Information locking and its resource-efficient extraction

Suchetana Goswami[1,2,*] and Saronath Halder[1,†]

[1]*Centre for Quantum Optical Technologies, Centre of New Technologies, University of Warsaw, Banacha 2c, 02-097 Warsaw, Poland*

[2]*Harish-Chandra Research Institute, A CI of Homi Bhabha National Institute, Chhatnag Road, Jhunsi, Allahabad 211 019, India*

(Received 3 November 2022; accepted 21 June 2023; published 6 July 2023)

Locally indistinguishable states are useful to distribute information among spatially separated parties such that the information is locked. This implies that the parties are not able to extract the information completely via local operations and classical communication (LOCC), while it might be possible via LOCC when the parties share entanglement. In this work, we consider an information distribution protocol using orthogonal states for $m \geqslant 3$ spatially separated parties such that even if any $k \leqslant (m-1)$ parties collaborate still the information cannot be revealed completely. Such a protocol is useful to understand up to what extent the encoded information remains locked. However, if required, the parties can share entanglement and extract the information completely by LOCC. To make the process resource efficient, it should consume less number of entangled states. We show that though the set of states, which are locally indistinguishable across every bipartition, are sufficient for the above protocol, they may consume a higher number of entangled states when aiming for complete information extraction. We establish this by constructing a class of locally indistinguishable sets of orthogonal states which can be employed to accomplish the above protocol and these sets consume less number of entangled states, compared with the former sets, for complete information extraction. In fact, this difference in the number of required entangled states for complete information extraction grows linearly with the number of parties. This study sheds light on suitable use of local indistinguishability property of quantum states as a resource, and thus we demonstrate an efficient way of information distribution.

DOI: 10.1103/PhysRevA.108.012405

I. INTRODUCTION

Distinguishing quantum states [1–4] is one of the key steps in many information processing protocols. Such a step can be thought of in the following way: Suppose a quantum system is prepared in an unknown state, but the state is taken from a known set. The goal is to identify the state of the quantum system. If the states of the known set are pairwise orthogonal to each other, then, in principle, it is possible to identify the state of the system perfectly by performing an appropriate measurement on the whole system. On the other hand, nonorthogonal states cannot be distinguished perfectly [5].

We assume that a composite quantum system is distributed among several spatially separated parties and the parties are restricted to perform local quantum operations and classical communication (LOCC) only. In such a situation, it may not always be possible to identify the state of the system perfectly even though the states of the known set are orthogonal to each other [6–18]. For a given set, if it is not possible to identify the state of the system perfectly then the set is said to be a locally indistinguishable set, otherwise, the set is distinguishable. Locally indistinguishable sets find applications in data hiding [19–22], secret sharing [23,24], etc.

In this work, we consider an information distribution task and ask which type of locally indistinguishable sets are appropriate to complete the task. In this context, we keep in our mind that local indistinguishability of quantum states is a resource and one should use it suitably. Anyway, the task can be described in the following manner: Suppose there is a referee who wishes to distribute an N-level classical information among m spatially separated parties, $N > 2$ and $m \geqslant 3$. But this should be done in such a way that, even if certain number of parties k, $2 \leqslant k \leqslant (m-1)$, collaborate, the information is not revealed completely. These collaborating parties are allowed to perform joint measurements on their subsystems and the rest of the parties stand alone, i.e., they are only allowed to perform measurements on their own subsystems. But to make strategies, any sequence of classical communication is allowed among the parties. However, if required, then there must be a way such that the parties can extract the information completely by sharing entangled states as resource among them along with LOCC. Now, sharing entanglement among spatially separated parties is always a difficult job to implement. Therefore, the referee should try to accomplish the task in a way that consumption of entangled states can be reduced for complete information extraction when required. Here comes the role of suitably using local indistinguishability of quantum states as resource.

We note that one way to implement the collaboration among some parties is to allow them to share classical communication (CC) while the noncollaborating parties do not use CC. To beat any such collaboration, here we allow the collaborating parties to use joint measurements. Thus, we basically are in search of robust information distribution

*suchetana.goswami@gmail.com
†saronath.halder@gmail.com

protocol. Clearly, such a protocol is also useful to understand up to what extent the privacy of the encoded information remains intact.

Implementing the above task might be easier if we drop the condition that one has to reduce the consumption of entangled states for complete information extraction (we say this condition as "resource-efficient" condition). A quick solution is given as follows: We consider a set of N orthogonal pure m-partite states. The classical information is encoded against the states of the set. We also assume that the set is locally indistinguishable across every bipartition. [For sets which have local indistinguishability across bipartition(s), one can go through the Refs. [18,25–34] and the references therein.] Such a set is always sufficient for the implementation of the present task. Here the orthogonality is to preserve the condition that there must be a way for complete information extraction when it is required. Now, given a set of orthogonal quantum states, if the states cannot be perfectly distinguished by LOCC across every bipartition, then these states must also not be perfectly distinguished by LOCC in any multipartition. So, for such a set, it does not matter how many parties are collaborating, in the newly produced partition the set always remains locally indistinguishable and thus the information encoded against the states of the set cannot be extracted completely. Probably, we are now ready to rephrase the main question which is addressed in this work: Is it possible to find more suitable sets to implement the present task compared with the sets which are locally indistinguishable across every bipartition? This question is particularly important when we do not drop the resource-efficient condition.

