Quantum scheme for secret sharing based on local distinguishability

Ramij Rahaman[1,2,3,*] and Matthew G. Parker[3,†]

[1]*Department of Mathematics, University of Allahabad, Allahabad-211002, U.P., India*
[2]*Institute of Theoretical Physics & Astrophysics, University of Gdańsk, 80-952 Gdańsk, Poland*
[3]*Department of Informatics, University of Bergen, Post Box 7803, 5020 Bergen, Norway*

(Received 22 May 2014; revised manuscript received 14 December 2014; published 20 February 2015)

In this paper, we analyze the (im)possibility of the exact distinguishability of orthogonal multipartite entangled states under *restricted local operation and classical communication*. Based on this local distinguishability analysis, we propose a quantum secret sharing scheme (which we call LOCC-QSS). Our LOCC-QSS scheme is quite general and cost efficient compared to other schemes. In our scheme, no joint quantum operation is needed to reconstruct the secret. We also present an interesting $(2,n)$-threshold LOCC-QSS scheme, where any two cooperating players, one from each of two disjoint groups of players, can always reconstruct the secret. This LOCC-QSS scheme is quite uncommon, as most (k,n)-threshold quantum secret sharing schemes have the restriction $k \geqslant \lceil \frac{n}{2} \rceil$.

DOI: 10.1103/PhysRevA.91.022330 PACS number(s): 03.67.Dd, 03.67.Mn, 03.67.Ac, 03.65.Ud

I. INTRODUCTION

Classical secret sharing (CSS) is a cryptographic protocol in which a dealer splits the secret and distributes shares to various shareholders. The secret can be reconstructed only when a sufficient number of shareholders cooperate with each other by sharing their individual parts of the secret. The CSS scheme was invented independently by Shamir [1] and Blakley [2] in 1979. The main drawback with all existing CSS schemes is that they are not perfectly secure from eavesdropper attack. To defeat the eavesdropper attack perfectly, Hillery *et al.* [3] and Cleve *et al.* [4] simultaneously presented the quantum secret sharing (QSS) scheme in 1999, whereas Żukowski *et al.* had previously mentioned this type of scheme in a different context [5]. In a (k,n)-threshold QSS scheme, the dealer encodes her secret (classical or quantum) within a multipartite quantum state then distributes the shares of the quantum state to n pairwise distant parties. Any group of k or more parties can collaboratively reconstruct the secret from their shares, while no group of fewer than k parties can.

Several works have considered the area of QSS [6–9]. Although these QSS schemes are secure, either they are very restricted or they require more than one particle measurement, i.e., joint quantum measurement, to reveal the secret. To perform a joint quantum operation, one must bring the relevant subsystems into one place, which is, practically, quite expensive due to high quantum noise for a large number of players. Recently, Fortescue *et al.* [10] and Gheorghiu *et al.* [11] proposed two different QSS schemes where they partially reduced the required quantum communication at the cost of some classical communication. Still, both of them required a number of large (joint) quantum operations to reveal the secret, especially in the multipartite scenario. To deal with this joint measurement problem completely, here we demonstrate a simple but very efficient construction of a perfect (k,n)-threshold quantum scheme for secret sharing based on only local quantum operations and classical communication (here called an LOCC-QSS scheme). In this paper we mainly concentrate on the implementation of classical secret sharing by quantum means. There are some works on QSS that deal with classical secrets, but they are quite restricted and have loopholes [12–14]. We encode our secret into several pairs of locally distinguishable orthogonal multipartite entangled states and distribute different particles to different parties depending on the context. Only a sufficient number of cooperating parties can distinguish these pairs of orthogonal entangled states by local operation and thereby reconstruct the secret as well. Another restriction for most (k,n)-threshold LOCC-QSS schemes is that they work only if $k \geqslant \lceil \frac{n}{2} \rceil$ [4,8]. In this context, we provide a restricted $(2,n)$-threshold LOCC-QSS scheme, where any two cooperating parties from two disjoint groups, taken over all parties, can always reconstruct the secret. This type of feature is quite uncommon and not present in the existing QSS schemes.

Our LOCC-QSS scheme protocol is largely based on local distinguishability of a pair of orthogonal entangled states so, before describing our LOCC-QSS scheme, we first discuss several local distinguishability problems that are relevant for our LOCC-QSS scheme. Then we present our LOCC-QSS scheme for various thresholds and also discuss how our scheme is perfectly secure from eavesdropper attack. We end with a conclusion.

II. LOCAL DISTINGUISHABILITY OF SYMMETRIC STATES

The question of local discrimination of a set of multipartite orthogonal states is as follows: a number of parties share a quantum system prepared in one of a known set of mutually orthogonal quantum states. The goal of all of the parties is to determine the state in which the quantum system was prepared using local operations and classical communication (LOCC) [15–17]. We now discuss several distinguishability problems related to an orthogonal pair of n-qubit

[*] ramijrahaman@gmail.com
[†] Matthew.Parker@ii.uib.no

symmetric states, i.e., Greenberger-Horne-Zeilinger (GHZ) [18] and Dicke [19] states, under *restricted local operation and classical communication* (rLOCC). Here, rLOCC means only a subset of the parties is allowed to communicate with each other.

