvalues.

For example, if Alice chooses $O_{t_s} = g_1 g_2 \in \mathcal{S}_1$, then $\sigma_1(t_{p_1(s)}) = XZ^{d-1}$, $\sigma_2(t_{p_2}(s)) = XZ$, $\sigma_j(t_{p_j(s)}) = X\,(j = 3, 4, \ldots, n)$. $\mathrm{Bob}_1$ uses the eigenstates of $XZ^{d-1}$ as measurement basis to complete projective measurement, and measurement result can be denoted by eigenvalues. Other $\mathrm{Bob}_i$ have the similar way to completed measurement. If the unknown state is $|\psi_1\rangle$, then $\Pi_{j=1}^n v_j(t_{p_j(s)}) = 1$. If the unknown state is $|\psi_2\rangle$, then $\Pi_{j=1}^n v_j(t_{p_j(s)}) = \omega$.

In this step, two very important points should be emphasized. First, when Alice prepares list $C_i$ for $\mathrm{Bob}_i$ and sends it to him, $\mathrm{Bob}_i$ still does not know which $n$ qudits come from the same entangled state. It is very crucial for design of eavesdropping detection in a concrete LOCC-QSS scheme. Second, Alice starts to send lists $C_i$ only if all of the receivers confirm the receipt of all their $L$ qudits.

*Step 4*. For each selected run $t_s$, Alice check whether or not the the product of local measurement results is equal to the corresponding eigenvalue $\lambda(a,t_s)$, i.e., $\lambda(a, t_s) = \Pi_{j=1}^n v_j(t_{p_j(s)})$. If $|S[a, r(b_{t_{p(s)}})]\rangle = |\psi_1\rangle$, then

$$\lambda(a, t_s) = +1, \forall O_{t_s} \in \mathcal{S}_1, \tag{6}$$

and if $|S[a, r(b_{t_{p(s)}})]\rangle = |\psi_2\rangle$, then

$$\lambda(a, t_s) = \begin{cases} 1 & \text{if } O_{t_s} = g_1; \\ \omega & \text{if } O_{t_s} = g_1 g_2; \\ \ldots & \ldots; \\ \omega^{d-1} & \text{if } O_{t_s} = g_1 g_d. \end{cases} \tag{7}$$

By analyzing the measurement results, Alice can easily detect whether there is an eavesdropper or not. If there is one, she aborts the protocol and starts again from step 1.

*Step 5*. If no eavesdropper is detected, Alice announces, to the respective parties, all qudit positions of an unmeasured state $|S[a, r(b_t)]\rangle$. Alice selects this $|S[a, r(b_t)]\rangle$ according to her secret $a$ (=0 or 1). The mapping between classical bit value and orthogonal entangled states is fixed and is communicated securely from Alice and Bobs in advance. If Alice's secret is more than one bit, then she reveals the qudit positions of a sequence of unmeasured states $|S[a, r(b_t)]\rangle$.

According to Theorem 2, the states $|\psi_1\rangle$, $|\psi_2\rangle$ can be uniquely determined by the set $S_1$ according to eigenvalues if $d$ is prime. It makes the protocol be more secure. On the other hand, although $|\psi_1\rangle$ and $|\psi_2\rangle$ cannot be uniquely determined if $d$ is not prime, the protocol is still secure due to the design method of this scheme. It will be shown in the section of security analysis.

Employing Theorem 1, the two states can be exactly distinguished by no less than two cooperating participants using LOCC. But they cannot be distinguished by only one participant. Thus, this is a standard (2, $n$)-threshold LOCC-QSS scheme.

*Example 1*. In a (2,3)-threshold LOCC-QSS scheme, the pair of the states are

$$|\psi_1\rangle = \frac{1}{\sqrt{3}}(|000\rangle + |111\rangle + |222\rangle),$$
$$|\psi_2\rangle = \frac{1}{\sqrt{3}}(|012\rangle + |120\rangle + |201\rangle),$$

and $\mathcal{S}_1 = \{X^{\otimes 3}, XZ^2 \otimes XZ \otimes X, XZ^2 \otimes X \otimes XZ\}$. The steps are described in detail in the standard (2, $n$)-threshold LOCC-QSS scheme. Here, we only consider the Step 4. If $|S[a, r(b_t)]\rangle = |\psi_1\rangle$, then

$$\lambda(a, t_s) = +1, \forall O_{t_s} \in \mathcal{S}_1,$$

and if $|S[a, r(b_t)]\rangle = |\psi_2\rangle$, then

$$\lambda(a, t_s) = \begin{cases} 1 & \text{if } O_{t_s} = X^{\otimes 3}; \\ \omega & \text{if } O_{t_s} = XZ^2 \otimes XZ \otimes X; \\ \omega^2 & \text{if } O_{t_s} = XZ^2 \otimes X \otimes XZ. \end{cases}$$