The answer to the above question is not obvious. In fact, when the number of parties is three, the sets which can be used to accomplish the present task are indeed locally indistinguishable across every bipartition. This can be understood in the following way: Suppose, there are three parties A, B, and C. Then, in this case the only value of k is two. So, if any two of the three parties collaborate, then the partitions, which are produced due to collaboration, are $A-BC$, $B-AC$, and $C-AB$. Again, in a tripartite system these are the only possible bipartitions. Therefore, the tripartite sets of orthogonal states which are locally indistinguishable across the aforesaid bipartitions are indeed locally indistinguishable across every bipartition.

Nevertheless, when the number of parties increases, i.e., $m \geqslant 4$, it is possible to show that there are sets which are not only sufficient to accomplish the present task but they may also be resource-efficient compared with the sets which are locally indistinguishable across every bipartition. For the construction of the present sets, we use pairwise orthogonal Greenberger–Horne–Zeilinger-type (GHZ-type) states [35] (for distinguishability of the GHZ basis, see Ref. [36]). We mention that, here within a set, the states are pure and they are equally probable. We also mention that the entangled states, which are available as a resource, are two-qubit maximally entangled states, which can be shared between two parties.

The main contributions of this paper is given as follows: (i) We construct a class of sets which contains maximally entangled multiqubit GHZ states. These sets are locally indistinguishable across some bipartitions but not in every bipartition. Again, these sets are sufficient to accomplish the present task for certain values of N. (ii) We show that this sets can be more resource-efficient than the sets which are locally indistinguishable across every bipartition. (iii) We define a quantity ΔE as the difference in the number of entangled states which are consumed for complete information extraction in case of the present sets and the sets which are locally indistinguishable across every bipartition. We also show that ΔE increases with increasing m, $m \geqslant 4$ and m is either even or odd.

Due to above findings, a few things are clear now. If for a given m-partite ($m \geqslant 4$) set of orthogonal states, any $(m-1)$ parties collaborate and they are not able to extract the information completely, then it does not mean that all parties have to collaborate for complete information extraction. This fact can be utilized in an information processing protocol. In fact, equivalently, for the present protocol, it is not necessary to use an m-partite ($m \geqslant 4$) set which is locally indistinguishable across every bipartition. Our task and corresponding examples also exhibit instances where more local indistinguishability cannot guarantee more efficiency.

II. RESULTS

We consider an m-partite system where each party holds only one qubit. To encode N-level classical information, one needs a set of N quantum states. Therefore, the cardinality of the considered set is N. In fact, N changes with increasing m as $N = m + 2$ in our case. We also mention that we consider only orthogonal pure states and perfect discrimination of these states is considered.

A. Four-qubit case

We consider a four-partite qubit system ($\mathcal{C}^2 \otimes \mathcal{C}^2 \otimes \mathcal{C}^2 \otimes \mathcal{C}^2$) shared between four parties, A_1, A_2, A_3, and A_4. Let us construct a set (say, S_1^4) of four-qubit states which only contains pure maximally entangled GHZ states. The form of the set is given below:

$$\begin{aligned} S_1^4 : \{&|0000\rangle \pm |1111\rangle, \\ &|1000\rangle + |0111\rangle, \\ &|0100\rangle + |1011\rangle, \\ &|0010\rangle + |1101\rangle, \\ &|0001\rangle + |1110\rangle\}. \end{aligned} \tag{1}$$

Note that, for simplicity, we do not consider the normalization factors. These factors do not have any relevance in the discrimination process. For now on, we can use the notation $d \otimes d'$ instead of $\mathcal{C}^d \otimes \mathcal{C}^{d'}$. For S_1^4, the value of N is six.

Proposition 1. S_1^4 is locally indistinguishable across every $2 \otimes 2^3$ bipartition but locally distinguishable across every $4 \otimes 4$ bipartition.

Proof. Let us first consider the bipartition as $A_1 - A_2A_3A_4$. We denote the three-qubit basis of $A_2A_3A_4$ (or A_3') as $\{|i_3'\rangle\}_{i=0}^7$, where $|0_3'\rangle \equiv |000\rangle$, $|1_3'\rangle \equiv |001\rangle$, and so on. Hence the states in S_1^4 can be rewritten as $\{(|0\rangle|0_3'\rangle \pm |1\rangle|7_3'\rangle)$, $(|1\rangle|0_3'\rangle + |0\rangle|7_3'\rangle)$, $(|0\rangle|4_3'\rangle + |1\rangle|3_3'\rangle)$, $(|0\rangle|2_3'\rangle + |1\rangle|5_3'\rangle)$, $(|0\rangle|1_3'\rangle + |1\rangle|6_3'\rangle)\}$. Now, the side A_3' performs a measurement on the three qubits. Note that while it is possible to distinguish the last three states by LOCC, it is impossible to distinguish

among the first three. The reason behind this indistinguishability is that the three states resemble three Bell states of two qubits. Now it has already been shown in the literature that it is not possible to distinguish three or four Bell states perfectly via LOCC [7]. Following similar technique, if we consider any $2 \otimes 2^3$ bipartition, it is always possible to find three Bell-like indistinguishable states. Thus, the above set cannot be perfectly distinguished by LOCC in these bipartitions.