A. Local distinguishability of GHZ states

The canonical representation of an $n(\geqslant 2)$-qubit GHZ state can be written as (up to a global phase and proper basis transformation)

$$|\,\mathrm{GHZ}(i_1,i_2,i_3,\ldots,i_n)\rangle_{123\ldots n} = \frac{1}{\sqrt{2}}[|\,0 i_2 i_3\ldots i_n\rangle + (-1)^{i_1}|\,1\overline{i_2}\overline{i_3}\ldots\overline{i_3}\rangle],$$

where $i_1,i_2,i_3,\ldots,i_n \in \{0,1\}$, and the bar over a bit value indicates its logical negation. For $n=2$, these states are generally known as *Bell states* or two-qubit maximally entangled states.

Let us define a pair of orthogonal distance-$r(0 \leqslant r \leqslant \lfloor \frac{n}{2} \rfloor)$, n-qubit GHZ states as follows:

$$\begin{aligned} |\mathrm{GHZ}\rangle &= \frac{1}{\sqrt{2}}[|\overbrace{000\ldots00}^{r}\overbrace{000\ldots00}^{n-r}\rangle + |111\ldots11111\ldots11\rangle], \\ |\,\mathrm{GHZ}\rangle_r &= \frac{1}{\sqrt{2}}[|\overbrace{111\ldots11}^{r}\overbrace{000\ldots00}^{n-r}\rangle - |000\ldots00111\ldots11\rangle], \end{aligned} \tag{1}$$

where r is a non-negative integer. If $r > \frac{n}{2}$, then we consider $n-r$ as the distance for the above pair (1).

Theorem 1. No orthogonal pair of distance-0 n-qubit GHZ states can be distinguished by any less than n cooperating parties.

Lemma 1. Classical communication is necessary to distinguish any pair of Bell states locally.

Proof. Without any loss of generality, let Alice and Bob share the following pair of Bell states:

$$|\Phi^{\pm}\rangle = \frac{1}{\sqrt{2}}[|0\rangle_A|0\rangle_B \pm |1\rangle_A|1\rangle_B]. \tag{2}$$

Their goal is to distinguish the above pair of Bell states by only local operations (LO) on their respective qubits and they are not allowed to communicate, classically, with each other.

Let Alice and Bob be spatially separated, and share the known Bell state $|\Phi^+\rangle$. Bob applies $\mathbb{I}$ or σ_z on his qubit to communicate the message 0 or 1, respectively, and the desired state may change to another orthogonal Bell state as

$$\begin{aligned} (\mathbb{I}^A \otimes \mathbb{I}^B)|\Phi^+\rangle &= \frac{1}{\sqrt{2}}[|0\rangle_A|0\rangle_B + |1\rangle_A|1\rangle_B], \\ (\mathbb{I}^A \otimes {\sigma_z}^B)|\Phi^+\rangle &= \frac{1}{\sqrt{2}}[|0\rangle_A|0\rangle_B - |1\rangle_A|1\rangle_B] = |\Phi^-\rangle. \end{aligned} \tag{3}$$

If Alice (alone) is able to distinguish the above pair without any communication from Bob, then she can recover Bob's message as well, which is impossible as that would imply signaling.[1] ■

Proof (*of Theorem 1*). Without any loss of generality, let us assume that the orthogonal GHZ pair of distance 0 can be distinguished by the first $m(<n)$ cooperative parties. A necessary condition for distinguishability of a pair of n-qubit states under m-cooperative LOCC (where m parties agree to do local operations on their respective qubit and share the measurement outcomes with each other) would be the following: *The pair of states should remain distinguishable when m out of n qubits are operated on jointly at one place, whereas the remaining* $(n-m)$ *qubits are kept at a different place and no classical communication is allowed between these two places*. Keeping the condition in mind, the first m qubits are kept in laboratory A and the remaining $(n-m)$ qubits are kept together in a different laboratory B. Under this arrangement, any given pair of kind (9), for a proper choice of basis, can be written in the following bipartite form:

$$\begin{aligned} |\mathrm{GHZ}\rangle &= \frac{1}{\sqrt{2}}[|0\rangle_A|0\rangle_B + |1\rangle_A|1\rangle_B], \\ |\mathrm{GHZ}\rangle_0 &= \frac{1}{\sqrt{2}}[|0\rangle_A|0\rangle_B - |1\rangle_A|1\rangle_B], \end{aligned} \tag{4}$$

which is equivalent to pair (2). Therefore, using Lemma 1, we conclude that without any classical communication between laboratory A and laboratory B, local distinguishability of the above pair is impossible. Hence, no less than n cooperating parties can distinguish a pair of orthogonal distance-0 GHZ states. ■

Theorem 2. An orthogonal pair of distance-$r(\geqslant 1)$ GHZ states (1) can always be exactly distinguished by any two cooperating LOCC parties, one from the first r and the other from the last $n-r$ parties.