**The security analysis of standard (2, *n*)-threshold LOCC-QSS scheme.** The standard (2, *n*)-threshold LOCC-QSS scheme can be regarded as secure because the shared secret cannot be eavesdropped without being detected. Usually, there are three eavesdropping strategies for Eve (she may be dishonest Bob). Now we consider the security of our scheme under the three attacks.

The first eavesdropping strategy is called "intercept-measure-resend", that is, Eve intercepts the legal particles when Alice sends them to $\text{Bob}_i$, chooses local or global measurement basis to measure them, then resends them to $\text{Bob}_i$. (i) If Eve wants to obtain Alice's secret, she can choose and measure *n* qudits by global measurement to distinguish the unknown state. However, Eve does not know which *n* qudits come from the same entangled state because Alice has scrambled the order of qudits using permutation $\Pi_i$, and no one has the information about $\Pi_i$ except for Alice. Therefore, this attack will be detected in the eavesdropping detection if Eve chooses this method of attack. (ii) If Eve wants to obtain $\text{Bob}_i'$s secret or wants to obtain Alice's secret according to more than *t* (threshold value) $\text{Bob}_i'$s secrets, she can measure one or more qudits by local measurement. However, the original correlations of quantum states will be destroyed. For example, Eve chooses computation basis to locally measure the unknown state $|\psi_?\rangle$. Then $|\psi_?\rangle$ collapses to a product state, which does not satisfy the conditions of eavesdropping detection. This attack will be detected in the eavesdropping detection.

The second one is "intercept-replace-resend", i.e., Eve intercepts the legal particles and replaces them by her counterfeit ones. If Eve escapes from the detection of Alice, she will obtain Alice's secret. Now we show that our scheme is security under the attack. (i) If *d* is a prime, according to Theorem 2 Eve cannot find a quantum state which satisfies the conditions of eavesdropping detection to replace the legal particles. (ii) if *d* is not a prime, $|\psi_1\rangle, |\psi_2\rangle$ cannot be uniquely determined by the set $S_1$ according to eigenvalues, that is, there exists another state which satisfies $\lambda(a, t_s) = \Pi_{j=1}^n \nu_j(t_{p_j(s)})$. However, Alice has scrambled the order of qudits using permutation $\Pi_i$, according to Step 2 and 3 anyone does not know which *n* qudits come from the same entangled state except for Alice before the end of the eavesdropping detection. Thus the eavesdropper cannot use the illegal states satisfying $\lambda(a, t_s) = \Pi_{j=1}^n \nu_j(t_{p_j(s)})$ to replace the states which are sent by Alice. Otherwise, the eavesdropping will be found by Alice.

The third one is "entangle-measure", i.e., Eve entangles an ancilla with the *n*-qudit, at some later time she can measure the ancilla to gain information. Without loss of generality, assume that Eve uses a unitary operator such that the ancilla $|0\rangle$ entangles with the quantum state $|\psi_i\rangle$, i.e., $U|\psi_1\rangle_B|0\rangle_E = |\phi_1\rangle_{BE}$, $U|\psi_2\rangle_B|0\rangle_E = |\phi_2\rangle_{BE}$, where the subscripts *B* and *E* express the particles belonging to $\text{Bob}_i$ and Eve, respectively. In fact, This kind of attack is general, it contains the above two attacks. Now we will show that the legal particles (*B*) and the ancilla (*E*) must be not entangled if no error is introduced into the QSS procedures. It means that Eve will gain no information about the secret by observing the ancilla.

(i) If *d* is a prime, according to Theorem 2, $|\psi_1\rangle$ and $|\psi_2\rangle$ are uniquely determined by $S_1$. In other words, the state $|\phi_i\rangle_{BE}$ $(i = 1, 2)$ must be not entangled between *B* and *E*, otherwise, this attack will be detected by Alice with certain probability.