On the other hand, when we consider the bipartition of the form $A_1A_2 - A_3A_4$, we show that it is possible to distinguish the states of S_1^4 with local measurements. Here, we denote the two-qubit basis of the first subsystem A_1A_2 (or, $A_2^{(1)}$) as $\{|j_2^{(1)}\rangle\}_{j=0}^3$ such that $|0_2^{(1)}\rangle \equiv |00\rangle$, $|1_2^{(1)}\rangle \equiv |01\rangle$, and so on. Similarly, for the second subsystem A_3A_4 (or, $A_2^{(2)}$) as $\{|j_2^{(2)}\rangle\}_{j=0}^3$ such that $|0_2^{(2)}\rangle \equiv |00\rangle$, $|1_2^{(2)}\rangle \equiv |01\rangle$ and so on. Hence, the states in S_1^4 can be rewritten as $\{(|0_2^{(1)}\rangle|0_2^{(2)}\rangle \pm |3_2^{(1)}\rangle|3_2^{(2)}\rangle)$, $(|2_2^{(1)}\rangle|0_2^{(2)}\rangle + |1_2^{(1)}\rangle|3_2^{(2)}\rangle)$, $(|1_2^{(1)}\rangle|0_2^{(2)}\rangle + |2_2^{(1)}\rangle|3_2^{(2)}\rangle)$, $(|0_2^{(1)}\rangle|2_2^{(2)}\rangle + |3_2^{(1)}\rangle|1_2^{(2)}\rangle)$, $(|0_2^{(1)}\rangle|1_2^{(2)}\rangle + |3_2^{(1)}\rangle|2_2^{(2)}\rangle)\}$. Notice that, when $A_2^{(2)}$ performs the projective measurements where the projectors are $(|0_2^{(2)}\rangle\langle 0_2^{(2)}| + |3_2^{(2)}\rangle\langle 3_2^{(2)}|)$ and $(|1_2^{(2)}\rangle\langle 1_2^{(2)}| + |2_2^{(2)}\rangle\langle 2_2^{(2)}|)$, it is possible to distinguish between the subspaces, spanned by the first four states and the last two. Now, for the last two states, being orthogonal pure states, they are always locally distinguishable [37]. On the other hand, for the first four states, one can consider projective measurement on $A_2^{(1)}$, where the projectors are given by $(|0_2^{(1)}\rangle\langle 0_2^{(1)}| + |3_2^{(1)}\rangle\langle 3_2^{(1)}|)$ and $(|1_2^{(1)}\rangle\langle 1_2^{(1)}| + |2_2^{(1)}\rangle\langle 2_2^{(1)}|)$. This is to separate out the subspaces, spanned by the first two and last two states. Finally, after subspace discrimination, only two orthogonal pure states are left, which can be distinguished by LOCC [37]. This analysis also holds for other $4 \otimes 4$ bipartition. These complete the proof. ■

Here we consider four parties: A_1, A_2, A_3, and A_4. We suppose that k parties among them collaborate then either $k = 2$ or $k = 3$. If $k = 3$ then the possible bipartitions are $A_1 - A_2A_3A_4$, $A_2 - A_1A_3A_4$, $A_3 - A_1A_2A_4$, and $A_4 - A_1A_2A_3$. Again, if $k = 2$, then the possible partitions are tripartitions which are given by $A_1A_2 - A_3 - A_4$, $A_1A_3 - A_2 - A_4$, $A_1A_4 - A_2 - A_3$, $A_1 - A_2A_3 - A_4$, $A_1 - A_2A_4 - A_3$, and $A_1 - A_2 - A_3A_4$. Clearly, we can encode the information against the four-qubit states of a set which is locally indistinguishable across all $2 \otimes 8$ bipartitions. Such a set can be found from Eq. (1). Now, we want to think about the complete information extraction part. The set S_1^4 is distinguishable across $A_1A_2 - A_3A_4$ bipartition. In this case, if the parties A_1, A_2 and A_3, A_4 share two-qubit pure maximally entangled states (Bell states), then it is sufficient to locally distinguish the states perfectly. It is due to a teleportation [38] based protocol. A_1 can teleport the qubit to the location of A_2. Similarly, A_3 can teleport the qubit to the location of A_4. In this way, the bipartition $A_1A_2 - A_3A_4$ is produced.

On the other hand, it is already explained that given any set which is locally indistinguishable across every bipartition, are also sufficient to accomplish the present task. Now, for four qubits, two entangled states cannot be sufficient for complete information extraction using such sets. Because for a four-qubit set S_2^4 which is locally indistinguishable across every bipartition, if one uses two bipartite maximally entangled states and follow a teleportation based protocol, then ultimately, a new bipartition will be produced in which S_2^4 is again, locally indistinguishable. So, entangled states required for complete information extraction when the set is S_1^4, given by $E(S_1^4) = 2$ and similarly, $E(S_2^4) = 3$ (at least necessary). Thus, $\Delta E = E(S_2^4) - E(S_1^4) = 1$.

