


Self-testing of different entanglement resources via fixed measurement settingsXinhui Li ¹, Yukun Wang,^{2,3,*} Yunguang Han,^{4,†} and Shi-Ning Zhu¹¹*National Laboratory of Solid State Microstructures, School of Physics,**and Collaborative Innovation Center of Advanced Microstructures, Nanjing University, Nanjing 210093, China*²*Beijing Key Laboratory of Petroleum Data Mining, China University of Petroleum, Beijing 102249, China*³*State Key Laboratory of Cryptology, P.O. Box 5159, Beijing 100878, China*⁴*College of Computer Science and Technology, Nanjing University of Aeronautics and Astronautics, Nanjing 211106, China*

(Received 14 June 2022; revised 14 September 2022; accepted 18 October 2022; published 17 November 2022)

Self-testing, which refers to device-independent characterization of the state and the measurement, enables the security of a quantum information processing task certified independently of the operation performed inside the devices. Quantum states lie at the core of self-testing as key resources. However, for different entangled states, usually, different measurement settings should be taken in self-testing recipes. This may lead to the redundancy of measurement resources. In this work, we use fixed two-binary measurements and answer the question of which states can be self-tested with the same settings. By investigating the structure of generalized tilted-Clauser-Horne-Shimony-Holt Bell operators with the sum-of-squares decomposition method, we show that a family of two-qubit entangled states can be self-tested with the same measurement settings. The robustness analysis indicates that our scheme is feasible for practical experiment instruments. Moreover, our results can be applied to various quantum information processing tasks.

DOI: [10.1103/PhysRevA.106.052418](https://doi.org/10.1103/PhysRevA.106.052418)**I. INTRODUCTION**

Bell nonlocality [1,2] is central to the understanding of quantum physics. With the advent of quantum information, Bell nonlocality has been studied as a resource and applied to various quantum information processing tasks, such as quantum key distribution [3,4], randomness expansion [5,6], and entanglement witnesses [7,8].

Moreover, if we assume quantum mechanics is the underlying theory, it is shown that certain extremal quantum correlations uniquely identify the state and measurements under consideration, a phenomenon known as self-testing [9,10]. It is a concept of device independence whose verdict relies only on the observed statistics of measurement outcomes under the sole assumption of no signaling and the validity of quantum theory [11]. In the 1990s, Popescu and Rohrlich pointed out that the maximal violation of the Clauser-Horne-Shimony-Holt (CHSH) Bell inequality identifies uniquely the maximally entangled state of two qubits [12,13]. In recent decades, self-testing has received substantial attention. The scenarios for bipartite and multipartite entangled states were presented in Refs. [14–21]. The analysis of robustness to small deviations from the ideal case for self-testing these quantum states and measurements was presented in Refs. [22–25], which made self-testing more practical. Beyond these works focusing on single-copy states, parallel self-testing of tensor-product states was recently studied. The first parallel self-testing protocol was proposed for two

Einstein-Podolsky-Rosen (EPR) pairs in [26,27]. The result was subsequently generalized for arbitrary n via parallel repetition of the CHSH game in [28] and via parallel repetition of the magic-square game in [29]. Self-testing of n EPR pairs via parallel repetition of the Mayers-Yao self-test is given in [30].

In the most previous works, one measurement setting is always sufficient to self-test one target state up to local unitaries. For example, the tilted-CHSH inequality can self-test two-qubit pure states $|\psi(\theta)\rangle = \cos\theta|00\rangle + \sin\theta|11\rangle$ with corresponding measurements settings $\{\sigma_z, \sigma_x\} \otimes \{\cos\mu\sigma_z + \sin\mu\sigma_x, \cos\mu\sigma_z - \sin\mu\sigma_x\}$; meanwhile, μ is uniquely determined by θ . However, the tasks of quantum information processing may involve multiple states with different entanglement degrees [31]. The whole self-testing of quantum states results in an increased consumption of the measurement resource, thus decreasing the feasibility of practical realization. Therefore, a self-testing protocol with high practical performance is meaningful and necessary. In this work, we focus on this goal and provide a device-independent scheme that certifies a series of quantum states with reduced measurement resources. Our results show that the generalized tilted-CHSH operators allowing optimal measurements for one party could rotate on the Pauli x - z plane. Multiple different target states can be self-tested via a common measurement setting by choosing a properly generalized tilted-CHSH operator. Hence, by utilizing a set of Bell inequalities, we can self-test two-qubit states with different entanglement degrees based on only two binary measurements per party. Thus, our scheme simplifies the measurement instruments and leads to lower consumption of measurement resources. In addition, our scheme demonstrates satisfactory robustness in tolerance

*wykun06@gmail.com

†hanyunguang@nuaa.edu.cn

of noise. Further, our scheme can serve for various quantum information processing tasks with low measurement-resource costs and, meanwhile, provides secure certification of the device used in the task. This paper is structured as follows: In Sec. II A, we give a brief description of the underlying model and key definitions of our work. In Sec. II B, we propose a scheme that self-tests different two-qubit entangled states with the same measurements using a generalized tilted-CHSH inequality. During this study, we develop a family of self-testing criteria beyond the standard tilted-CHSH inequality and prove these criteria using the technique of sum-of-squares (SOS) decomposition. In Sec. III, the robustness analysis is illustrated through an example using the SWAP method and semidefinite programming (SDP). In Sec. IV, the applications of our results for quantum information processing tasks of device-independent quantum key distribution, private queries, and randomness generation are presented. In Sec. V, we summarize the results and discuss future research.

II. SELF-TESTING DIFFERENT ENTANGLED STATES VIA TWO BINARY MEASUREMENTS

A. Self-testing

Consider the simplest scenario of two noncommunicating parties, Alice and Bob. Each has access to a black box with inputs denoted respectively by $x, y \in \{0, 1\}$ and outputs denoted by $a, b \in \{+1, -1\}$. One could model these boxes with an underlying state $|\psi\rangle_{AB}$ and measurement projectors $\{M_x^a\}_{x,a}$ and $\{M_y^b\}_{y,b}$, which commute for different parties. The state can be taken to be pure, and the measurements can be taken to be projective without loss of generality because the dimension of the Hilbert space is not fixed and the possible purification and auxiliary systems can be given to any of the parties. After sufficiently many repetitions of the experiment one can estimate the joint conditional statistics, known as the behavior $p(a, b|x, y) = \langle \psi | M_x^a M_y^b | \psi \rangle$. Self-testing refers to a device-independent certification method where the non-trivial information about the state and the measurements is uniquely certified by the observed behavior $p(ab|xy)$, without assumptions about the underlying degrees of freedom. Usually, self-testing can be defined formally in the following way.

