

Self-testing of binary Pauli measurements requiring neither entanglement nor any dimensional restriction

Ananda G. Maity^{1,*}, Shiladitya Mal,^{2,3,†} Chellasamy Jebarathinam^{1,3,4,‡} and A. S. Majumdar^{1,§}

¹*S. N. Bose National Centre for Basic Sciences, Block JD, Sector III, Salt Lake, Kolkata 700 106, India*

²*Harish-Chandra Research Institute, HBNI, Chhatnag Road, Jhansi, Allahabad 211 019, India*

³*Department of Physics and Center for Quantum Frontiers of Research and Technology (QFort), National Cheng Kung University, Tainan 701, Taiwan*

⁴*Center for Theoretical Physics, Polish Academy of Sciences, Aleja Lotników 32/46, 02-668 Warsaw, Poland*



(Received 23 December 2020; revised 26 April 2021; accepted 20 May 2021; published 4 June 2021)

Characterization of quantum devices received from unknown providers is a significant primary task for any quantum information processing protocol. Self-testing protocols are designed for this purpose of certifying quantum components from the observed statistics under a set of minimal assumptions. Here we propose a self-testing protocol for certifying binary Pauli measurements employing the violation of a Leggett-Garg inequality. The scenario based on temporal correlations does not require entanglement, a costly and fragile resource. Moreover, unlike previously proposed self-testing protocols in the prepare and measure scenario, our approach requires neither dimensional restrictions, nor other stringent assumptions on the type of measurements. We further analyze the robustness of this hitherto unexplored domain of self-testing of measurements.

DOI: [10.1103/PhysRevA.103.062604](https://doi.org/10.1103/PhysRevA.103.062604)

I. INTRODUCTION

It is hard to overemphasise the role of emerging quantum technology in recent times. Various real life applications, such as quantum key distribution [1], quantum sensing [2], quantum metrology [3], quantum internet [4], and machine learning [5] have been investigated with great prospects. For such prospects to materialize in practice, it becomes of utmost importance to design experiments which can test whether the quantum components of the required devices function properly. To this end, various certification or verification protocols have been employed, such as those based on tomography and benchmarking [6], as well as self-testing protocols based essentially on observed statistics [7,8].

Among several certification protocols generic quantum tomography is the most powerful, but at the same time it is the most resource consuming. Randomized benchmarking refers to a collection of methods that aim at reliably estimating the figure of merit of the overlap between the physical quantum process and its ideal counterpart. For both randomized benchmarking or quantum tomography, trusted measurements are required to certify quantum devices. On the other hand, self-testing of quantum components based on statistics, collected from lesser number of measurements and minimal physical assumptions, require lesser trust on the measurement devices and are experimentally more efficient and less resource consuming [6].

Self-testing based on the Bell test was proposed initially in the context of quantum cryptography [7,8], where it was shown that maximum violation of the Bell-CHSH inequality [9,10] implies that the underlying quantum state is maximally entangled and the local measurements performed by two distant parties are anticommuting [11]. In such self-testing protocols one can uniquely identify quantum states and measurements (up to some local isometries) by observing extreme correlations in measurement statistics. The underlying assumptions are the same as those required for the implementation of loophole-free Bell tests [12–15]. Since then all pure bipartite entangled states and certain multipartite quantum states, such as graph states, have been self-tested [8,16] in this scenario. Self-testing of pure entangled bipartite states has also been investigated [17–20] employing Einstein-Podolski-Rosen steering [21]. Self-testing using steering is weaker in the sense that it requires more assumptions compared to that based on Bell tests, but the self-testing is easier to verify experimentally [22].

In this regard, it is worthwhile to mention that self-testing based on maximal violation of some nonclassicality revealing criterion is very fragile as idealized situations in the laboratory rarely occur. Therefore, a self-testing statement is useful for practical purposes if it has reasonable robustness [23–26]. For instance, there are robust self-testing protocols for which, given a certain level of violation of a Bell inequality (but not necessarily maximal), the nontrivial lower bound on the fidelity between the initially unknown state and a given target state has been shown. Robust self-testing of higher-dimensional state has also been studied [27–29]. Apart from various special classes of quantum states, different types of measurements including maximally incompatible observables [11], entangling Bell-measurement [30,31], binary

*anandamaity289@gmail.com

†shiladityamal@hri.res.in

‡jebarathinam@cft.edu.pl

§archan@bose.res.in

observables [32], more than two dichotomic observables [33,34], and nonmaximally anticommuting observables [25] have also been self-tested (see Ref. [35] for a review).

Apart from the above schemes of self-testing of measurements based on the use of quantum correlations in entangled states, some certification methods for self-testing have been proposed that do not require entanglement [36–39]. A pair of anticommuting Pauli observables have been self-tested in the prepare and measure scenario [40], employing the quantum advantage of $2 \mapsto 1$ random access code (RAC) [41,42]. Such approaches in the context of self-testing of local states and measurements are more resource efficient and experimentally feasible compared to schemes based on nonlocal quantum correlations since they do not require entanglement, an expensive resource. However, the assumption of an upper bound on the system dimension has been crucial for such approaches, and hence, the verifier needs to trust the measurement devices more.

Another self-testing protocol has been constructed for three-dimensional states and measurements [43] based on the contextuality of quantum theory [44], which requires certain restrictive assumptions such as the compatibility between subsequent projective measurements [35]. Recently, an extension of the scheme has been proposed based on the sum of squares decomposition of a family of noncontextual inequalities [45], relaxing some of the above restrictions [46]. Self-testing of arbitrary high-dimensional local quantum systems using contextuality has also been proposed where the assumption of projective measurement is necessary [47]. The above protocols pertain to local measurements in three and above dimensions. On the other hand, among all measurements in quantum information processing, the measurements with dichotomic settings and outcomes are the most widely used ones. Hence, the design of resource efficient self-testing protocols for such measurements with minimal assumptions is necessary for practical purposes.

In the present work, we develop a scheme of self-testing binary Pauli measurements in a hitherto unexplored scenario, i.e., employing nonclassicality of temporal correlations exhibited via violation of the Leggett-Garg inequality (LGI) [48,49] and predictability [50,51], which does not require any entanglement. LGI has been employed to probe macroscopic coherence and to study quantum to classical transition [48–50,52–57]. Various aspects of temporal correlations have been investigated [51,58–66] and experimentally realized [67–72]. Here, we employ the violation of LGI, and invoke a minimal set of assumptions which can be easily met in a real experiment, in order to provide a self-testing statement for binary Pauli measurements without any need to restrict the dimension of the Hilbert space accessed by the quantum devices. We further perform the robustness analysis of our self-testing protocol by deriving a lower bound on the fidelity of the measured observables with that of ideal ones.

II. DESCRIPTION OF THE SCENARIO

We start with a brief description of the Leggett-Garg (LG) test (Fig. 1) which enables self-testing of Pauli measurements whenever extremal correlations of LGI are observed. In a LG test, a single system is measured sequentially at different

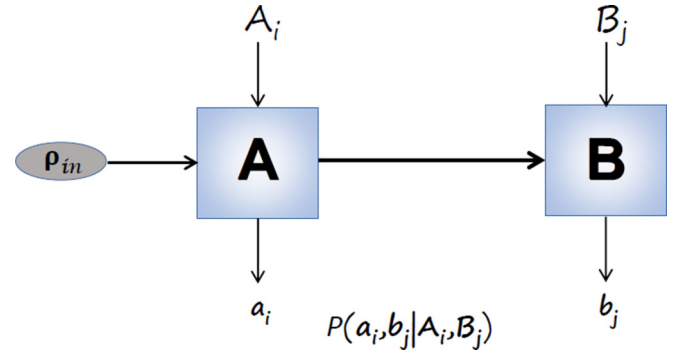


FIG. 1. Sequential-measurement setup. The joint probability distribution $P(a_i, b_j | A_i, B_j)$, i.e., the probability of obtaining outcome a_i and b_j when Alice measures A_i in an arbitrary input state at some instant t_m and Bob performs measurement B_j at some later instant t_{m+1} , respectively, is observed to obtain the violation of LGI (3).

instants of time to obtain temporal correlations. Two sequential binary measurements are performed (by Alice and Bob, respectively) on an identical initial state prepared by the experimenter in every run of the experiment. In contrast to the sequential measurement scenario of self-testing using contextuality [43], here subsequent measurements are not required to commute with each other.