Proof. The proof is very simple. Both cooperating parties (one from the first r and the other from the last $n-r$ parties) measure their own qubit in the computational basis (this is σ_z) locally, and if both of them get the same result, then their shared state was $|\mathrm{GHZ}\rangle$, otherwise the state was $|\mathrm{GHZ}\rangle_r$. ■

B. Local distinguishability of Dicke states

The n-qubit symmetric Dicke state of weight $m(1 \leqslant m < n)$ is defined by

$$|m,n\rangle = \frac{1}{\sqrt{\binom{n}{m}}}\left[\sum_{j=1}^{\binom{n}{m}} P_j(|1_1 1_2\ldots 1_m 0_{m+1}\ldots 0_n\rangle)\right], \tag{5}$$

where $\{P_j(|1_1 1_2\ldots 1_m 0_{m+1}\ldots 0_n\rangle)\}$ is the set of all possible distinct permutations of m 1's and $n-m$ 0's [20]. For $m=1$,

[1] No message can travel faster than the speed of light in a vacuum.

the state given in (5) is generally called an n-qubit W state. Let us define the n-qubit generalized Dicke state of weight $m(1 \leqslant m < n)$ by

$$|m,n\rangle_G = \sum_{j=1}^{\binom{n}{m}} c_j P_j(|1_1 1_2 \ldots 1_m 0_{m+1} \ldots 0_n\rangle), \tag{6}$$

where $\sum |c_j|^2 = 1$. We define the weight difference between two n-qubit Dicke states as the distance[2] between them. For our purpose, the distance r is less or equal to $n-2$. An orthogonal pair of distance-$r(0 \leqslant r \leqslant n-2)$ generalized Dicke states of n qubit can be written (under appropriate basis transformation) as

$$\begin{aligned} |m,n\rangle_G &= \sum_{j=1}^{\binom{n}{m}} c_j P_j(|1_1 1_2 \ldots 1_m 0_{m+1} \ldots 0_n\rangle), \\ |m+r,n\rangle_G &= \sum_{j=1}^{\binom{n}{m+r}} c'_j P_j(|1_1 1_2 \ldots 1_{m+r} 0_{m+r+1} \ldots 0_n\rangle) \\ &\text{with} \quad 0 \leqslant r \leqslant n-2, \end{aligned} \tag{7}$$

where $0 < (m+r) < n$ and $\sum_{j=1}^{\binom{n}{m}} |c_j|^2 = \sum_{j=1}^{\binom{n}{m+r}} |c'_j|^2 = 1$. For $r = 0$, $\sum_{j=1}^{\binom{n}{m}} c_j^* c'_j = 0$.

Theorem 3. No less than $n-r+1$ cooperating parties can perfectly distinguish any pair of orthogonal n-qubit generalized Dicke states (7) of distance r $(0 < r \leqslant n-2)$.

Proof. Without loss of generality, let us assume that the first $k(<n-r+1)$ cooperating parties can perfectly distinguish the pair of orthogonal n-qubit generalized Dicke states (7) of distance r $(0 < r \leqslant n-2)$. Distinguishing these states by the first k cooperating parties implies distinguishing them with respect to the bipartition $(1,2,\ldots,k)$ vs $(k+1,k+2,\ldots,n)$ by local operation (LO) only (without any classical communication between these two partitions). Keeping this in mind, we put the first k qubits in laboratory A and the remaining $(n-k)$ qubits in laboratory B. Under this arrangement, any given pair of type (7), for a proper choice of basis, reduces to the form

$$\begin{aligned} |m,n\rangle_G &= \sum_{i,j} a_{ij} |e_i\rangle_A |e_j\rangle_B, \\ |m+r,n\rangle_G &= \sum_{i,j} a'_{ij} |e_i\rangle_A |e_j\rangle_B, \end{aligned} \tag{8}$$

where $\sum_{i,j} |a_{ij}|^2 = 1 = \sum_{i,j} |a'_{ij}|^2$ and $\{|e_i\rangle_{A(B)}\}$ is an orthonormal basis associated with the joint subsystem $A(B)$. For any $r > 0$, $a_{ij} a'_{ij} = 0 \forall i,j$. Let us define two subspaces of the Hilbert space $\mathcal{H}_A$ (associated with the first joint subsystem A), $\mathcal{S}_m = \{|e_i\rangle_A;\ \text{if}\ \exists j s.t. a_{ij} \neq 0\}$ and $\mathcal{S}_{m+r} = \{|e_i\rangle_A;\ \text{if}\ \exists j s.t. a'_{ij} \neq 0\}$. The proof of Theorem 3 follows immediately from Lemma 2, stated below.

Lemma 2. The pair of orthogonal bipartite states (8) can be perfectly distinguished under LO only if $\mathcal{S}_m \perp \mathcal{S}_{m+r}$ i.e., $a_{ij} a'_{il} = 0 \forall i,j,l$.

We now show that $\mathcal{S}_m \not\perp \mathcal{S}_{m+r}$ for the pair (8) if $k < n-r+1$. Let us first assume that $k \leqslant m$. Then the product term $|e_{i^*}\rangle_A = |1_1 1_2 \ldots 1_k\rangle_A \in \mathcal{S}_m \bigcap \mathcal{S}_{m+r}$ for some $i^* \in \{i\}$. Similarly, for $m < k(<n-r+1)$, the product term $|e_{j^*}\rangle_A = |1_1 1_2 \ldots 1_m 0_{m+1} 0_{m+2} \ldots 0_k\rangle_A \in \mathcal{S}_m$ for some $j^* \in \{i\}$. Since $k < n-r+1$, i.e., $k - m \leqslant n-m-r$, therefore $|e_{j^*}\rangle_A \in \mathcal{S}_{m+r}$ as well. Hence, $\mathcal{S}_m \not\perp \mathcal{S}_{m+r}$ if $k < n-r+1$. This completes the proof. ■

Corollary 1. Any $(n-r+1)$ cooperating parties can always perfectly distinguish any pair of orthogonal n-qubit generalized Dicke states (7) of distance $r(>0)$.

