Controlled state reconstruction and quantum secret sharing

Pahulpreet Singh [1,2,*] and Indranil Chakrabarty [1,3,†]

[1] *Centre for Quantum Science and Technology, International Institute of Information Technology Hyderabad, Gachibowli, Hyderabad 500032, Telangana, India*

[2] *Center for Computational Natural Science and Bioinformatics, International Institute of Information Technology Hyderabad, Gachibowli, Hyderabad 500032, Telangana, India*

[3] *Center for Security, Theory and Algorithmic Research, International Institute of Information Technology Hyderabad, Gachibowli, Hyderabad 500032, Telangana, India*

(Received 23 June 2023; revised 10 January 2024; accepted 2 February 2024; published 6 March 2024)

In this article we present a benchmark for resource characterization in the process of controlled quantum state reconstruction and secret sharing for general three-qubit states. This is achieved by providing a closed expression for the reconstruction fidelity, which relies on the genuine tripartite correlation and the bipartite channel between the dealer and the reconstructor characterized by the respective correlation parameters. We formulate the idea of quantum advantage in approximate state reconstruction as surpassing the classical limit set at $\frac{2}{3}$. This article introduces new interoperability between teleportation and state reconstruction. This is detailed through a case-by-case analysis of relevant correlation matrices. We reformulate the idea of quantum secret sharing by setting up additional constraints on the teleportation capacity of the bipartite channels between dealer and shareholders by ensuring that, individually, the shareholders cannot reconstruct the secret. We believe that this will give us an ideal picture of how quantum secret sharing should be.

DOI: 10.1103/PhysRevA.109.032406

I. INTRODUCTION

With the advent of quantum information theory, sending and sharing quantum [1–7] as well as classical [8–13] information using quantum resources has become a significant area of study. During the transmission, security of the message becomes a key consideration and has to be taken care of to set up quantum networks [14–21] in the longer run. Secret sharing is a procedure that allows secure distribution of a secret message into multiple n parts so that a certain number k of parts can be used to get back the original message and forbids any subset smaller than k from obtaining useful information about it. Quantum secret sharing (QSS) [22–36] is the extension of this idea where we use a quantum resource (usually a multiparty entangled state) to distribute the secret [26–28]. The secret itself can be classical or quantum in nature and of any size. In this article we are interested in sharing of a qubit with two parties such that when both parties cooperate, they can reconstruct it at one of the locations. Here we refer to this process as controlled state reconstruction (CSR). Controlled state reconstruction is a slightly broader term than the secret sharing in the sense that it need not account for the security aspects that come with secret sharing. The security here is defined by the condition that no shareholders can reveal the secret without the help of the other shareholders. This process has been termed controlled quantum teleportation (CQT) since it is analogous to teleporting a qubit from an initial location (dealer) to a final location (reconstructor) with the help of a third party (assistant) acting as the control qubit [37–39]. It has been shown that a witness operator can be constructed to estimate the power of the controller in CQT [40].

In this paper we differentiate between the two scenarios by using the term quantum secret sharing specifically when security is a requirement (i.e., individual shareholders do not have enough information about the secret) and controlled state reconstruction as the general term for transmitting quantum information from one location to another with the help of an assistant. Most of our work focuses on CSR; however, at the end, we investigate some intricacies that accompany QSS.

We consider the simple setting where a dealer (say, Alice) aims to share an unknown qubit with two shareholders (say, Bob and Charlie). At the start of the protocol, one of the shareholders decides to be the reconstructor (Charlie, for example), which makes the other one (Bob, in this case) the assistant. Perfect reconstruction of the state after sharing has already been shown using the Greenberger-Horne-Zeilinger (GHZ) state as the resource [22]. We study approximate controlled reconstruction of the state using general tripartite entangled states. Hence, if we are using a resource which does not allow perfect reconstruction, we want the final qubit to be as close as possible to the original qubit. By quantum advantage we refer to a situation where the reconstruction fidelity is better than what can be achieved classically without having any shared quantum resource.

Our first finding is the classical limit of controlled reconstruction, which happens to be $\frac{2}{3}$. This matches the classical limit of teleportation fidelity of a bipartite two-qubit

*pahulpreet.singh@research.iiit.ac.in
†indranil.chakrabarty@iiit.ac.in

channel [2]. Subsequently, we find an expression for the reconstruction fidelity in terms of the Bloch parameters of the resource state, which then enables us to find conditions under which a three-qubit state will have quantum advantage in the process of CSR or CQT. It turns out that the reconstruction fidelity is dependent on two significant parameters: One is the correlation tensor between three parties and the other is the correlation matrix of the dealer-reconstructor pair. It is intriguing to note that this fidelity does not depend on the correlation matrix of the assistant-reconstructor pair. In a sense, this fidelity just quantifies how much quantum information from the initial state is transferred to the final location. There can be situations with quantum advantage despite the absence of tripartite correlation. This leads us to believe that this fidelity does not originate solely from CSR. Rather, there is also a contribution of the teleportation capacity of the bipartite channel between the dealer and the reconstructor. We not only prove this but consider several cases based on the correlation matrices that appear in our expression. This helps us analyze the interoperability between the reconstruction fidelity and the teleportation fidelity for three-qubit resources in a holistic manner. In the latter part of our article we develop this idea further to introduce QSS in a different but meaningful way. This paves the way to distinguish QSS from CSR or CQT. For a QSS protocol to be successful, we make sure that neither of the shareholders has useful information about the secret by enforcing additional constraints on the teleportation capacities of the dealer to the shareholders' channels. We also specify the states that can be used as resources for successful QSS.

In Sec. II we obtain the classical limit of this fidelity without using any quantum channel to share the state. In Sec. III we give an expression for the maximum possible reconstruction fidelity using the parameters of the resource state. This lets us quantify the quantum advantage that an arbitrary three-qubit resource can provide in reconstruction. In the same section we discuss a potential relationship between (two-party) quantum teleportation and (three-party) state reconstruction. In Sec. IV we give criteria to discern QSS from CSR by adding additional constraints that need to be satisfied for QSS. We summarize in Sec. V.