Alice and Bob have two choices of binary measurements, say, $\{A_1, A_2\}$ and $\{B_1, B_2\}$ to perform in each run. The probability of obtaining outcome a_i and b_j is denoted by $P(a_i, b_j | A_i, B_j)$, when Alice measures A_j at time t_m and Bob measures B_j at some later instant t_{m+1} , with $i, j \in \{1, 2\}$ and $a_i, b_j \in \{0, 1\}$. Let us denote, $\mathcal{P}_{a_i|A_i}$, $\mathcal{P}_{b_j|B_j}$ as projectors so that $\sum_{a_i} \mathcal{P}_{a_i|A_i} = \mathbb{I}$, $\sum_{b_j} \mathcal{P}_{b_j|B_j} = \mathbb{I}$. The two-time joint probability can be obtained using Bayes' rule as

$$\begin{aligned} P(a_i, b_j | A_i, B_j) &= P(a_i | A_i)P(b_j | a_i, A_i, B_j) \\ &= \text{Tr}[\mathcal{P}_{a_i|A_i} \rho_{in}] \text{Tr} \left[\mathcal{P}_{b_j|B_j} \frac{\mathcal{P}_{a_i|A_i} \rho_{in} \mathcal{P}_{a_i|A_i}^\dagger}{\text{Tr}[\mathcal{P}_{a_i|A_i} \rho_{in} \mathcal{P}_{a_i|A_i}^\dagger]} \right]. \end{aligned} \quad (1)$$

The two-time correlation is defined as

$$C_{ij} = \sum_{a_i, b_j} (-1)^{a_i \oplus b_j} P(a_i, b_j | A_i, B_j), \quad (2)$$

where \oplus denotes addition modulo 2. The four-term LGI in terms of the above correlators is given by

$$\mathcal{K}_4 = C_{11} + C_{21} + C_{22} - C_{12} \leq 2. \quad (3)$$

Any model compatible with classical theory predicts that the maximal value of the above expression is 2, whereas the quantum theory can violate this inequality up to $2\sqrt{2}$. Suppose, in a single run, Alice performs a projective qubit measurement, $A_1 \equiv \hat{a}_1 \cdot \vec{\sigma}$ (to make the preliminary discussion simple, but it can be any general measurement too) on an arbitrary input state, ρ_{in} at time t_1 , and Bob performs a qubit measurement, $B_1 \equiv \hat{b}_1 \cdot \vec{\sigma}$ at some later time t_2 , where \hat{a}_1 and \hat{b}_1 are the Bloch vectors denoting Alice's and Bob's measurement directions, respectively, and $\vec{\sigma}$ is the vector of Pauli matrices. Then the maximum quantum violation, $2\sqrt{2}$, can be achieved

by the following measurement settings:

$$\begin{aligned}
 A_1^{\text{ideal}} &= \sigma_z, \\
 A_2^{\text{ideal}} &= \sigma_x, \\
 B_1^{\text{ideal}} &= \frac{\sigma_x + \sigma_z}{\sqrt{2}}, \\
 B_2^{\text{ideal}} &= \frac{\sigma_x - \sigma_z}{\sqrt{2}},
 \end{aligned}
 \tag{4}$$

up to some local unitary. In the context of self-testing, all the four measurements are *a priori* unknown to Alice and Bob. Our goal is to certify above measurements from the observed statistics, under some suitable and minimal assumptions.

III. DERIVATION OF LEGGETT-GARG INEQUALITY

LGI has been earlier derived using the assumptions of non-invasive measurement and realism [54,55]. However, those assumptions are at an ontological level, and hence, cannot be verified individually. Rather a conjunction of them can be verified in an experiment. On the other hand, in Ref. [51], LGI was derived from some operational assumptions called predictability and no signaling in time (NSIT) [50]. Subsequently, the NSIT condition has been experimentally observed on a variety of input states [73]. Here we present the essential features of the LGI derivation [51]. Let us first state the two assumptions in precise mathematical form.

Predictability: A model is said to be predictable if the joint statistics $P(a_i, b_j | A_i, B_j) \in \{0, 1\} \forall a_i, b_j, A_i, B_j$ [74].

NSIT: NSIT is defined by the condition that measurement statistics is not influenced by the earlier measurements. Mathematically, $P(b_j | B_j) = P(b_j | A_i, B_j) \forall A_i, B_j, b_j$.

To derive LGI from the above two assumptions, our aim is to show that

$$\text{NSIT} \wedge \text{Predictability} \Rightarrow \text{LGI}. \tag{5}$$

Suppose λ denotes some underlying variable at the ontological level, averaging over which we obtain joint probabilities observed in an experiment, i.e.,

$$P(a_i, b_j | A_i, B_j) = \int_{\lambda} d\lambda p(\lambda) P(a_i, b_j | A_i, B_j, \lambda).$$

LGI follows in a straightforward way when the joint probability at the ontological level gets factorized, or in other words, we have to show that predictability together with NSIT leads to

$$P(a_i, b_j | A_i, B_j, \lambda) = P(a_i | A_i, \lambda) P(b_j | B_j, \lambda). \tag{6}$$

As further conditioning does not change the deterministic probability distribution, we have from the predictability, $P(a_i, b_j | A_i, B_j, \lambda) = P(a_i, b_j | A_i, B_j)$. Using Bayes' rule one has

$$P(a_i, b_j | A_i, B_j) = P(a_i | A_i, B_j, b_j) P(b_j | A_i, B_j).$$

The condition of NSIT implies $P(b_j | A_i, B_j) = P(b_j | B_j)$. Also, as physically reasonable and broadly accepted, a later measurement cannot influence the past measurement result, and hence $P(a_i | A_i, B_j, b_j) = P(a_i | A_i)$. With the above implications, one can construct a theory at the ontological level

where $P(a_i | A_i, \lambda) = P(a_i | A_i)$, $P(b_j | B_j, \lambda) = P(b_j | B_j)$, which lead to Eq. (6). Now, a straightforward calculation leads us to derive the four-term LGI (3) which is bounded by 2.

Despite some structural similarities, the LG test is essentially different from the Bell test [75], and also has some loopholes which are different from that of the Bell test [76]. The approach adopted in this paper for the derivation of LGI is based on the conjunction of *Predictability* and *NSIT*. In the present scenario it is ensured that NSIT condition is satisfied, as we see in the next section. This means that if LGI is violated, then predictability must have to be violated. Thus, the violation of predictability naturally guarantees non-classicality which is required for the purpose of self-testing.

IV. SELF-TESTING OF MEASUREMENTS USING LEGGETT-GARG INEQUALITY

The above derivation of LGI with the assumptions of predictability and NSIT helps us to devise a self-testing protocol for binary Pauli measurements (4) whenever extremal non-classical temporal correlations are observed. We formulate the self-testing protocol in such a way that the NSIT condition is satisfied so that maximal violation of the LGI will imply the violation of the predictability condition, and hence, no classical strategy is able to reproduce the statistics. We now make a minimal assumption which is again very natural in the sequential measurement scenario, since otherwise, a classical model may simulate the quantum violation of LGI.

Assumption. The measurement device of Alice acts only on the input state prepared by the experimenter, and the measurement device of Bob acts only on the state produced by Alice's measurement, with both returning only the respective post-measurement states.

A similar assumption was also considered in Ref. [46] for the purpose of self-testing of local three-dimensional measurements using the sum-of-squares decomposition of a family of noncontextual inequalities [45]. However, in our approach using LGI we are interested here in the self-testing of binary qubit measurements. Employing the maximum violation of LGI along with NSIT condition we can self-test the binary qubit measurements given by Eq. (4) up to some local unitaries. Our self-testing protocol does not depend on the input state. However, for the sake of a formal proof of self-testing, we first consider a general qubit state (in lemma 1). Then, making use of this proof, we extend our result for states in any dimension (lemma 2). Our formal proof of self-testing is thus accomplished in the following two steps (lemmas 1 and 2), and finally we present the proof of isometry in Theorem 1.

Lemma 1. The maximum violation of LGI (i.e, $\mathcal{K}_4^{\text{max}} = 2\sqrt{2}$) implies implementation of the qubit measurement observables given by equation (4) upto some local unitaries, satisfying the NSIT condition.

Proof. Maximum quantum violation of LGI can only be achieved if the measurements are taken to be projective. We maximize the LGI considering the most general positive-operator-valued measure (POVM) with two outcomes. Maximizing the four-time LGI expression numerically over all the POVM parameters, it is found that the maximum value $2\sqrt{2}$ can only be achieved if the measurements are

taken to be projective (the details of the proof are given in Appendix A). Hence, without any loss of generality, we restrict ourselves to projective measurements only.