Definition 1. We say that the correlations $p(a, b|x, y)$ allow for self-testing if for every quantum behavior $(|\psi\rangle, \{M_x^a, M_y^b\})$ compatible with $p(a, b|x, y)$ a local isometry $\Phi = \Phi_A \otimes \Phi_B$ exists such that

$$\begin{aligned} \Phi |\psi\rangle_{AB} |00\rangle_{A'B'} &= |\text{junk}\rangle_{AB} \otimes |\bar{\psi}\rangle_{A'B'}, \\ \Phi(M_x^a |\psi\rangle_{AB} |00\rangle_{A'B'}) &= |\text{junk}\rangle_{AB} \otimes \bar{M}_x^a |\bar{\psi}\rangle_{A'B'}, \end{aligned} \quad (1)$$

where $|00\rangle_{A'B'}$ is the trusted auxiliary qubits attached by Alice and Bob locally in their systems and $(|\bar{\psi}\rangle, \{\bar{M}_x^a, \bar{M}_y^b\})$ are the target system [10].

That is, the correlations $p(a, b|x, y)$ predicted by quantum theory could determine uniquely the state and the measurements, up to a local isometry.

B. Self-testing of entangled two-qubit states with the generalized tilted-CHSH inequality

In this section, we show that different pure entangled two-qubit states can be self-tested via fixed measurement settings with the generalized tilted-CHSH inequality. The candidate target states we considered are $\{|\bar{\psi}_i\rangle\}$, with

$$|\bar{\psi}_i\rangle = \cos \theta_i |00\rangle + \sin \theta_i |11\rangle, \quad (2)$$

where $\theta_i \in (0, \frac{\pi}{4}]$. It has already been proved that a pure entangled two-qubit state can be self-tested using the standard tilted-CHSH inequality [14,24]. In the standard scheme, one measurement setting is required for self-testing one target state, which results in an increased consumption of the measurement resources. Utilizing the property of the generalized tilted-CHSH inequality, we show that all these entangled states can be self-tested with the given fixed measurements, thus simplifying the measurement instruments. We have the following theorem.

Theorem 1. The family of entangled two-qubit states in Eq. (2) can be self-tested using the same quantum measurement settings as in Eq. (3) with fixed angle μ . The validity of the self-testing result comes from the maximum quantum violation of generalized tilted-CHSH inequalities in Eq. (4).

The measurements in our scheme are chosen to be

$$\begin{aligned} A_0 &= \sigma_z, & B_0 &= \cos \mu \sigma_z + \sin \mu \sigma_x, \\ A_1 &= \sigma_x, & B_1 &= \cos \mu \sigma_z - \sin \mu \sigma_x, \end{aligned} \quad (3)$$

with the fixed angle $\mu \in (0, \frac{\pi}{4}]$.

The key idea of our self-testing scheme is that for a given μ in the unit measurement settings, a family of Bell inequalities can be maximally violated by different entangled pairs at the same time. Once the form of the target source is confirmed, the Bell inequalities which achieve their self-testing are determined based on the observed statistics $p(a, b|x, y)$. More precisely, the Bell inequalities have the following form, depending on the input $i \in \{0, 1, 2, \dots, n\}$:

$$\mathcal{B}_{[\alpha_i, \beta_i]} = \beta_i A_0 + \alpha_i (A_0 B_0 + A_0 B_1) + A_1 B_0 - A_1 B_1, \quad (4)$$

called the generalized tilted CHSH inequality [32], where $\alpha_i \geq 1$. The maximal classical and quantum bounds are $C_{[\alpha_i, \beta_i]} = 2\alpha_i + \beta_i$ and $\eta_{[\alpha_i, \beta_i]} = \sqrt{(4 + \beta_i^2)(1 + \alpha_i^2)}$, respectively. It has already been proved both theoretically and numerically that a pure entangled two-qubit state can be self-tested using a standard tilted-CHSH inequality with $\alpha = 1$ in Eq. (4) [14,24]. However, whether the generalized tilted-CHSH inequality can be used in self-testing is still unknown.

We claim that the maximal quantum violation in Eq. (4) uniquely certifies the corresponding entangled pairs in Eq. (2)

and measurements in Eq. (3) with $\sin 2\theta_i = \sqrt{\frac{4 - \alpha_i^2 \beta_i^2}{4 + \beta_i^2}}$ and

$\tan \mu = \frac{\sin 2\theta_i}{\alpha_i}$. Thus, the family of pure entangled two-qubit states is self-tested with the given α and β and the two fixed measurement settings μ using the generalized tilted-CHSH inequality. The self-testing recipe for our scheme is shown in Fig. 1. In the following, we give a detailed proof of Theorem 1.

Proof. The proof of Theorem 1 is divided into two steps. First, we give two types of SOS decompositions for the

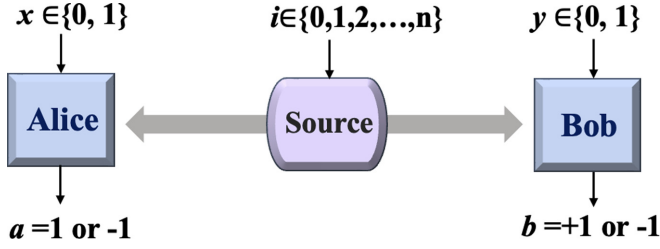


FIG. 1. Self-testing recipe. The fixed untrusted measurement settings are able to test different input states. For a given target state $|\psi_i\rangle$, two observers randomly choose their measurements, x for Alice and y for Bob, and collect outcomes a and b to construct the observation of $\mathcal{B}_{[\alpha, \beta]_i}$.

generalized tilted-CHSH operator $\mathcal{B}_{[\alpha, \beta]}$ (see the Appendix for details). Moreover, these SOS decompositions establish algebraic relations that are necessarily satisfied by any quantum state and observables, yielding a maximal violation of the generalized tilted-CHSH inequality. Then these algebraic relations are used in the isometry map to provide the self-testing of any partially entangled two-qubit state.

a. SOS decompositions for generalized tilted-CHSH inequalities. The generalized tilted-CHSH inequalities $\mathcal{B}_{[\alpha, \beta]}$ have the maximum quantum violation value $\eta_{[\alpha, \beta]}$. This implies that the operator $\widehat{\mathcal{B}} = \eta_{[\alpha, \beta]}\mathbb{I} - \mathcal{B}_{[\alpha, \beta]}$ is positive semidefinite for all possible quantum states and measurement operators A_x and B_y . This can be proven by providing a set of operators $\{P_i\}$ which are polynomial functions of A_x and B_y such that $\widehat{\mathcal{B}}_{[\alpha, \beta]} = \sum_i P_i^\dagger P_i$ holds for any set of measurement operators satisfying the algebraic properties $A_x^2 = \mathbb{I}$, $B_y^2 = \mathbb{I}$ and $[A_x, B_y] = 0$.