(ii) Next we consider that *d* is not a prime. Firstly, since Eve does not know which *n* qudits come from the same entangled state, the unitary operator can only act on one qudit from $|\psi_i\rangle$ and the ancilla. Secondly, note that the operator $Z^{\otimes n}$ can be generated by the elements of $S_1$, i.e., $Z^{\otimes n} = \Pi_{i=1}^n O_i$, $O_i \in S_1$ in Eq. (3). Then $\lambda = \Pi_{i=1}^n \lambda_i$, where $Z^{\otimes n}|\psi_i\rangle = \lambda|\psi_i\rangle$, $O_i|\psi_i\rangle = \lambda_i|\psi_i\rangle$. Therefore, only if the state $|\phi_i\rangle_{BE}$ satisfies the property that the product of all $\text{Bob}_i'$s measurement results measured by computation basis is equal to $\lambda$ (=1), may Eve escape from the detection of Alice. So $|\phi_1\rangle_{BE}$ and $|\phi_2\rangle_{BE}$ have the form $|\phi_1\rangle_{BE} = \sum_{j=0}^{d-1}|jj\cdots j\rangle_B|\alpha_j\rangle_E$ and $|\phi_2\rangle_{BE} = \sum_{j=0}^{d-1}|j, j+1, \ldots, j+d-1\rangle_B|\beta_j\rangle_E$, where $|\alpha_j\rangle_E = \sum_{i=0}^{m-1} a_{ij}|i\rangle$, $|\beta_j\rangle_E = \sum_{i=0}^{m-1} b_{ij}|i\rangle$. It should be noted that we do not put constraints on the dimensions of $|\alpha_j\rangle_E$ and $|\beta_j\rangle_E$. Next we will show that this attack will be detected when participants check eavesdropping with the basis $X \otimes X \otimes \cdots \otimes X$. Using the inverse Fourier transform $|j\rangle = \frac{1}{\sqrt{d}}\sum_{k=0}^{d-1} w^{-jk}|x_k\rangle$, we consider the form of the *n* legal qudits of quantum state $|\phi_1\rangle_{BE}$ in the Fourier basis, where $\{|j\rangle\}_{j=0}^{d-1}$ is the computation basis, $\{|x_k\rangle\}_{k=0}^{d-1}$ is the Fourier basis and $w = e^{2\pi i/d}$. It is easy to calculate the terms

$$|x_0x_0\cdots x_0x_j\rangle_B(|\alpha_0\rangle + w^{-1\cdot j}|\alpha_1\rangle + w^{-2\cdot j}|\alpha_2\rangle + \cdots + w^{-(d-1)\cdot j}|\alpha_{d-1}\rangle),$$

$j\neq 0$. Obviously, they must be eliminated, i.e., $|\alpha_0\rangle + w^{-1\cdot j}|\alpha_1\rangle + w^{-2\cdot j}|\alpha_2\rangle + \cdots + w^{-(d-1)\cdot j}|\alpha_{d-1}\rangle = 0$, $j\neq 0$. Otherwise, this attack will be found by Alice. It means $(a_{ij})_{m\times d}\cdot(w_{ij})_{d\times(d-1)} = 0$, where

$$(a_{ij})_{m\times d} = \begin{bmatrix} a_{00} & a_{01} & \cdots & a_{0,d-1} \\ a_{10} & a_{11} & \cdots & a_{1,d-1} \\ \vdots & \vdots & \ddots & \vdots \\ a_{m-1,0} & a_{m-1,1} & \cdots & a_{m-1,d-1} \end{bmatrix}, (w_{ij})_{d\times(d-1)} = \begin{bmatrix} 1 & 1 & \cdots & 1 \\ w^{-1} & w^{-1\cdot 2} & \cdots & w^{-1\cdot(d-1)} \\ \vdots & \vdots & \ddots & \vdots \\ w^{-(d-1)} & w^{-(d-1)\cdot 2} & \cdots & w^{-(d-1)\cdot(d-1)} \end{bmatrix}.$$

So $rank[(a_{ij})_{m\times d}] + rank[(w_{ij})_{d\times(d-1)}] \leq d$. Since the matrix $(w_{ij})_{d\times(d-1)}$ contains a Vandermonde submatrix with the order $d-1$, we have $rank[(w_{ij})_{d\times(d-1)}] = d-1$. Thus $rank[(a_{ij})_{m\times d}] \leq 1$. It means that $|\alpha_0\rangle = |\alpha_1\rangle = \cdots = |\alpha_{d-1}\rangle$ (up to global phase). So $|\phi_1\rangle_{BE}$ is a product state between legal qudits and the ancilla. The similar discussion can be applied for the analysis of quantum state $|\phi_2\rangle_{BE}$, and we can obtain the same result.