To obtain the two-time correlation C_{ij} we have to calculate joint probabilities $P(a_i, b_j | A_i, B_j)$ given in Eq. (1). Considering the general qubit input state $\rho_{in} = \frac{\mathbb{I} + \hat{n} \cdot \vec{\sigma}}{2}$, the first term of Eq. (1) can be simplified to $\text{Tr}[\mathcal{P}_{a_i|A_i} \rho_{in}] = \frac{1}{2}(1 + (-1)^{a_i} \hat{a}_i \cdot \hat{n})$. The postmeasurement state after obtaining outcome a_i is given by $\frac{\mathcal{P}_{a_i|A_i} \rho_{in} \mathcal{P}_{a_i|A_i}^\dagger}{\text{Tr}[\mathcal{P}_{a_i|A_i} \rho_{in} \mathcal{P}_{a_i|A_i}^\dagger]} = \frac{1}{2}[\mathbb{I} + (-1)^{a_i} \hat{a}_i \cdot \vec{\sigma}]$. Now, the term, $\text{Tr}[\mathcal{P}_{b_j|B_j} \frac{\mathcal{P}_{a_i|A_i} \rho_{in} \mathcal{P}_{a_i|A_i}^\dagger}{\text{Tr}[\mathcal{P}_{a_i|A_i} \rho_{in} \mathcal{P}_{a_i|A_i}^\dagger]}]$ can be simplified to $\frac{1}{2}[1 + (-1)^{a_i+b_j} \hat{a}_i \cdot \hat{b}_j]$. So, the joint probability distribution of getting outcomes a_i and b_j when measurements A_i and B_j are performed, respectively, is given by

$$P(a_i, b_j | A_i, B_j) = \frac{1}{4}[1 + (-1)^{a_i} \hat{a}_i \cdot \hat{n}][1 + (-1)^{a_i+b_j} \hat{a}_i \cdot \hat{b}_j]. \quad (7)$$

After simplification, we get, $C_{ij} = \hat{a}_i \cdot \hat{b}_j$. Then, the four-time LGI in terms of four correlators will be

$$\mathcal{K}_4 = \hat{a}_1 \cdot \hat{b}_1 + \hat{a}_2 \cdot \hat{b}_1 + \hat{a}_2 \cdot \hat{b}_2 - \hat{a}_1 \cdot \hat{b}_2 \leq 2. \quad (8)$$

It follows that the maximum value of \mathcal{K}_4 is $2\sqrt{2}$ when all $|\hat{a}_i \cdot \hat{b}_j| = \frac{1}{\sqrt{2}}$ [58], which can be obtained for the settings described in Eq. (4) or their local unitary rotation.

Here, one can verify that the NSIT condition is also satisfied in case of maximum LGI violation when $|\hat{a}_i \cdot \hat{b}_j| = \frac{1}{\sqrt{2}}$. The NSIT condition on the probabilities, $P(b_j | A_i, B_j) = P(b_j | B_j) \forall b_j, A_i, B_j$, implies $(-1)^{a_1+b_1} \hat{a}_1 \cdot \hat{b}_1 = (-1)^{a_2+b_1} \hat{a}_2 \cdot \hat{b}_1 = (-1)^{a_1+b_2} \hat{a}_1 \cdot \hat{b}_2 = (-1)^{a_2+b_2} \hat{a}_2 \cdot \hat{b}_2$. Thus clearly, when maximum violation of \mathcal{K}_4 is observed along with the NSIT condition, it is obvious that the predictability condition does not hold anymore. ■

We now show how maximal violation of LGI can also be used to self-test the Pauli measurements even if the measurement operators act on a higher-dimensional Hilbert space. Let the initial state be ρ_{in} in an arbitrary dimensional Hilbert space, and the measurements A_i, B_j both act on this space.

Lemma 2. The maximum violation of LGI (i.e., $\mathcal{K}_4^{\max} = 2\sqrt{2}$) implies implementation of the block diagonal measurement, i.e., $A_1 = \oplus_i \sigma_z^i, A_2 = \oplus_i \sigma_x^i, B_1 = \oplus_j (\sigma_x^j + \sigma_z^j)/\sqrt{2}, B_2 = \oplus_j (\sigma_x^j - \sigma_z^j)/\sqrt{2}$.

Proof. Suppose $\{\mathcal{P}_{a_i|A_i}\}$ and $\{\mathcal{P}_{b_j|B_j}\}$ are two dichotomic measurements which act on an arbitrary-dimensional Hilbert space. Then, according to Jordan's lemma [26], $\mathcal{P}_{a_i|A_i} = \oplus_m \mathcal{P}_{a_i|A_i}^m$ and $\mathcal{P}_{b_j|B_j} = \oplus_n \mathcal{P}_{b_j|B_j}^n$, where $\mathcal{P}_{a_i|A_i}^m$ and $\mathcal{P}_{b_j|B_j}^n$ are projectors on \mathcal{H}_d with $d \leq 2$ (here, in view of our proof of lemma 1, we again stick to projective measurements without any loss of generality). Therefore, one has

$$P(a_i, b_j | A_i, B_j) = \sum_{m,n} p_m \text{Tr}[\mathcal{P}_{a_i|A_i}^m \rho_m] \text{Tr}\left[\mathcal{P}_{b_j|B_j}^n \frac{\mathcal{P}_{a_i|A_i}^m \rho_m \mathcal{P}_{a_i|A_i}^{m\dagger}}{\text{Tr}[\mathcal{P}_{a_i|A_i}^m \rho_m \mathcal{P}_{a_i|A_i}^{m\dagger}]}\right]$$

where $p_m = \text{Tr}(\rho_{in} \Pi_m)$, with $\Pi_m = \sum_{a_i} \mathcal{P}_{a_i|A_i}^m$, and $\rho_m = (\Pi_m \rho_{in} \Pi_m) / p_m$, which is at most a qubit state. Now, the operators of the above equation acting on \mathcal{H}_d with $d = 2$ implies

that

$$P(a_i, b_j | A_i, B_j) = \sum_m p_m \frac{1}{4}[1 + (-1)^{a_i} \hat{a}_i^m \cdot \hat{r}][1 + (-1)^{a_i+b_j} \hat{a}_i^m \cdot \hat{b}_j^n].$$

From the above equation it follows that

$$C_{ij} = \sum_{m,n} p_m \hat{a}_i^m \cdot \hat{b}_j^n \quad (9)$$

The above expectation implies $C_{11} + C_{21} + C_{22} - C_{12} = 2\sqrt{2}$ if and only if $\hat{a}_1^m = \hat{z}, \hat{a}_2^m = \hat{x}, \hat{b}_1^n = (\hat{z} + \hat{x})/\sqrt{2}, \hat{b}_2^n = (\hat{z} - \hat{x})/\sqrt{2}$ and $\sum_m p_m = 1$. This is achieved if and only if $A_1 = \oplus_m \sigma_z^m, A_2 = \oplus_m \sigma_x^m, B_1 = \oplus_n (\sigma_x^n + \sigma_z^n)/\sqrt{2}, B_2 = \oplus_n (\sigma_x^n - \sigma_z^n)/\sqrt{2}$ and $\rho_{in} = \oplus_m p_m \rho_m$.

The above two lemmas enables us to present the following theorem. ■

Theorem 1. If $\mathcal{K}_4^{\max} = 2\sqrt{2}$ is observed in LG-test under Assumption 1, with the measurements of Alice, A_i acting on \mathcal{H}_d , producing the post measurement states $\left\{ \frac{\mathcal{P}_{a_i|A_i} \rho_{in} \mathcal{P}_{a_i|A_i}^\dagger}{\text{Tr}[\mathcal{P}_{a_i|A_i} \rho_{in} \mathcal{P}_{a_i|A_i}^\dagger]} \right\}_a$, and the measurements of Bob B_j acting on these post measurement states, then there exists an isometry $\Phi : \mathcal{H}^d \rightarrow \mathcal{C}^2 \otimes \mathcal{H}^d$ such that

$$\Phi \left(B_j \frac{\mathcal{P}_{a_i|A_i} \rho_{in} \mathcal{P}_{a_i|A_i}^\dagger}{\text{Tr}[\mathcal{P}_{a_i|A_i} \rho_{in} \mathcal{P}_{a_i|A_i}^\dagger]} \right) \Phi^\dagger = B_j^{\text{ideal}} |\psi_{a_i|A_i}^{\text{ideal}}\rangle \langle \psi_{a_i|A_i}^{\text{ideal}}| \otimes |\text{junk}\rangle \langle \text{junk}|,$$

where $|\psi_{a_i|A_i}^{\text{ideal}}\rangle$ are the eigenstates of Alice's ideal measurements and B_j^{ideal} are Bob's ideal measurements given by Eq. (4), respectively, and $|\text{junk}\rangle$ is a junk state acting on \mathcal{H}^d .

