Controlled quantum teleportation in the presence of an adversary

Sayan Gangopadhyay,[1,2,*] Tiejun Wang,[3] Atefeh Mashatan [ORCID],[4] and Shohini Ghose[1,2,5,†]

[1]*Institute for Quantum Computing, University of Waterloo, Waterloo, Ontario N2L 3G1, Canada*
[2]*Department of Physics and Astronomy, University of Waterloo, Waterloo, Ontario N2L 3G1, Canada*
[3]*School of Science, Beijing University of Posts and Telecommunications, Beijing 100876, China*
[4]*Ted Rogers School of Information Technology Management, Toronto Metropolitan University, Toronto, Ontario M5B 2K3, Canada*
[5]*Department of Physics and Computer Science, Wilfrid Laurier University, Waterloo, Ontario N2L 3C5, Canada*

We present a device-independent analysis of controlled quantum teleportation where the receiver is not trusted. We show that the notion of genuine tripartite nonlocality allows us to certify control power in such a scenario. By considering a specific adversarial attack strategy on a device characterized by depolarizing noise, we find that control power is a monotonically increasing function of genuine tripartite nonlocality. These results are relevant for building practical quantum communication networks and also shed light on the role of nonlocality in multipartite quantum information processing.

I. INTRODUCTION

Controlled quantum teleportation (CQT) is a paradigmatic multipartite quantum communication protocol where a third party (or parties) determines the success or failure of quantum teleportation [1]. In the standard quantum teleportation protocol [2], an arbitrary qubit is teleported from Alice to Bob using maximally entangled Einstein-Podolsky-Rosen (EPR) states. This idea has found applications in several quantum information schemes such as quantum gate teleportation [3], cluster state quantum computing [4], and quantum repeaters [5]. Controlled quantum teleportation is an important multipartite extension of bipartite quantum teleportation [1]. CQT is an integral part of the design of quantum teleportation networks (QTN) that could form the backbone of the future quantum internet [6–9].

In the simplest CQT scheme, the success or failure of teleportation of a qubit from the sender to the receiver can be decided by a third party, also known as the controller, Charlie [1]. This scheme works under the assumption that all parties are trusted, i.e., their devices and measurements are working exactly according to the specifications provided by the supplier. However, this is often not the case in real applications. There may be physical imperfections in the devices and measurement directions, which can not only lead to a lower teleportation fidelity but also can be used by an adversary to control the success or failure of teleportation. In scenarios where the precise knowledge of the underlying quantum state and measurement settings is not available, the framework of device-independent (DI) quantum information processing can be useful [10].

Traditionally, the notion of Bell nonlocality has been used for DI quantum information applications [11]. Bell nonlocality refers to the phenomenon in which correlations obtained by performing local measurements on distant entangled states cannot be explained by any local hidden variable (LHV) model [12]. Bell nonlocality is often quantified by the violation of Bell inequalities. In applications such as DI quantum key distribution (DIQKD) [13], the violation of a Bell inequality strictly bounds the information leaked to an eavesdropper. Other notable applications of DI analysis include randomness amplification [14] and obtaining computational advantages [15]. What makes the DI formulation so powerful is the minimalism in assumptions regarding the functioning of the devices involved; it relies only on the observed measurement outcome correlations.

Recently, a stronger form of Bell's inequality has been used in the DI study of a multipartite quantum communication protocol called secret sharing [16]. A secret bit is split among $n - 1$ parties in such a way that at least $m \leqslant n - 1$ parties must collaborate to reveal it. Moreover, up to $n - 2$ parties can be untrusted. It was shown that the maximal violation of Svetlichny's inequality [17] guarantees that no information is leaked to an untrusted receiver. For nonmaximal violation, it was observed that the larger the Svetlichny inequality violation, the smaller the information leaked to the untrusted parties. In Ref. [16], the secret message was a classical bit, whereas a quantum secret sharing protocol can also share qubits. In the tripartite case, a quantum secret sharing (QSS) protocol becomes equivalent to a CQT protocol where Alice's secret qubit can be recovered by Bob if and only if Charlie assists [18]. This naturally leads one to ask what the role and nature of nonlocality is in the DI analysis of QSS where the secret is quantum. A first step towards that goal would be to study DI tripartite QSS or equivalently, DI CQT. While DI quantum teleportation of a qubit was published close to a decade ago [19], a DI study of CQT is still an open question.

In this work, we consider a CQT scenario where the receiver is untrusted. The receiver can collude with an external eavesdropper to increase the fidelity of teleportation beyond

*sgangopa@uwaterloo.ca
†sghose@wlu.ca

the classical limit even when the controller has not allowed it. Despite the allowed collusion and depending on the nature of the device used, it might still be impossible for Bob to achieve a teleportation fidelity as high as that with Charlie's participation. Therefore, an untrusted receiver may lead to a decrease in control power but not entirely nullify it. We quantify the effective control power in this scenario and show that the maximal violation of the Svetlichny inequality guarantees maximum control power. We also show that the effective control power is nonzero for a significant range of the Svetlichny inequality violation where it is monotonically increasing. Finally, we emphasize the necessity of genuine tripartite nonlocality in the DI certification of the CQT scheme. We discuss the relevance and importance of these results in Sec. V.

II. BACKGROUND

A. Control power in CQT

The controlled quantum teleportation protocol is similar to the standard quantum teleportation protocol with an added step. The objective is to teleport an unknown qubit from Alice to Bob only with the permission of the controller, Charlie.

(1) Let Alice, Bob, and Charlie share a GHZ state of the form $(|000\rangle_{ABC} + |111\rangle_{ABC})/\sqrt{2}$. It can be equivalently expressed as $(|\phi^+\rangle_{AB}|+\rangle_C + |\phi^-\rangle_{AB}|-\rangle_C)/\sqrt{2}$. Henceforth, the subscripts A, B, C will be dropped.

(2) Charlie performs a projective measurement in the σ_X basis and gets an outcome $\gamma \in \{\pm 1\}$. His measurement operators are given by

$$M_C^\gamma = \frac{(\mathbb{I}_2 + \gamma\sigma_X)}{2}; \quad \gamma \in \{\pm 1\}. \tag{1}$$

After Charlie's measurement, Alice and Bob's joint state can be written as

$$\rho_\gamma^{AB} = tr^C\left[\rho_{GHZ}\left(\mathbb{I} \otimes \mathbb{I} \otimes M_C^\gamma\right)\right] \tag{2}$$

$$= |\phi^\gamma\rangle\langle\phi^\gamma|. \tag{3}$$

(3) Let the arbitrary state to be teleported be

$$\rho^a = \frac{\mathbb{I}_2 + \vec{a} \cdot \vec{\sigma}}{2}. \tag{4}$$

Alice performs a Bell state measurement on the first two qubits of the state $\rho^a \otimes \rho_\gamma^{AB}$. The Bell state measurement is

described by the following measurement operators:

$$M_{c_0c_1}^A = |\phi^{c_0c_1}\rangle\langle\phi^{c_0c_1}|, \tag{5}$$

where

$$|\phi^{00}\rangle = \frac{|00\rangle + |11\rangle}{\sqrt{2}}; |\phi^{01}\rangle = \frac{|00\rangle - |11\rangle}{\sqrt{2}},$$

$$|\phi^{10}\rangle = \frac{|01\rangle + |10\rangle}{\sqrt{2}}; |\phi^{11}\rangle = \frac{|01\rangle - |10\rangle}{\sqrt{2}}.$$

After Alice's measurement, Bob's state is projected into

$$\rho_{c_0c_1}^B = \frac{\mathbb{I}_2 + (R_{c_0c_1\gamma}\vec{a}) \cdot \vec{\sigma}}{2}, \tag{6}$$

where

$$R_{0,0,+1} = \mathbb{I}_3; R_{0,1,+1} = R_z(\pi),$$
$$R_{1,0,+1} = R_x(\pi); R_{1,1,+1} = R_y(\pi),$$
$$R_{0,0,-1} = R_z(\pi); R_{0,1,-1} = \mathbb{I}_3,$$
$$R_{1,0,-1} = R_y(\pi); R_{1,1,-1} = R_x(\pi). \tag{7}$$

$R_x(\pi)$, $R_y(\pi)$, $R_z(\pi)$ represent rotations by π along the three orthogonal directions.