Intuitively, maybe it is surprised that the scheme is secure despite $|\psi_i\rangle$ cannot be uniquely determined by the set $S_1$ for non-prime $d$. The reason is that Alice has scrambled the order of qudits such that the states satisfying conditions of eavesdropping detection are excluded. If the unitary operator can only act on one qudit from $|\psi_i\rangle$ and the ancilla, Eve cannot obtain any information according to the above proof.

**The quantification of information leakages.** It is difficult to design a *perfect* (without any information leakage) $(k, n)$-threshold LOCC-QSS scheme. At present all of the existing $(k, n)$-threshold LOCC-QSS schemes are ramp schemes. We try to quantify the information leakages.

Now we consider conspiracy attack for $(k, n)$-threshold LOCC-QSS scheme. If there exist $l(<k)$ dishonest $Bob_i$, they can recover the secret together. This attack method is called conspiracy attack. For the $(k, n)$-threshold LOCC-QSS scheme[12], according to the following two intentions, they can choose different ways to eavesdrop.

(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. For simplicity, the eavesdropping probability of success is called *unambiguous* probability.

(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 eavesdropping probability of success is called *guessing* probability.

For the sake of simplicity, we only analyze the example 3 in ref. [12], i.e., (5, 6)-threshold LOCC-QSS scheme. It is easy to be generalized for $(k, n)$-threshold LOCC-QSS scheme. First we recall the key steps in the original scheme.

*Step 1*. Alice randomly chooses the states from the pair orthogonal Dicke states

$$\begin{aligned} |1,6\rangle &= \frac{1}{\sqrt{6}}[|100000\rangle + |010000\rangle + |001000\rangle \\ &\quad + |000100\rangle + |000010\rangle + |000001\rangle], \\ |3,6\rangle &= \frac{1}{\sqrt{20}}[\sum_P P(|111000\rangle)]. \end{aligned} \tag{8}$$

*Step 4*. If $|S[a, r(b_t)]\rangle = |1, 6\rangle$, then

$$\lambda(a, t_s) = -1, \text{if } O_{t_s} = Z^{\otimes 6}, \tag{9}$$

and if $|S[a, r(b_t)]\rangle = |3, 6\rangle$, then

$$\lambda(a, t_s) = \begin{cases} -1 & \text{if } O_{t_s} = Z^{\otimes 6}, \\ +1 & \text{if } O_{t_s} = X^{\otimes 6} \text{ or } Y^{\otimes 6}. \end{cases} \tag{10}$$

Other steps are similar to the standard $(2, n)$–threshold LOCC-QSS scheme. It should be noted that there is a mistake in original (5, 6)-threshold LOCC-QSS scheme, i.e., if $|S[a, r(b_t)]\rangle = |3,6>$, then $\lambda(a, t_s) = +1, \forall O_{t_s} \in \{X^{\otimes 6}, Y^{\otimes 6}, Z^{\otimes 6}\}$.

Now we consider conspiracy attack for (5, 6)-threshold LOCC-QSS scheme.

*The method of conspiracy attack*: these dishonest $Bob_i$ will faithfully perform the protocol until Alice believes no eavesdropper. For intention (i): when Alice announces all qubit positions of unmeasured

| $l$ | 1 | 2 | 3 | 4 |
|---|---|---|---|---|
| $p_u$ | 0 | 1/10 | 1/4 | 17/30 |
| $p_g$ | 0.5833 | 0.6167 | 0.625 | 0.7 |
| $r$ | 2.01% | 3.97% | 4.56% | 11.87% |

**Table 1. The information leakages of (5, 6) scheme.**

states, these $l(<5)$ dishonest $\text{Bob}_i$ measure their own qubit in the computational basis locally to recover the secret together. For intention (ii): when Alice announces all qubit positions of unmeasured states, these $l(<5)$ dishonest $\text{Bob}_i$ use joint quantum measurement to measure their $l$ qubits according to the minimum-error state discrimination.