B. Six-qubit case

Now we consider the case consisting of six qubits ($\mathcal{C}^2 \otimes \mathcal{C}^2 \otimes \mathcal{C}^2 \otimes \mathcal{C}^2 \otimes \mathcal{C}^2 \otimes \mathcal{C}^2$) shared between six parties A_1, A_2, A_3, A_4, A_5, and A_6. We construct a set (S_1^6) of six-qubit states which only contains pure maximally entangled GHZ states. The form of the set is given below:

$$\begin{aligned} S_1^6 : \{&|000000\rangle \pm |111111\rangle, \\ &|100000\rangle + |011111\rangle, \\ &|010000\rangle + |101111\rangle, \\ &|001000\rangle + |110111\rangle, \\ &|000100\rangle + |111011\rangle, \\ &|000010\rangle + |111101\rangle, \\ &|000001\rangle + |111110\rangle\}. \end{aligned} \tag{2}$$

For simplicity we discard the normalization as before because it does not play any important role in our protocol.

Proposition 2. S_1^6 is locally indistinguishable across every $2 \otimes 2^5$ bipartition but locally distinguishable across every $4 \otimes 4 \otimes 4$ tripartition.

Proof. Following the similar mechanism as used in the proof of the previous proposition, we consider first the bipartition as $A_1 - A_2A_3A_4A_5A_6$. We then define the five-qubit basis of $A_2A_3A_4A_5A_6$ (or,A_5') as $\{|i_5'\rangle\}_{i=0}^{31}$ where $|0_5'\rangle \equiv |00000\rangle$, $|1_5'\rangle \equiv |00001\rangle, \ldots, |31_5'\rangle \equiv |11111\rangle$. Hence, the set S_1^6 can be rewritten as $\{(|0\rangle|0_5'\rangle \pm |1\rangle|31_5'\rangle)$, $(|1\rangle|0_5'\rangle + |0\rangle|31_5'\rangle)$, $(|0\rangle|16_5'\rangle + |1\rangle|15_5'\rangle)$, $(|0\rangle|8_5'\rangle + |1\rangle|23_5'\rangle)$, $(|0\rangle|4_5'\rangle + |1\rangle|27_5'\rangle)$, $(|0\rangle|2_5'\rangle + |1\rangle|29_5'\rangle)$, $(|0\rangle|1_5'\rangle + |1\rangle|30_5'\rangle)\}$. Note that, if on the second composite system, i.e., on A_5' projective measurements are performed then the last five states (last five states of the above equation) can be distinguished. But the first three states can be seen as three Bell states in the bipartite system $A_1 - A_5'$ which cannot be perfectly distinguished by LOCC [7]. Following a similar technique, if we consider any $2 \otimes 2^5$ bipartition, it is always possible to find three Bell-like indistinguishable states. Thus, the above set cannot be perfectly distinguished by LOCC in these bipartitions.

On the other hand, while considering the tripartition, the subsystems can be grouped as A_1A_2 (or $A_2^{(1)}$), A_3A_4 (or $A_2^{(2)}$), and A_5A_6 (or $A_2^{(3)}$). We define the new basis of the corresponding subsystems as, $\{j_2^{(1)}\}_{j=0}^3$, $\{j_2^{(2)}\}_{j=0}^3$, and $\{j_2^{(3)}\}_{j=0}^3$ respectively (as defined in the proof of the Proposition 1). Hence the states in the set S_1^6 can be rewritten as $\{(|0_2^{(1)}\rangle|0_2^{(2)}\rangle|0_2^{(3)}\rangle \pm |3_2^{(1)}\rangle|3_2^{(2)}\rangle|3_2^{(3)}\rangle)$, $(|2_2^{(1)}\rangle|0_2^{(2)}\rangle|0_2^{(3)}\rangle + |1_2^{(1)}\rangle|3_2^{(2)}\rangle|3_2^{(3)}\rangle)$, $(|1_2^{(1)}\rangle|0_2^{(2)}\rangle|0_2^{(3)}\rangle + |2_2^{(1)}\rangle|3_2^{(2)}\rangle|3_2^{(3)}\rangle)$, $(|0_2^{(1)}\rangle|2_2^{(2)}\rangle|0_2^{(3)}\rangle + |3_2^{(1)}\rangle|1_2^{(2)}\rangle|3_2^{(3)}\rangle)$, $(|0_2^{(1)}\rangle|1_2^{(2)}\rangle|0_2^{(3)}\rangle + |3_2^{(1)}\rangle|2_2^{(2)}\rangle|3_2^{(3)}\rangle)$, $(|0_2^{(1)}\rangle|0_2^{(2)}\rangle|2_2^{(3)}\rangle + |3_2^{(1)}\rangle|3_2^{(2)}\rangle|1_2^{(3)}\rangle)$, $(|0_2^{(1)}\rangle|0_2^{(2)}\rangle|1_2^{(3)}\rangle + |3_2^{(1)}\rangle|3_2^{(2)}\rangle|2_2^{(3)}\rangle)\}$. First, the subsystem $A_2^{(3)}$ performs projective measurement with projectors given