Proof. The details proof are given in the Appendix B. Choosing the eigenbasis of A_1 as the computational basis, from lemmas 1 and 2, it follows that the postmeasurement states of Alice can be written as $\frac{\mathcal{P}_{a_i|A_i} \rho_{in} \mathcal{P}_{a_i|A_i}^\dagger}{\text{Tr}[\mathcal{P}_{a_i|A_i} \rho_{in} \mathcal{P}_{a_i|A_i}^\dagger]} = \oplus_m p_m |\psi_{a_i|A_i}^m\rangle \langle \psi_{a_i|A_i}^m|$, with $|\psi_{0|A_1}^m\rangle = |2m\rangle$ and $|\psi_{1|A_1}^m\rangle = |2m+1\rangle$. We append an ancilla qubit prepared in the state $|0\rangle$ and look for an isometry Φ such that

$$\Phi \left(B_j \frac{\mathcal{P}_{a_i|A_i} \rho_{in} \mathcal{P}_{a_i|A_i}^\dagger}{\text{Tr}[\mathcal{P}_{a_i|A_i} \rho_{in} \mathcal{P}_{a_i|A_i}^\dagger]} \otimes |0\rangle \langle 0| \right) \Phi^\dagger = B_j^{\text{ideal}} |\psi_{a_i|A_i}^{\text{ideal}}\rangle \langle \psi_{a_i|A_i}^{\text{ideal}}| \otimes |\text{junk}\rangle \langle \text{junk}|.$$

This can be achieved for Φ defined by the map

$$\begin{aligned} \Phi|2m, 0\rangle &\rightarrow |2m, 0\rangle, \\ \Phi|2m+1, 0\rangle &\rightarrow |2m, 1\rangle. \end{aligned}$$

V. ROBUST SELF-TESTING OF MEASUREMENTS

Robustness of self-testing of measurements is quantified as how the actual observables which are to be self-tested differ from the ideal ones. Hence, characterization of the fidelities between the real measurements and the ideal measurements is warranted. Let us first perform the robustness analysis of the measurements on Alice's side, i.e., $\{\mathcal{P}_{a_i|A_i}\}$. Given an arbitrary

set of measurements $\{\mathcal{P}_{a_i|A_i}\}$, the average fidelity with the ideal measurements are

$$S(\{\mathcal{P}_{a_i|A_i}\}) = \max_{\Lambda} \sum_{i,a_i} F(\mathcal{P}_{a_i|A_i}^{\text{ideal}}, \Lambda[\mathcal{P}_{a_i|A_i}]) / 4. \quad (10)$$

Here Λ is a quantum channel and the fidelities are defined as usual, $F(\rho, \sigma) = \text{Tr}(\sqrt{\sqrt{\rho}\sigma\sqrt{\rho}})$. The fidelities between the real and the ideal measurements $F(\mathcal{P}_{a_i|A_i}^{\text{ideal}}, \Lambda[\mathcal{P}_{a_i|A_i}])$ simplify to $\text{Tr}(\Lambda[\mathcal{P}_{a_i|A_i}] \mathcal{P}_{a_i|A_i}^{\text{ideal}})$. The lower bound on the smallest possible value of the average fidelity S , given a particular violation of the four-time LGI \mathcal{K}_4 , can be found by minimizing over all sets of four measurements of $\mathcal{P}_{a_i|A_i}$,

$$\mathcal{F}(\mathcal{K}_4) = \min_{\mathcal{P}_{a_i|A_i}} S(\{\mathcal{P}_{a_i|A_i}\}). \quad (11)$$

To obtain a lower bound for \mathcal{F} as a function of LGI-violation \mathcal{K}_4 , we use the operator inequality approach given in Refs. [26,40]. Rewriting \mathcal{K}_4 in terms of an operator $W_{i a_i}$ and $\mathcal{P}_{a_i|A_i}$, where $W_{i a_i} = \frac{1}{2}[(-1)^{a_i}(\mathcal{P}_{B_1} + (-1)^{i-1}\mathcal{P}_{B_2})]$, $\mathcal{P}_{B_i} \equiv \mathcal{P}_{0|B_i} - \mathcal{P}_{1|B_i}$, we have

$$\mathcal{K}_4 = \sum_{i,a_i} \text{Tr}[W_{i a_i} \mathcal{P}_{a_i|A_i}]. \quad (12)$$

Let us now define another operator $K_{i a_i}(\mathcal{P}_{B_1}, \mathcal{P}_{B_2}) \equiv \Lambda^\dagger(\mathcal{P}_{B_1}, \mathcal{P}_{B_2})[\mathcal{P}_{a_i|A_i}^{\text{ideal}}]$. Considering an operator inequality of the form

$$K_{i a_i}(\mathcal{P}_{B_1}, \mathcal{P}_{B_2}) \geq s W_{i a_i} + \mu_{i a_i}(\mathcal{P}_{B_1}, \mathcal{P}_{B_2}) \mathbb{I}, \quad (13)$$

with s and $\mu_{i a_i}(\mathcal{P}_{B_1}, \mathcal{P}_{B_2})$ being real coefficients, the average fidelity S (and hence \mathcal{F}) can be lower bounded as

$$\begin{aligned} \mathcal{F} &\geq S \geq \frac{1}{4} \sum_{i,a_i} F(\mathcal{P}_{a_i|A_i}^{\text{ideal}}, \Lambda[\mathcal{P}_{a_i|A_i}]) \\ &= \frac{1}{4} \sum_{i,a_i} \text{Tr}[K_{i a_i} \mathcal{P}_{a_i|A_i}] \\ &\geq \frac{s}{4} \sum_{i,a_i} \text{Tr}[W_{i a_i} \mathcal{P}_{a_i|A_i}] + \frac{1}{4} \sum_{i,a_i} \mu_{i a_i} \\ &= \frac{s}{4} \mathcal{K}_4 + \mu, \end{aligned} \quad (14)$$

where $\mu \equiv 1/4 \min_{\mathcal{P}_{B_1}, \mathcal{P}_{B_2}} \sum_{i,a_i} \mu_{i a_i}(\mathcal{P}_{B_1}, \mathcal{P}_{B_2})$.

Since we can use Jordan's lemma to write the observables of Alice in a block-diagonal form with block of size at most 2×2 , it suffices for our purpose to focus on each block as in Ref. [26] to find the constants s and μ for lower bounding the fidelity. The goal of the robustness analysis is to obtain a self-testing bound as tight as possible. Following the authors of Ref. [40], adoption of the dephasing channel Λ , as an extraction map suffices to achieve our aim of finding an optimal self-testing bound

$$\Lambda_\theta(\rho) = \frac{1 + \xi(\theta)}{2} \rho + \frac{1 - \xi(\theta)}{2} \Gamma(\theta) \rho \Gamma(\theta); \quad (15)$$

where $\xi(\theta) \in [-1, 1]$ and

$$\Gamma(\theta) = \begin{cases} \sigma_z & \text{for } \theta \in [0, \frac{\pi}{4}], \\ \sigma_x & \text{for } \theta \in (\frac{\pi}{4}, \frac{\pi}{2}]. \end{cases}$$

For the interval $0 \leq \theta \leq \pi/4$

$$\begin{aligned} K_{10} &= \Lambda^\dagger[\mathcal{P}_{0|A_1}] \\ &= \frac{1 + \xi(\theta)}{2} \left[\frac{\mathbb{I} + \sigma_z}{2} \right] + \frac{1 - \xi(\theta)}{2} \left[\sigma_z \frac{\mathbb{I} + \sigma_z}{2} \sigma_z \right] \\ &= \frac{\mathbb{I} + \sigma_z}{2}, \end{aligned}$$

and similarly $K_{20} = \frac{\mathbb{I} + \xi(\theta)\sigma_x}{2}$, $K_{21} = \frac{\mathbb{I} - \xi(\theta)\sigma_x}{2}$, $K_{11} = \frac{\mathbb{I} - \sigma_z}{2}$, whereas, for the interval $\pi/4 \leq \theta \leq \pi/2$,

$$\begin{aligned} K_{10} &= \frac{\mathbb{I} + \xi(\theta)\sigma_z}{2}, & K_{20} &= \frac{\mathbb{I} + \sigma_x}{2} \\ K_{11} &= \frac{\mathbb{I} - \xi(\theta)\sigma_z}{2}, & K_{21} &= \frac{\mathbb{I} - \sigma_x}{2}. \end{aligned}$$

We can, without loss of generality, represent the two measurements in the x - z plane as

$$\begin{aligned} \mathcal{P}_{B_1} &= \cos(\theta)\sigma_z + \sin(\theta)\sigma_x, \\ \mathcal{P}_{B_2} &= \cos(\theta)\sigma_z - \sin(\theta)\sigma_x, \end{aligned} \quad (16)$$

and therefore, $W_{10} = \cos(\theta)\sigma_z$, $W_{20} = \sin(\theta)\sigma_x$, and $W_{21} = -\sin(\theta)\sigma_x$, $W_{11} = -\cos(\theta)\sigma_z$.