Proof. If the combined subsystem A, mentioned in the proof of Theorem 3, contains $(n-r+1)$ qubits, then all the a_{ij}'s and a'_{ij}'s given in (8) satisfy $a_{ij} a'_{il} = 0, \forall i,j,l$. The proof then follows immediately from Lemma 2. ■

Corollary 2. Any pair of orthogonal n-qubit generalized Dicke states (7) of distance 0 can be perfectly distinguished iff all of the n parties cooperate with each other.

Proof. Proof of the sufficiency part follows from the result that *two orthogonal states of any quantum system, shared in any proportion between any number of separated parties, can be perfectly distinguished*, as proven in Ref. [15]. The necessary part follows from Lemma 2, as in this case all of the a_{ij}'s and a'_{ij}'s given in (8) satisfy the relation $a_{ij} a'_{ij} \neq 0, \forall i,j$, for all $k < n$. ■

III. QUANTUM SCHEME FOR SECRET SHARING (LOCC-QSS)

Suppose Alice wants to share a key between n separated parties. The sender is Alice and the receivers are $\text{Bob}_1, \text{Bob}_2, \ldots, \text{Bob}_n$, and only k or more of the receivers may cooperate to recover the key, i.e., we have a (k,n)-threshold secret sharing scheme. To implement this scheme, Alice does the following steps:

Step 1 (S1). Alice first prepares a large number (say $L > n$) of states chosen randomly from a specified pair of orthogonal n-qubit entangled states 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*.[3] 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 qubits of a prepared state $|S(a,b_t)\rangle$ at time t.

Step 2 (S2). In order to prevent the eavesdropper Eve or less than k dishonest Bob_i from learning the secret, Alice now prepares, at random, a different sequence, $r_i = \Pi_i(1,2,3,\ldots,L)$, for each Bob_i, and sends the i_tth qubit $(i = 1,2,\ldots,n;\ t = 1,2,\ldots,L)$ to Bob_i according to the r_i sequence order, where Π_i is an arbitrary permutation of the sequence $(1,2,3,\ldots,L)$. Note that Alice only sends the qubits and not the information about Π_i. Hence, except Alice, no one has the information about Π_i. It is also interesting to note that the lth qubit of r_i and the lth qubit from r_j in general may not be associated with the same entangled state, $|S(a,b_t)\rangle$, as $r_i \neq r_j$, for $i \neq j$. After receiving their associated sequence of qubits (i.e., r_i for the ith party), all of

[2] Like the GHZ case, here also the distance is nothing else but the Hamming distance between the strings of bits of the two corresponding Dicke states.

[3] Run t is associated with the prepared state $|S(a,b_t)\rangle$ at time t.

the receivers now share L n-qubit entangled states $|S[a,r(b_t)]\rangle$. Here, $r(b_t) = [\Pi_1(t),\Pi_2(t),\ldots,\Pi_n(t)]$. Only Alice has any information about $|S[a,r(b_t)]\rangle$.

Step 3 (S3). Alice now randomly selects some run, say $\{t_j\}_{j=1}^{u} (\subset \{1,2,\ldots,L\})$, and also computes n arbitrarily chosen permutations, p_i of $\{1,2,\ldots,u\}$, only known to herself. She then prepares list $C_i = \{[\sigma_i(t_{p_i(j)}),\Pi_i(t_{p_i(j)})]\}_{j=1}^{u}$ for Bob$_i$ (for $i = 1,2,\ldots,n$) and sends it to him. It is important to mention that Alice starts to send lists C_i only if all of the receivers confirm the receipt of all their L qubits.

After receiving the list C_i, Bob$_i$ measures his $\Pi_i(t_{p_i(j)})$th qubit in the $\sigma_i(t_{p_i(j)})$ basis and sends the measurement outcome $v_i(t_{p_i(j)})$ to Alice. The details of measurement settings $\sigma_i(t_j)$ are discussed later, case by case.

Step 4 (S4). By analyzing the measurement results and associated measurement settings, Alice can easily detect the eavesdropper and, if there is one, she aborts the protocol and starts again with a new set of resources.

Step 5 (S5). If no eavesdropper is detected, Alice announces, to the respective parties, all qubit positions of an unmeasured state $|S[a,r(b_t)]\rangle$. Alice selects this $|S[a,r(b_t)]\rangle$ according to her secret $a(=0/1)$. The mapping between classical bit value and orthogonal entangled pair is fixed and is communicated, securely, 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 $|S[a,r(b_t)]\rangle$.

We now discuss, in detail, the choice of measurements (i.e., S3 and S4) and the choice of states (S1) for different threshold scenarios.