(4) Now Bob performs an $R_{c_0c_1\gamma}^{-1}$ rotation to retrieve ρ^a,

$$\rho^B = \frac{\mathbb{I}_2 + (R_{c_0c_1\gamma}^{-1}R_{c_0c_1\gamma}\vec{a}) \cdot \vec{\sigma}}{2} = \frac{\mathbb{I}_2 + \vec{a} \cdot \vec{\sigma}}{2} = \rho^a. \tag{8}$$

The average fidelity of teleportation between the unknown pure state (ρ^a) and Bob's final state (ρ^B) is calculated as

$$F = \int \frac{d\vec{a}}{4\pi}\langle a|\rho^B|a\rangle, \tag{9}$$

where the averaging has been performed over all pure qubit states. Henceforth, we will refer to the average fidelity of teleportation performed with Charlie's participation as F_C and that without Charlie's participation as F_{NC}. From Eqs. (8) and (9),

$$F_C = \int \frac{d\vec{a}}{4\pi}\langle a|\frac{\mathbb{I}_2 + \vec{a} \cdot \vec{\sigma}}{2}|a\rangle = 1. \tag{10}$$

Suppose Charlie does not reveal γ. Bob will randomly perform either $R_{c_0c_1,+1}^{-1}$ or $R_{c_0c_1,-1}^{-1}$. In that case, the average teleportation fidelity is given by

$$F_{NC} = \int \frac{d\vec{a}}{4\pi} \sum_{\gamma,\gamma'\in\{1,-1\}} \sum_{c_0,c_1\in\{0,1\}} P(\gamma,\gamma',c_0,c_1)\langle a|\frac{\mathbb{I}_2 + (R_{c_0c_1\gamma}^{-1}R_{c_0c_1\gamma'}\vec{a}) \cdot \vec{\sigma}}{2}|a\rangle = \frac{2}{3}. \tag{11}$$

The higher the difference between the above fidelities, the higher the control. The control power (P) of Charlie is therefore expressed as follows [20]:

$$P = F_C - F_{NC} = 1 - \frac{2}{3} = \frac{1}{3}. \tag{12}$$

B. Device-independent certification of quantum resources used in teleportation

In the usual two-party teleportation protocol using EPR states, Bancal *et al.* [19] suggested a construction by which

it is possible to device-independently certify whether a teleportation device is using quantum resources. Alice and Bob are given a pair of black boxes that supposedly perform the quantum teleportation of a qubit. The input of each box is a unit vector of the Bloch sphere. Alice's box takes the state to be teleported as the input given by the vector $\vec{a}$ and outputs two bits $(c_0c_1) \in \{0, 1\}^2$. In the black box scenario of teleportation, it is assumed that Alice knows the state to be teleported. Bob's box takes a vector $\vec{b}$ as input and gives one bit output $\beta \in \{+1, -1\}$. $\vec{b}$ represents a measurement of the

teleported state in the $\vec{b} \cdot \vec{\sigma}$ direction. The vendor claims that their boxes contain EPR states, using which the teleportation is performed on each run. Alice and Bob wish to verify the vendor's claim. In Ref. [19], it was shown that it is possible to infer *a posteriori* whether the black boxes used quantum resources to perform the teleportation from the input/output statistics of the boxes.

In a teleportation protocol, Alice is typically required to send (c_0, c_1) to Bob such that he can perform the appropriate corrective rotation based on some preestablished agreement to prepare the unknown qubit. However, it was shown [21] that two classical bits of information are enough to simulate the statistical correlations of the maximally entangled singlet state. Hence, a black box certification of quantum resources is not possible if Alice communicates with Bob. Therefore, Alice and Bob do not reveal any of their measurement input/output until several (ideally infinite) rounds have been completed. Each round consists of the pair of boxes taking inputs $(\vec{a}, \vec{b})$ and giving outputs $(c_0 c_1, \beta)$. In the end, they can construct the probability distributions $P(c_0 c_1, \beta | \vec{a}, \vec{b})$. Alice and Bob have no knowledge of the inner working of the composite black boxes except that they are not communicating. It is also assumed that Alice and Bob have free will. At the end of the protocol, the only information they have is the data table of inputs and outputs $(c_0 c_1, \beta | \vec{a}, \vec{b})$ for each round. Using this, they must test whether the source of correlations is quantum. This scenario can be easily mapped into a Bell scenario.

Let Alice choose from state settings $\{\vec{a_1}, \vec{a_2}\}$ and Bob choose from measurement setting $\{\vec{b_1}, \vec{b_2}\}$. Alice's black box gives two bits (c_0, c_1) as the output, which must be mapped to one bit. This can be done by choosing $\alpha = 2c_j - 1$ if Alice's input is a_j. Thus, one can construct the distributions $P(\alpha, \beta | j, k)$ from $P(c_0 c_1, \beta | \vec{a}, \vec{b})$. Finally, the Clauser-Horne-Shimony-Holt (CHSH) Bell function can be calculated as

$$CHSH = \sum_{j,k \in \{0,1\}} P(\alpha = \beta | j, k) - P(\alpha \neq \beta | j, k). \quad (13)$$

If $CHSH > 2$, it is guaranteed that the pair of black boxes generate statistical correlations that are not possible to obtain using only classical resources [12]. In other words, if $CHSH > 2$, it is certified that quantum resources are being used for teleportation.

III. DEVICE-INDEPENDENT CONTROLLED TELEPORTATION OF A QUBIT TO AN UNTRUSTED RECEIVER

Here we consider the controlled teleportation scenario where a qubit in the possession of Alice (sender) is teleported to Bob (receiver) only when Charlie (controller) participates. However, we assume that Bob is not a trusted party. Bob can collude with external agents henceforth labeled Derek to extract extra information that can increase the fidelity of teleportation beyond the classical limit of 2/3 even without Charlie's participation. The presence of an untrusted receiver does not necessarily imply that the controller has no impact on the teleportation fidelity. In spite of the allowed collusion and depending on the nature of the device used, it might still be impossible for Bob to achieve a teleportation fidelity as high

as that with Charlie's participation. In this section, we address the question of how to device-independently certify control power in such a scenario.

The goal of a CQT protocol is to ensure that Charlie can control whether quantum resources are being used for teleportation. Hence, it is necessary to first certify that the given device is capable of using quantum resources for teleportation. We will present a construction using which it is possible to certify whether quantum resources are being used for controlled teleportation to an untrusted receiver.

The idea of certification of quantum resources used in black box teleportation described in Sec. II B can be adapted for black box controlled teleportation.

A. Scenario

Derek supplies three black boxes to Alice, Bob, and Charlie that can allegedly perform controlled quantum teleportation of a qubit such that Charlie is the controller, Alice is the sender, and Bob is the receiver. The ideal functions of the three black boxes are as follows:

(1) Charlie's black box accepts a measurement setting $\vec{c} \in S^2$ as input and upon measurement gives an outcome $\gamma \in \{+1, -1\}$.

(2) Alice's black box accepts the state to be teleported $\vec{a} \in S^2$ as input and upon Bell measurement [Eq. (5)] gives an outcome $s_0 s_1 \in \{0, 1\}^2$.

(3) Bob's black box performs a corrective rotation $R^{-1}_{s_0 s_1 \vec{c} \gamma}$ which is specified in the instruction manual of the device. It accepts a measurement setting $\vec{b} \in S^2$ as input and upon measurement gives an outcome $\beta \in \{+1, -1\}$.