Now we calculate the probability when $l(<5)$ participants recover the secret together.

(1) $l=4$. For intention (i): if the local measurement results of the four dishonest $\text{Bob}_i$ are three same states $|1\rangle$ and one state $|0\rangle$ or two states $|1\rangle$ and two states $|0\rangle$, they can determine the state is $|3, 6\rangle$. If the local measurement result are four same states $|0\rangle$, they can determine the state is $|1, 6\rangle$. So the *unambiguous* probability is 17/30. On the other hand, for intention (ii), we can calculate that the *guessing* probability is 0.7 according to the probability formula of the minimum-error state discrimination, i.e., the rate of information leakages is 11.87%.

(2) $l=3$. For intention (i): if the local measurement results of the three dishonest $\text{Bob}_i$ are three same states $|1\rangle$ or two states $|1\rangle$ and one state $|0\rangle$, they can determine the state is $|3, 6\rangle$. The *unambiguous* probability is 1/4. For intention (ii): the *guessing* probability is 0.625, namely, the rate of information leakages is 4.56%.

(3) $l=2$. For intention (i): Only the local measurement results of the two dishonest $\text{Bob}_i$ are two same states $|1\rangle$, they can determine the state is $|3, 6\rangle$. For other local measurement results they cannot distinguish the states. So the *unambiguous* probability is 1/10. For intention (ii): the *guessing* probability is 0.6167, that is, the rate of information leakages 3.97%.

(4) $l=1$. Obviously, the *unambiguous* probability is zero. The *guessing* probability is 7/12. That is, the rate of information leakages 2.01%.

All the cases can be shown in Table 1, where $l$ is the number of dishonest $\text{Bob}_i$, $p_u$, $p_g$, $r$ are *unambiguous* probability, *guessing* probability and the rate of information leakages, respectively. The intention (i) is very interesting. Since dishonest $\text{Bob}_i$ can always exactly recover the secret with nonzero probability if the *unambiguous* probability is nonzero, and they cannot disturb the authorized groups to recover the shared secret.

Now we introduce two parameters $k_1$, $k_2$ in $(k, n)$-threshold LOCC-QSS scheme, denoted as $(k_1, k_2, k, n)$, to describe the information leakages. It means that (i) any fewer than $k_1$ participants cannot obtain any information; (ii) any $l$ $(k_1 \le l < k)$ participants can obtain the shared secret with *guessing* probability more than 1/2; (iii) any $l$ $(k_2 \le l < k)$ participants can obtain the shared secret with nonzero *unambiguous* probability. Obviously, for ramp LOCC-QSS scheme, it has $1 \le k_1 \le k_2 \le k$. And the more $k_1$, $k_2$ are close to $k$, the less information leakages are. For perfect LOCC-QSS scheme, it has $k_1 = k_2 = k$. For the above (5, 6)-threshold LOCC-QSS scheme, it can be denoted as (1, 2, 5, 6)-threshold LOCC-QSS scheme.

Finally, we show that a secure (3, 4)-threshold LOCC-QSS scheme cannot be designed based on the model of $(k, n)$-threshold LOCC-QSS scheme in ref. [12]. Since threshold $k = n - r + 1 = 3$, the distance[12] $r$ between the pair of states is 2. If the pair of states which Alice chooses contains the Dicke state $|2, 4\rangle$, the other is $|0, 4\rangle$, or $|4, 4\rangle$. It contradicts with the definition of Dicke state. If the pair of states does not contain the state $|2, 4\rangle$, the pair of states must be $|1, 4\rangle$ and $|3, 4\rangle$. In the stage of eavesdropping detection, only condition $\sigma_z^{\otimes 4}|\text{m}, 4\rangle = (-1)^m|\text{m}, 4\rangle$ ($m=1$ or 3) can be used to detect eavesdropping. Obviously it is insecure. Since the eavesdropper Eve can always measure all the qubit in the computational basis then send the post-measurement states to $\text{Bob}_i$, but Alice cannot find Eve's eavesdropping.

**The (3, 4)-threshold LOCC-QSS scheme.** Now we propose a (3, 4)-threshold LOCC-QSS scheme, in which dishonest $\text{Bob}_i$ cannot obtain the shared secret with nonzero *unambiguous* probability. All the steps are similar to the standard $(2, n)$-threshold LOCC-QSS scheme, so we only show the differences.