We analyze the operator inequality in the interval $0 \leq \theta \leq \pi/4$ and $\pi/4 \leq \theta \leq \pi/2$ separately. One can see that the effective number of inequalities may be reduced since there are symmetries in the expression of $K_{i a_i}$ and $W_{i a_i}$, and hence, without loss of generality we can choose $\mu_o \equiv \mu_{20} = \mu_{21}$ and $\mu_e \equiv \mu_{10} = \mu_{11}$. After simplification we get

$$\begin{aligned} \mu_e &\leq 1 - s \cos(\theta), \\ \mu_o &\leq s \cos(\theta), \end{aligned} \quad (17)$$

and

$$\begin{aligned} \mu_o &\leq \frac{1}{2} + \frac{1}{2}\xi(\theta) - s \sin(\theta), \\ \mu_o &\leq \frac{1}{2} - \frac{1}{2}\xi(\theta) + s \sin(\theta). \end{aligned} \quad (18)$$

To obtain the strongest bound, we have to choose the largest value of μ_o and μ_e consistent with their respective constraints, i.e., in the first interval,

$$\begin{aligned} \mu_e &= \min\{1 - s \cos(\theta), s \cos(\theta)\}, \\ \mu_o &= \min\left\{\frac{1}{2} + \frac{1}{2}\xi(\theta) - s \sin(\theta), \frac{1}{2} - \frac{1}{2}\xi(\theta) + s \sin(\theta)\right\}. \end{aligned} \quad (19)$$

A similar procedure in the second interval leads to

$$\begin{aligned} \mu_o &= \min\{1 - s \sin(\theta), s \sin(\theta)\}, \\ \mu_e &= \min\left\{\frac{1}{2} + \frac{1}{2}\xi(\theta) - s \cos(\theta), \frac{1}{2} - \frac{1}{2}\xi(\theta) + s \cos(\theta)\right\}. \end{aligned} \quad (20)$$

The expressions in the two intervals are related to each other by the transformations $\mu_o \leftrightarrow \mu_e$ and $\sin(\theta) \leftrightarrow \cos(\theta)$.

Hence, the lower bound in fidelity becomes

$$\mathcal{F}(\mathcal{K}_4) \geq \frac{s}{4} \mathcal{K}_4 + \min_{\mathcal{P}_{B_1}, \mathcal{P}_{B_2}} \mu(\mathcal{P}_{B_1}, \mathcal{P}_{B_2}), \quad (21)$$

where $\mu(\mathcal{P}_{B_1}, \mathcal{P}_{B_2}) = (\mu_e + \mu_o)/2$. To compute this value, we fix $s = \frac{1+\sqrt{2}}{2}$, and choosing the dephasing function as $\xi(\theta) = \min\{1, 2s \sin(\theta)\}$ in the interval $\theta \in [0, \pi/4]$, and $\xi(\theta) = \min\{1, 2s \cos(\theta)\}$ in the interval $\theta \in (\pi/4, \pi/2]$. After simplification, we get, $\mu = \frac{2-\sqrt{2}}{4}$ which gives the lower bound

$$\mathcal{F}(\mathcal{K}_4) \geq \frac{(1 + \sqrt{2})}{8} \mathcal{K}_4 + \frac{2 - \sqrt{2}}{4}. \quad (22)$$

This provides robust self-testing of Alice's measurements. Clearly, the maximal quantum violation of the LGI, i.e., $\mathcal{K}_4 = 2\sqrt{2}$ implies $\mathcal{F}(\mathcal{K}_4) = 1$, which suggests that the measurements must be the ideal ones. For $\mathcal{K}_4 = 2$, $\mathcal{F}(\mathcal{K}_4) \geq 3/4$. This bound can be obtained by $A_1 = A_2 = B_1 = B_2 = \sigma_z$. Therefore, we see that our bound is optimal.

We now quantify the average fidelity of the measurements on Bob's side with respect to the ideal ones: $\mathcal{S}'(\{\mathcal{P}_{b_i|B_i}\}) = \max_{\Lambda} \sum_{i,b_i} F\{(\mathcal{P}_{b_i|B_i})^{\text{ideal}} \Lambda[\mathcal{P}_{b_i|B_i}]\}/4$, where Λ must be a unital channel. Now, define

$$\mathcal{F}'(\mathcal{K}_4) = \min_{\{\mathcal{P}_{b_i|B_i}\}} \mathcal{S}'(\{\mathcal{P}_{b_i|B_i}\}). \quad (23)$$

First, we rewrite $\mathcal{K}_4 = \sum_{i,b_i} \text{Tr}[\mathcal{P}_{b_i|B_i} Z_{ib_i}]$ where $Z_{ib_i} = \frac{1}{2}(-1)^{b_i}[\mathcal{P}_{A_1} + (-1)^{i-1}\mathcal{P}_{A_2}]$ and $\mathcal{P}_{A_i} \equiv \mathcal{P}_{0|A_i} - \mathcal{P}_{1|A_i}$.

Let us take an operator inequality of the form

$$K_{ib_i}(\{\mathcal{P}_{A_1}, \mathcal{P}_{A_2}\}) \geq sZ_{ib_i} + \mu_{ib_i}(\{\mathcal{P}_{A_1}, \mathcal{P}_{A_2}\})\mathbb{I}, \quad (24)$$

with $K_{ib_i} = \Lambda^\dagger[\mathcal{P}_{b_i|B_i}^{\text{ideal}}]$. Similar to the previous case

$$\mathcal{F}'(\mathcal{K}_4) \geq \min_{\mathcal{P}_{A_1}, \mathcal{P}_{A_2}} \frac{1}{4} \sum_{i,b_i} \text{Tr}[K_{ib_i} \mathcal{P}_{b_i|B_i}]. \quad (25)$$

Using the same map and the same technique, we have $\xi(\theta) = \min\{1, 2s \sin(\theta)\}$ in interval $\theta \in [0, \pi/4]$ and $\xi(\theta) = \min\{1, 2s \cos(\theta)\}$ $\theta \in (\pi/4, \pi/2]$. If we repeat the same procedure as in Alice's measurements, we get the bound, $\mathcal{F}'(\mathcal{K}_4) \geq \frac{(1+\sqrt{2})}{8} \mathcal{K}_4 + \frac{2-\sqrt{2}}{4}$. This provides robust self-testing of Bob's measurements, which is again optimal.

To provide an operational analysis of robustness, let us choose a dephasing channel $\Lambda_\theta(\rho) = \frac{1+\xi(\theta)}{2}\rho + \frac{1-\xi(\theta)}{2}\sigma_z\rho\sigma_z$. It keeps the measurement $A_1 = \sigma_z$ as it is and dephases the measurement $A_2 = \sigma_x$ to $\xi(\theta)\sigma_x$. Let us consider Bob's measurements as $B_1 = \cos(\phi)\sigma_z + \sin(\phi)\sigma_x$ and $B_2 = \cos(\phi)\sigma_z - \sin(\phi)\sigma_x$. Taking $\xi(\theta) = \tan(\phi)$, we get

$$\mathcal{K}_4 = 2\sqrt{1 + \tan^2(\phi)} \quad \text{and} \quad \mathcal{F} = \frac{1}{4}[3 + \tan(\phi)].$$

The above expressions provide a parametric curve as a function of $\phi \in [0, \pi/4]$, which is the dashed (blue) line in Fig. 2. The straight (red) line represents the lower bound of fidelity as given by Eq. (22). A straightforward calculation shows that the robustness analysis for Bob's measurements (\mathcal{F}') produces a matching parametric curve.