In an ideal CQT scheme, the shared state of Alice's, Bob's, and Charlie's black boxes is the Greenberger—Horne—Zeilinger (GHZ) state $(|000\rangle + |111\rangle)/\sqrt{2}$. The analysis of this ideal scheme has been shown in Sec. II A. The control power of Charlie for the ideal CQT scheme is $P = \frac{1}{3}$.

However, we do not assume anything *a priori* regarding the inner working of the black boxes—including the underlying composite state of Alice, Bob, and Charlie and their individual measurement basis. Additionally, we do not trust the receiver Bob. Therefore, Alice and Charlie are *trusted* and Bob is *untrusted*.

B. The adversary

In the above scenario III A, let Bob be the untrusted part and Derek be the eavesdropper. Together, they play the role of an *adversary*.

1. Adversarial goal

The goal of the adversary is to maximize the average teleportation fidelity when Charlie has not allowed the teleportation, i.e., not revealed the input setting $\vec{c}$ and the outcome γ of his measurement.

2. Adversarial capabilities

(1) The eavesdropper Derek is restricted to acting on individual signals separately.

(2) Derek can generate the shared states of the black boxes, i.e., hold the common source of correlations, but has no direct access to the input/output variables of the three parties.

(3) The untrusted party, Bob, can correlate his inputs with that of the common source of correlations held by Derek.

(4) Derek and Bob can jointly extract another outcome δ that can be potentially used to increase the fidelity of teleportation. This means that the corrective rotation performed by Bob can also depend on δ. This extra capability of the adversary allows us to write Bob's corrective rotations as $R^{-1}_{s_0 s_1 \vec{c} \gamma \delta}$ in contrast to $R^{-1}_{s_0 s_1 \vec{c} \gamma}$ in the ideal scenario.

C. Device-independent test of quantum resources

In order to account for the adversary, we consider here a modification of the ideal scenario of Sec. III A:

1. Device-independent test scenario

(1) Derek is the manufacturer and supplier of the black boxes of Alice, Bob, and Charlie.

(2) Alice's, Bob's, and Charlie's black boxes cannot communicate with each other.

(3) Charlie's black box accepts a measurement setting out of two distinct choices $\vec{c} \in \{\vec{c}_0, \vec{c}_1\}$ as input and upon measurement gives an outcome $\gamma \in \{+1, -1\}$.

(4) Alice's black box accepts the state to be teleported out of two distinct states $\vec{a} \in \{\vec{a}_0, \vec{a}_1\}$ as input and, upon Bell measurement [Eq. (5)], gives an outcome $s_0 s_1 \in \{0, 1\}^2$.

(5) Bob's black box performs a corrective rotation R^{-1}_δ given to him by Derek. It accepts a measurement setting out of two distinct choices $\vec{b}' \in \{\vec{b}'_0, \vec{b}'_1\}$ as input and, upon measurement, gives an outcome $\beta \in \{+1, -1\}$. Equivalently, the corrective rotation can be included in the measurement of Bob such that the new measurement choices are $\vec{b} = \{\vec{b}_0 = R^{-1}_\delta \vec{b}'_0, \ \vec{b}_1 = R^{-1}_\delta \vec{b}'_1\}$.

(6) Alice and Charlie independently choose their individual measurement setting. Their choice of measurement setting depends only on their free will. However, Bob's choice of measurement setting can be influenced by Derek. Therefore, the untrusted receiver does not have free will.

(7) We require that the announcement of inputs and measurement outcomes be made simultaneously by all parties after several rounds of the experiment have been completed. This ensures that the inputs or outcomes of the trusted parties are not used to the advantage of the untrusted party.

(8) The announcements at the end of several rounds of sending in inputs and recording outcomes from each black box will be a table of $(s_0 s_1, \beta, \gamma)$ given (j, k, l) for each round where j, k, l denote the input setting (0 or 1) of Alice, Bob, and Charlie, respectively. From this data, the joint probability distribution $p(s_0 s_1, \beta, \gamma | j, k, l)$ can be computed.

For the purpose of device-independent testing, we require that Alice's output $s_0 s_1$ be mapped into a single bit α in the following way:

$$\alpha = 2s_j - 1, \quad \text{where Alice's input is } \vec{a}_j.$$

Using this map, one can construct the distributions $P(\alpha, \beta, \gamma | j, k, l)$ from $P(s_0 s_1, \beta, \gamma | j, k, l)$. We note that the choice of input merely indicates that each party can choose to
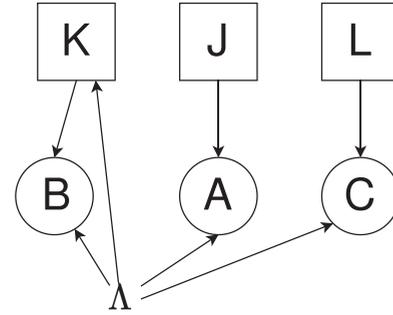

FIG. 1. DAG representation of the causal model where Λ is the common source of correlations supplied by Derek. In a classical model, Λ is a shared random variable, whereas in a quantum model, Λ is a potentially entangled quantum state ρ. Here J, K, L denote the inputs of Alice, Bob, and Charlie, respectively. A, B, C denote the outcomes of Alice, Bob, and Charlie, respectively. Note that since Bob is untrusted, he can correlate his inputs with that of the common source of correlations.

press one out of two buttons. It is assumed that the parties do not know which measurement basis the buttons correspond to.

2. Causal structure of the device-independent test scenario

The formalism of directed acyclic graphs (DAG) [22] will be used in later sections to characterize the correlations generated in the DI scenario of CQT with an untrusted receiver. The causal structure of inputs, outcomes, and common source of correlations of the different parties involved can be represented in the following way using DAG: In Fig. 1, each directed edge represents a causal relation between two nodes. The start of each edge is called the parent node and the arrival of each edge is called the child node. In a classical causal model, the source of correlations and all other nodes are random variables such that the parent nodes completely characterize a child node.

The explanation of how to interpret the DAG in Fig. 1 is as follows:

(1) The node Λ represents the common source of correlations (the underlying state in the black boxes) supplied by the eavesdropper Derek.

(2) J, K, L denote the inputs (measurement choices) of Alice, Bob, and Charlie, respectively. A, B, C denote the outcomes α, β, γ of Alice, Bob, and Charlie, respectively.

(3) The arrows from Λ to A, B, and C represent the fact that the outputs of Alice, Bob, and Charlie depend on the underlying state of their black boxes.

(4) The arrows from J, K, L to A, B, C respectively represent the dependence of the outcomes of each party on the choice of their measurement setting.

(5) There are no arrows from the input or outcome of one party to another because their black boxes are not allowed to communicate with each other (Sec. III C 1).

(6) Since the inputs of the trusted parties Alice and Charlie can be independently chosen (measurement setting choice independence/free will), J and L have no parent nodes.

(7) Since Bob is untrusted, his input may be correlated with that of the common source of correlations. Hence, Bob does not have measurement independence. The arrow from

Λ to K represents the fact that Bob's choice of measurement setting depends on the information he receives from Derek through the black box.

(8) Extra arrows from inputs/outcomes from one party to another were avoided due to the requirement that all announcements be made simultaneously at the end of several rounds.

If $\{v_i\}_{i=1}^n$ denotes the nodes of the graph, $p(v_k|v_1, v_2, ..., v_n) = p[v_k|pa(v_k)]$, where $pa(v_k)$ denotes all parent nodes of v_k. Thus, the joint probability distribution of all the nodes is given by $p(v_1, v_2, ..., v_n) = \Pi_{v_i} p[v_i|pa(v_i)]$.