For convenience, we define three classes CHSH operators:

$$\begin{aligned} S_0 &= A_0(B_0 - B_1) + \frac{1}{\alpha}A_1(B_0 + B_1), \\ S_1 &= \frac{1}{\alpha}A_0(B_0 + B_1) - A_1(B_0 - B_1), \\ S_2 &= A_0(B_0 - B_1) - \alpha A_1(B_0 + B_1). \end{aligned} \quad (5)$$

Then we can give two types of SOS decompositions for the generalized tilted-CHSH operator in Eq. (4). The first decomposition is given as

$$\begin{aligned} \widehat{\mathcal{B}}_{[\alpha, \beta]} &= \frac{1}{\Delta + 2\eta_{[\alpha, \beta]}} \left\{ (\widehat{\mathcal{B}}_{[\alpha, \beta]})^2 + \alpha^2(\beta A_1 - S_0)^2 \right. \\ &+ (\alpha^2 - 1) \left[\left(-\beta A_0 + \frac{\eta_{[\alpha, \beta]}}{\alpha^2 + 1} - A_1(B_0 - B_1) \right)^2 \right. \\ &\left. \left. + \left(-\frac{\eta_{[\alpha, \beta]}\alpha}{\alpha^2 + 1} A_0 + B_0 + B_1 \right)^2 \right] \right\}. \end{aligned} \quad (6)$$

The second one is

$$\begin{aligned} \widehat{\mathcal{B}}_{[\alpha, \beta]} &= \frac{\alpha^2}{\Delta + 2\eta_{[\alpha, \beta]}} \left\{ \frac{\alpha^2 - 1}{\alpha^2} \left[\left(-\frac{\eta_{[\alpha, \beta]}\alpha}{\alpha^2 + 1} A_0 + B_0 + B_1 \right)^2 \right. \right. \\ &\left. \left. + \left(-\beta A_0 + \frac{\eta_{[\alpha, \beta]}}{\alpha^2 + 1} - A_1(B_0 - B_1) \right)^2 \right] \right\} \end{aligned}$$

$$\begin{aligned} &+ \left(2A_0 - \frac{\eta_{[\alpha, \beta]}}{2\alpha}(B_0 + B_1) + \frac{\beta}{2}S_1 \right)^2 \\ &+ \frac{1}{\alpha^2} \left(2A_1 - \frac{\eta_{[\alpha, \beta]}}{2}(B_0 - B_1) + \frac{\beta}{2}S_2 \right)^2 \Big\}, \end{aligned} \quad (7)$$

where $\Delta = 2(\alpha^2 - 1)\sqrt{\frac{\beta^2 + 4}{\alpha^2 + 1}}$.

For the special case $\alpha = 1$ of the standard tilted-CHSH inequality, our result gives the following decomposition:

$$\widehat{\mathcal{B}}_{[1, \beta]} = \frac{1}{2\eta_{[1, \beta]}} [(\widehat{\mathcal{B}}_{[1, \beta]})^2 + (\beta A_1 - S_0)^2] \quad (8)$$

and

$$\begin{aligned} \widehat{\mathcal{B}}_{[1, \beta]} &= \frac{1}{2\eta_{[1, \beta]}} \left[\left(2A_0 - \eta_{[1, \beta]} \frac{B_0 + B_1}{2} + \frac{\beta}{2}S_1 \right)^2 \right. \\ &\left. + \left(2A_1 - \eta_{[1, \beta]} \frac{B_0 - B_1}{2} + \frac{\beta}{2}S_2 \right)^2 \right], \end{aligned} \quad (9)$$

which reproduce the results in Ref. [14]. Thus, we develop a family of SOS decompositions for generalized tilted-CHSH inequalities, which is beyond the standard form.

If one observes the maximal quantum violation of the generalized tilted-CHSH inequality in Eq. (4) by any state $|\psi\rangle$ and measurements A_x and B_y for $x, y \in \{0, 1\}$, then each square of the polynomial functions in the two SOS decompositions acting on $|\psi\rangle$ is equal to zero, i.e., $P_i|\psi\rangle = 0$. Then we can obtain the anticommutation relations for the measurement operators acting on the underlying state from the two SOS decompositions (6) and (7) as follows (for details refer to the Appendix):

$$(Z_A - Z_B)|\psi\rangle = 0, \quad (10a)$$

$$[\sin\theta X_A(\mathbb{I} + Z_B) - \cos\theta X_B(\mathbb{I} - Z_A)]|\psi\rangle = 0. \quad (10b)$$

Next, we will show that these algebraic relations lead to the self-testing statement for any partially entangled two-qubit state.

b. Self-testing of partially entangled states. Based on Definition 1 for self-testing, one needs to construct the isometry map such that the underlying system can extract the information about the target state. The isometry is a virtual protocol; all that must be done in the laboratory is to query the boxes and derive $p(a, b|x, y)$. A useful way is the so-called SWAP method, and the isometry is shown in Fig. 2. The idea of the SWAP method comes from the ideal case. If state $|\psi\rangle$ is indeed two qubits and the operators are $Z = \sigma_z$ and $X = \sigma_x$, the SWAP operations can extract state $|\psi\rangle$ from the ancilla system. However, in the device-independent framework, it cannot assume the dimension of the inner state or any form of the operators. Hence, Z and X are constructed based on real performed measurements A_x and B_y such that one can swap out the desired states and measurements, as shown in Definition 1. Therefore, we define the unitary operators of Alice and Bob as

$$\begin{aligned} Z_A &= A_0, \quad Z_B = \frac{B_0 + B_1}{2 \cos \mu}, \\ X_A &= A_1, \quad X_B = \frac{B_0 - B_1}{2 \sin \mu}. \end{aligned} \quad (11)$$

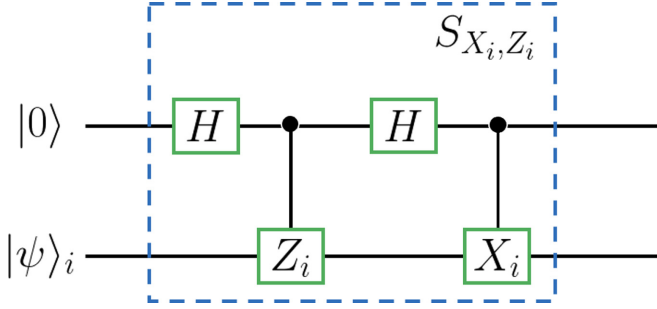


FIG. 2. The local unit S_i of the SWAP gate $S = S_A \otimes S_B$ for $i \in \{A, B\}$. Each unit acts on the corresponding particle of $|\psi\rangle$ and one ancillary qubit prepared in state $|0\rangle$. H is the standard Hadamard gate; Z_i and X_i are controlled by the auxiliary qubits.