VI. CONCLUSION

With the rapid development of quantum technologies, it is important to first characterize and certify various quantum devices. Among various certification protocols, self-testing protocols are designed for the purpose of certifying quantum components from the observed statistics under a set of

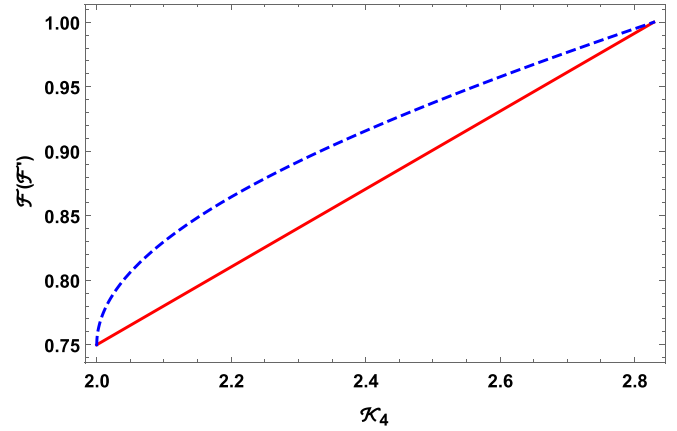


FIG. 2. The average fidelity $\mathcal{F}(\mathcal{F}')$, for Alice's (Bob's) measurement as a function of \mathcal{K}_4 is plotted. The red (solid) line represents the lower bound of average fidelity obtained analytically from Eq. (22). The blue (dotted) line is the average fidelity under dephasing noise.

minimal assumptions. Self-testing is regarded to be more resource efficient, and requires lesser trust on measurement devices. Previously, self-testing of measurements has been performed mainly employing nonlocal spatial quantum correlations [8,16,28,30,31,35], as exhibited by the violation of Bell-type inequalities, which require entanglement, a costly resource. Schemes of self-testing measurements without entanglement proposed earlier require either dimensional restrictions [40,42], or other stringent assumptions like compatibility and projectivity of the measurements [43,47] in the case of approaches based on contextuality, though it may be possible to relax some of these assumptions for local measurements in three and higher dimensions [46].

In this work our purpose is to self-test binary measurements with dichotomic settings and outcomes without using entangled states. To this end we exploited another fundamental property of quantum mechanics, *viz.*, temporal quantum correlations exhibited by violation of Leggett-Garg inequalities together with violation of predictability [48–51,54]. We presented a scheme of self-testing of binary Pauli measurements through LGI violation using a minimal assumption that is inevitable in the present context. We showed how the maximum quantum violation of the four-term LGI along with the NSIT condition can be used to provide a self-testing statement of binary measurements without entanglement, which requires neither compatibility or projectivity, nor any dimensional restriction. Moreover, we have formulated the robustness bound of our self-testing protocol, and analysed it with an example of dephasing noise.

Before concluding, we would like to highlight certain salient features of our analysis. First, it is evident from our analysis that the proposed self-testing protocol for binary qubit measurements does not depend on the input state. Second, though in the present work we have not discussed self-testing of quantum states, once the measurement devices are characterized through our approach of self-testing through the LGI framework, any subsequent certification of quantum states using such devices may reduce essentially to the task of decoherence control. Finally, the NSIT condition used here is experimentally implementable, as shown recently, for a

variety of states [73]. Experimental viability of our protocol is ensured in the backdrop of several recent LG tests [67–73].

ACKNOWLEDGMENTS

A.G.M. would like to thank D. Das and D. Saha for helpful comments. C.J. thanks H.-Y. Ku for discussions and acknowledges the financial support from the Ministry of Science and Technology, Taiwan (Grant No. MOST 108-2811-M-006-516) and the Foundation for Polish Science through the First Team project (No. First TEAM/2017-4/31). A.S.M. acknowledges support from the project DST/ICPS/QuEST/Q98 from the Department of Science and Technology, India. S.M. acknowledges the Ministry of Science and Technology in Taiwan (Grant No. 110-2811-M-006-501).

APPENDIX A: MAXIMAL VIOLATION OF THE LGI WITH POVMS

Here we obtain the maximal of the Leggett-Garg inequality for POVMs [64,77], which are a set of positive operators that add to identity, i.e., $E \equiv \{E_i | \sum_i E_i = \mathbb{I}, 0 < E_i \leq \mathbb{I}\}$. Each of the operators E_i , called effect operator determines the probability $\text{Tr}[\rho E_i]$ of obtaining the i th outcome when applied on the state ρ . The most general POVM with two outcomes are defined by two parameters: the sharpness parameter and biasedness parameter. Let us consider that γ_a, γ_b are the biasedness parameter and λ_i and μ_j are the sharpness parameters for Alice’s i th and Bob’s j th measurements, respectively. The most general effect operators with two outcomes can be written as

$$E_{a_i}^{\lambda_i} = \lambda_i \mathcal{P}_{a_i|A_i} + (1 \pm \gamma_a - \lambda_i) \frac{\mathbb{I}_2}{2},$$

$$E_{b_j}^{\mu_j} = \mu_j \mathcal{P}_{b_j|B_j} + (1 \pm \gamma_b - \mu_j) \frac{\mathbb{I}_2}{2}. \quad (A1)$$

The post measurement state can be derived using generalized von Neumann-Lüders transformation rule, $\frac{\sqrt{E_{a_i}^{\lambda_i}} \rho \sqrt{E_{a_i}^{\lambda_i}}}{\text{Tr}[E_{a_i}^{\lambda_i} \rho]}$.

Now, to derive the LGI we shall follow the same scenario and procedure as discussed in the main text. The two-time joint probability is obtained using Bayes’s rule

$$P(a_i, b_j | A_i, B_j) = P(a_i | A_i)P(b_j | a_i, A_i, B_j) = \text{Tr}[E_{a_i}^{\lambda_i} \rho_{in}] \text{Tr} \left[\frac{E_{b_j}^{\mu_j} \sqrt{E_{a_i}^{\lambda_i}} \rho \sqrt{E_{a_i}^{\lambda_i}}}{\text{Tr}[E_{a_i}^{\lambda_i} \rho]} \right]. \quad (A2)$$

$$\oplus_n \frac{\sigma_x^n + \sigma_z^n}{\sqrt{2}} \oplus_m p_m |2m\rangle \langle 2m| = \left(\frac{|0\rangle \langle 0| - |1\rangle \langle 1| + |0\rangle \langle 1| + |1\rangle \langle 0|}{\sqrt{2}} + \frac{|2\rangle \langle 2| - |3\rangle \langle 3| + |2\rangle \langle 3| + |3\rangle \langle 2|}{\sqrt{2}} + \dots + \frac{|2m\rangle \langle 2m| - |2m+1\rangle \langle 2m+1| + |2m\rangle \langle 2m+1| + |2m+1\rangle \langle 2m|}{\sqrt{2}} \right) \cdot (p_0 |0\rangle \langle 0| + p_1 |2\rangle \langle 2| + \dots + p_m |2m\rangle \langle 2m|) = \left(p_0 \frac{|0\rangle + |1\rangle}{\sqrt{2}} \langle 0| + p_1 \frac{|2\rangle + |3\rangle}{\sqrt{2}} \langle 2| + \dots + p_m \frac{|2m\rangle + |2m+1\rangle}{\sqrt{2}} \langle 2m| \right). \quad (B2)$$

The two-time correlation is defined as

$$C_{ij} = \sum_{a_i, b_j} (-1)^{a_i \oplus b_j} P(a_i, b_j | A_i, B_j), \quad (A3)$$

where \oplus denotes addition modulo 2. The four-term LGI in terms of the above correlators is given by

$$\mathcal{K}_4 = C_{11} + C_{21} + C_{22} - C_{12} \leq 2. \quad (A4)$$

For a general input state $\rho_{in} = \frac{\mathbb{I} + \hat{n} \cdot \vec{\sigma}}{2}$, the first term (probability obtained by Alice) reduces to

$$\text{Tr}[E_{a_i}^{\lambda_i} \rho_{in}] = \frac{1}{2} [(1 \pm \gamma_a) + (-1)^{a_i} \lambda_i \hat{a}_i \cdot \hat{n}]$$

Similarly, one can calculate $\text{Tr}[E_{b_j}^{\mu_j} \frac{\sqrt{E_{a_i}^{\lambda_i}} \rho \sqrt{E_{a_i}^{\lambda_i}}}{\text{Tr}[E_{a_i}^{\lambda_i} \rho]}]$ One can now calculate \mathcal{K}_4 and maximize it numerically. It can be found that the maximum quantum value of \mathcal{K}_4 is $2\sqrt{2}$ when all $|\hat{a}_i \cdot \hat{b}_j| = \frac{1}{\sqrt{2}}$ along with $\lambda_i = \mu_j = 1$ and $\gamma_a = \gamma_b = 0$. Hence, the maximum value of LGI can only be achieved if Alice and Bob perform sharp-projective measurements.