Therefore, in the causal structure with an untrusted receiver (Fig. 1), if Λ is a classical random variable then the joint probabilities must admit the following decomposition:

$$p(\alpha\beta\gamma|jkl) = \sum_\lambda p(\alpha|j\lambda)p(\beta|k\lambda)p(\gamma|l\lambda)\frac{p(k|\lambda)p(\lambda)}{p(k)}. \tag{14}$$

3. Bell inequality characterizing the device-independent test scenario

In Ref. [22], it was shown that the following DAGs are equivalent:

This means that the DAG representing the device-independent scenario of controlled teleportation with an untrusted receiver (leftmost DAG) is equivalent to the broadcasting scenario (rightmost DAG). Broadcasting represents a scenario where one or more parties can openly communicate their choice of input to other parties. Here, in the rightmost DAG it is seen that Bob communicates his choice of input to Alice and Charlie.

In Ref. [23], the Bell inequalities characterizing the broadcasting scenario were studied. In the case of n parties, out of which $n - m$ parties broadcast their inputs to all other parties and the remaining m parties do not communicate their input to any other party, the tight bound to a specific Bell inequality called the Svetlichny inequality was found.

The Svetlichny function involves distributions of the form $p(\alpha\beta\gamma|jkl)$ which is obtained from the device-independent test rounds.

$$\begin{aligned} S = &p_A(+1 \mid 0)\text{CHSH}_{(+1)0} - p_A(-1 \mid 0)\text{CHSH}_{(-1)0} \\ &+ p_A(+1 \mid 1)\text{CHSH}'_{(+1)1} - p_A(-1 \mid 1)\text{CHSH}'_{(-1)1}, \end{aligned} \tag{15}$$

where $p_A(\alpha \mid j)$ is the marginal probability of Alice, $\text{CHSH}_{\alpha j}$ and $\text{CHSH}'_{\alpha j}$ refer to symmetries of the CHSH inequality given by $\text{CHSH}_{\alpha j} = E_{(+1)0}^{\alpha j} + E_{(+1)1}^{\alpha j} + E_{(-1)0}^{\alpha j} - E_{(-1)1}^{\alpha j}$ and $\text{CHSH}'_{\alpha j} = E_{(+1)0}^{\alpha j} - E_{(+1)1}^{\alpha j} - E_{(-1)0}^{\alpha j} - E_{(-1)1}^{\alpha j}$, and $E_{kl}^{\alpha j} = \sum_{\beta,\gamma=+1,-1} \beta\gamma \ p(\beta, \gamma \mid j, \alpha, k, l)$ is the expectation value of the measurement outcome of Bob and Charlie conditioned on a given outcome α and the input j of Alice.

The result from Ref. [23] that we will use in this chapter is given by the following statement:

For the broadcasting scenario where $n - m$ is odd, $|S| \leqslant 2^{(n-m)/2+3/2}$.

Moreover, this bound is tight, i.e., there exists a classical strategy (Λ) such that $|S| = 2^{(n-m)+3/2}$.

In the broadcasting scenario of our interest (rightmost DAG in Fig. 2), $n = 3$ and $n - m = 1$. Therefore, in this case,

$$|S| \leqslant 4. \tag{16}$$

Using this result [Eq. (16)] and the equivalence of DAG (Fig. 2), we can immediately state the following:

Theorem 1. Any probability distribution $p(\alpha\beta\gamma|jkl)$ admitted by the DAG representing the device-independent test scenario of controlled quantum teleportation with an untrusted receiver (as defined in Sec. III C 1) using classical strategies must satisfy the Svetlichny inequality $|S| \leqslant 4$. Moreover, this bound is tight.

Condition for certification of quantum resources: If the Svetlichny inequality $|S| \leqslant 4$ is violated, it is guaranteed that the observed probability distribution $p(\alpha\beta\gamma|jkl)$ was not generated entirely by classical means. Hence, the source of correlations (Λ) must be quantum.

4. Comparison with the device-independent scenario of fully trusted controlled quantum teleportation

In controlled quantum teleportation where all parties are trusted, it is easy to see that the device-independent test scenario is represented by the DAG given in Fig. 3. This device-independent scenario is certified to be quantum if the obtained correlations violate Mermin's inequality [24]. A maximal violation of Mermin's inequality implies that the underlying state is the GHZ state, therefore guaranteeing maximum control power. However, it was shown in Ref. [16] that there exists a local model in the broadcasting scenario of Fig. 2 that violates Mermin's inequality maximally. Since the device-independent scenario of controlled teleportation with an untrusted receiver is equivalent to the broadcasting scenario (Fig. 2), Mermin's inequality is not sufficient for its certification.

The presence of an untrusted part makes it necessary to use a stronger notion of nonlocality also known as genuine tripartite nonlocality/Svetlichny nonlocality for the certification of controlled teleportation.

5. When is the controller's authority maximum?

Theorem 2. Controller's authority is maximum with $P = \frac{1}{3}$ in the controlled quantum teleportation scheme if $S = 4\sqrt{2}$ is obtained from the device-independent test.

Because of the normalization of $p_A(a \mid j)$, to achieve the maximum quantum violation $S = 4\sqrt{2}$, we must necessarily have $\text{CHSH}_{(-1)0} = \text{CHSH}'_{(-1)1} = -2\sqrt{2}$ and $\text{CHSH}_{(+1)0} = \text{CHSH}'_{(+1)1} = 2\sqrt{2}$. For any given α and j, Charlie and Bob's joint state must maximally violate the CHSH. Only maximally entangled two-qubit pure states can generate such a correlation.

Thus, by the monogamy of entanglement, $\rho^{BCD} = \rho^{BC} \otimes \rho^D$, where ρ^{BC} is a maximally entangled pure state of Bob and Charlie. This means that if $S = 4\sqrt{2}$, then Derek cannot remain entangled to Bob's and Charlie's devices.

Now suppose the same device which yielded $S = 4\sqrt{2}$ during the device-independent test is used for the standard controlled quantum teleportation scheme (Sec. II A). If Charlie does not give permission to teleport, i.e., does not reveal
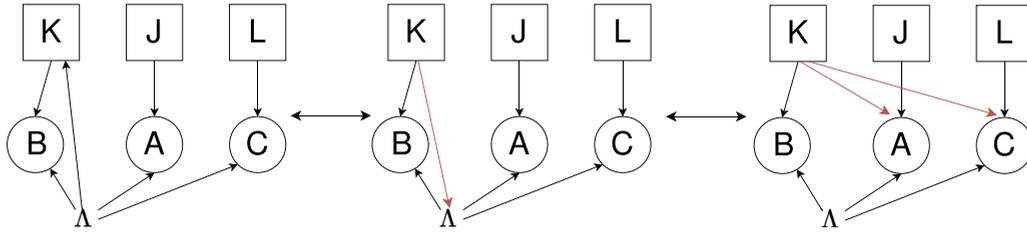
FIG. 2. DAG equivalence.

γl, then $p(\delta = \gamma l) = \frac{1}{4}$. This reflects the fact that Derek's state is separate from Bob and Charlie's composite state and therefore cannot obtain information about their systems by performing local operations on his system. Essentially, it means that Bob has no extra information about what the corrective rotations $R^{-1}_{s_0 s_1 \gamma l}$ are beyond what the trusted parties Alice and Charlie choose to reveal.

Alternatively, we note that only the maximally entangled GHZ state $\frac{|000\rangle + |111\rangle}{2}$ (up to local unitary operations) violates the Svetlichny inequality maximally, i.e., gives $S = 4\sqrt{2}$. It directly follows that Derek's state must be separated from the tripartite state of Alice, Bob, and Charlie since the maximally entangled GHZ state is a pure quantum state. The controller's authority for the GHZ state was derived in Sec. II A and P was shown to be $1/3$.

IV. CONTROLLER'S AUTHORITY FROM NONMAXIMAL VIOLATION OF SVETLICHNY INEQUALITY

In Sec. II B we proposed a setup using which the Svetlichny function can be computed. We showed that a maximal violation of the Svetlichny inequality [Eq. (16)] implies that Bob can get no useful information from Derek to increase the average teleportation fidelity without Charlie's permission. This ensures that the controller's authority is maximized. However, one can expect that the controller's authority will not be maximized in case of nonmaximal violation of the Svetlichny inequality.