II. CLASSICAL LIMIT OF CONTROLLED STATE RECONSTRUCTION

We define the classical limit as the expected fidelity score obtained if only classical channels are used to share a qubit. This will allow us to define the threshold above which a quantum advantage can be claimed. Here we consider a three-party scheme where Alice is the dealer, Bob is the assistant, and Charlie is the reconstructor. Let $|q\rangle$ denote Alice's qubit which is to be shared. She can measure in some basis (say, $|\uparrow\rangle$ and $|\downarrow\rangle$), which would be agreed upon by the parties beforehand. Then this measurement result can be encoded into a single classical bit s (say, 0 for $|\uparrow\rangle$ and 1 for $|\downarrow\rangle$). This can be split into two shares s_1 and s_2 such that $s_1 \oplus s_2 = s$. It can be shown that (for a given s) it would be optimal for Alice to choose the appropriate s_1 and s_2 from a uniform distribution (see the Appendix). Alice transmits the respective bits to Bob and Charlie through classical channels. During the reconstruction phase, Bob and Charlie cooperate to find s, which they can use to construct the corresponding quantum state $|s\rangle$ (again, $|\uparrow\rangle$ for $s = 0$ and $|\downarrow\rangle$ for $s = 1$) which is an approximation of Alice's original quantum state $|q\rangle$, which we represent as

$$|q\rangle = \cos\frac{\theta}{2}\,|\uparrow\rangle + e^{i\phi}\sin\frac{\theta}{2}\,|\downarrow\rangle\,. \tag{1}$$

Since the final state $|s\rangle$ is eventually dependent only on Alice's measurement, we can say $|s\rangle$ is $|\uparrow\rangle$ with probability $\cos^2\frac{\theta}{2}$ and $|\downarrow\rangle$ with probability $\sin^2\frac{\theta}{2}$. Now calculating the fidelity between the two-qubit states,

$$\begin{aligned} F(q,s) &= \|\langle q|s\rangle\|^2 \\ &= \Pr(s=0)\|\langle q|\uparrow\rangle\|^2 + \Pr(s=1)\|\langle q|\downarrow\rangle\|^2 \\ &= 1 - \tfrac{1}{2}\sin^2\theta. \end{aligned} \tag{2}$$

Taking the expectation fidelity over all states $|q\rangle$ on the Bloch sphere,

$$\begin{aligned} \mathcal{F} &= \langle F(q,s)\rangle \\ &= \frac{1}{4\pi}\int_{\theta=0}^{\pi}\int_{\phi=0}^{2\pi}\sin\theta\,d\theta\,d\phi\left(1-\frac{1}{2}\sin^2\theta\right) \\ &= \frac{1}{2}(2) - \frac{1}{4}\left(\frac{4}{3}\right) = \boxed{\frac{2}{3}}. \end{aligned} \tag{3}$$

Hence the fidelity for reconstruction is $\mathcal{F}_c = \frac{2}{3}$.

This is the value of the classical limit of the reconstruction fidelity of the state shared by the dealer. If one is able to achieve a fidelity more than this with the help of a shared quantum resource (in this case, a tripartite entangled state), we say that there is a quantum advantage. Note that in [41] this calculation was done for a similar scenario and arrived at the same value, i.e., $\frac{2}{3}$.

III. APPROXIMATE CONTROLLED RECONSTRUCTION AND QUANTUM ADVANTAGE

We start with a three-qubit resource state ρ_{ABC} in the space $\mathcal{H}_A \otimes \mathcal{H}_B \otimes \mathcal{H}_C$. We can write it in parametric form as

$$\begin{aligned} \rho_{ABC} = \frac{1}{8}\Bigg(& I^{\otimes 3} + \sum_{i=1}^{3} a_i\sigma_i \otimes I^{\otimes 2} \\ &+ \sum_{j=1}^{3} I \otimes b_j\sigma_j \otimes I + \sum_{k=1}^{3} I^{\otimes 2} \otimes c_k\sigma_k \\ &+ \sum_{i,j=1}^{3} q_{ij}\sigma_i \otimes \sigma_j \otimes I + \sum_{i,k=1}^{3} r_{ik}\sigma_i \otimes I \otimes \sigma_k \\ &+ \sum_{j,k=1}^{3} s_{jk} I \otimes \sigma_j \otimes \sigma_k + \sum_{i,j,k=1}^{3} t_{ijk}\sigma_i \otimes \sigma_j \otimes \sigma_k\Bigg). \end{aligned} \tag{4}$$

Here a_i, b_j, and c_k are local Bloch vectors and the correlation matrices are given by $Q = \{q_{ij}\} = \mathrm{Tr}[\rho_{ABC}(\sigma_i \otimes \sigma_j \otimes I)]$, $R = \{r_{ik}\} = \mathrm{Tr}[\rho_{ABC}(\sigma_i \otimes I \otimes \sigma_k)]$, and $S = \{s_{jk}\} = \mathrm{Tr}[\rho_{ABC}(I \otimes \sigma_j \otimes \sigma_k)]$, which are of order 3×3. Here $\tau = t_{ijk} = \mathrm{Tr}[\rho_{ABC}(\sigma_i \otimes \sigma_j \otimes \sigma_k)]$ is the correlation tensor.

Now we find the reconstruction fidelity of the state shared in terms of the Bloch parameters of the three-qubit resource state ρ_{ABC}. The qubit § on Alice's side, parametrized by the Bloch vector ϕ, is given by

$$\rho_{\S} = \frac{1}{2}\left(I + \sum_i \phi_i \sigma_i\right). \tag{5}$$

In the standard scheme, measurement takes place at two phases of the protocol: first, on Alice's side of the shared qubit § along with Alice's share of the resource A, with projectors $P_l = |\Psi_l\rangle\langle\Psi_l|$ $(l = 0, 1, 2, 3)$, and second, on Bob's qubit, with projectors $P_x = |x\rangle\langle x|$ $(x = +, -)$. Here the Bell states are given as $|\Psi^3_{(0)}\rangle = \frac{1}{\sqrt{2}}(|01\rangle \pm |10\rangle)$ and $|\Psi^2_{(1)}\rangle = \frac{1}{\sqrt{2}}(|00\rangle \pm |11\rangle)$ and the Hadamard states are $|x_\pm\rangle = \frac{1}{\sqrt{2}}(|0\rangle \pm |1\rangle)$, respectively. The Bell state projectors can be written in the form

$$P_l = \frac{1}{4}\left(I^{\otimes 2} + \sum_{ij} t_{ij}\sigma_i \otimes \sigma_j\right). \tag{6}$$

The coefficients t_{ij} form a correlation matrix T_l ($l = 0, 1, 2, 3$ for different projectors). These are given by $T_0 = \mathrm{diag}(-1, -1, -1)$, $T_1 = \mathrm{diag}(-1, +1, +1)$, $T_2 = \mathrm{diag}(+1, -1, +1)$, and $T_3 = \mathrm{diag}(+1, +1, -1)$. The set of Hadamard projectors on Bob's side is given by $P_x = \frac{1}{2}(I + \mathbf{x}\cdot\sigma)$, with $\mathbf{x} = (\pm 1, 0, 0)$.