APPENDIX B: DETAILS OF PROOF OF THEOREM 1

Appending an ancilla qubit prepared in the state $|0\rangle$, let us show that there exists an isometry Φ defined by the map

$$\Phi |2m, 0\rangle \rightarrow |2m, 0\rangle, \quad \Phi |2m+1, 0\rangle \rightarrow |2m, 1\rangle, \quad (B1)$$

such that

$$\Phi \left(B_j \frac{\mathcal{P}_{a_i|A_i} \rho_{in} \mathcal{P}_{a_i|A_i}^\dagger}{\text{Tr}[\mathcal{P}_{a_i|A_i} \rho_{in} \mathcal{P}_{a_i|A_i}^\dagger]} \otimes |0\rangle \langle 0| \right) \Phi^\dagger = B_j^{\text{ideal}} |\psi_{a|A_i}^{\text{ideal}}\rangle \langle \psi_{a|A_i}^{\text{ideal}}| \otimes |\text{junk}\rangle \langle \text{junk}|$$

holds.

We present here the calculation for one term (say, $\Phi(B_1 \frac{\mathcal{P}_{a_1|A_1} \rho_{in} \mathcal{P}_{a_1|A_1}^\dagger}{\text{Tr}[\mathcal{P}_{a_1|A_1} \rho_{in} \mathcal{P}_{a_1|A_1}^\dagger]} \otimes |0\rangle \langle 0|) \Phi^\dagger$) explicitly. Other terms can be calculated in a similar fashion.

Choosing the eigenbasis of A_1 as the computational basis, from lemmas 1 and 2, it follows that the postmeasurement states of Alice can be written as $\frac{\mathcal{P}_{a_i|A_i} \rho_{in} \mathcal{P}_{a_i|A_i}^\dagger}{\text{Tr}[\mathcal{P}_{a_i|A_i} \rho_{in} \mathcal{P}_{a_i|A_i}^\dagger]} = \oplus_m p_m |\psi_{a|A_1}^m\rangle \langle \psi_{a|A_1}^m|$, with $|\psi_{0|A_1}^m\rangle = |2m\rangle$ and $|\psi_{1|A_1}^m\rangle = |2m+1\rangle$. The measurement B_1 on Bob’s side is $\oplus_n (\sigma_x^n + \sigma_z^n) / \sqrt{2}$. Expanding the sum for $a = 0$ leads to

Now, for the map defined above,

$$\begin{aligned} & \Phi \left(\bigoplus_n \frac{\sigma_x^n + \sigma_z^n}{\sqrt{2}} \bigoplus_m p_m |2m\rangle \langle 2m| \otimes |0\rangle \langle 0| \right) \Phi^\dagger \\ &= \frac{|0\rangle + |1\rangle}{\sqrt{2}} \langle 0| \otimes \bigoplus_m p_m |2m\rangle \langle 2m| \\ &= B_1^{\text{ideal}} |\psi_{0|A_1}^{\text{ideal}}\rangle \langle \psi_{0|A_1}^{\text{ideal}}| \otimes |\text{junk}\rangle \langle \text{junk}|, \end{aligned} \quad (\text{B3})$$

with $|\text{junk}\rangle \langle \text{junk}| = \sum_m p_m |2m\rangle \langle 2m|$.

Next, for $a = 1$, we have

$$\begin{aligned} & \bigoplus_n \frac{\sigma_x^n + \sigma_z^n}{\sqrt{2}} \bigoplus_m p_m |2m+1\rangle \langle 2m+1| \\ &= \left(p_0 \frac{|0\rangle - |1\rangle}{\sqrt{2}} \langle 0| + p_1 \frac{|2\rangle - |3\rangle}{\sqrt{2}} \langle 2| + \cdots + p_m \frac{|2m\rangle - |2m+1\rangle}{\sqrt{2}} \langle 2m| \right). \end{aligned} \quad (\text{B4})$$

Hence, for the map defined above,

$$\begin{aligned} & \Phi \left(\bigoplus_n \frac{\sigma_x^n + \sigma_z^n}{\sqrt{2}} \bigoplus_m p_m |2m+1\rangle \langle 2m+1| \otimes |0\rangle \langle 0| \right) \Phi^\dagger \\ &= \frac{|0\rangle - |1\rangle}{\sqrt{2}} \langle 0| \otimes \bigoplus_m p_m |2m\rangle \langle 2m| \\ &= B_1^{\text{ideal}} |\psi_{1|A_1}^{\text{ideal}}\rangle \langle \psi_{1|A_1}^{\text{ideal}}| \otimes |\text{junk}\rangle \langle \text{junk}|. \end{aligned} \quad (\text{B5})$$

-
- [1] N. Gisin *et al.*, *Rev. Mod. Phys.* **74**, 145 (2002); M. Dusek, N. Lutkenhaus, and M. Hendrych, in *Progress in Optics*, edited by E. Wolf (Elsevier, New York, 2006), Vol. 49, p. 381.
- [2] C. L. Degen, F. Reinhard, and P. Cappellaro, *Rev. Mod. Phys.* **89**, 035002 (2017).
- [3] L. Pezze, A. Smerzi, M. K. Oberthaler, R. Schmied, and P. Treutlein, *Rev. Mod. Phys.* **90**, 035005 (2018).
- [4] H. J. Kimble, *Nature (London)* **453**, 1023 (2008).
- [5] J. Biamonte, P. Wittek, N. Pancotti, P. Rebentrost, N. Wiebe, and S. Lloyd, *Nature* **549**, 195 (2017); V. Dunjko and H. J. Briegel, *Rep. Prog. Phys.* **81**, 074001 (2018).
- [6] J. Eisert, D. Hangleiter, N. Walk, I. Roth, D. Markham, R. Parekh, U. Chabaud, and E. Kashefi, *Nat. Rev. Phys.* **2**, 382 (2020).
- [7] D. Mayers and A. Yao, in *Proceedings of the 39th FOCS (IEEE Computer Society, Washington, DC, 1998)*, p. 503.
- [8] D. Mayers and A. Yao, *Quantum Inf. Comput.* **4**, 273 (2004).
- [9] J. S. Bell, *Physics* **1**, 195 (1964).
- [10] J. F. Clauser, M. A. Horne, A. Shimony, and R. A. Holt, *Phys. Rev. Lett.* **23**, 880 (1969).
- [11] S. Popescu and D. Rohrlich, *Phys. Lett. A* **169**, 411 (1992).
- [12] B. Hensen *et al.*, *Nature* **526**, 682 (2015).
- [13] L. K. Shalm, E. Meyer-Scott, B. G. Christensen, P. Bierhorst, M. A. Wayne, M. J. Stevens, T. Gerrits, S. Glancy, D. R. Hamel *et al.*, *Phys. Rev. Lett.* **115**, 250402 (2015).
- [14] M. Giustina, M. A. M. Versteegh, S. Wengerowsky, J. Handsteiner, A. Hochrainer, K. Phelan, F. Steinlechner, J. Kofler, J. A. Larsson, C. Abellan *et al.*, *Phys. Rev. Lett.* **115**, 250401 (2015).
- [15] W. Rosenfeld, D. Burchardt, R. Garthoff, K. Redeker, N. Ortengel, M. Rau, and H. Weinfurter, *Phys. Rev. Lett.* **119**, 010402 (2017).
- [16] A. Coladangelo, K. T. Goh, and V. Scarani, *Nat. Commun.* **8**, 15485 (2017).
- [17] I. Supic and M. J. Hoban, *New J. Phys.* **18**, 075006 (2016).
- [18] S. Goswami, B. Bhattacharya, D. Das, S. Sasmal, C. Jebaratnam, and A. S. Majumdar, *Phys. Rev. A* **98**, 022311 (2018).
- [19] K. T. Goh, J.-D. Bancal, and V. Scarani, *New J. Phys.* **18**, 045022 (2016).
- [20] H. Shrotriya, K. Bharti, and L.-C. Kwok, [arXiv:2007.04020](https://arxiv.org/abs/2007.04020).
- [21] H. M. Wiseman, S. J. Jones, and A. C. Doherty, *Phys. Rev. Lett.* **98**, 140402 (2007).
- [22] Z. Bian, A. S. Majumdar, C. Jebarathinam, K. Wang, L. Xiao, X. Zhan, Y. Zhang, and P. Xue, *Phys. Rev. A* **101**, 020301 (R) (2020).
- [23] M. McKague, T. H. Yang, and V. Scarani, *J. Phys. A: Math. Theor.* **45**, 455304 (2012).
- [24] T. H. Yang and M. Navascues, *Phys. Rev. A* **87**, 050102(R) (2013).
- [25] C. Bamps and S. Pironio, *Phys. Rev. A* **91**, 052111 (2015).
- [26] J. Kaniewski, *Phys. Rev. Lett.* **117**, 070402 (2016).
- [27] X. Wu, Y. Cai, T.-H. Yang, H.-N. Le, J. D. Bancal, and V. Scarani, *Phys. Rev. A* **90**, 042339 (2014).