After this isometry, the underlying systems and the trusted auxiliary qubits will be

$$\begin{aligned} \Phi(|\psi\rangle) &= \frac{1}{4}[(\mathbb{I} + Z_A)(\mathbb{I} + Z_B)|\psi\rangle|00\rangle \\ &\quad + X_B(\mathbb{I} + Z_A)(\mathbb{I} - Z_B)|\psi\rangle|01\rangle \\ &\quad + X_A(\mathbb{I} - Z_A)(\mathbb{I} + Z_B)|\psi\rangle|10\rangle \\ &\quad + X_A X_B(\mathbb{I} - Z_A)(\mathbb{I} - Z_B)|\psi\rangle|11\rangle]. \end{aligned} \quad (12)$$

From relation (10a), the second and third terms of Eq. (12) cancel and become zero. Then relation (10b) eventually leads Eq. (12) to be

$$\begin{aligned} \Phi(|\psi\rangle) &= \frac{\mathbb{I} + Z_A}{2}|\psi\rangle|00\rangle + \frac{\mathbb{I} + Z_A}{2} \frac{\sin \theta}{\cos \theta} |\psi\rangle|11\rangle \\ &= |\text{junk}\rangle \otimes |\bar{\psi}\rangle, \end{aligned} \quad (13)$$

where

$$|\text{junk}\rangle = \frac{\mathbb{I} + Z_A}{2 \cos \theta} |\psi\rangle. \quad (14)$$

Thus, the underlying state is equal to the optimal target form $|\bar{\psi}\rangle = \cos \theta |00\rangle + \sin \theta |11\rangle$, with $\sin 2\theta = \sqrt{\frac{4-\alpha^2\beta^2}{4+\beta^2}}$. This completes the self-testing statement.

The generalized tilted-CHSH operator $B_{[\alpha, \beta]}$ with two parameters such that the optimal measurements for one party can rotate on the Pauli x - z plane with respect to the target one satisfies $\alpha \tan \mu = \sqrt{\frac{4-\alpha^2\beta^2}{4+\beta^2}}$. The result is that in a self-testing scenario involving different targets $|\bar{\psi}_i\rangle$ defined as in Eq. (2), one can choose a common measurement setting (3) satisfying $\tan \mu = \frac{\sin 2\theta_i}{\alpha_i}$ to construct the Bell inequality $\eta_{[\alpha_i, \beta_i]}$ for each target state. In turn, the maximal violations uniquely certify the family of states $|\bar{\psi}_i\rangle$. Thus, we complete the proof of Theorem 1.

To be specific, $B_{[\alpha, \beta]}$ has two special forms when $\beta = 0$ and $\alpha = 1$, which correspond to biased CHSH [33] and standard tilted-CHSH operators [25], respectively.

Biased CHSH inequality. If $\beta = 0$, the Bell inequality in Eq. (4) is simplified as a symmetrical biased CHSH operator

$$B_{[\alpha, 0]} = \alpha(A_0 B_0 + A_0 B_1) + A_1 B_0 - A_1 B_1 \leq 2\alpha, \quad (15)$$

where $\alpha = \frac{1}{\tan \mu}$, which belongs to the whole set of self-testing criteria for the Bell state [17]. Its maximal quantum violation

$\eta_{[\alpha, 0]} = \frac{4}{\sqrt{1+\tan \mu}}$ is able to self-test the maximum entangled state $|\bar{\psi}\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$ and measurement setting (3).

Standard tilted-CHSH inequality. If $\alpha = 1$, the Bell inequality in Eq. (4) turns out to be the standard form

$$B_{[1, \beta]} = \beta A_0 + A_0 B_0 + A_0 B_1 + A_1 B_0 - A_1 B_1 \leq 2 + \beta, \quad (16)$$

with $\beta = 2\sqrt{2 \cos^2 \mu - 1}$. The maximal quantum violation of this inequality is given by $\eta_{[1, \beta]} = \sqrt{8 + 2\beta^2} = 4 \cos \mu$, achievable with the measurement settings in Eq. (3), and satisfies $\sin 2\theta = \sqrt{\frac{4-\beta^2}{4+\beta^2}}$.

III. ROBUSTNESS ANALYSIS

If the observed statistics deviate from the ideal ones, one can estimate how far the actual state and measurements are from the ideal ones, a property known as robustness. Here the robust self-testings of the different sources are analyzed using a numerical tool named the Navascués-Pironio-Acín (NPA) hierarchy and the SDP method [25,34]. For convenience in the calculations, we take $\mu = \arctan \frac{3}{4}$ ($\mu \approx 0.208\pi$) in the measurements settings (3) as an example to self-test the following three states:

$$\begin{aligned} |\bar{\psi}_0\rangle &= \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle), \\ |\bar{\psi}_1\rangle &= \cos \theta |00\rangle + \sin \theta |11\rangle \text{ for } \theta = \frac{1}{2} \arcsin \left(\frac{3}{4} \right), \\ |\bar{\psi}_2\rangle &= \frac{1}{2}(|00\rangle + \sqrt{3}|11\rangle), \end{aligned} \quad (17)$$