A. The (n,n)-threshold LOCC-QSS scheme

S1. Alice prepares the states, each chosen at random from a pair of distance-0 orthogonal n-qubit GHZ states,

$$\begin{aligned}|\mathrm{GHZ}\rangle &= \frac{1}{\sqrt{2}}[|000\ldots00\rangle + |111\ldots11\rangle],\\ |\mathrm{GHZ}\rangle_0 &= \frac{1}{\sqrt{2}}[|000\ldots00\rangle - |111\ldots11\rangle].\end{aligned} \tag{9}$$

S3. In order to fix the choice of measurement for a selected run from $\{t_s\}_{s=1}^{u}$, Alice randomly chooses an n-tuple binary vector $\mathcal{O}_{t_s}$ from

$$\begin{aligned}\{\mathcal{O}\} \equiv \{\mathcal{O}(0) = (0_1 0_2 0_3 0_4 \ldots 0_n)\} \bigcup \{\mathcal{O}(ij) = \mathcal{O}(ji)\\ = (0_1 0_2 \ldots 0_{i-1} 1_i 0_{i+1} \ldots 0_{j-1} 1_j 0_{j+1} \ldots 0_n); \forall i \neq j\},\end{aligned}$$

and, for the $t_{p_i(s)}$th run from the list $C_i = \{[\sigma_i(t_{p_i(s)}),\Pi_i(t_{p_i(s)})]\}_{s=1}^{u}$, either selects observable $\sigma_i(t_{p_i(s)}) = \sigma_x = \left(\begin{smallmatrix}0 & 1\\ 1 & 0\end{smallmatrix}\right)$ or observable $\sigma_i(t_{p_i(s)}) = \sigma_y = \left(\begin{smallmatrix}0 & -i\\ i & 0\end{smallmatrix}\right)$, depending on whether the ith bit value of the binary vector $\mathcal{O}_{t_s}$ is 0 or 1, respectively. Here, $\mathcal{O}_{t_s}$ refers both to the binary vector and to its associated local operator. Alice now sends list C_i to Bob$_i$, and 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 for all such $[\sigma_i(t_{p_i(s)}),\Pi_i(t_{p_i(s)})] \in C_i$.

The elements of $\{\mathcal{O}\}$ are the stabilizers[4] (or antistabilizers) of the pair of states given in (9) and they satisfy the following eigenvalue relation:

$$\mathcal{O}_{t_s}\big|S\big[a,r\big(b_{t_{p(s)}}\big)\big]\big\rangle = \lambda(a,t_s)\big|S\big[a,r\big(b_{t_{p(s)}}\big)\big]\big\rangle, \quad \forall \mathcal{O}_{t_s} \in \{\mathcal{O}\}, \tag{10}$$

where $\lambda(a,t_s)$ is an eigenvalue with $\lambda(a,t_s) \in \{\pm 1\}$ 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 outcomes $v_i(t_{p_i(s)})$ for the observable $\mathcal{O}_{t_s}$ must be equal to the corresponding eigenvalue for the state $|S[a,r(b_{t_{p(s)}})]\rangle$ i.e., $\lambda(a,t_s) = \Pi_{i=1}^{n} v_i(t_{p_i(s)})$.

S4. For each selected run t_s, Alice checks whether or not the products of local results satisfy the corresponding eigenvalue equation:

$$\mathcal{O}_{t_s}|\mathrm{GHZ}\rangle = \begin{cases} +1|\mathrm{GHZ}\rangle & \text{if} \quad \mathcal{O}_{t_s} = \mathcal{O}(0)\\ -1|\mathrm{GHZ}\rangle & \text{otherwise,}\end{cases} \quad \text{and} \quad \mathcal{O}_{t_s}|\mathrm{GHZ}\rangle_0$$

$$= \begin{cases} -1|\mathrm{GHZ}\rangle_0 & \text{if} \quad \mathcal{O}_{t_s} = \mathcal{O}(0)\\ +1|\mathrm{GHZ}\rangle_0 & \text{otherwise.}\end{cases}$$

This protocol is secure in two ways. First, the eavesdropper does not have any information about the sequence of qubits, so she cannot create a measurement outcome to satisfy all of the above relations. Second, the above relations hold specifically for unique states (up to local unitary equivalence), so the action of an eavesdropper at any stage will be detected, as this uniqueness will be compromised.

Theorem 1 tells us that the pair (9) can only be distinguished if all parties cooperate, otherwise the secret key cannot be recovered.

Example 1. In a (3,3)-threshold LOCC-QSS scheme, the desired pair of the states which Alice prepares in step S1 is

$$\begin{aligned}|\mathrm{GHZ}\rangle &= \frac{1}{\sqrt{2}}[|000\rangle + |111\rangle],\\ |\mathrm{GHZ}\rangle_0 &= \frac{1}{\sqrt{2}}[|000\rangle - |111\rangle],\end{aligned} \tag{11}$$

and the set of 3-tuple binary vectors for step S3 is

$$\begin{aligned}\{\mathcal{O}\} &\equiv \{\mathcal{O}(0),\mathcal{O}(12),\mathcal{O}(13),\mathcal{O}(23)\}\\ &\equiv \{(0_1 0_2 0_3),(1_1 1_2 0_3),(1_1 0_2 1_3),(0_1 1_2 1_3)\}\\ &\equiv \{\sigma_x\sigma_x\sigma_x,\sigma_y\sigma_y\sigma_x,\sigma_y\sigma_x\sigma_y,\sigma_x\sigma_y\sigma_y\}.\end{aligned} \tag{12}$$

(i) Alice prepares L number of states chosen randomly from the pair (11).