Now we find the output state of Charlie's qubit, after the two measurements followed by applying appropriate unitaries:

$$p_\alpha \varrho_\alpha = \mathrm{Tr}_{123}[(P_l \otimes P_x \otimes U_\alpha)(\rho_{\S} \otimes \rho_{ABC})(P_l \otimes P_x \otimes U_\alpha^\dagger)]. \tag{7}$$

The trace is taken over the original qubit, Alice's share, and Bob's share. The α acts as a multi-index for the pair (l, x). Here $p_\alpha = \mathrm{Tr}[(P_l \otimes P_x \otimes I)(\rho_{\S} \otimes \rho_{ABC})]$ is the probability of getting the measurement corresponding to the combination (P_l, P_x). Finally, U_α is the unitary operator chosen to reconstruct (a close approximation of) the state at Charlie's side. Substituting the expressions for the states and the projection operators, we obtain

$$\begin{aligned}\varrho_\alpha = \frac{1}{16 p_\alpha}\Bigg[\Bigg(1 + \frac{1}{2}\sum_i (T_l)_{ii} A_i \phi_i + \sum_i B_i \phi_i \\ + \frac{1}{2}\sum_{i,j}(T_l)_{ii} Q_{ij}\phi_i x_j\Bigg) I + \sum_{jk}\Omega_{jk}\Bigg(\sum_j C_j + \sum_{ij} S_{ij} x_i \\ + \frac{1}{2}\sum_{ij}(T_l)_{ii} R_{ij}\phi_i + \frac{1}{2}\sum_{ijm}(T_l)_{mm} t_{mij} x_i \phi_m\Bigg)\sigma_k\Bigg].\end{aligned} \tag{8}$$

Here $\{\Omega_\alpha\}$ are rotations in $\mathbb{R}^3$ obtained from the unitaries $\{U_\alpha\}$, given by the relation

$$U_\alpha \hat{n}\sigma U_\alpha^\dagger = (\Omega^\dagger \hat{n})\sigma = \sum_{ij}\Omega_{ij} n_i \sigma_j. \tag{9}$$

Now the expected fidelity of reconstruction, i.e., the closeness of Charlie's qubit to the original state, is given by the following integral over the Bloch sphere with uniform distribution M:

$$\mathcal{F} = \oint dM(\phi)\sum_\alpha p_\alpha \mathrm{Tr}(\varrho_\alpha \rho_{\S}). \tag{10}$$

After substituting expressions from Eqs. (8) and (5), omitting the terms that do not contribute to the integral, and using the relation

$$\oint \langle\phi, Y\phi\rangle dM(\phi) = \frac{1}{3}\mathrm{Tr}(Y), \tag{11}$$

the integral in (10) reduces to

$$\begin{aligned}\mathcal{F} = \frac{1}{16}\sum_\alpha \Bigg\{1 + \mathbf{B}\cdot\mathbf{x} + \frac{1}{3}\mathrm{Tr}(\Omega_\alpha^\dagger R^\dagger T_l) \\ + \frac{1}{3}\mathrm{Tr}[\Omega_\alpha^\dagger(\tau_{\lambda\mu\nu}x^\mu)^\dagger T_l]\Bigg\}.\end{aligned} \tag{12}$$

This is summed up over all α, i.e., all the (l, x) possibilities of the two measurements. Note that $\sum_\alpha \mathbf{B}\cdot\mathbf{x} = \sum_l\sum_x \mathbf{B}\cdot\mathbf{x} = 0$. Let T be the matrix formed by the elements $\{\sum_j t_{ijk}x_j\}$, or in tensor notation

$$T = \tau_{\lambda\mu\nu}x^\mu, \tag{13}$$

for $\mathbf{x} = (+1, 0, 0)$. Then, for $\mathbf{x} = (-1, 0, 0)$ we have $\tau_{\lambda\mu\nu}x^\mu = -T$. Thus, the summation can be split into two, based on x,

$$\begin{aligned}\mathcal{F} = \frac{1}{2} + \frac{1}{16}\frac{1}{3}\sum_l \mathrm{Tr}[T_l^\dagger(R + T)\Omega_{(l,+)}] \\ + \frac{1}{16}\frac{1}{3}\sum_l \mathrm{Tr}[T_l^\dagger(R - T)\Omega_{(l,-)}].\end{aligned} \tag{14}$$

Here we have expanded the multi-index α back in the pair form (l, x). Now we want to choose the rotations to maximize $\mathcal{F}$. As $-T_l^\dagger$ is also a rotation, the Ω_α's can be chosen independently to maximize each term. We take Ω' to be the rotation that maximizes the terms corresponding to $T_l^\dagger(R - T)$ and Ω'' for the terms corresponding to $T_l^\dagger(R + T)$. Now this expression is independent of l,

$$\mathcal{F}_{\max} = \max_{\Omega', \Omega''} \tfrac{1}{2}\big\{1 - \tfrac{1}{6}\mathrm{Tr}[(R + T)\Omega] - \tfrac{1}{6}\mathrm{Tr}[(R - T)\Omega']\big\}, \tag{15}$$

where the maximum is taken over all rotations Ω' and Ω''. Since Ω' and Ω'' can be independent of each other, we get the maximum as

$$\begin{aligned}\mathcal{F}_{\max} = \tfrac{1}{2}\big\{1 + \tfrac{1}{6}\mathrm{Tr}[\sqrt{(R + T)^\dagger(R + T)}] \\ + \tfrac{1}{6}\mathrm{Tr}[\sqrt{(R - T)^\dagger(R - T)}]\big\}.\end{aligned} \tag{16}$$

A tripartite resource state ϱ is useful for reconstruction of the state only when $\mathcal{F}_{\max} > \frac{2}{3}$, or when $\vartheta(\varrho) > 1$, where we define $\vartheta(\varrho)$ as

$$\vartheta(\varrho) := \tfrac{1}{2}(\|R + T\|_1 + \|R - T\|_1) \tag{17}$$

such that $\mathcal{F}_{\max} = \frac{1}{2}[1 + \frac{1}{3}\vartheta(\varrho)]$ and $\|\cdot\|_1$ denotes the trace norm of a matrix, given by $\|Z\|_1 = \mathrm{Tr}\sqrt{Z^\dagger Z}$. Hereon, we shall simply use $\mathcal{F}$ to denote the fidelity possible in the optimal case (which was denoted by $\mathcal{F}_{\max}$ until this point). Since R shows up in the expression, we conclude that the reconstruction of the state is not entirely because of the controlled reconstruction capability. There can be a situation when $T = O$ (O

TABLE I. Expression of $\vartheta(\rho)$ for different settings of (dealer, assistant, reconstructor).