which satisfy $\tan \mu = \frac{\sin 2\theta_i}{\alpha_i}$, with $\alpha_0 = \frac{4}{3}$, $\alpha_1 = 1$, and $\alpha_2 = \frac{2}{\sqrt{3}}$. Choosing these three states not only leads to an association with three special Bell operators (biased CHSH, standard tilted-CHSH, and generalized tilted-CHSH operators) but also is convenient for the calculations in the robustness analysis. To self-test these three target states, the parameters β_i in Bell inequality (4) are set to $\beta_0 = 0$, $\beta_1 = \frac{2\sqrt{7}}{5}$, and $\beta_2 = \frac{2\sqrt{3}}{5}$, satisfying $\sin 2\theta_i = \sqrt{\frac{4-\alpha_i^2\beta_i^2}{4+\beta_i^2}}$, respectively. By substituting $[\alpha_i, \beta_i]$ in $B_{[\alpha_i, \beta_i]}$ in Eq. (4) for $i = 0, 1, 2$, it can be found that the first two pairs respectively recover to the biased inequality (15) and tilted-CHSH inequalities (16), while the third pair is complex. In particular, by fixing $\tan \mu = \frac{3}{4}$, the parameter α can be expressed by β , i.e., $\alpha = \frac{8}{\sqrt{25\beta^2+36}}$; thus,

we can plot the bounds of the Bell inequality $B_{[\alpha_i, \beta_i]}$ with respect to β . As shown in Fig. 3, with the increase of β , the classical bound gets close to but is not greater than the quantum one. The maximal quantum bounds for the ideal self-testing of the three states (17) and measurement settings (3) are presented by red triangles in Fig. 3. The gap between classical and quantum bounds at (α_0, β_0) is much larger than the other points.

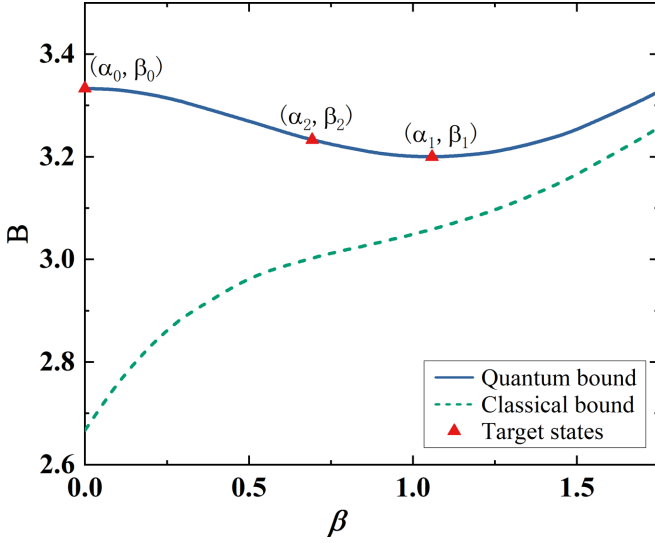


FIG. 3. The maximal violations of Bell inequalities $\mathcal{B}_{\alpha, \beta}$ with respect to β for $\tan \mu = 3/4$. The blue solid and green dashed lines represent the maximal quantum and classical bounds, respectively. The red triangles on the blue line are obtained with $[\alpha_i, \beta_i]$ for $i = 0, 1, 2$, which are ideal scenarios to self-test the three target states in Eq. (17).

After the isometry given in Fig. 2, the trusted auxiliary systems will be left in the state

$$\rho_{\text{swap}} = \sum_{ijst} C_{ijst} |j\rangle \langle i| \otimes |t\rangle \langle s|, \quad (18)$$

where $C_{ijst} = \frac{1}{16} \text{tr}_{AB} [(1 + Z_A)^{1-i} (X_A - Z_A X_A)^i (1 + Z_A)^{1-j} (X_A - X_A Z_A)^j \otimes (1 + Z_B)^{1-s} (X_B - Z_B X_B)^s (1 + Z_B)^{1-t} (X_B - X_A Z_B)^t]$. Finally, we can express the fidelity for $i = 0, 1, 2$,

$$f_i = \langle \bar{\psi}_i | \rho_{\text{swap}} | \bar{\psi}_i \rangle. \quad (19)$$

Here f_i is a linear function of two types of operator expectations: some observed behavior and some nonobservable correlations which involve different measurements on the same party, such as $\langle \psi | M_x^a M_{x'}^{a'} | \psi \rangle$, with $x \neq x'$, which are left as variables.

To get a lower bound on the fidelity, one needs to minimize the fidelity running over all the states and measurements satisfying observed statistics. Optimizations over the set of quantum momenta are computationally hard; especially, that for the underlying Hilbert space dimension is unknown. To resolve this technical difficulty, here we employ the NPA hierarchy which was introduced in Refs. [25,34] to bound fidelity. The NPA hierarchy works as follows. Consider a generic state and measurement operators $\{|\psi\rangle, A_x, B_y\}$. Then, define sets Q_l , each corresponding to a level of the hierarchy composed of the identity operator and all (noncommuting) products of operators A_x and B_y up to degree l , e.g., $Q_1 = \{\mathbb{I}, A_x, B_y\}$, $Q_2 = \{Q_1\} \cup \{Q_1^i Q_1^j\}, \dots, Q_k = Q_k \cup \{Q_k^i Q_k^j\}$, where Q_k^i is the i th element of Q_k . Define the moment matrix of order l , Γ^k , by $\Gamma_{ij} = \langle \psi | Q_i^{\dagger} Q_j | \psi \rangle$. For any state and measurements $\{|\psi\rangle, A_x, B_y\}$, the matrix Γ^l is Hermitian positive semidefinite and satisfies some linear constraints given by the orthogonality conditions of the measurement operators [34]. Thus, we

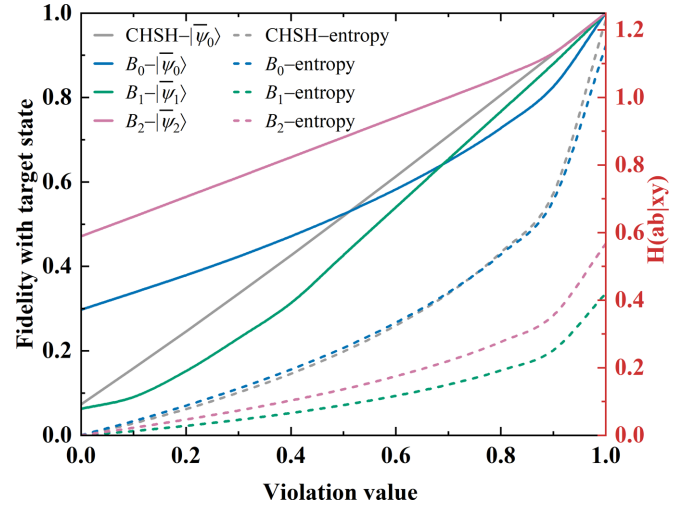


FIG. 4. The lower bounds of fidelity with the target state (left vertical axis) and randomness entropy (right vertical axis) with respect to the observation of Bell inequality. We denote $B_{[\alpha_i, \beta_i]}$ as B_i for $i = 0, 1, 2$. The observed violation is transformed $V_i = \frac{\text{observation} - C_{[\alpha_i, \beta_i]}}{\eta_{[\alpha_i, \beta_i]} - C_{[\alpha_i, \beta_i]}}$. The fidelity with Bell state $|\bar{\psi}_0\rangle$ using the standard CHSH and biased forms are presented by gray and blue solid lines, respectively. The fidelities with $|\bar{\psi}_1\rangle$ and $|\bar{\psi}_2\rangle$ are represented by green and purple solid lines, respectively. The randomness for each Bell inequality is plotted on the right vertical axis with dashed colored lines.