as,$(|0_2^{(3)}\rangle\langle 0_2^{(3)}| + |3_2^{(3)}\rangle\langle 3_2^{(3)}|)$ and $(|1_2^{(3)}\rangle\langle 1_2^{(3)}| + |2_2^{(3)}\rangle\langle 2_2^{(3)}|)$ revealing the subspaces consisting the first six states and the last two. Note that the last two states can be seen as a pair of orthogonal maximally entangled states in the newly defined basis for the grouped subsystems and hence can be distinguished via LOCC [37]. Similarly, for first six states when the subsystem $A_2^{(2)}$ performs the projective measurement with projectors $(|0_2^{(2)}\rangle\langle 0_2^{(2)}| + |3_2^{(2)}\rangle\langle 3_2^{(2)}|)$ and $(|1_2^{(2)}\rangle\langle 1_2^{(2)}| + |2_2^{(2)}\rangle\langle 2_2^{(2)}|)$ to separate out between the first four and last two states, the last two are again distinguishable by performing LOCC [37]. Following a similar logic when we consider only first four states, on the first subsystem $A_2^{(1)}$ a suitable projective measurement can be performed. The corresponding projectors are $(|0_2^{(1)}\rangle\langle 0_2^{(1)}| + |3_2^{(1)}\rangle\langle 3_2^{(1)}|)$ and $(|1_2^{(1)}\rangle\langle 1_2^{(1)}| + |2_2^{(1)}\rangle\langle 2_2^{(1)}|)$. Then, it is possible to distinguish between the first two and the other two states of the first four states. Note that the two pure states in the groups are mutually orthogonal to each other and hence can be distinguished perfectly via LOCC [37]. This analysis also holds for other $4 \otimes 4 \otimes 4$ tripartitions. These suffice to prove the proposition. ■

In this case we consider a six-qubit system consisting of parties A_1, A_2, A_3, A_4, A_5, and A_6. As can be seen from the above proof, the set of states S_1^6 in Eq. (2) cannot be distinguished locally in any $2 \otimes 2^5$ bipartition. As a result of which if any k parties collaborate and $(m-k)$ parties stand alone, in the produced bipartition the set remains locally indistinguishable. On the other hand, it can be locally distinguished in the tripartition $A_1A_2 - A_3A_4 - A_5A_6$. Note that, following the similar logic as of the four-qubit system in this case, the subsystems can be grouped to produce any $4 \otimes 4 \otimes 4$ bipartition and for this it is required to share three bipartite maximally entangled states. This is to reveal an eight level information perfectly. Hence, in this case, $E(S_1^6) = 3$ for complete information extraction. On the other hand, when we have a set (say, S_2^6) which is locally indistinguishable across every bipartition, then following the similar logic as in the case of four qubits, we have $E(S_2^6) = 5$ for revealing the information perfectly. Hence, for six qubits we have $\Delta E = E(S_2^6) - E(S_1^6) = 2$. Notice that the difference ΔE is increased as the number of qubits is increased from four to six.

C. Generalisation to *m*-qubit case

In this section we try to generalize the above findings for an m-qubit (considering m to be even) $(\mathcal{C}_1^2 \otimes \mathcal{C}_2^2 \otimes \cdots \otimes \mathcal{C}_m^2)$ system shared between parties $\{A_i\}_{i=1}^m$. Following the same trajectory as before we construct a set S_1^m of m-qubit states and it is given as follows:

$$\begin{aligned} S_1^m : \{&|0_1 0_2 \cdots 0_m\rangle \pm |1_1 1_2 \cdots 1_m\rangle, \\ &|1_1 0_2 \cdots 0_m\rangle + |0_1 1_2 \cdots 1_m\rangle, \\ &|0_1 1_2 \cdots 0_m\rangle + |1_1 0_2 \cdots 1_m\rangle, \\ &\vdots \\ &|0_1 \cdots 1_{m-1} 0_m\rangle + |1_1 \cdots 0_{m-1} 1_m\rangle, \\ &|0_1 0_2 \cdots 1_m\rangle + |1_1 1_2 \cdots 0_m\rangle\}. \end{aligned} \tag{3}$$

For simplicity we discard the normalization as before as it does not interrupt our findings. Now, we are ready to state the proposition for the general m-qubit system.

Proposition 3. S_1^m is locally indistinguishable across every $2 \otimes 2^{(m-1)}$ bipartition but locally distinguishable across every $4 \otimes 4 \otimes \cdots \otimes 4m/2$ partition.

Proof. The sketch of the proof relies on the good old method of mathematical induction. First we consider the bipartition as, $A_1 - \{A_i\}_{i=2}^m$. We define the $(m-1)$-qubit basis of $\{A_i\}_{i=2}^m$ (or, A'_{m-1}) as $\{|i'_{m-1}\rangle\}_{i=0}^{(2^{m-1}-1)}$. Therefore, the states in the set S_1^m can be rewritten as, $\{(|0_1\rangle|0'_{m-1}\rangle \pm |1_1\rangle|(2^{m-1}-1)'_{m-1}\rangle), (|1_1\rangle|0'_{m-1}\rangle + |0_1\rangle|(2^{m-1}-1)'_{m-1}\rangle), \cdots\}$. Note that the first three states in the set are three orthogonal maximally entangled bipartite states (Bell-like states) while $(m-1)$ parties collaborate between themselves to form the second composite subsystem A'_{m-1}. Hence these states can never be distinguished via LOCC [7]. Following a similar technique, if we consider any $2 \otimes 2^{m-1}$ bipartition, it is always possible to find three Bell-like indistinguishable states. Thus, the above set cannot be perfectly distinguished by LOCC in these bipartitions.