Step 1. Alice prepares the states, the desired pair of the states are in Eq. (4).

Step 4. If $|S[a, r(b_{t_{p(s)}})]\rangle = |\varphi_1\rangle$, then $\lambda(a, t_s) = +1$, $\forall O_{t_s} \in \mathcal{S}'$, and if $|S[a, r(b_{t_{p(s)}})]\rangle = |\varphi_2\rangle$, then $\lambda(a, t_s) = +1$, $\forall O_{t_s} \in \mathcal{S}'$, where

$$\mathcal{S}' = \{X \otimes X \otimes X \otimes X, Z^2 \otimes Z^2 \otimes Z^2 \otimes Z^2\}.$$

Because both $|\varphi_1\rangle$ and $|\varphi_2\rangle$ are the eigenstates of the element in $\mathcal{S}'$ with eigenvalue 1.

According to Theorem 3, we know it is a (3, 4)-threshold LOCC-QSS scheme. Employing the forms of the two states in Eq.(4), it is easy to see that the *unambiguous* probability is zero for any $l$ dishonest $\text{Bob}_i$ $(l<3)$. According to the proof of Theorem 3, we know that the *guessing* probability is zero when

$l = 1$, and the *guessing* probability is 0.5536 when $l = 2$. The rate of information leakages is 0.83%. So the scheme can be denoted as (2, 3, 3, 4)-threshold LOCC-QSS scheme. It is close to perfect (3, 4)-threshold LOCC-QSS scheme.

## Discussion

In ref. [11], Gheorghiu *et al.* also proposed an efficient QSS scheme by LOCC, which is based on quantum error-correcting codes to distribute a quantum secret. In their QSS scheme, they reduced the required quantum communication at the cost of some classical communication. But our schemes are based on local discrimination of quantum states to distribute classical secrets. And any joint quantum operations and quantum communication are not required in secret recovery stage. Although the designs of these schemes have all used LOCC, their essences are completely different.

In this paper, based on the distinguishability of orthogonal multipartite entangled states by rLOCC in $d$-qudit system, we present a standard $(2, n)$-threshold LOCC-QSS scheme, which work out the open question in ref. [12]. In addition, we take (5, 6)-threshold LOCC-QSS scheme as a example to present that all the existing $(k, n)$-threshold LOCC-QSS schemes are ramp schemes. Then we propose a (3, 4)-threshold LOCC-QSS scheme, which is close to perfect. We hope that these results will encourage researchers to study generalized $(k, n)$-threshold LOCC-QSS scheme.