(ii) Alice now prepares, at random, three different $r_i = \Pi_i(1,2,3,\ldots,L)$, $i = 1,2,3$, for each Bob$_i$, and sends the i_tth qubit ($i = 1,2,3$; $t = 1,2,\ldots,L$) to Bob$_i$ according to the r_i sequence order, where Π_i is an arbitrary permutation of the sequence $(1,2,3,\ldots,L)$.

(iii) Alice randomly selects some run, say $\{t_s\}_{s=1}^{u} (\subset \{1,2,\ldots,L\})$, and also computes three arbitrarily chosen permutations, p_i of $\{1,2,\ldots,u\}$, 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 Bob$_i$ (for $i = 1,2,3$) and sends it to him. Here, $(t_{p_1(s)} t_{p_2(s)} t_{p_3(s)}) \in \{\mathcal{O}\}$,

[4] $\mathcal{O}$ is called a stabilizer (antistabilizer) of the state $|\Psi\rangle$ if $\mathcal{O}|\Psi\rangle = +(-)|\Psi\rangle$.

given in (12), for $s = 1,2,\ldots,u$. Therefore, if $t_{p_i(s)} = 0$ for some $i = 1,2,3$, and $s = 1,2,\ldots,u$, then the corresponding observable $\sigma_i(t_{p_i(s)}) = \sigma_x$, and if $t_{p_i(s)} = 1$, then $\sigma_i(t_{p_i(s)}) = \sigma_y$.

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 $v(t_{p_i(s)})$ to Alice.

(iv) Alice checks whether or not the product of local results $\lambda(a,t_s) = v(t_{p_1(s)})v(t_{p_2(s)})v(t_{p_3(s)})$ satisfies the corresponding eigenvalue equation (10) for each selected run t_s with $O_{t_s} = [\sigma_1(t_{p_1(s)})\sigma_2(t_{p_2(s)})\sigma_3(t_{p_3(s)})]$ and $r(b_{t_{p(s)}}) = [\Pi_1(t_{p_1(s)}),\Pi_2(t_{p_2(s)}),\Pi_3(t_{p_3(s)})]$ $\forall s = 1,2,\ldots,u$. If $|S[a,r(b_{t_{p(s)}})]\rangle = |\mathrm{GHZ}\rangle$, then

$$\lambda(a,t_s) = \begin{cases} +1 & \text{if} \quad \mathcal{O}_{t_s} = \mathcal{O}(0) \\ -1 & \text{otherwise,} \end{cases}$$

and if $|S[a,r(b_{t_{p(s)}})]\rangle = |\mathrm{GHZ}\rangle_0$, then

$$\lambda(a,t_s) = \begin{cases} -1 & \text{if} \quad \mathcal{O}_{t_s} = \mathcal{O}(0) \\ +1 & \text{otherwise.} \end{cases}$$

By analyzing the measurement results and associated measurement settings, Alice can easily detect the eavesdropper and, if there is one, she aborts the protocol and starts again with a new set of resources.

(v) If no eavesdropper is detected, then Alice announces, to the respective parties, all qubit positions of an unmeasured state $|S[a,r(b_t)]\rangle$. Alice selects this $|S[a,r(b_t)]\rangle$ according to her secret $a(=0/1)$, e.g., $|\mathrm{GHZ}\rangle_0$ represents the secret $a = 0$ and $|\mathrm{GHZ}\rangle$ represents $a = 1$.

Now, according to Theorem 1, cooperation from all three parties is necessary to distinguish the pair (11). Hence, to recover the secret, all three parties need to cooperate.

B. The restricted $(2,n)$-threshold LOCC-QSS scheme

S1. Alice prepares the states, each chosen at random from a pair of distance-r orthogonal n-qubit GHZ states, as given in Eq. (1).

S3. Same as step S3 described in Sec. III A.

S4. The product of local results of each measurement satisfies the following eigenvalue relations:

$$\mathcal{O}_{t_s}|\mathrm{GHZ}\rangle = \begin{cases} +1|\mathrm{GHZ}\rangle & \text{if} \quad \mathcal{O}_{t_s} = \mathcal{O}(0) \\ -1|\mathrm{GHZ}\rangle & \text{otherwise,} \end{cases}$$

$$\mathcal{O}_{t_s}|\mathrm{GHZ}\rangle_r = \begin{cases} +1|\mathrm{GHZ}\rangle_r & \text{if} \quad \mathcal{O}_{t_s} = \mathcal{O}(ij) \quad \text{with} \quad i,j \leqslant r, \quad \forall i \neq j, \\ & \qquad\qquad\qquad\qquad\quad \text{or} \quad i,j \geqslant r, \quad \forall i \neq j, \\ -1|\mathrm{GHZ}\rangle_r & \text{otherwise.} \end{cases}$$

Here, also, the above relations uniquely define the states and hence the protocol is secure in the same two ways as described in Sec. III A.

According to Theorem 2, any two cooperating parties, i.e., one from the first r parties and the other from the remaining $n-r$ parties, can distinguish the pair (1) perfectly. Hence, they are also able to recover the key.