Setting No.	Setting	Expression for $\vartheta(\rho)$
1	(Alice, Bob, Charlie)	$\vartheta_{AC}(\rho) = \frac{1}{2}(\|R + T_{AC}\|_1 + \|R - T_{AC}\|_1)$
2	(Charlie, Bob, Alice)	$\vartheta_{AC}(\rho) = \frac{1}{2}(\|R + T_{AC}\|_1 + \|R - T_{AC}\|_1)$
3	(Alice, Charlie, Bob)	$\vartheta_{AB}(\rho) = \frac{1}{2}(\|Q + T_{AB}\|_1 + \|Q - T_{AB}\|_1)$
4	(Bob, Charlie, Alice)	$\vartheta_{AB}(\rho) = \frac{1}{2}(\|Q + T_{AB}\|_1 + \|Q - T_{AB}\|_1)$
5	(Bob, Alice, Charlie)	$\vartheta_{BC}(\rho) = \frac{1}{2}(\|S + T_{BC}\|_1 + \|S - T_{BC}\|_1)$
6	(Charlie, Alice, Bob)	$\vartheta_{BC}(\rho) = \frac{1}{2}(\|S + T_{BC}\|_1 + \|S - T_{BC}\|_1)$

denotes the null matrix), but the value of $\mathcal{F}$ is greater than $\frac{2}{3}$. Here, as there is no tripartite correlation[1], Bob's involvement seems inconsequential. In a sense, this fidelity quantifies the information that can be retrieved as a result of this process. Hence, the CSR fidelity has contributions from both the reconstruction capacity of the three-qubit resource and the teleportation capacity of the two-qubit channel between the dealer and receiver.

Here the dealer-reconstructor subsystem of the resource ρ_{ABC} [from Eq. (4)] is given by

$$\rho_{AC} = \mathrm{Tr}_B(\rho_{ABC}) = \frac{1}{4}\left(I^{\otimes 2} + \sum_i a_i\sigma_i \otimes I + \sum_k I \otimes c_k\sigma_k + \sum_{ik} r_{ik}\sigma_i \otimes \sigma_k\right). \tag{18}$$

Using the result from [2], we can write the teleportation fidelity of ρ_{AC} as

$$\mathcal{F}'_{AC} = \tfrac{1}{2}\left(1 + \tfrac{1}{3}\mathrm{Tr}\sqrt{R^\dagger R}\right). \tag{19}$$

This analysis is for the case when Alice is the dealer and the final qubit is being reconstructed at Charlie's end with the assistance of Bob. However, there can be other cases with the same resource state when the roles are interchanged. This gives us an ordered triplet of (dealer, assistant, reconstructor), which we call the setting.

For some resource states like the GHZ state, all six settings are equivalent due to its symmetry. However, this cannot be generalized, as $\mathcal{F}$ for all the settings need not be the same. We thus need to define three different T matrices $T_{AB} = \{\mathrm{Tr}[\rho_{ABC}(\sigma_i \otimes \sigma_j \otimes \sigma_x)]\}_{ij}$, $T_{AC} = \{\mathrm{Tr}[\rho_{ABC}(\sigma_i \otimes \sigma_x \otimes \sigma_j)]\}_{ij}$, and $T_{BC} = \{\mathrm{Tr}[\rho_{ABC}(\sigma_x \otimes \sigma_i \otimes \sigma_j)]\}_{ij}$. Here the subscripts denote the subsystems that contribute to the matrix. For example, in T_{AB} the matrix indices correspond to the first and second subsystems of the three-qubit resource, as seen above. We can hence rewrite Eq. (17) for the six settings, as shown in Table I. As the table shows, the expression varies only based on the assistant and is symmetric in swapping the dealer and reconstructor. This symmetry is shared with the expression for fidelity of teleportation [2].

For simplicity, we will henceforth use the setting (Alice, Bob, Charlie) by default and follow the representation in Eq. (17), i.e., $T = T_{AC}$ and $\vartheta(\varrho) = \vartheta_{AC}(\varrho)$, unless specified otherwise. We have seen that the correlation matrix S is not present in Eq. (17). It is important to note that this does not rule out the role of Bob in the reconstruction of the state. It only tells us that the prior correlation between Bob and Charlie does not affect reconstruction fidelity. The only factors in determining it are the genuine correlation between Alice, Bob, and Charlie, captured by T, and the correlation matrix between the dealer and the reconstructor, denoted by R. Hence, we study different cases based on R and T which give an overview of how this score captures both state reconstructing fidelity and the teleportation fidelity of the channel between the source and the reconstructor. These also present us with some conditions on quantum advantage in terms of R and T.

A. Case 1: $R \neq O$ and $T \neq O$

This is the most general scenario when both R and T can take any value. In this case, it is not evident whether the fidelity score is entirely because of the state reconstruction capacity of the entire three-qubit state or due to the teleportation capacity of the dealer-reconstructor channel, or both. Consequently, we cannot pinpoint the main reason behind the quantum advantage. One way to address this situation is to look into the teleportation fidelity of the dealer-reconstructor subsystem. If the teleportation fidelity is at most $\frac{2}{3}$ and the reconstruction fidelity is greater than $\frac{2}{3}$, then we can conjecture that there is a quantum advantage because of the state reconstruction resource. We discuss different cases with the help of the following examples.

Example 1. As the first simple case we consider the GHZ state $|\mathrm{GHZ}\rangle = \frac{1}{\sqrt{2}}(|000\rangle + |111\rangle)$. The matrices R and T for the GHZ state can be found after writing the corresponding density state in its Bloch form

$$R = \begin{pmatrix} 0 & 0 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & 1 \end{pmatrix}, \quad T = \begin{pmatrix} 1 & 0 & 0 \\ 0 & -1 & 0 \\ 0 & 0 & 0 \end{pmatrix}.$$

This gives

$$\vartheta(\rho_W) = 3, \quad \mathcal{F}_{\max} = 1, \tag{20}$$

which is expected since it is already known that the GHZ state is used for perfect reconstruction. Note that the teleportation fidelity [from Eq. (19)] for the dealer-reconstructor subsystem

[1]In later sections of this paper, the term tripartite correlation or correlation tensor is sometimes used to talk about the matrix T. It is important to note that although it is derived from the tensor τ of order 3, T itself has order 2, and hence is described by a matrix [the reader can refer to Eq. (13) for clarification]. Regardless, we can use this terminology for simplicity, since T does capture a part of the tripartite correlation.

of this state is $\mathcal{F}' = \frac{1}{2}(1 + \frac{1}{3}) = \frac{2}{3}$. This clearly gives us a case with a quantum advantage arising from the state reconstruction ability of three-qubit resource states.