Now, on the other hand, we consider the $m/2$-partition $(4 \otimes 4 \otimes \cdots \otimes 4)$ and see if the states remain locally indistinguishable. For this purpose following the similar technique used in the previous propositions, we group the subsystems as A_1A_2 (or $A_2^{(1)}$), A_3A_4 (or $A_2^{(2)}$), ..., and $A_{m-1}A_m$ (or $A_2^{(m/2)}$). Now we define the basis of the newly defined subsystems as $\{|j_2^{(1)}\rangle\}_{j=0}^3$, $\{|j_2^{(2)}\rangle\}_{j=0}^3$, ..., and $\{|j_2^{(m/2)}\rangle\}_{j=0}^3$, respectively. Hence the states in S_1^m can be rewritten as, $\{(|0_2^{(1)}\rangle|0_2^{(2)}\rangle\cdots|0_2^{(m/2)}\rangle \pm |3_2^{(1)}\rangle|3_2^{(2)}\rangle\cdots|3_2^{(m/2)}\rangle)$, $(|2_2^{(1)}\rangle|0_2^{(2)}\rangle\cdots|0_2^{(m/2)}\rangle + |1_2^{(1)}\rangle|3_2^{(2)}\rangle\cdots|3_2^{(m/2)}\rangle)$, ..., $(|0_2^{(1)}\rangle|0_2^{(2)}\rangle\cdots|2_2^{(m/2)}\rangle + |3_2^{(1)}\rangle|3_2^{(2)}\rangle\cdots|1_2^{(m/2)}\rangle)$, and $(|0_2^{(1)}\rangle|0_2^{(2)}\rangle\cdots|1_2^{(m/2)}\rangle + |3_2^{(1)}\rangle|3_2^{(2)}\rangle\cdots|2_2^{(m/2)}\rangle)\}$. We claim that these states are locally distinguishable in this given partition. Note that, when the subsystem $A_2^{(m/2)}$ performs the projective measurement given by the projectors, $(|0_2^{(m/2)}\rangle\langle 0_2^{(m/2)}| + |3_2^{(m/2)}\rangle\langle 3_2^{(m/2)}|)$ and $(|1_2^{(m/2)}\rangle\langle 1_2^{(m/2)}| + |2_2^{(m/2)}\rangle\langle 2_2^{(m/2)}|)$, it separates the last two states in the set and these two states are mutually orthogonal to each other as can be easily seen. Hence, they can be distinguished via LOCC [37]. Next we consider the subsystem $A_2^{(m/2-1)}$ and it performs the similar projective measurement separating two more mutually orthogonal states, and hence they are locally distinguishable. The procedure can be repeated until the subsystem $A_2^{(1)}$ while finally separates between four remaining states into two sets of a pair of pure orthogonal states which are again locally distinguishable [37]. This analysis also holds for other $4 \otimes 4 \otimes \cdots \otimes 4$ $(m/2)$ partitions. Hence the claim. ■

D. Resource efficiency of the task

Here, we see how the introduced set of states for m-qubit system (m being even) S_1^m is more useful than a set of states say, S_2^m which is locally indistinguishable across every bipartition. Note that, for a m-party system when they have access to the set S_2^m, to perform the task efficiently they need to share at least $(m-1)$ bipartite entangled states. The logic is the

same as for the two previously discussed cases. We assume that the shared states are maximally entangled and they are used in a teleportation based protocol. Then, if the number of such states is less than $(m-1)$ for the set S_2^m, it will give rise to a new bipartition along which the set would be locally indistinguishable again. On the other hand, if the set is S_1^m then it is possible to reveal the information completely with less number of maximally entangled states.

Theorem 1. The number of bipartite entangled states required for the perfect simulation of the present task with S_1^m is $m/2$ and hence the difference in resource requirement for complete information extraction corresponding to the sets S_1^m and S_2^m grows with the number of parties among which the composite quantum system is distributed.

Proof. As can be seen from Proposition 3 the states in S_1^m are locally indistinguishable across every 1 vs $(m-1)$ bipartition but locally distinguishable in every $4 \otimes 4 \otimes \cdots \otimes 4m/2$ partition. Hence, if the two parties in the individual subgroups of $m/2$ partitions share a two-qubit maximally entangled state then it is possible to teleport one qubit to the other location. This will enable the set S_1^m to perform the task using only $m/2$ number of bipartite entangled states.

Now, the difference in resource requirement ΔE can be defined as follows: The number of bipartite entangled states, necessary for complete information extraction from S_2^m, i.e., $E(S_2^m)$ difference the number of bipartite entangled states, sufficient for complete information extraction from S_1^m, i.e., $E(S_1^m)$:

$$\begin{aligned}\Delta E &= E\left(S_2^m\right) - E\left(S_1^m\right) \\ &= (m-1) - \frac{m}{2} \\ &= \frac{m-2}{2}. \end{aligned} \tag{4}$$

Note that for $m = 4$, $\Delta E = 1$; for $m = 6$, $\Delta E = 2$ as obtained in the previous individual cases. From Eq. (4) it is clear that as the number of qubits m grows (m is even and $m \geqslant 4$), the task can be made more resource efficiently by using the set of states S_1^m. ■

Remark. For an odd number of parties, i.e., when m is odd, similar results follow starting from $m = 5$ while the set, which is considered, is locally indistinguishable across every 1 vs $(m-1)$ bipartition but locally distinguishable across some $(m-1)/2$ partition. In this case also the difference in resource requirement for complete extraction of information grows with the number of qubits compared with a set of states which is locally distinguishable across every bipartition.