Example 2. In a restricted (2,3)-threshold LOCC-QSS scheme, the desired pair of the states which Alice prepares in step S1 can be

$$|\mathrm{GHZ}\rangle = \frac{1}{\sqrt{2}}[|000\rangle + |111\rangle], \quad |\mathrm{GHZ}\rangle_1 = \frac{1}{\sqrt{2}}[|110\rangle - |011\rangle], \tag{13}$$

and the set of 3-tuple binary vectors for step S3 is given in (12). The rest of the steps are similar to those mentioned in the previous example of a (3,3)-threshold LOCC-QSS scheme in Example 1, except for some technical points in step (iv):

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

$$\lambda(a,t_s) = \begin{cases} +1 & \text{if} \quad \mathcal{O}_{t_s} = \mathcal{O}(0) \\ -1 & \text{otherwise,} \end{cases}$$

and if $|S[a,r(b_{t_{p(s)}})]\rangle = |\mathrm{GHZ}\rangle_1$, then

$$\lambda(a,t_s) = \begin{cases} +1 & \text{if} \quad \mathcal{O}_{t_s} = \mathcal{O}(ij) \quad \text{with} \quad i \neq j, \quad \text{and} \quad i,j \geqslant 1, \\ -1 & \text{otherwise.} \end{cases}$$

According to Theorem 2, the first party and any one from the other two parties can distinguish the pair (13) perfectly and, consequently, they are also able to decode the key.

C. The (k,n)-threshold LOCC-QSS scheme

S1. Alice prepares the states, each chosen at random from a pair of distance-$r(>0)$ orthogonal n-qubit Dicke states, as given in Eq. (7), with $c_j = c$ and $c_i' = c'$ both fixed real constants. Note that we already discussed the (n,n)-threshold LOCC-QSS scheme in Sec. III A, so here we consider the case when $k < n$.

S3. All n-qubit Dicke states $|m,n\rangle$ given in Eq. (5) are eigenstates of $\sigma_z^{\otimes n}$ with eigenvalue $(-1)^m$, where $\sigma_z = \begin{pmatrix}1 & 0\\ 0 & -1\end{pmatrix}$. For even n, the Dicke state $|\frac{n}{2},n\rangle$ is also an eigenstate of $\sigma_x^{\otimes n}$ and $\sigma_y^{\otimes n}$ with eigenvalue 1 [21]. Therefore, if n is even, Alice chooses (for more security) the pair of states such that the pair contains the state $|\frac{n}{2},n\rangle$.

To detect an eavesdropper for a (k,n)-threshold LOCC-QSS scheme with even n, Alice chooses (randomly) the same measurement settings [i.e., $\sigma_1(t_{p_1(s)}) = \sigma_2(t_{p_2(s)}) = \cdots = \sigma_n(t_{p_n(s)})$] from $\{\sigma_x,\sigma_y,\sigma_z\}$ for all Bob$_i$ for the run t_s, whereas for odd n, Alice prepares L, $(n+1)$-qubit states $|S(a,b_t)\rangle$ instead of n-qubit states. She keeps one qubit from each of $|S(a,b_t)\rangle$ and behaves like player Bob$_{(n+1)}$ from steps S2 to S4. But she does not take any part to reveal the key (secret), i.e., in step S5.

S4. If there is no eavesdropping, then the product of all local measurement results must satisfy the following eigenvalue relations:

$$\begin{aligned} \sigma_z\sigma_z\ldots\sigma_z|m,n\rangle &= (-1)^m|m,n\rangle, \\ \sigma_x\sigma_x\ldots\sigma_x\left|\frac{n}{2},n\right\rangle &= \left|\frac{n}{2},n\right\rangle \quad \text{(when } n \text{ is even)}, \qquad (14) \\ \sigma_y\sigma_y\ldots\sigma_y\left|\frac{n}{2},n\right\rangle &= \left|\frac{n}{2},n\right\rangle \quad \text{(when } n \text{ is even)}. \end{aligned}$$

Note that if one of the Dicke states in the pair (7) is of the form $|\frac{n}{2},n\rangle$, then we have the restriction $r < \frac{n}{2}$ and all three conditions of (14) are useful to detect eavesdropping, whereas in the other case,[5] the security depends only on the first condition of (14). According to Theorem 3, to distinguish the pair (7) perfectly, cooperation between $k = n - r + 1$ or more parties is necessary and, thus, the secret key is only revealed if $k \geqslant \lceil\frac{n}{2}\rceil$ or more parties cooperate. If $|\frac{n}{2},n\rangle$ is one of the states, then the desired condition becomes $k > \frac{n}{2} + 1$.