can tackle the optimization problem by minimizing the corresponding elements of the matrix Γ under linear constraints on $\Gamma \geq 0$ to obtain certified lower bounds to the optimal solution:

$$\begin{aligned} \min \quad & f_i = \langle \bar{\psi}_i | \rho_{\text{swap}} | \bar{\psi}_i \rangle \\ \text{such that} \quad & \Gamma \geq 0, \\ & \mathcal{B}_{[\alpha_i, \beta_i]} = \text{observed violation value } i = 0, 1, 2, \end{aligned} \quad (20)$$

where Γ is a 46×46 moment matrix of the quantum local level one $Q_1 = \{I, Z_A, X_A\} \otimes \{I, Z_B, X_B\}$ and is augmented by necessary terms such as $Z_A X_A, X_A Z_B X_B, Z_A X_A Z_B$, etc., to express the fidelity. Thus, we are able to formulate this problem as a SDP, a type of convex optimization for which efficient numerical solvers exist to find global minima and that also returns the error bounds on the optimal guess.

The robustness analyses are shown in Fig. 4 on the left vertical axis. For the Bell state, the fidelity bound by the standard CHSH is higher than using the biased one when the violations are close to the maximal quantum bounds. This result agrees with the work in Ref. [17] that for μ closer to $\frac{\pi}{4}$, the criterion has a greater capacity for noise tolerance. For partially entangled states, the tilted-CHSH inequality is sensitive to noise for the weakly entangled state, while the generalized tilted-CHSH operator performs better. This may result from the fact that, for $\mu = \arctan(\frac{3}{4})$, the gap between the quantum and classical bounds for the generalized tilted-CHSH operator is larger than the standard one shown in Fig. 3, thus providing better distinguishability between different states.

So far, we have provided a scheme to self-test different entangled states using fixed measurement settings based on

the generalized tilted-CHSH inequality, which is robust with regard to the tolerance of noise. Next, we demonstrate the applications of our results to simplify the implementations of secure quantum information tasks such as quantum key distribution (QKD), quantum random number generation (QRNG), and a quantum private query (QPQ).

IV. APPLICATIONS IN QUANTUM INFORMATION TASKS

Quantum systems with the self-testing property play important roles in quantum information processing. Especially, for protocols which have a high demand for security, self-testing is able to guarantee the security independently of the devices. This is precisely the fact that motivates device-independent (DI) quantum information processing. In last few years, DI technologies have been studied intensively. Among them, QKD, QRNG, and QPQ, as the core and bases of quantum cryptography, have attracted huge attention.

A. Device-independent quantum key distribution and private query

DIQKD allows distant parties to create and share a cryptographic key, whose security relies only on the certification of nonlocal quantum correlations [4]. In the simplest protocol, entangled particles are repeatedly prepared and distributed between two parties, Alice and Bob. Alice holds two measurements A_x for $x \in \{0, 1\}$, Bob has three measurements B_y , $y \in \{0, 1, 2\}$. To ensure the security of the task, Alice and Bob perform the CHSH test by randomly choosing two measurements A_x and B_y , $x, y \in \{0, 1\}$, respectively, to certify the source device independently. The maximal quantum bound $2\sqrt{2}$ implies that the source is the maximum entangled state $|\psi\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$ and measurements are $A_0 = \sigma_z$, $A_1 = \sigma_x$, $B_0 = \frac{\sigma_x + \sigma_z}{\sqrt{2}}$, and $B_1 = \frac{\sigma_x - \sigma_z}{\sqrt{2}}$. Then the measurement A_0 for Alice and the last one, $B_2 = \sigma_z$, for Bob are used to extract a secure key.

Later, motivated by this idea, Yang *et al.* proposed a DIQPQ protocol [35]. In the protocol, Alice and Bob share an entangled state with $\frac{1}{\sqrt{2}}(|0\rangle_A |\phi_0\rangle_B + |1\rangle_A |\phi_1\rangle_B)$, where

$$\begin{aligned} |\phi_0\rangle_B &= \cos \frac{\theta}{2} |0\rangle + \sin \frac{\theta}{2} |1\rangle, \\ |\phi_1\rangle_B &= \cos \frac{\theta}{2} |0\rangle - \sin \frac{\theta}{2} |1\rangle. \end{aligned} \quad (21)$$

Before the process of QPQ [36], Alice and Bob perform a CHSH-like test to certify the source and measurements, which guarantee the measurements for Alice are in the bases $\{|0\rangle, |1\rangle\}$ and $\{|+\rangle, |-\rangle\}$ and Bob's are in basis $\{|\psi_0\rangle, |\psi_0^\perp\rangle\}$ or $\{|\psi_1\rangle, |\psi_1^\perp\rangle\}$. If the outcome for Bob is $|\psi_0^\perp\rangle$ ($|\psi_1^\perp\rangle$), he can conclude that the raw key bit at Alice must be 0 (1). Bob and Alice execute classical postprocessing, so that information from Bob in the key reduces to one bit or more. Alice knows the whole key, whereas Bob generally knows several bits of the key.

According to our work, the measurements for Alice and Bob in the two protocols above can be set as

$$\begin{aligned} A_0 &= \sigma_z \quad B_0 = \cos 2\theta \sigma_z + \sin 2\theta \sigma_x, \\ A_1 &= \sigma_x \quad B_1 = \cos 2\theta \sigma_z - \sin 2\theta \sigma_x, \end{aligned} \quad (22)$$

which are available to self-test the two entangle sources in DIQKD and DIQPQ tasks at the same time. For instance, the parameters in Eq. (4) can be set according to the task, i.e., $\alpha = \frac{1}{\tan 2\theta}$ and $\beta = 0$ for the DIQKD protocol and $\alpha = 1$ and $\beta = \frac{2\cos\theta}{\sqrt{1+\sin^2\theta}}$ for the DIQPQ protocol. In this way, different entangled states not only can be certified as the source in QKD but also can be used to generate a secure key in the QPQ task. This simplifies the measurement resources to achieve different types of quantum information processing.