Therefore, the type of sets, we are talking about, exist in all qubit dimensions when $m \geqslant 4$.

III. CONCLUSION

In quantum information, when the system in consideration is a composite one, advantages obtained in different tasks are mainly governed by the presence of nonlocal correlations in the system. Among these correlations quantum entanglement is mostly responsible in speed ups of quantum domain than its classical counterpart [39–41] but in reality it is an expensive resource. Hence, it is always useful to reduce the use of the same without hindering the effectiveness of the main protocol [40,42].

In this paper, we have presented an efficient protocol for information sharing such that the information remains locked to a certain extent. Particularly, we have constructed a set of states that are locally indistinguishable across some bipartitions. At the same time, the sets are locally distinguishable across remaining bipartitions. Thus, to decode the information encoded against the states of a present set, we need less number of bipartite entangled states. Hence the set of states prescribed are more useful than the states that are locally indistinguishable across every bipartition when the present task is considered. Because in the latter case all the parties need to collaborate together to reveal the information systematically.

Our construction also depicts the fact that even if $(m-1)$ parties collaborate, the information is not extracted completely—this does not mean that to extract the information completely all parties have to collaborate. Interestingly, we have noted that the difference in the number of shared bipartite entangled states required in these two types of sets of states, to reveal the information completely, increases linearly with the increasing number of parties. The present task and corresponding examples also exhibit the instances where more local indistinguishability cannot guarantee more efficiency.

For further research one may consider the following problems: (a) applications of local indistinguishability in information distribution protocols—here one may consider to implement the present task using mixed states or assuming probabilistic setting, (b) understanding the instances like—more resources may not guarantee more effectiveness, (c) exploring entanglement as resource in complete information extraction, etc.

ACKNOWLEDGMENTS

We thank Alexander Streltsov for helpful discussions. This work was supported by the "Quantum Optical Technologies" project, carried out within the International Research Agendas programme of the Foundation for Polish Science co-financed by the European Union under the European Regional Development Fund and the "Quantum Coherence and Entanglement for Quantum Technology" project, carried out within the First Team programme of the Foundation for Polish Science co-financed by the European Union under the European Regional Development Fund.

[1] S. M. Barnett and S. Croke, Quantum state discrimination, Adv. Opt. Photonics **1**, 238 (2009).

[2] A. Chefles, Quantum state discrimination, Contemp. Phys. **41**, 401 (2000).

[3] J. A. Bergou, Discrimination of quantum states, J. Mod. Opt. **57**, 160 (2010).

[4] J. Bae and L.-C. Kwek, Quantum state discrimination and its applications, J. Phys. A: Math. Theor. **48**, 083001 (2015).