Example 2. In a case where both of the fidelities $\mathcal{F}'$ and $\mathcal{F}$ are greater than $\frac{2}{3}$, we cannot be sure whether the quantum advantage in the reconstruction fidelity $\mathcal{F}$ is entirely because of the state reconstruction resource. The W state, known to exhibit a different nature of entanglement from the GHZ state [42], is given by $|W\rangle = \frac{1}{\sqrt{3}}(|001\rangle + |010\rangle + |100\rangle)$. The R and T for the W state, from its Bloch representation of $\rho_W = |W\rangle\langle W|$, are

$$R = \begin{pmatrix} \frac{2}{3} & 0 & 0 \\ 0 & \frac{2}{3} & 0 \\ 0 & 0 & -\frac{1}{3} \end{pmatrix}, \quad T = \begin{pmatrix} 0 & 0 & \frac{2}{3} \\ 0 & 0 & 0 \\ \frac{2}{3} & 0 & 0 \end{pmatrix},$$

which gives

$$\vartheta(\rho_W) = \tfrac{7}{3}, \quad \mathcal{F}_{\max} = \tfrac{8}{9} \approx 0.89. \tag{21}$$

We see that $\mathcal{F}_{\max} \neq 1$, which is expected since it is already known that W states cannot be used for perfect controlled reconstruction [43], but $\vartheta(\rho_W) > 1$ (equivalently, $\mathcal{F}_{\max} > \frac{2}{3}$). In this case, the subsystem-teleportation fidelity for the dealer-reconstructor channel is found to be $\mathcal{F}' = \frac{1}{2}(1 + \frac{5}{9}) = \frac{7}{9}$. Since in this case $\mathcal{F}' > \frac{2}{3}$, we cannot claim that the quantum advantage here is due to genuine tripartite entanglement.

Example 3. Next we consider another example where we show the existence of a state within the paradigm of $R \neq O$ and $T \neq O$, for which the reconstruction fidelity is greater than $\frac{2}{3}$, whereas the teleportation fidelity of the dealer-reconstructor subsystem is less than or equal to $\frac{2}{3}$. This is a clear example of a state (other than the well-known GHZ state) for which quantum advantage is because of tripartite controlled reconstruction. In this context, let us consider a generalized W class of states. These states can be expressed as [44,45]

$$|\psi_W\rangle = \lambda_0 |000\rangle + \lambda_1 |100\rangle + \lambda_2 |101\rangle + \lambda_3 |110\rangle, \tag{22}$$

where $\lambda_i \in \mathbb{R}$, $\lambda_i \geqslant 0$, and $\sum_i \lambda_i^2 = 1$. For $\rho_{\tilde{W}} = |\psi_W\rangle\langle\psi_W|$, the matrices of interest are

$$R_{\tilde{W}} = 2\begin{pmatrix} \lambda_0\lambda_2 & 0 & \lambda_0\lambda_1 \\ 0 & -\lambda_0\lambda_2 & 0 \\ -\lambda_1\lambda_2 & 0 & \frac{1}{2} - \lambda_1^2 - \lambda_3^2 \end{pmatrix},$$

$$T_{\tilde{W}} = 2\begin{pmatrix} 0 & 0 & \lambda_0\lambda_3 \\ 0 & 0 & 0 \\ -\lambda_2\lambda_3 & 0 & -\lambda_1\lambda_3 \end{pmatrix}.$$

In Fig. 1 we plot the teleportation fidelity of the dealer-reconstructor subsystem [given by Eq. (19)] against the reconstruction fidelity [given by Eq. (17)] of these states, denoted by F' and F, respectively. The figure represents the entire set of W states (irrespective of R and T), with the orange region depicting states with $F' \leqslant \frac{2}{3}$, which is of interest, and correspondingly, the blue region has states with $F' > \frac{2}{3}$. This tells us that states in the orange region are depicting quantum advantage not because of the teleportation channel, while it is still inconclusive for the blue region. Since these are all pure states, $F \geqslant \frac{2}{3}$. Not all of these states satisfy $R \neq O$ and $T \neq O$, but one state that falls in this paradigm has been marked in the figure as an example of quantum advantage, as it lies in the orange region. This state is described by the parameters $\lambda_0 = \lambda_1 = 0.7$, $\lambda_2 \approx 0.09$, and $\lambda_3 \approx 0.11$. The standard W state has also been marked, which lies in the blue region, as expected from the discussion in Example 2.

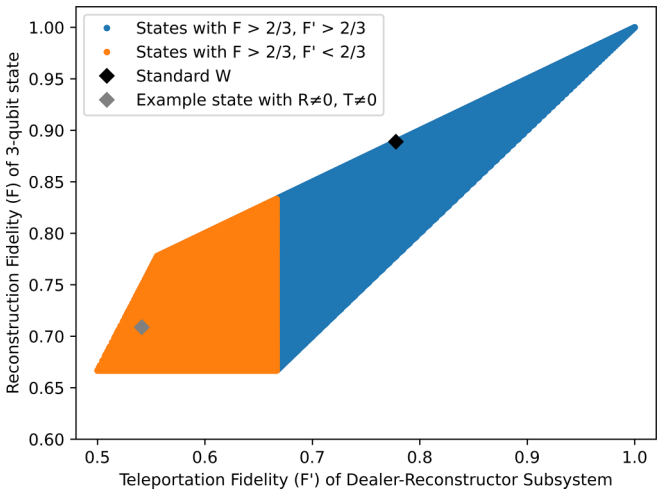

FIG. 1. Comparison of the reconstruction fidelity and subsystem-teleportation fidelity for 4×10^6 pure state resources uniformly sampled from the entire W class.

B. Case 2: $R = O$ and $T \neq O$

In this case, since the correlation matrix $R = O$, it can be said with certainty that there is no direct correlation between the dealer and the reconstructor. This means there will be no teleportation capacity of the channel between them and hence it will not affect the total reconstruction fidelity. In other words, if there is a quantum advantage in this region, we can surely claim that this is because of the tripartite controlled reconstruction capacity. However, the converse is not true. There can be states with $R \neq O$ for which there is no correlation between the dealer and the reconstructor. In other words, there can be quantum states whose quantum advantage arises solely from the T component of correlation even when $R \neq O$.