B. Device-independent quantum random number generation

DIQRNG is able to access randomness by observing the violation of Bell inequalities without any assumptions about the source and measurement device. The randomness of the output pairs conditioned on the input pairs for the entangled pairs can be quantified by the min-entropy [5] $H_\infty(ab|xy) = -\log_2 \max p(ab|xy)$. For a given observed violation V_i of the Bell inequality $\mathcal{B}_{[\alpha_i, \beta_i]}$, where V_i is defined in the caption of Fig. 4, we are able to obtain a lower bound on the min-entropy,

$$H_\infty(ab|xy) \geq V_i, \quad (23)$$

satisfied by all quantum realizations of the Bell scenario. Let $P^*(ab|xy)$ denote the solution to the following optimization problem:

$$\begin{aligned} \text{obj} \quad & P^*(ab|xy) = \max p(ab|xy) \\ \text{such that} \quad & \Gamma \geq 0, \\ & \mathcal{B}_{[\alpha_i, \beta_i]} = \text{observed violation value } i = 0, 1, 2, \end{aligned}$$

where the optimization is carried over all states ρ and all measurement operators, defined over Hilbert spaces of arbitrary dimension. The minimal value of the min-entropy compatible with the Bell violation V and quantum theory is then given by $H_\infty(ab|xy) = -\log_2 \max_{ab} P(ab|xy)$.

Using the same Bell inequalities as in Sec. III and running SDP with the NPA hierarchy, we plot the lower bounds of the entropy in Fig. 4 on the right vertical axis. It is worth pointing out that in a device-independent framework, if the violation is a maximal quantum bound for CHSH $2\sqrt{2}$, the randomness is obtained with 1.2283 bits and the underlying structure is a Bell state with an orthogonal basis [5]. Here we show that if the two observers self-test the state with the biased basis in Eq. (3), the lower bound of randomness is 1.1519 bits, which is slightly lower than in the CHSH scenario. However, we point out that with this biased basis, the random numbers can also be certified by partially entangled states. As for the two partially entangled target states whose concurrences are $C(|\bar{\psi}_1\rangle) = \frac{3}{4}$ and $C(|\bar{\psi}_2\rangle) = \frac{\sqrt{3}}{2} \approx 0.866$, the secure randomness can be extracted with 0.4195 and 0.5669 bit, respectively. In other words, with these measurement settings, we can extract randomness in both the maximum entangled and partially entangled states.

V. CONCLUSION

Self-testing results are usually known for a set of a quantum state and the corresponding measurement simultaneously. However, different entangled resources are needed for various quantum information tasks with diverse requirements. In this paper we proposed a scheme that self-tests a family of entangled states with different entanglement degrees using the same fixed measurement settings. By providing the SOS decompositions of the generalized tilted-CHSH inequality, we extended the self-testing criteria of general two-qubit states with two binary measurements per party. Previous work based on symmetric biased CHSH [33] and standard tilted-CHSH [14] operators can be regarded as special cases of these criteria. The self-testing criteria obtained in our work are appealing from two aspects. For general two-qubit entangled states, we broaden their self-testing criteria. The self-testing can be carried out with a series of different measurement settings on the Pauli x - z plane by setting different values of α in the generalized tilted-CHSH inequality. More importantly, different entangled states can be self-tested by maximally violating the corresponding Bell inequalities with the same fixed measurement settings. This can simplify the measurement instruments of self-testing in an experimental realization. Moreover, our scheme demonstrates satisfactory robustness in relation to tolerance of noise.

Furthermore, our scheme can provide secure certification for different device-independent quantum information processing tasks with fewer resources. This work is instrumental for improving the practical performance of self-testing. In addition, this work is of intrinsic interest for foundational studies on Bell nonlocality and quantum certification. In the future, it would be interesting to study more Bell nonlocalities with the self-testing property and to find more criteria with the same measurements for different states.

ACKNOWLEDGMENTS

This work was supported by the National Natural Science Foundation of China (Grants No. 62101600, No. 51890861, No. 11974178, and No. 62201252), Science Foundation of China University of Petroleum, Beijing (Grant No. 2462021YJRC008), the State Key Laboratory of Cryptology (Grant No. MMKFKT202109), the National Key Research and Development Program of China (Grant No. 2019YFA0705000), and the Leading-edge technology Program of the Jiangsu Natural Science Foundation (Grant No. BK20192001).

APPENDIX: THE SOS DECOMPOSITION FOR THE GENERALIZED TILTED-CHSH INEQUALITY

We provide the method to obtain the SOS decompositions of the generalized tilted-CHSH operator

$$\mathcal{B}_{[\alpha,\beta]} = \beta A_0 + \alpha A_0 B_0 + \alpha A_0 B_1 + A_1 B_0 - A_1 B_1, \quad (A1)$$

where $\alpha \geq 1$, in detail.

The optimal quantum violation of (A1) is proved to be $\eta_{[\alpha,\beta]} = \sqrt{(1 + \alpha^2)(4 + \beta^2)}$ by optimizing over all quantum states and measurements [32]. The bound implies the operator

$\widehat{\mathcal{B}} = \eta_{[\alpha,\beta]} \mathbb{I} - \mathcal{B}_{[\alpha,\beta]}$ is positive semidefinite for all possible quantum states and measurement operators A_x and B_y . This, in turn, can be proven by providing a set of operators $\{P_i\}$ which are polynomial functions of A_x and B_y such that

$$\widehat{\mathcal{B}}_{[\alpha,\beta]} = \sum_i P_i^\dagger P_i \quad (A2)$$

holds for any set of measurement operators satisfying the algebraic properties $A_x^2 = \mathbb{I}$, $B_y^2 = \mathbb{I}$, and $[A_x, B_y] = 0$. The form (A2) is called a SOS decomposition.