[5] M. A. Nielsen and I. L. Chuang, *Quantum Computation and Quantum Information* (Cambridge University Press, Cambridge, 2000).
[6] C. H. Bennett, D. P. DiVincenzo, C. A. Fuchs, T. Mor, E. Rains, P. W. Shor, J. A. Smolin, and W. K. Wootters, Quantum nonlocality without entanglement, Phys. Rev. A **59**, 1070 (1999).
[7] S. Ghosh, G. Kar, A. Roy, A. Sen(De), and U. Sen, Distinguishability of Bell States, Phys. Rev. Lett. **87**, 277902 (2001).
[8] J. Walgate and L. Hardy, Nonlocality, Asymmetry, and Distinguishing Bipartite States, Phys. Rev. Lett. **89**, 147901 (2002).
[9] S. Ghosh, G. Kar, A. Roy, D. Sarkar, A. Sen(De), and U. Sen, Local indistinguishability of orthogonal pure states by using a bound on distillable entanglement, Phys. Rev. A **65**, 062307 (2002).
[10] M. Horodecki, A. Sen(De), U. Sen, and K. Horodecki, Local Indistinguishability: More Nonlocality with Less Entanglement, Phys. Rev. Lett. **90**, 047902 (2003).
[11] H. Fan, Distinguishability and Indistinguishability by Local Operations and Classical Communication, Phys. Rev. Lett. **92**, 177905 (2004).
[12] S. Ghosh, G. Kar, A. Roy, and D. Sarkar, Distinguishability of maximally entangled states, Phys. Rev. A **70**, 022304 (2004).
[13] J. Watrous, Bipartite Subspaces Having No Bases Distinguishable by Local Operations and Classical Communication, Phys. Rev. Lett. **95**, 080505 (2005).
[14] M. Hayashi, D. Markham, M. Murao, M. Owari, and S. Virmani, Bounds on Multipartite Entangled Orthogonal State Discrimination Using Local Operations and Classical Communication, Phys. Rev. Lett. **96**, 040501 (2006).
[15] S. Bandyopadhyay, More Nonlocality with Less Purity, Phys. Rev. Lett. **106**, 210402 (2011).
[16] N. Yu, R. Duan, and M. Ying, Four Locally Indistinguishable Ququad-Ququad Orthogonal Maximally Entangled States, Phys. Rev. Lett. **109**, 020506 (2012).
[17] S. Halder, Several nonlocal sets of multipartite pure orthogonal product states, Phys. Rev. A **98**, 022303 (2018).
[18] S. Halder, M. Banik, S. Agrawal, and S. Bandyopadhyay, Strong Quantum Nonlocality without Entanglement, Phys. Rev. Lett. **122**, 040403 (2019).
[19] B. M. Terhal, D. P. DiVincenzo, and D. W. Leung, Hiding Bits in Bell States, Phys. Rev. Lett. **86**, 5807 (2001).
[20] T. Eggeling and R. F. Werner, Hiding Classical Data in Multipartite Quantum States, Phys. Rev. Lett. **89**, 097905 (2002).
[21] L. Lami, Quantum data hiding with continuous-variable systems, Phys. Rev. A **104**, 052428 (2021).
[22] S. Bandyopadhyay and S. Halder, Genuine activation of nonlocality: From locally available to locally hidden information, Phys. Rev. A **104**, L050201 (2021).
[23] D. Markham and B. C. Sanders, Graph states for quantum secret sharing, Phys. Rev. A **78**, 042309 (2008).
[24] R. Rahaman and M. G. Parker, Quantum scheme for secret sharing based on local distinguishability, Phys. Rev. A **91**, 022330 (2015).
[25] S. Rout, A. G. Maity, A. Mukherjee, S. Halder, and M. Banik, Genuinely nonlocal product bases: Classification and entanglement-assisted discrimination, Phys. Rev. A **100**, 032321 (2019).
[26] Z.-C. Zhang and X. Zhang, Strong quantum nonlocality in multipartite quantum systems, Phys. Rev. A **99**, 062108 (2019).
[27] S. Halder and R. Sengupta, Distinguishability classes, resource sharing, and bound entanglement distribution, Phys. Rev. A **101**, 012311 (2020).
[28] P. Yuan, G. Tian, and X. Sun, Strong quantum nonlocality without entanglement in multipartite quantum systems, Phys. Rev. A **102**, 042228 (2020).
[29] F. Shi, M. Hu, L. Chen, and X. Zhang, Strong quantum nonlocality with entanglement, Phys. Rev. A **102**, 042202 (2020).
[30] S. Rout, A. G. Maity, A. Mukherjee, S. Halder, and M. Banik, Multiparty orthogonal product states with minimal genuine nonlocality, Phys. Rev. A **104**, 052433 (2021).
[31] F. Shi, M.-S. Li, L. Chen, and X. Zhang, Strong quantum nonlocality for unextendible product bases in heterogeneous systems, J. Phys. A: Math. Theor. **55**, 015305 (2022).
[32] Y.-L. Wang, M.-S. Li, and M.-H. Yung, Graph-connectivity-based strong quantum nonlocality with genuine entanglement, Phys. Rev. A **104**, 012424 (2021).
[33] M.-S. Li, Y.-L. Wang, F. Shi, and M.-H. Yung, Local distinguishability based genuinely quantum nonlocality without entanglement, J. Phys. A: Math. Theor. **54**, 445301 (2021).
[34] F. Shi, M.-S. Li, M. Hu, L. Chen, M.-H. Yung, Y.-L. Wang, and X. Zhang, Strongly nonlocal unextendible product bases do exist, Quantum **6**, 619 (2022).
[35] D. M. Greenberger, M. A. Horne, and A. Zeilinger, Going beyond Bell's theorem, arXiv:0712.0921.
[36] S. Bandyopadhyay, S. Halder, and M. Nathanson, Optimal resource states for local state discrimination, Phys. Rev. A **97**, 022314 (2018).
[37] J. Walgate, A. J. Short, L. Hardy, and V. Vedral, Local Distinguishability of Multipartite Orthogonal Quantum States, Phys. Rev. Lett. **85**, 4972 (2000).
[38] C. H. Bennett, G. Brassard, C. Crépeau, R. Jozsa, A. Peres, and W. K. Wootters, Teleporting an Unknown Quantum State via Dual Classical and Einstein-Podolsky-Rosen channels, Phys. Rev. Lett. **70**, 1895 (1993).
[39] N. Linden and S. Popescu, Good Dynamics versus Bad Kinematics: Is Entanglement Needed for Quantum Computation? Phys. Rev. Lett. **87**, 047901 (2001).
[40] M. Van den Nest, Universal Quantum Computation with Little Entanglement, Phys. Rev. Lett. **110**, 060504 (2013).
[41] R. Jozsa and N. Linden, On the role of entanglement in quantum-computational speed-up, Proc. R. Soc. London, Ser. A **459**, 2011 (2003).
[42] M. Naseri, T. V. Kondra, S. Goswami, M. Fellous-Asiani, and A. Streltsov, Entanglement and coherence in Bernstein-Vazirani algorithm, Phys. Rev. A **106**, 062429 (2022).