Theorem 1. If $R = O$ and $T \neq O$, the observed quantum advantage is only because of tripartite state reconstruction.

Proof. Putting $R = O$ in the expression for subsystem-teleportation fidelity [from Eq. (19)] gives $\mathcal{F}' = \frac{1}{2}$. Hence, no quantum information can flow from dealer to reconstructor through teleportation alone. Then the contribution to the reconstruction fidelity has to come from the tripartite channel. ■

Example. Consider the following states:

$$|\gamma_\pm\rangle = \frac{|000\rangle \pm |100\rangle \pm |110\rangle + |111\rangle}{2}.$$

Both these states fall into Case 1 but if we take their equal mixture $\rho_\gamma = \frac{1}{2}(|\gamma_-\rangle\langle\gamma_-| + |\gamma_+\rangle\langle\gamma_+|)$, R is found to be O. Moreover, we get $\mathcal{F} = \frac{3}{4} > \frac{2}{3}$, giving us a quantum advantage. Since $R = O$ and teleportation cannot contribute to the final fidelity, we infer that this advantage arises purely from the tripartite state reconstruction.

C. Case 3: $R \neq O$ and $T = O$

If in Eq. (17) $R \neq O$ but $T = O$, it can be said that there is no tripartite correlation and hence there is no involvement of Bob. So, in principle, there is no question of controlled reconstruction in this case. In such a case, if the reconstruction fidelity is greater than $\frac{2}{3}$, that is purely because of the teleportation capacity of the subsystem. However, the converse is not true as there can be tripartite states with $T \neq O$ but not having genuine quantum correlation.

Theorem 2. If $R \neq O$ and $T = O$, then the quantum advantage in the reconstruction is entirely because of the teleportation capacity of the subsystem between the dealer and the reconstructor.

Proof. Putting $T = O$ in Eq. (17), we get the expression

$$\vartheta(\rho_{ABC}) = \|R\|_1. \tag{23}$$

The expression in Eq. (19) now matches with the expression for reconstruction fidelity given by

$$\mathcal{F}_{\max} = \tfrac{1}{2}\big[1 + \tfrac{1}{3}\vartheta(\rho_{ABC})\big] = \tfrac{1}{2}\big(1 + \tfrac{1}{3}\|R\|_1\big).$$

Hence, it can be concluded that quantum advantage in this case is solely because of the teleportation channel between the dealer and the reconstructor. ■

Example. Consider the following states:

$$|\delta_\pm\rangle = \frac{|000\rangle \pm |100\rangle \pm |110\rangle + |111\rangle}{2}.$$

Both of these have $R \neq O \neq T$, but when their equal mixture is considered, for the mixed state ρ_δ we find $T = O$, where $\rho_\delta = \frac{1}{2}(|\delta_-\rangle\langle\delta_-| + |\delta_+\rangle\langle\delta_+|)$. In this case as well, we get $\mathcal{F} = \frac{3}{4} > \frac{2}{3}$. However, since T is O, we argue that this fidelity arises solely from the teleportation capacity of the channel between the sender and the reconstructor and hence the quantum advantage.

D. Case 4: $R = O$ and $T = O$

Here $\vartheta(\rho) = 0$, giving us $\mathcal{F}_{\max} = \frac{1}{2}$, which is no better than a random guess. In this case, there cannot be any quantum advantage because there is no flow of information from the dealer to the reconstructor.

IV. QUANTUM SECRET SHARING

For any secret-sharing protocol to be successful, neither of the shareholders should have useful information about the secret on their own. In other words, Charlie should not be able to reconstruct the secret without Bob's involvement and vice versa. In this context, we use the term useful information as the amount of extra information that can be obtained over the classical limit of the respective channels. One quantification can be the teleportation capability of the bipartite channels between the dealer and the shareholders. If this is more than $\frac{2}{3}$, then there is an information gain through the bipartite channel compared to what can be achieved classically. This enforces additional conditions on the resource to ensure the protocol is secure against dishonest parties. The maximum expected fidelity that Bob can obtain on his own accord is equivalent to the teleportation capacity of subsystem ρ_{AB} of the resource

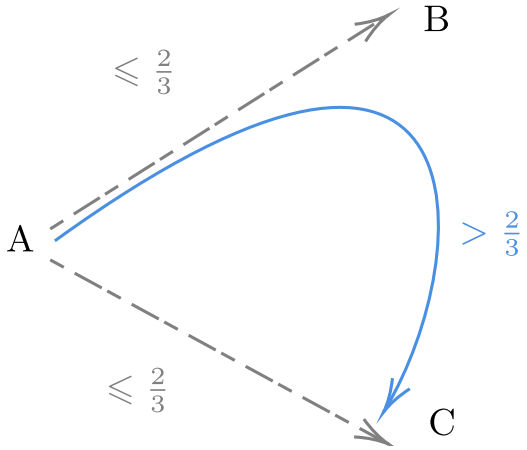

FIG. 2. Conditions for secret sharing (A denotes dealer, B assistant, and C reconstructor).

since Charlie is not involved. The state ρ_{AB} is given by

$$\begin{aligned}\rho_{AB} &= \mathrm{Tr}_C(\rho_{ABC}) \\ &= \frac{1}{4}\Bigg(I^{\otimes 2} + \sum_i a_i\sigma_i \otimes I + \sum_j I \otimes b_j\sigma_j \\ &\quad + \sum_{ij} q_{ij}\sigma_i \otimes \sigma_j\Bigg).\end{aligned}$$

The teleportation capacity of this bipartite resource, i.e., the maximum expected share of Bob without involving Charlie, is

$$\mathcal{F}'_{AB} = \tfrac{1}{2}\big(1 + \tfrac{1}{3}\mathrm{Tr}\sqrt{Q^\dagger Q}\big). \tag{24}$$

We have already seen the expression of $\mathcal{F}'_{AC}$ for Charlie's case in Eq. (19). Since we know that a state is useful for quantum teleportation when $\mathcal{F}' > \frac{2}{3}$ [2], we want

$$\begin{aligned}&\mathcal{F}'_{AB} \leqslant \tfrac{2}{3}, \quad \mathcal{F}'_{AC} \leqslant \tfrac{2}{3} \\ \Rightarrow\ &\mathrm{Tr}\sqrt{Q^\dagger Q} \leqslant 1, \quad \mathrm{Tr}\sqrt{R^\dagger R} \leqslant 1.\end{aligned} \tag{25}$$

These constraints, along with $\vartheta(\rho) > 1$ (or, equivalently, $\mathcal{F} > \frac{2}{3}$), together form the three conditions for successful QSS (see Fig. 2). This ensures that the secret is faithfully reconstructed. Additionally, it accounts for dishonest recipients (either Bob or Charlie), as this ensures that the information they can retrieve from the quantum resource, without faithfully cooperating, does not exceed the information that can be obtained classically even in the absence of the quantum channel. Thus, we are able to provide a way to characterize the states useful for secret sharing more precisely.