## References


1. Hillery, M., Buzek, V. & Berthiaume, A. Quantum secret sharing. *Phys. Rev. A* **59,** 1829 (1999).
2. Cleve, R., Gottesman, D. & Lo, H.-K. How to share a quantum secret. *Phys. Rev. Lett.* **83,** 648 (1999).
3. Karlsson, A., Koashi, M. & Imoto, N. Quantum entanglement for secret sharing and secret splitting. *Phys. Rev. A* **59,** 162 (1999).
4. Gottesman, D. Theory of quantum secret sharing. *Phys. Rev. A* **61,** 042311 (2000).
5. Bandyopadhyay, S. Teleportation and secret sharing with pure entangled states. *Phys. Rev. A* **62,** 012308 (2000).
6. Nascimento, A. C. A., Mueller-Quade, J. & Imai, H. Improving quantum secret-sharing schemes. *Phys. Rev. A* **64,** 042311 (2001).
7. Karimipour, V., Bahraminasab, A. & Bagherinezhad, S. Entanglement swapping of generalized cat states and secret sharing. *Phys. Rev. A* **65,** 042320 (2002).
8. Xiao, L., Long, G. L., Deng, F. G. & Pan, J. W. Efficient multiparty quantum-secret-sharing schemes. *Phys. Rev. A* **69,** 052307 (2004).
9. Singh, S. K. & Srikanth, R. Generalized quantum secret sharing. *Phys. Rev. A* **71,** 012328 (2005).
10. Fortescue, B. & Gour, G. Reducing the quantum communication cost of quantum secret sharing. *IEEE Trans. Inf. Theory* **58,** 6659 (2012).
11. Gheorghiu, V. & Sanders, B. C. Accessing quantum secrets via local operations and classical communication *Phys. Rev. A* **88,** 022340 (2013).
12. Rahaman, R. & Parker, M. G. Quantum scheme for secret sharing based on local distinguishability. *Phys. Rev. A* **91,** 022330 (2015).
13. Bennett, C. H. *et al.* Quantum nonlocality without entanglement. *Phys. Rev. A* **59,** 1070 (1999).
14. Walgate, J., Short, A. J., Hardy, L. & Vedral, V. Local distinguishability of multipartite orthogonal quantum states. *Phys. Rev. Lett.* **85,** 4972 (2000).
15. Chen, P. X. & Li, C. Z. Distinguishing the elements of a full product basis set needs only projective measurements and classical communication. *Phys. Rev. A* **70,** 022306 (2004).
16. Duan, R. Y., Feng, Y., Ji, Z. F. & Ying, M. S. Distinguishing arbitrary multipartite basis unambiguously using local operations and classical communication. *Phys. Rev. Lett.* **98,** 230502 (2007).
17. Duan, R. Y., Feng, Y., Xin, Y. & Ying, M. S. Distinguishability of quantum states by separable operations. *IEEE Trans. Inf. Theory* **55,** 1320 (2009).
18. Duan, R., Xin, Y. & Ying, M. Locally indistinguishable subspaces spanned by three-qubit unextendible product bases. *Phys. Rev. A* **81** 032329 (2010).
19. Yu, N., Duan, R. & Ying, M. Any $2 \otimes n$ subspace is locally distinguishable. *Phys. Rev. A* **84,** 012304, (2011).
20. Yu, N., Duan, R. & Ying, M. Four locally indistinguishable ququad-ququad orthogonal maximally entangled states. *Phys. Rev. Lett.* **109** 020506 (2012).
21. Yang, Y. H., Gao, F., Tian, G. J., Cao, T. Q. & Wen, Q. Y. Local distinguishability of orthogonal quantum states in a $2 \otimes 2 \otimes 2$ system. *Phys. Rev. A* **88** 024301 (2013).
22. Nathanson, M. Three maximally entangled states can require two-way local operations and classical communication for local discrimination *Phys. Rev. A* **88,** 062316 (2013).
23. Zhang, Z. C., Feng, K. Q., Gao, F. & Wen, Q. Y. Distinguishing maximally entangled states by one-way local operations and classical communication. *Phys. Rev. A* **91,** 012329 (2015).
24. Yang, Y. H. *et al.* Bound on local unambiguous discrimination between multipartite quantum states. *Quant. Inf. Proc.* **14,** 731 (2015).
25. Yang, Y. H. *et al.* Characterizing unextendible product bases in qutrit-ququad system. *Sci. Rep.* **5,** 11963 (2015).
26. Hostens, E., Dehaene, J. & De Moor, B. Stabilizer states and Clifford operations for systems of arbitrary dimensions and modular arithmetic. *Phys. Rev. A* **71,** 042315 (2005).
27. Bae, J. & Kwek, L. C. Quantum state discrimination and its applications. *J. Phys. A: Math. Theor.* **48,** 083001 (2015).


## Acknowledgements

This work is supported by NSFC (Grant Nos 61272057, 61572081, 61402148), Beijing Higher Education Young Elite Teacher Project (Grant Nos YETP0475, YETP0477), Natural Science Foundation of Hebei Province (F2015205114).

## Author Contributions

Y.Y., F.G., X.W. and S.Q. initiated the idea. Y.Y., F.G., H.Z. and Q.W. wrote the main manuscript text and prepared table. All authors reviewed the manuscript.

## Additional Information

**Competing financial interests:** The authors declare no competing financial interests.

**How to cite this article**: Yang, Y.-H. *et al.* Quantum secret sharing via local operations and classical communication. *Sci. Rep.* **5**, 16967; doi: 10.1038/srep16967 (2015).

This work is licensed under a Creative Commons Attribution 4.0 International License. The images or other third party material in this article are included in the article's Creative Commons license, unless indicated otherwise in the credit line; if the material is not included under the Creative Commons license, users will need to obtain permission from the license holder to reproduce the material. To view a copy of this license, visit http://creativecommons.org/licenses/by/4.0/