Example 3. The (5,6) threshold is a nontrivial case of a (k,n)-threshold LOCC-QSS protocol where one of the states of the desired pair is of the form $|\frac{n}{2},n\rangle$. In this (5,6)-threshold scheme, the pair of states which Alice prepares in step S1 is

$$\begin{aligned} |1,6\rangle &= \frac{1}{\sqrt{6}}[|100000\rangle + |010000\rangle + |001000\rangle \\ &\quad + |000100\rangle + |000010\rangle + |000001\rangle], \qquad (15) \\ |3,6\rangle &= \frac{1}{\sqrt{20}}\left[\sum P(|111000\rangle)\right], \end{aligned}$$

and the set of 6-tuple observables for step S3 is given by $\{\mathcal{O}\} = \{\sigma_x\sigma_x\sigma_x\sigma_x\sigma_x\sigma_x, \sigma_y\sigma_y\sigma_y\sigma_y\sigma_y\sigma_y, \sigma_z\sigma_z\sigma_z\sigma_z\sigma_z\sigma_z\}$. The rest of the steps are similar, with four parties instead of three parties, as mentioned in the previous two examples except the step (iv):

(iv) Here, if $|S[a,r(b_{t_{p(s)}})]\rangle = |1,6\rangle$, then

$$\lambda(t_s) = -1 \quad \text{if} \quad \mathcal{O}_{t_s} = \sigma_z\sigma_z\sigma_z\sigma_z\sigma_z\sigma_z,$$

and if $|S[a,r(b_{t_{p(s)}})]\rangle = |3,6\rangle$, then

$$\lambda(a,t_s) = +1, \forall \mathcal{O}_{t_s} \in \{\mathcal{O}\}.$$

Therefore, in virtue of Theorem 3, we conclude that any five of the six parties can reconstruct the secret.

IV. CONCLUSION

In this paper, we explore various interesting cases of quantum secret sharing schemes based on local distinguishability of orthogonal multipartite entangled states. To reconstruct the secret, a group of single-qubit quantum operations is sufficient for our schemes. Therefore, our schemes are cost efficient as well as quite competent compared to other existing QSS schemes, where several multiparty quantum operations are required to reveal the secret. Multipartite joint quantum operations are fairly expensive when the individual parties are in different places and the quantum cost increases exponentially as the number of parties increases. We also demonstrate an unusual $(2,n)$-threshold scheme where the set of players is partitioned into two disjoint groups and where the key can be recovered if any two players cooperate, on condition that the two players do not belong to the same group. This setup is quite nonstandard for a quantum secret sharing scheme and we hope that this result will encourage researchers to develop the field further.

ACKNOWLEDGMENTS

We thank Marek Żukowski for stimulating discussions. R.R. acknowledges financial support from the Norwegian Research Council while at UiB. R.R. also acknowledges partial support by the Foundation for Polish Science (FNP) TEAM/2011-8/9 project co-financed by the EU European Regional Development Fund, ERC grant QOLAPS (Grant No. 291348), and UGC (University Grants Commission, Govt. of India) Start-Up Grant.

[5] That is, pair (7) does not contain a state of the form $|\frac{n}{2},n\rangle$.

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

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

[3] M. Hillery, V. Bužek, and A. Berthiaume, Quantum secret sharing, Phys. Rev. A **59**, 1829 (1999).

[4] R. Cleve, D. Gottesman, and H.-K. Lo, How to share a quantum secret, Phys. Rev. Lett. **83**, 648 (1999).

[5] M. Żukowski, A. Zeilinger, M. A. Horne, and H. Weinfurter, Quest for GHZ states, Acta Phys. Pol. A **93**, 187 (1998).

[6] D. Gottesman, Theory of quantum secret sharing, Phys. Rev. A **61**, 042311 (2000).

[7] A. C. A. Nascimento, J. Mueller-Quade, and H. Imai, Improving quantum secret-sharing schemes, Phys. Rev. A **64**, 042311 (2001).

[8] S. Kumar 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. Theory **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] Z.-J. Zhang and Z.-X. Man, Multiparty quantum secret sharing of classical messages based on entanglement swapping, Phys. Rev. A **72**, 022303 (2005).

[13] S. Lin, F. Gao, F.-Z. Guo, Q.-Y. Wen, and F.-C. Zhu, Comment on Multiparty quantum secret sharing of classical messages based on entanglement swapping, Phys. Rev. A **76**, 036301 (2007).

[14] Z.-J. Zhang and Z.-X. Man, Reply to Comment on Multiparty quantum secret sharing of classical messages based on entanglement swapping, Phys. Rev. A **76**, 036302 (2007).

[15] J. Walgate, A. J. Short, L. Hardy, and V. Vedral, Local distinguishability of multipartite orthogonal quantum states, Phys. Rev. Lett. **85**, 4972 (2000).

[16] S. Ghosh, G. Kar, A. Roy, A. Sen(De), and U. Sen, Distinguishability of Bell states, Phys. Rev. Lett. **87**, 277902 (2001).

[17] S. Bandyopadhyay, S. Ghosh, and G. Kar, LOCC distinguishability of unilaterally transformable quantum states, New J. Phys. **13**, 123013 (2011).

[18] D. M. Greenberger, M. A. Horne, and A. Zeilinger, in *Bell's Theorem, Quantum Theory, and Conceptions of the Universe*, edited by M. Kafatos (Kluwer, Dordrecht, 1989).

[19] R. Dicke, Coherence in spontaneous radiation processes, Phys. Rev. **93**, 99 (1954).

[20] D. Li, X. Li, H. Huang, and X. Li, Stochastic local operations and classical communication properties of the n-qubit symmetric Dicke states, Europhys. Lett. **87**, 20006 (2009).

[21] C. D. Cenci, D. W. Lyons, L. M. Snyder, and S. N. Walck, Symmetric states: Local unitary equivalence via stabilizers, Quantum Inf. Comput. **10**, 1029 (2010).