Example. Consider the following states:

$$|\beta_\pm\rangle = \frac{|000\rangle + |100\rangle + |101\rangle \pm |110\rangle}{2}.$$

The equal mixture of $|\beta_+\rangle\langle\beta_+|$ and $|\beta_-\rangle\langle\beta_-|$ gives $\mathrm{Tr}\sqrt{Q^\dagger Q} = \frac{1}{2} = \mathrm{Tr}\sqrt{R^\dagger R}$ and still gives $\mathcal{F} > \frac{2}{3}$, fulfilling all three conditions. This example demonstrates successful secret sharing, in addition to the well-known GHZ state. This is contrary to the belief that only the GHZ state is useful for secret sharing.

V. CONCLUSION

In this article we have given an expression for the maximum expected CSR fidelity for general three-qubit states in terms of their Bloch parameters. This fidelity has contributions from both the tripartite correlation tensor and the correlation matrix between the dealer-reconstructor subsystem. We reported a quantum advantage in the reconstruction of the state over its classical limit $\frac{2}{3}$. Different cases, in terms of the involved correlation matrices, were then investigated with respect to the CSR fidelity. We provided examples where the advantage is only because of the teleportation capacity of the subsystem and those where the advantage is mainly because of the state reconstruction capacity of the tripartite resource. We also discussed cases which are ambiguous when it comes to the cause of the quantum advantage. Our results revealed interoperability between quantum teleportation and CSR. This also led to avenues of research related to the interoperability that can exist in different quantum information processing tasks. We extended our analysis by outlining additional conditions that must be satisfied to ensure the protocol is secure by preventing any dishonest participant from having a quantum advantage. These conditions distinguish CSR from QSS in a true sense. Further work can be done in this context, analyzing the interference of eavesdroppers and how they can be detected. From a resource point of view, we were able to characterize the states that provide quantum advantage in CSR. In addition, we were able to identify the states that can be used as resources for QSS.

ACKNOWLEDGMENTS

The authors thank Dr. Shantanav Chakrabarty (Centre for Quantum Science & Technology, IIIT Hyderabad) and Dr. Nirman Ganguly (Department of Mathematics, BITS-Pilani Hyderabad) for their valuable input.

APPENDIX: CASE OF A DISHONEST PARTY IN THE CLASSICAL SCENARIO

Here we wish to see what happens in the case if one of the receiving parties (either Bob or Charlie) is dishonest. Since information from both the parties is required to reconstruct the qubit, the honest one can keep a check on the dishonest one. However, we also have to take a look at what might happen in the case where the dishonest person wants to guess the shared qubit based on what information they have.

Before we move on, let us look at the possible distributions of the values s_1 and s_2. Let $s_i \leftarrow \{p_0, p_1\}$ denote that s_i takes the value 0 with probability p_0 and 1 with probability p_1. Now if we have $s_1 \leftarrow \{p, 1-p\}$, then either $s_2 \leftarrow \{p, 1-p\}$ (if $s = 0$) or $s_2 \leftarrow \{1-p, p\}$ (if $s = 1$). In either case, both distributions are dependent on each other, and once one of the bits is sampled, the other bit is known with certainty.

Since the distributions are symmetric, without loss of generality, we can take Bob* as the dishonest party. He knows s_1 but has no knowledge of s_2 without communicating with Charlie. So he has to guess the bit s; we denote his guess of the bit by s', which is either the same as his bit s_1 or the negation of it.

The first case is for $s' = s_1$, or, equivalently, Bob* guesses $s_2 = 0$. Let $s_2 \leftarrow \{p, 1-p\}$. The fidelity between the original qubit and the one reconstructed by Bob can be expressed as (F^g is used to denote fidelity with the guess)

$$
\begin{aligned}
F^g(q, s') &= \Pr(s = s')F(q, s) + \Pr(s \neq s')F(q, \neg s) \\
&= \Pr(s_2 = 0)[\Pr(s = 0)\|\langle q|\uparrow\rangle\|^2 + \Pr(s = 1)\|\langle q|\downarrow\rangle\|^2] + \Pr(s_2 = 1)[\Pr(\neg s = 0)\|\langle q|\uparrow\rangle\|^2 + \Pr(\neg s = 1)\|\langle q|\downarrow\rangle\|^2] \\
&= (p)\left(\cos^2\frac{\theta}{2}\cos^2\frac{\theta}{2} + \sin^2\frac{\theta}{2}\sin^2\frac{\theta}{2}\right) + (1-p)\left(\sin^2\frac{\theta}{2}\cos^2\frac{\theta}{2} + \cos^2\frac{\theta}{2}\sin^2\frac{\theta}{2}\right) \\
&= p\left(1 - \frac{1}{2}\sin^2\theta\right) + \frac{1}{2}(1-p)\sin^2\theta = p\cos^2\theta + \frac{1}{2}\sin^2\theta.
\end{aligned}
$$

Hence the expected guess fidelity in this case is

$$
\mathcal{F}'^g = \langle F^g(q, s')\rangle = \frac{1}{4\pi}\int_{\theta=0}^{\pi}\int_{\phi=0}^{2\pi}\sin\theta\, d\theta\, d\phi\left(p\cos^2\theta + \frac{1}{2}\sin^2\theta\right) = \frac{1}{4\pi}2\pi\left(\frac{4}{3} - \frac{2}{3}p\right) = \boxed{\frac{2-p}{3}}.
$$

We want Bob*'s guess to be no better than a random one, or, equivalently, we want

$$
\mathcal{F}'^g \leqslant \frac{1}{2} \Rightarrow \frac{2-p}{3} \leqslant \frac{1}{2} \Rightarrow \boxed{p \geqslant \frac{1}{2}}. \tag{A1}
$$

The second case is for $s' = \neg s_1$, or, equivalently, Bob* guesses $s_2 = 1$. In this case,

$$
F^g(q, s') = \Pr(s_2 = 1)F(q, s) + \Pr(s_2 = 0)F(q, \neg s) = (1-p)\cos^2\theta + \frac{1}{2}\sin^2\theta
$$

$$
\text{and} \quad \mathcal{F}'^g = \langle F^g(q, s')\rangle = \boxed{\frac{1+p}{3}}.
$$

Enforcing the same condition as last time,

$$\mathcal{F}'^{g} \geqslant \frac{1}{2} \Rightarrow \frac{1+p}{3} \leqslant \frac{1}{2} \Rightarrow \boxed{p \leqslant \frac{1}{2}}. \tag{A2}$$

Both conditions will be satisfied if we set $p = \frac{1}{2}$. Hence, Alice can prevent either party from cheating if the uniform distribution is used to sample one of the bits.