- [28] I. Supic, A. Coladangelo, R. Augusiak, and A. Acin, *New J. Phys.* **20**, 083041 (2018).
- [29] W.-H. Zhang, G. Chen, X.-X. Peng, X.-J. Ye, P. Yin, Y. Xiao, Z.-B. Hou, Z.-D. Cheng, Y.-C. Wu, J.-S. Xu, C.-F. Li, and G.-C. Guo, *Phys. Rev. Lett.* **121**, 240402 (2018).
- [30] J. D. Bancal, N. Sangouard, and P. Sekatski, *Phys. Rev. Lett.* **121**, 250506 (2018).
- [31] M. O. Renou, J. Kaniewski, and N. Brunner, *Phys. Rev. Lett.* **121**, 250507 (2018).
- [32] J. Kaniewski, *Phys. Rev. A* **95**, 062323 (2017).
- [33] M. McKague and M. Mosca, in *Theory of Quantum Computation, Communication, and Cryptography*, edited by W. van Dam, V. M. Kendon, and S. Severini (Springer, Berlin, 2011), pp. 113–130.
- [34] J. Bowles, I. Supic, D. Cavalcanti, and A. Acin, *Phys. Rev. A* **98**, 042336 (2018).
- [35] I. Supic and J. Bowles, *Quantum* **4**, 337 (2020).
- [36] H.-W. Li, Z.-Q. Yin, Y.-C. Wu, X.-B. Zou, S. Wang, W. Chen, G.-C. Guo, and Z.-F. Han, *Phys. Rev. A* **84**, 034301 (2011).
- [37] T. Lunghi, J. B. Brask, Charles Ci Wen Lim, Q. Lavigne, J. Bowles, A. Martin, H. Zbinden, and N. Brunner, *Phys. Rev. Lett.* **114**, 150501 (2015).
- [38] P. Mironowicz, A. Tavakoli, A. Hameedi, B. Marques, M. Pawowski, and M. Bourennane, *New J. Phys.* **18**, 065004 (2016).
- [39] A. Tavakoli, M. Smania, T. Vertesi, N. Brunner, and M. Bourennane, *Sci. Adv.* **6**, 16 (2020).
- [40] A. Tavakoli, J. Kaniewski, T. Vertesi, D. Rosset, and N. Brunner, *Phys. Rev. A* **98**, 062307 (2018).
- [41] A. Ambainis, A. Nayak, A. Ta-Shama, and U. Vazirani, in *Proceedings of 31st ACM Symposium on Theory of Computing* (ACM, Atlanta, 1999), pp. 376–383.
- [42] A. Tavakoli, A. Hameedi, B. Marques, and M. Bourennane, *Phys. Rev. Lett.* **114**, 170502 (2015).
- [43] K. Bharti, M. Ray, A. Varvitsiotis, N. A. Warsi, A. Cabello, and L. C. Kwek, *Phys. Rev. Lett.* **122**, 250403 (2019).
- [44] S. Kochen and E. P. Specker, *J. Appl. Math. Phys.* (1950-1981) **17**, 59 (1967).
- [45] A. A. Klyachko, M. A. Can, S. Binicioglu, and A. S. Shumovsky, *Phys. Rev. Lett.* **101**, 020403 (2008).
- [46] D. Saha, R. Santos, and R. Augusiak, *Quantum* **4**, 302 (2020).
- [47] K. Bharti, M. Ray, A. Varvitsiotis, A. Cabello, and L. C. Kwek, [arXiv:1911.09448](https://arxiv.org/abs/1911.09448).
- [48] A. J. Leggett and A. Garg, *Phys. Rev. Lett.* **54**, 857 (1985).
- [49] C. Emary, N. Lambert, and F. Nori, *Rep. Prog. Phys.* **77**, 016001 (2014).
- [50] J. Kofler and C. Brukner, *Phys. Rev. A* **87**, 052115 (2013).
- [51] S. Mal, M. Banik, and S. K. Choudhury, *Quantum Inf. Proc.* **15**, 2993 (2016).
- [52] A. J. Leggett, *J. Phys.: Condens. Matter* **14**, R415 (2002); *Rep. Prog. Phys.* **71**, 022001 (2008).
- [53] J. Kofler and C. Brukner, *Phys. Rev. Lett.* **99**, 180403 (2007).
- [54] C. Brukner, S. Taylor, S. Cheung, and V. Vedral, [arXiv:quant-ph/0402127](https://arxiv.org/abs/quant-ph/0402127).
- [55] S. Mal and A. S. Majumdar, *Phys. Lett. A* **380**, 2265 (2016).
- [56] S. Bose, D. Home, and S. Mal, *Phys. Rev. Lett.* **120**, 210402 (2018).
- [57] S. Mukherjee, A. Rudra, D. Das, S. Mal, and D. Home, *Phys. Rev. A* **100**, 042114 (2019).
- [58] T. Fritz, *New J. Phys.* **12**, 083055 (2010).
- [59] C. Budroni, T. Moroder, M. Kleinmann, and O. Gühne, *Phys. Rev. Lett.* **111**, 020403 (2013).
- [60] C. Budroni and C. Emary, *Phys. Rev. Lett.* **113**, 050401 (2014).
- [61] S. Brierley, A. Kosowski, M. Markiewicz, T. Paterek, and A. Przysieszna, *Phys. Rev. Lett.* **115**, 120404 (2015).
- [62] A. R. Usha Devi, H. S. Karthik, Sudha, and A. K. Rajagopal, *Phys. Rev. A* **87**, 052103 (2013).
- [63] S. Kumari and A. K. Pan, *Phys. Rev. A* **96**, 042107 (2017).
- [64] D. Das, S. Mal, and D. Home, *Phys. Lett. A* **382**, 1085 (2018).
- [65] H.-Y. Ku, S.-L. Chen, N. Lambert, Y.-N. Chen, and F. Nori, *Phys. Rev. A* **98**, 022104 (2018).
- [66] T. Chanda, T. Das, S. Mal, A. Sen De, and U. Sen, *Phys. Rev. A* **98**, 022138 (2018).
- [67] G. C. Knee, S. Simmons, E. M. Gauger, J. J. L. Morton, H. Riemann, N. V. Abrosimov, P. Becker, H.-J. Pohl, K. M. Itoh, M. L. W. Thewalt, G. A. D. Briggs, and S. C. Benjamin, *Nat. Commun.* **3**, 606 (2012).
- [68] C. Robens, W. Alt, D. Meschede, C. Emary, and A. Alberti, *Phys. Rev. X* **5**, 011003 (2015).
- [69] G. C. Knee, K. Kakuyanagi, M.-C. Yeh, Y. Matsuzaki, H. Toida, H. Yamaguchi, S. Saito, A. J. Leggett, and W. J. Munro, *Nat. Commun.* **7**, 13253 (2016).
- [70] H.-Y. Ku, N. Lambert, F.-R. Jhan, C. Emary, Y.-N. Chen, and F. Nori, *npj Quantum Information* **6**, 98 (2020).
- [71] S. S. Majidy, H. Katiyar, G. Anikeeva, J. Halliwell, and R. Laflamme, *Phys. Rev. A* **100**, 042325 (2019).
- [72] C. Spee, H. Siebeneich, T. F. Gloger, P. Kaufmann, M. Johanning, M. Kleinmann, C. Wunderlich, and O. Gühne, *New J. Phys.* **22**, 023028 (2020).
- [73] C. Flühmann, V. Negnevitsky, M. Marinelli, and J. P. Home, *Phys. Rev. X* **8**, 021001 (2018).
- [74] E. G. Cavalcanti and H. M. Wiseman, *Found. Phys.* **42**, 1329 (2012).
- [75] L. Clemente and J. Kofler, *Phys. Rev. Lett.* **116**, 150401 (2016).
- [76] M. M. Wilde and A. Mizel, *Found. of Phys.* **42**, 256 (2012).
- [77] P. Busch, P. J. Lahti, and P. Mittelstaedt, *The Quantum Theory of Measurement* (Springer, Berlin, 1991).