In this section, we study the quantitative relationship between genuine three-way nonlocality and the controller's authority using the example of two specific families of quan-
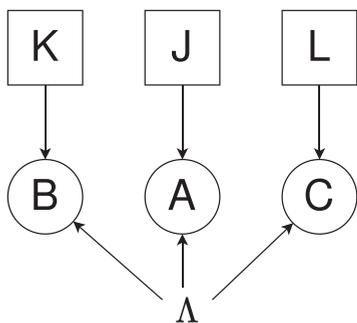

FIG. 3. DAG for the device-independent test scenario of fully trusted controlled quantum teleportation. Note that there are no arrows from Λ to K, unlike the scenario of untrusted receiver considered earlier. Here, all parties have measurement choice independence and there is no communication between each other.

tum states. We consider two noise models of the tripartite GHZ state—the total depolarizing channel and the qubit depolarizing channel—and compute the controller's authority as a function of Svetlichny inequality [Eq. (16)] violation. We consider a specific attack strategy using which Bob can try to increase the average fidelity of teleportation without Charlie's permission. This strategy is based on the assumption that Alice, Bob, Charlie, and Derek are restricted to performing quantum operations on their respective systems—no joint quantum operations allowed between any two parties. Charlie's authority will be quantified by the effective control power (P_{eff}), which we define as

$$P_{\text{eff}} = F_C^{NE} - F_{NC}^E. \tag{17}$$

Here, F_C^{NE} indicates the average fidelity of teleportation with Charlie's permission and no eavesdropping. F_{NC}^E indicates the average fidelity of teleportation without Charlie's permission but with eavesdropping (i.e., Derek's participation). The general definition of the controller's authority would be

$$P = F_C^E - F_{NC}^E. \tag{18}$$

The superscript E indicates that eavesdropping has been considered in both cases of control (with and without Charlie's permission). We shall leave the more general quantification of the controller's authority as future work and focus on the P_{eff} of Charlie in this section. Note that $F_C^E \geqslant F_C^{NE}$ because eavesdropping will always increase fidelity. Therefore, P_{eff} is a lower bound to the more general definition of the controller's authority quantified by Eq. (18). It is guaranteed that for the adversarial strategy under consideration, Charlie has at least P_{eff} amount of control.

A. Adversarial strategy

The ideal CQT scheme (Sec. II A) using the tripartite GHZ state allows teleportation with perfect average fidelity with Charlie's permission. Alice and Bob's composite state is projected into one of the EPR states after Charlie performs a measurement and reveals the measurement setting and outcome to Bob. When Charlie does not make his measurement information known to Bob, i.e., does not give permission to teleport, Bob does not know which EPR state the teleportation channel has been projected into. This prevents Bob from achieving an average teleportation fidelity higher than $2/3$. Recall that the goal of the adversary (Sec. III B) is to maximize the average teleportation fidelity when Charlie has not allowed the teleportation. Also, note that the standard teleportation protocol works optimally when Alice and Bob share an EPR state. Therefore, we expect that the average teleportation fidelity will be maximized when the fidelity of

Alice and Bob's shared state with an EPR state is maximized after Derek's measurement on his system. Bob's best option is to ask Derek to perform a measurement in a suitable basis and reveal its outcome (δ) to Bob such that Alice and Bob's composite state is projected close to one of the four EPR states. This gives Bob some relevant information regarding the corrective rotations, using which he can recover the state to be teleported with higher fidelity (see point 4 of Adversarial Capabilities, Sec. III B 2). Our goal is to find the maximum fidelity of teleportation that Bob can achieve without permission from Charlie using this extra information (δ). This will allow us to evaluate the worst-case P_{eff} of Charlie.

The adversarial strategy can thus be formulated as the following problem: Find the optimal positive operator-valued measure (POVM) operators of Derek such that the fidelity between the bipartite postmeasurement state of Alice and Bob and one of the EPR states is maximized.

1. Execution of adversarial strategy

The adversarial strategy in Sec. IV A can be executed in the following way:

Let $\{M_i\}$ denote Derek's POVMs, and $Pr(i)$ denote the probability of getting an outcome i. ρ^{ABD} is the joint state of Alice, Bob, and Derek. Note that Charlie's state is irrelevant in this case since he is not participating.

Then, the post measurement state of Alice and Bob is given by

$$\rho_i^{AB} = \frac{\text{Tr}^D[\rho^{ABD}(\mathbb{I} \otimes \mathbb{I} \otimes M_i)]}{Pr(i)}. \tag{19}$$

Let $F(\rho_1, \rho_2)$ denote the fidelity between two density matrices ρ_1 and ρ_2. Then the problem of finding the optimal POVMs can be formulated as follows:

$$\text{Maximize} \quad \sum_i Pr(i)F(\rho_i^{AB}, |\phi_i\rangle\langle\phi_i|)$$

$$\text{subject to} \quad M_i \geqslant 0, \ \sum_i M_i = \mathbb{I}, \tag{20}$$

$$Pr(i)F(\rho_i^{AB}, |\phi_i\rangle\langle\phi_i|)$$
$$= \text{Tr}\{\text{Tr}^D[\rho^{ABD}(\mathbb{I} \otimes \mathbb{I} \otimes M_i)]|\phi_i\rangle\langle\phi_i|\}$$
$$= \text{Tr}[(|\phi_i\rangle\langle\phi_i| \otimes \mathbb{I})\rho^{ABD}(\mathbb{I} \otimes \mathbb{I} \otimes M_i)] \tag{21}$$
$$= \text{Tr}[\text{Tr}^{AB}[(|\phi_i\rangle\langle\phi_i| \otimes \mathbb{I})\rho^{ABD}]M_i].$$

Let $\tilde{\rho}_i = \text{Tr}^{AB}[(|\phi_i\rangle\langle\phi_i| \otimes \mathbb{I})\rho^{ABD}]$.

After substituting $\tilde{\rho}_i$ in Eq. (20), we get

$$\text{Maximize} \quad \sum_i \text{Tr}(\tilde{\rho}_i M_i)$$

$$\text{subject to} \quad M_i \geqslant 0, \ \sum_i M_i = \mathbb{I}, M_i = M_i^\dagger \tag{22}$$

$$\text{variable} \quad M_i.$$

The optimization problem in Eq. (22) can be cast into a semidefinite program (SDP) using the procedure given in the Appendix. The SDP can be solved numerically using the CVX module [25,26] on MATLAB to obtain the optimal POVM measurements.

B. Examples of controller's authority with nonmaximal Svetlichny inequality violation

A useful approach to analyze the adversarial strategy and Derek's role is to describe the problem using the framework of decoherence and noise models in open systems. The ideal CQT scheme assumes that the tripartite state shared by Alice, Bob, and Charlie is a pure GHZ state [$|\psi\rangle = (|000\rangle + |111\rangle)/\sqrt{2}$]. More generally, in a realistic scenario, the pure GHZ state would undergo decoherence due to entanglement with the environment. This environment could be the adversary Derek, and hence the decoherence model can be used to analyze Derek's effect on CQT as follows. The state ρ_f after a decoherence process ε is given by $\rho_f = \varepsilon\rho_i$. The action of ε can be described using Kraus operators $\{E_j\}_j$ in the following way [27,28]:

$$\varepsilon\rho_i = \sum_{j=1}^M E_j\rho_i E_j^\dagger. \tag{23}$$

First, we will consider the case where the whole state is affected by the same decoherence process described by the total depolarizing channel. It is a process in which the ideal GHZ state is mixed with white noise with probability p. Thus,

$$\rho_f^{\text{total}} = p\frac{\mathbb{I}}{8} + (1 - p)|\psi\rangle\langle\psi|. \tag{24}$$