[1] C. H. Bennett, G. Brassard, C. Crepeau, R. Jozsa, A. Peres, and W. K. Wootters, Phys. Rev. Lett. **70**, 1895 (1993).
[2] R. Horodecki, M. Horodecki, and P. Horodecki, Phys. Lett. A **222**, 21 (1996).
[3] I. Chakrabarty, Eur. Phys. J. D **57**, 265 (2010).
[4] S. Adhikari, N. Ganguly, I. Chakrabarty, and B. S. Choudhury, J. Phys. A: Math. Theor. **41**, 415302 (2008).
[5] C. H. Bennett, P. Hayden, D. W. Leung, P. W. Shor, and A. Winter, IEEE Trans. Inf. Theory, **51**, 56 (2005).
[6] Sohail, A. K. Pati, V. Aradhya, I. Chakrabarty, and S. Patro, Phys. Rev. A **108**, 042620 (2023).
[7] A. K. Pati, Phys. Rev. A **63**, 014302 (2000).
[8] C. H. Bennett and S. J. Wiesner, Phys. Rev. Lett. **69**, 2881 (1992).
[9] C. Srivastava, A. Bera, A. Sen De, and U. Sen, Phys. Rev. A **100**, 052304 (2019).
[10] T. Das, R. Prabhu, A. Sen De, and U. Sen, Phys. Rev. A **92**, 052330 (2015).
[11] S. Patro, I. Chakrabarty, and N. Ganguly, Phys. Rev. A **96**, 062102 (2017).
[12] M. Vempati, N. Ganguly, I. Chakrabarty, and A. K. Pati, Phys. Rev. A **104**, 012417 (2021).
[13] S. Roy, T. Chanda, T. Das, A. Sen De, and U. Sen, Phys. Lett. A **382**, 1709 (2018).
[14] S. Wehner, D. Elkouss, and R. Hanson, Science **362**, eaam9288 (2018).
[15] J. Biamonte, M. Faccin, and M. De Domenico, Commun. Phys. **2**, 53 (2019).
[16] G. Chiribella, G. M. D'Ariano, and P. Perinotti, Phys. Rev. A **80**, 022339 (2009).
[17] H. J. Kimble, Nature (London) **453**, 1023 (2008).
[18] C. Simon, Nat. Photon. **11**, 678 (2017).
[19] S. Sazim and I. Chakrabarty, Eur. Phys. J. D **67**, 174 (2013).
[20] K. Mukherjee, I. Chakrabarty, and G. Mylavarapu, Phys. Rev. A **107**, 032404 (2023).
[21] M. K. Shukla, M. Huang, I. Chakrabarty, and J. Wu, Mathematics **11**, 2440 (2023).
[22] M. Hillery, V. Bužek, and A. Berthiaume, Phys. Rev. A **59**, 1829 (1999).
[23] R. Cleve, D. Gottesman, and H.-K. Lo, Phys. Rev. Lett. **83**, 648 (1999).
[24] A. Karlsson, M. Koashi, and N. Imoto, Phys. Rev. A **59**, 162 (1999).
[25] S. Bandyopadhyay, Phys. Rev. A **62**, 012308 (2000).
[26] D. Markham and B. C. Sanders, Phys. Rev. A **78**, 042309 (2008).
[27] Q. Li, W. H. Chan, and D.-Y. Long, Phys. Rev. A **82**, 022303 (2010).
[28] S. Adhikari, I. Chakrabarty, and P. Agrawal, Quantum Inf. Comput. **12**, 253 (2012).
[29] M. Ray, S. Chatterjee, and I. Chakrabarty, Eur. Phys. J. D **70**, 114 (2016).
[30] S. Adhikari, arXiv:1011.2868.
[31] S. Sazim, C. Vanarasa, I. Chakrabarty, and K. Srinathan, Quantum Inf. Process. **14**, 4651 (2015).
[32] W. Tittel, H. Zbinden, and N. Gisin, Phys. Rev. A **63**, 042301 (2001).
[33] C. Schmid, P. Trojek, M. Bourennane, C. Kurtsiefer, M. Zukowski, and H. Weinfurter, Phys. Rev. Lett. **95**, 230505 (2005).
[34] C. Schmid, P. Trojek, S. Gaertner, M. Bourennane, C. Kurtsiefer, M. Zukowski, and H. Weinfurter, Fortschr. Phys. **54**, 831 (2006).
[35] J. Bogdanski, N. Rafiei, and M. Bourennane, Phys. Rev. A **78**, 062307 (2008).
[36] P. Mudholkar, C. Vanarasa, I. Chakrabarty, and S. Kannan, arXiv:2112.15556.
[37] X.-H. Li and S. Ghose, Phys. Rev. A **90**, 052305 (2014).
[38] A. Kumar, S. Haddadi, M. R. Pourkarimi, B. K. Behera, and P. K. Panigrahi, Sci. Rep. **10**, 13608 (2020).
[39] S. Gangopadhyay, T. Wang, A. Mashatan, and S. Ghose, Phys. Rev. A **106**, 052433 (2022).
[40] A. Garg and S. Adhikari, arXiv:2307.16574.
[41] A. Karlsson and M. Bourennane, Phys. Rev. A **58**, 4394 (1998).
[42] W. Dür, G. Vidal, and J. I. Cirac, Phys. Rev. A **62**, 062314 (2000).
[43] A. Das, S. Nandi, S. Sazim, and P. Agrawal, Eur. Phys. J. D **74**, 91 (2020).
[44] A. Acín, D. Bruß, M. Lewenstein, and A. Sanpera, Phys. Rev. Lett. **87**, 040401 (2001).
[45] P. Pandya, A. Misra, and I. Chakrabarty, Phys. Rev. A **94**, 052126 (2016).