Next, we will consider the decoherence process in which each qubit of the tripartite GHZ state undergoes a depolarizing channel. Note that the qubit depolarizing process is physically more appropriate than the total depolarizing process because the three qubits are distributed to three different parties who are usually at different locations. Each qubit is coupled to its local environment and undergoes depolarizing independently, though they were initially entangled at a single location. The qubit depolarizing channel is described by the Kraus operators $E_0 = \sqrt{1-p'}I$; $E_i = \sqrt{\frac{p'}{3}}\sigma_i$, where $p' = \frac{3p}{2}$ [28]. The final state after the qubit depolarizing process, assuming the same depolarizing parameter for each qubit, is given by

$$\rho_f^{\text{qubit}} = \sum_{ijk} E_i \otimes E_j \otimes E_k|\psi\rangle\langle\psi|[E_i \otimes E_j \otimes E_k]^\dagger. \tag{25}$$

$\rho_f^{\text{total}}, \rho_f^{\text{qubit}}$ are mixed states unless $p = 0$. One can think of these mixed states as a part of a bigger pure quantum state $|\psi^{ABCD}\rangle$ comprising Alice, Bob, Charlie, and Derek such that $\text{Tr}^D(|\psi^{ABCD}\rangle\langle\psi^{ABCD}|) = \rho_f^{\text{qubit/total}}$. In the language of quantum cryptography, one would say Derek "holds" a purification of the mixed tripartite state. Since $|\psi^{ABCD}\rangle$ is a pure state, Derek is the most general eavesdropper. Any larger quantum system $\rho^{ABCD\Delta}$ with more eavesdroppers $\Delta_1, \Delta_2, \ldots, \Delta_N$ will be of the separable form $\rho^{ABCD\Delta} = |\psi^{ABCD}\rangle\langle\psi^{ABCD}| \otimes \rho^{\Delta_1,\Delta_2,\ldots,\Delta_N}$, which means that $\Delta_1, \Delta_2, \ldots, \Delta_N$ cannot be correlated with $|\psi^{ABCD}\rangle$.

In this paper, we will use the spectral decomposition of a density matrix to obtain a purification of $|\psi^{ABCD}\rangle$ [29] from $\rho_f^{\text{total/qubit}}$. The purification $|\psi_f^{\text{total/qubit}}\rangle$ of $\rho_f^{\text{total/qubit}}$ is therefore given by

$$|\psi_f^{\text{total/qubit}}\rangle = \sum_{k\in\{1,2,\ldots,8\}} \frac{(\rho_f^{\text{total/qubit}} \otimes \mathbb{I}_8)|\Lambda_k\rangle|\Lambda_k\rangle}{\sqrt{\text{Tr}(|\Lambda_k\rangle\langle\Lambda_k|\rho_f^{\text{total/qubit}})}}, \tag{26}$$

where $\rho_f^{\text{total/qubit}} = \sum_{k \in \{1,2,\dots,8\}} \alpha_k |\Lambda_k\rangle\langle\Lambda_k|$. It can be easily verified that $\text{Tr}^D(|\psi_f^{\text{total/qubit}}\rangle\langle\psi_f^{\text{total/qubit}}|) = \rho_f^{\text{total/qubit}}$.

1. Computing the P_{eff} for the depolarized GHZ state

We have all the necessary ingredients to compute F_C^{NE} and F_{NC}^E (defined in Sec. IV) for the total depolarized and qubit depolarized GHZ states.

Let $\rho_{s_0 s_1 \gamma l}^B$ denote Bob's state when Alice's and Charlie's boxes have revealed the outputs $s_0 s_1$ and γl after performing

the measurements $\{M_{s_0 s_1}^{aA}\}_{s_0 s_1}$ and $\{M_{\gamma l}^C\}_{\gamma l}$, respectively.

$$\rho_{s_0 s_1 \gamma l}^B = \frac{\text{Tr}^{aAC}\left[\left(\frac{\mathbb{I}+\vec{a}\cdot\vec{\sigma}}{2} \otimes \rho_f^{\text{total/qubit}}\right)\left(M_{s_0 s_1}^{aA} \otimes \mathbb{I} \otimes M_{\gamma l}^C\right)\right]}{\text{Tr}\left[\left(\frac{\mathbb{I}+\vec{a}\cdot\vec{\sigma}}{2} \otimes \rho_f^{\text{total/qubit}}\right)\left(M_{s_0 s_1}^{aA} \otimes \mathbb{I} \otimes M_{\gamma l}^C\right)\right]}. \tag{27}$$

After the application of corrective rotation, Bob's qubit can be expressed as $R_{s_0 s_1 \gamma l}^{-1} \rho_{s_0 s_1 \gamma l}^B (R_{s_0 s_1 \gamma l}^{-1})^\dagger$. Then the fidelity of teleportation with Charlie's permission for a pure state $|a\rangle\langle a|$ is given by

$$F_C^{NE}(a) = \sum_{s_0,s_1,l \,\in\, \{0,1\};\, \gamma \in \{\pm 1\}} P(s_0 s_1 \gamma l) \; F[|a\rangle\langle a|, \; R_{s_0 s_1 \gamma l}^{-1} \rho_{s_0 s_1 \gamma l}^B (R_{s_0 s_1 \gamma l}^{-1})^\dagger]. \tag{28}$$

Here $P(s_0 s_1 \gamma l)$ represents the joint probability that Alice's and Charlie's boxes have revealed $s_0 s_1$ and γl, respectively. The fidelity function in the above equation simplifies to $F[|a\rangle\langle a|, \; R_{s_0 s_1 \gamma l}^{-1} \rho_{s_0 s_1 \gamma l}^B (R_{s_0 s_1 \gamma l}^{-1})^\dagger] = \text{Tr}[|a\rangle\langle a| R_{s_0 s_1 \gamma l}^{-1} \rho_{s_0 s_1 \gamma l}^B (R_{s_0 s_1 \gamma l}^{-1})^\dagger]$, for a pure state, $|a\rangle\langle a|$. After averaging over all pure qubit states and simplifying the trace,

$$F_C^{NE} = \int \frac{d\vec{a}}{4\pi} \sum_{s_0,s_1,l \,\in\, \{0,1\};\, \gamma \in \{\pm 1\}} P(s_0 s_1 \gamma l)\langle a| R_{s_0 s_1 \gamma l}^{-1} \rho_{s_0 s_1 \gamma l}^B (R_{s_0 s_1 \gamma l}^{-1})^\dagger |a\rangle. \tag{29}$$

The calculation of F_C^{NE} has been done assuming that the set of corrective rotations $\{R_{s_0 s_1 \gamma l}^{-1}\}_{s_0 s_1 \gamma l}$ of Bob are those that are required to exactly recover the qubit to be teleported, had the shared tripartite state ($\rho_f^{\text{total/qubit}}$) been the perfect GHZ state. In this paper, the set of rotation matrices have been assumed to be fixed. We have not considered variable rotations conditioned on the underlying tripartite state. To compute F_{NC}^E, we first need to determine the optimal POVMs of Derek which will execute the adversarial strategy (Sec. IV A).

ρ^{ABD} can be obtained from $\rho_f^{\text{total/qubit}}$ by first purifying it into $|\psi_f^{\text{total/qubit}}\rangle$ [Eq. (26)] and then tracing out Charlie's system,

$$\rho^{ABD} = \text{Tr}^C\left(|\psi_f^{\text{total/qubit}}\rangle\langle\psi_f^{\text{total/qubit}}|\right). \tag{30}$$

By substituting ρ^{ABD} in the expression $\tilde{\rho}_i = \text{Tr}^D((|\phi_i\rangle\langle\phi_i| \otimes \mathbb{I})\rho^{ABD})$, one can set up the optimization given in Eq. (22).

Derek can then use the optimal POVMs $\{M_i\}_i$ to measure his system and reveal $\delta = i \in \{(+1)0, (+1)1, (-1)0, (-1)1\}$ to Bob. Hence, Alice and Bob's joint state (ρ_i^{AB}) conditioned on the result of Derek's measurement is given by

$$\rho_i^{AB} = \frac{\text{Tr}^D[\rho^{ABD}(\mathbb{I}_2 \otimes \mathbb{I}_2 \otimes M_i)]}{\text{Tr}[\rho^{ABD}(\mathbb{I}_2 \otimes \mathbb{I}_2 \otimes M_i)]}. \tag{31}$$

Now Alice performs the Bell measurement $\{M_{s_0 s_1}^{aA}\}_{s_0 s_1}$ on the state to be teleported and her share of the composite state ρ_i^{AB}. After Alice reveals her measurement outcome, Bob's qubit is prepared in the following state:

$$\rho_{s_0 s_1 i}^B = \frac{\text{Tr}^{aA}\left[\left(\frac{\mathbb{I}+\vec{a}\cdot\vec{\sigma}}{2} \otimes \rho_i^{AB}\right)\left(M_{s_0 s_1}^{aA} \otimes \mathbb{I}\right)\right]}{\text{Tr}\left[\left(\frac{\mathbb{I}+\vec{a}\cdot\vec{\sigma}}{2} \otimes \rho_i^{AB}\right)\left(M_{s_0 s_1}^{aA} \otimes \mathbb{I}\right)\right]}. \tag{32}$$

Finally, the average fidelity of teleportation without Charlie's permission but with Derek's assistance (F_{NC}^E) can be computed

using a similar procedure as that for F_C^{NE} (Eq. 29):

$$F_{NC}^E = \int \frac{d\vec{a}}{4\pi} \sum_{s_0,s_1 \in \{0,1\};\, i \in \{0,1\}^2} P(s_0 s_1 i)\langle a| R_{s_0 s_1 i}^{-1} \rho_{s_0 s_1 i}^B (R_{s_0 s_1 i}^{-1})^\dagger |a\rangle. \tag{33}$$

2. Svetlichny inequality violation for depolarized GHZ states

We use the physical interpretation of the total depolarized GHZ state (TDGHZ) and the qubit depolarized GHZ state (QDGHZ) to derive the maximum Svetlichny inequality violation that can be obtained for a given depolarizing channel parameter.

As mentioned earlier, the total depolarized GHZ state can be seen as a probabilistic mixture of the perfect GHZ state ($\frac{|000\rangle+|111\rangle}{\sqrt{2}}$) and the completely mixed three qubit state ($\frac{\mathbb{I}}{8}$).

The qubit depolarizing channel can be described by the process in which each qubit can get replaced by the completely mixed single qubit state ($\frac{\mathbb{I}}{2}$), with probability p. For the GHZ state, it means that with probability $(1-p)^3$ the state is unaltered; with probability $3p(1-p)^2$, the GHZ state is transformed into a bipartite entangled state; and with probability $3p^2(1-p) + p^3$, it is transformed into a separable state.

It was shown in Ref. [17] that tripartite entangled states are required for violating the Svetlichny inequality ($S \leqslant 4$). Bipartite entangled states and separable states do not violate this inequality, while the tripartite entangled perfect GHZ state ($\frac{|000\rangle+|111\rangle}{\sqrt{2}}$) violates it maximally ($S = 4\sqrt{2}$). Moreover, according to Theorem 1 it is possible to achieve the ($S = 4$) bound using classical strategies. Therefore, the maximum Svetlichny inequality violation is given by the following equations:

$$S_{\text{TDGHZ}} = (1-p)S_{\text{GHZ}} + pS_{\text{Classical}} \tag{34}$$

$$= (1-p)4\sqrt{2} + 4p. \tag{35}$$

$$S_{\text{QDGHZ}} = (1-p)^3 S_{\text{GHZ}} + [1 - (1-p)^3]S_{\text{Classical}} \tag{36}$$

$$= (1-p)^3 4\sqrt{2} + 4[1 - (1-p)^3]. \tag{37}$$
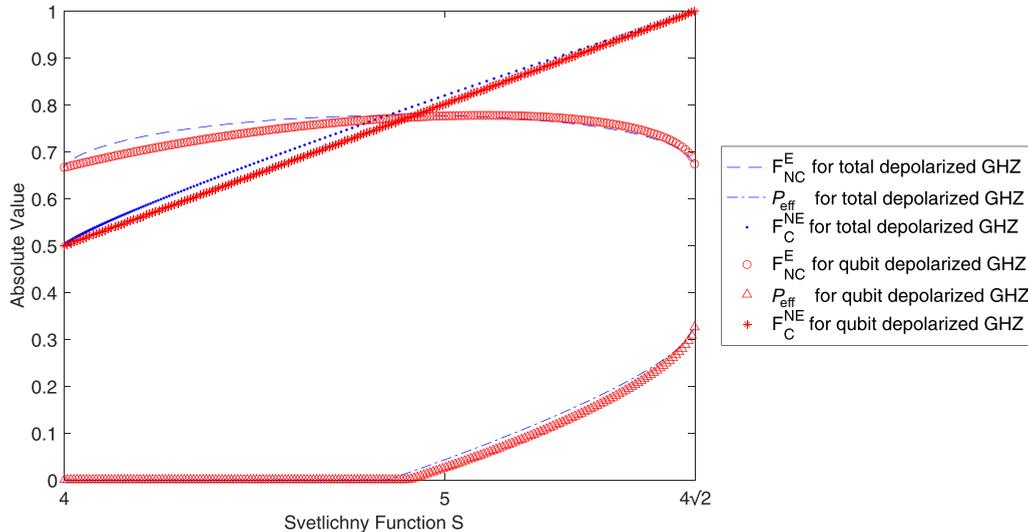
FIG. 4. P_{eff}, average fidelity of teleportation with controller's permission (F_C^{NE}), and average fidelity of teleportation without controller's permission but with eavesdropper's participation (F_{NC}^E) as a function of maximum Svetlichny inequality violation (S) given by Eq. (34) for both the qubit depolarized and total depolarized GHZ states with parameter $p \in (0, 1)$.

C. Numerical calculation of the relationship between effective control power and Svetlichny violation

For a given depolarizing parameter $p \in (0, 1)$, the maximum Svetlichny inequality violation was computed using Eq. (34). The P_{eff} was computed using the method described in Sec. IV B 1 and plotted against the maximum Svetlichny violation corresponding to the given value of parameter p in Fig. 4. It is interesting to note that P_{eff} is positive only when $S > 4.84$ for the total depolarized GHZ state and when $S > 4.90$ for the qubit depolarized GHZ state. The plots clearly show that P_{eff} is a monotonically increasing function of S. The highest value of P_{eff} is reached at the maximal violation of Svetlichny's inequality, which confirms our Claim 2. It is important to note that the violation of the Svetlichny inequality [Eq. (16)] does not necessarily imply that Charlie has positive control power. For nonmaximal violation, there is a small window in the range $4.84 < S < 4\sqrt{2}$ for the qubit-depolarized GHZ states and $4.90 < S < 4\sqrt{2}$ for the total depolarized GHZ states, where P_{eff} is positive, and hence Charlie maintains some level of control.

V. SUMMARY AND OUTLOOK

In this paper, we have performed a device-independent study of controlled teleportation of a qubit with an untrusted receiver. We constructed a device-independently testable scenario in a way that allowed us to certify, in the context of controlled teleportation, whether quantum resources were being used by the device despite the receiver being untrusted. We found in this case that the well-known Svetlichny inequality must be violated to certify quantum correlations. A maximal violation of the Svetlichny inequality guarantees maximum control power. This is in contrast to the controlled teleportation with all trusted parties, where the maximal violation of Mermin's inequality was sufficient to certify maximum control power. This indicates that a stronger form of non-

locality, also known as "genuine tripartite nonlocality," is required to device-independently test the controlled quantum teleportation with an untrusted receiver. Until recently [16], there was no application of higher-order Bell's inequalities in DI quantum cryptography. Our work demonstrates one of the first instances of the usefulness of stronger forms of Bell's inequalities (Svetlichny inequality in this case) in DI quantum communication protocols.

We proposed an adversarial strategy which, while not proven to be optimal, can effectively decrease the controller's authority by taking advantage of a nonideal device that nonmaximally violates Svetlichny inequality. By taking the example of two families of quantum states characterized by the total depolarized and the qubit-depolarized GHZ states, we showed that the controller's authority is a monotonically increasing function of the maximal Svetlichny inequality violation. For the given family of depolarized GHZ states, adversarial strategy, and a Svetlichny inequality violation, one can infer the controller's authority from our numerically obtained plot. We found a window of nonmaximal Svetlichny inequality violation where the controller's authority is nonzero. This shows that the controlled teleportation scheme with an untrusted receiver is robust to depolarizing noise present in the device. This result can be a guiding framework for practical implementations of DI CQT. Since the tripartite CQT network can be the fundamental component of a large-scale quantum communication network [7], our results are relevant for building practical communication networks where quantum information is shared among distrustful parties.

In this paper we have used effective control power as the figure of merit in DI CQT, whereas the authors of Ref. [16] used $(1 - p_{\text{guess}})$ (probability of the untrusted receiver guessing the wrong secret bit) as the figure of merit in the DI secret sharing of a bit. However, we see that in both cases, the relationship of these figures of merit with that of genuine tripartite nonlocality is very similar. From this observation,

intuition suggests that the von Neumann entropy of the quantum information revealed to the untrusted receiver would show similar trends to that of effective control power in DI CQT. The translation from effective control power to an entropic measure of quantum information would help to generalize our work to a multipartite QSS protocol.

ACKNOWLEDGMENTS

APPENDIX: SDP OPTIMIZATION

Consider the optimization program given in Eq. (22). We can cast it into a semidefinite program in the following way:

Let $\mathcal{X}$ be a Hilbert space of dimension D, where D is also the dimension of Derek's quantum system. Define Φ as a Hermitian preserving map $T(\mathcal{X}, \mathcal{X})$. Then the optimization problem is given by

Primal problem

maximize: $\langle (\tilde{\rho}_1, \tilde{\rho}_2, ..., \tilde{\rho}_n), (M_1, M_2, ..., M_n) \rangle$

subject to: $\Phi(M_1, M_2, ..., M_n) \triangleq \sum_{i=1}^{n} M_i = \mathbb{I}_D$ (A1)

$(M_1, M_2, ..., M_n) \in \mathrm{Pos}(\mathcal{X})^n$

Dual problem

minimize: $\langle \mathbb{I}_D, Y \rangle$

subject to: $\Phi^\dagger(Y) \succeq (\tilde{\rho}_1, \tilde{\rho}_2, ..., \tilde{\rho}_n)$ (A2)

$Y \in \mathrm{Herm}(\mathcal{X})$.

[1] A. Karlsson and M. Bourennane, Quantum teleportation using three-particle entanglement, Phys. Rev. A **58**, 4394 (1998).

[2] 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).

[3] D. Gottesman and I. L. Chuang, Demonstrating the viability of universal quantum computation using teleportation and single-qubit operations, Nature (London) **402**, 390 (1999).

[4] R. Raussendorf and H. J. Briegel, A One-Way Quantum Computer, Phys. Rev. Lett. **86**, 5188 (2001).

[5] N. Sangouard, C. Simon, H. de Riedmatten, and N. Gisin, Quantum repeaters based on atomic ensembles and linear optics, Rev. Mod. Phys. **83**, 33 (2011).

[6] D. Castelvecchi, The quantum internet has arrived (and it hasn't), Nature (London) **554**, 289 (2018).

[7] H. Yonezawa, T. Aoki, and A. Furusawa, Demonstration of a quantum teleportation network for continuous variables, Nature (London) **431**, 430 (2004).

[8] S. Braunstein and P. van Loock, Quantum information with continuous variables, Rev. Mod. Phys. **77**, 513 (2005).

[9] A. Barasiński, A. Černoch, and K. Lemr, Demonstration of Controlled Quantum Teleportation for Discrete Variables on Linear Optical Devices, Phys. Rev. Lett. **122**, 170501 (2019).

[10] S. Pironio, A. Acin, N. Brunner, N. Gisin, S. Massar, and V. Scarani, Device-independent quantum key distribution secure against collective attacks, New J. Phys. **11**, 045021 (2009).

[11] N. Brunner, D. Cavalcanti, S. Pironio, V. Scarani, and S. Wehner, Bell nonlocality, Rev. Mod. Phys. **86**, 419 (2014).

[12] J. S. Bell, On the einstein Podolsky Rosen paradox, Phys. Phys. Fiz. **1**, 195 (1964).

[13] L. Masanes, S. Pironio, and A. Acín, Secure device-independent quantum key distribution with causally independent measurement devices, Nat. Commun. **2**, 238 (2011).

[14] S. Pironio, A. Acín, S. Massar, A. B. de La Giroday, D. N. Matsukevich, P. Maunz, S. Olmschenk, D. Hayes, L. Luo, T. A. Manning, *et al.*, Random numbers certified by Bell's theorem, Nature (London) **464**, 1021 (2010).

[15] J. Anders and D. E. Browne, Computational Power of Correlations, Phys. Rev. Lett. **102**, 050502 (2009).

[16] M. G. M. Moreno, S. Brito, R. V. Nery, and R. Chaves, Device-independent secret sharing and a stronger form of Bell nonlocality, Phys. Rev. A **101**, 052339 (2020).

[17] G. Svetlichny, Distinguishing three-body from two-body non-separability by a Bell-type inequality, Phys. Rev. D **35**, 3066 (1987).

[18] S. Pirandola, J. Eisert, C. Weedbrook, A. Furusawa, and S. L. Braunstein, Advances in quantum teleportation, Nat. Photonics **9**, 641 (2015).

[19] M. Ho, J.-D. Bancal, and V. Scarani, Device-independent certification of the teleportation of a qubit, Phys. Rev. A **88**, 052318 (2013).

[20] X.-H. Li and S. Ghose, Control power in perfect controlled teleportation via partially entangled channels, Phys. Rev. A **90**, 052305 (2014).

[21] B. F. Toner and D. Bacon, Communication Cost of Simulating Bell Correlations, Phys. Rev. Lett. **91**, 187904 (2003).

[22] R. Chaves, D. Cavalcanti, and L. Aolita, Causal hierarchy of multipartite Bell nonlocality, Quantum **1**, 23 (2017).

[23] J.-D. Bancal, C. Branciard, N. Gisin, and S. Pironio, Quantifying Multipartite Nonlocality, Phys. Rev. Lett. **103**, 090503 (2009).

[24] N. D. Mermin, Extreme Quantum Entanglement in a Superposition of Macroscopically Distinct States, Phys. Rev. Lett. **65**, 1838 (1990).

[25] M. Grant and S. Boyd, CVX: Matlab software for disciplined convex programming, version 2.1, http://cvxr.com/cvx.

[26] M. Grant and S. Boyd, Graph implementations for nonsmooth convex programs, in *Recent Advances in Learning and Control*,

Lecture Notes in Control and Information Sciences, edited by V. Blondel, S. Boyd, and H. Kimura (Springer-Verlag, New York, 2008) pp. 95–110.

[27] K. Kraus, A. Böhm, J. D. Dollard, and W. Wootters, States, effects, and operations: Fundamental notions of quantum theory: Lectures in mathematical physics at the University of Texas at Austin, Lect. Notes Phys. **190**, 90 (1983).

[28] F.-L. Zhang, Y. Jiang, and M.-L. Liang, Speed of disentanglement in multiqubit systems under a depolarizing channel, Ann. Phys. **333**, 136 (2013).

[29] Y.-y. Nie, Y.-h. Li, J.-c. Liu, and M.-h. Sang, Quantum information splitting of an arbitrary three-qubit state by using two four-qubit cluster states, Quant. Info. Proc. **10**, 297 (2011).