Our goal is to find SOS decompositions of generalized tilted-CHSH inequalities as in Eq. (A2) in terms of a set of polynomials $\{P_i\}$. Our technique for SOS decompositions is based on Ref. [14]. For simplicity, the search space is restricted to the span of a canonical basis of nine monomials

$$\mathcal{S}_{1+AB} = \{\mathbb{I}, A_0, A_1\} \otimes \{\mathbb{I}, B_0, B_1\}. \quad (A3)$$

Let $\{R_i\}_i$ denote the different bases of the vector space of polynomial P_i . Therefore, P_i can be expressed by the bases $P_i = \sum_\mu q_i^\mu R_\mu$. Then $\widehat{\mathcal{B}}$ is rewritten as

$$\widehat{\mathcal{B}} = \sum_{\mu\nu} \sum_i R_\mu^\dagger q_i^\mu q_i^\nu R_\nu = \sum_{\mu\nu} R_\mu^\dagger M^{\mu\nu} R_\nu. \quad (A4)$$

The task becomes finding a positive-semidefinite matrix M such that Eq. (A4) holds. By decomposing both sides of the equality $\widehat{\mathcal{B}} = \sum_{\mu\nu} M^{\mu\nu} R_\mu^\dagger R_\nu$ in a basis of the quadratic products of all elements in \mathcal{S}_{1+AB} , we obtain a canonical basis with a size of 25 for these products as

$$\begin{aligned} \mathcal{S}_{1+AB}^2 = & \{\mathbb{I}, A_0, A_1, A_0 A_1, A_1 A_0\} \\ & \otimes \{\mathbb{I}, B_0, B_1, B_0 B_1, B_1 B_0\}. \end{aligned} \quad (A5)$$

We write $R_\mu^\dagger R_\nu = F_{\mu\nu}^i E_i$, where E_i takes over \mathcal{S}_{1+AB}^2 and each F_i is a matrix of coefficients such that $\widehat{\mathcal{B}} = \sum_i F_i E_i$. Then the SOS condition reduces to

$$s^i = \text{Tr}(M^\dagger F_i), \quad i = 1, 2, \dots, 25. \quad (A6)$$

The remaining task is to solve a set of 25 linear equality constraints on M as well as the positive-semidefiniteness constraint $M \geq 0$.

A valid SOS decomposition for $\widehat{\mathcal{B}}_{[\alpha,\beta]}$ must be made up of terms for which $P_i(\cos \theta |00\rangle + \sin \theta |11\rangle)$ vanishes in this maximally violating quantum system. Indeed, writing the most general P in the search space as $r \cdot \mathbf{V}$, where

$$\mathbf{V} = (\mathbb{I}, A_0, A_1, B_0, B_1, A_0 B_0, A_0 B_1, A_1 B_0, A_1 B_1), \quad (A7)$$

and requiring the four components of $P_i |\psi\rangle$ to vanish, Ref. [14] showed that for $\alpha = 1$ the space of candidates P_i is spanned by the following five operators:

$$\begin{aligned} & -Z_A + Z_B, \\ & -\mathbb{I} + Z_A Z_B, \\ & -\mathbb{I} + c Z_B + X_A X_B, \\ & -X_A + s X_B + c X_A Z_B, \\ & -c X_A + s Z_A X_B + X_A Z_B, \end{aligned} \quad (A8)$$

where $c = \cos 2\theta$, $s = \sin 2\theta$, and operators Z and X are defined as

$$\begin{aligned} Z_A &= A_0, Z_B = \frac{B_0 + B_1}{2 \cos \mu}, \\ X_A &= A_1, X_B = \frac{B_0 - B_1}{2 \sin \mu}. \end{aligned} \quad (\text{A9})$$

We express the maximal violation of the generalized tilted-CHSH operator (A1) with α and θ :

$$\eta_{[\alpha, \theta]} = \frac{2(\alpha^2 + 1)}{\sqrt{\alpha^2 + \sin^2 2\theta}}, \quad (\text{A10})$$

which can be achieved only by the state $|\psi\rangle = \cos \theta |00\rangle + \sin \theta |11\rangle$ and the corresponding measurements A_x and B_y for

$x, y \in \{0, 1\}$ defined in (A9), and the parameters satisfy

$$\begin{aligned} \beta &= \frac{2 \cos 2\theta}{\sqrt{\alpha^2 + \sin^2 2\theta}}, \cos \mu = \frac{\alpha}{\sqrt{\alpha^2 + \sin^2 2\theta}}, \\ \sin \mu &= \frac{\sin 2\theta}{\sqrt{\alpha^2 + \sin^2 2\theta}}. \end{aligned} \quad (\text{A11})$$

Now we choose the basis $R_i = \{r_i \cdot \mathbf{V}\}$ for the subspace containing the SOS polynomials for the generalized tilted-CHSH (A1) and label the columns with the operators defining \mathbf{V} , where the r_i vectors are defined as follows:

$$\begin{aligned} r_1 &= \left(\begin{array}{cccccccccc} \mathbb{I} & A_0 & A_1 & B_0 & B_1 & A_0 B_0 & A_0 B_1 & A_1 B_0 & A_1 B_1 \\ 0 & -\frac{2\alpha}{\sqrt{\alpha^2 + s^2}} & 0 & 1 & 1 & 0 & 0 & 0 & 0 \end{array} \right), \\ r_2 &= \left(\begin{array}{cccccccccc} -\frac{2\alpha}{\sqrt{\alpha^2 + s^2}} & 0 & 0 & 0 & 0 & 1 & 1 & 0 & 0 \end{array} \right), \\ r_3 &= \left(\begin{array}{cccccccccc} 0 & 0 & 0 & \frac{c}{\alpha} & \frac{c}{\alpha} & 0 & 0 & 1 & -1 \end{array} \right), \\ r_4 &= \left(\begin{array}{cccccccccc} 0 & 0 & -\frac{2}{\sqrt{\alpha^2 + s^2}} & 1 & -1 & 0 & 0 & \frac{c}{\alpha} & \frac{c}{\alpha} \end{array} \right), \\ r_5 &= \left(\begin{array}{cccccccccc} 0 & 0 & -\frac{2c}{\sqrt{\alpha^2 + s^2}} & 0 & 0 & 1 & -1 & \frac{1}{\alpha} & \frac{1}{\alpha} \end{array} \right). \end{aligned} \quad (\text{A12})$$

These basis operators separate the space into two isotypical subspaces, i.e., subspaces that fall under the same irreducible representation of the cyclic group: $R_{1,2,3}$ are invariant under the symmetry transformation of $\mathcal{B}_{[\alpha, \beta]}$, while $R_{4,5}$ change sign.

The block structure of symmetric SOS matrices is therefore $3 \oplus 2$, where the first block corresponds to the trivial representation and the second corresponds to the parity representation where the group generator is represented by -1 .

For convenience, we define three classes of CHSH operators:

$$\begin{aligned} S_0 &= A_0(B_0 - B_1) + \frac{1}{\alpha} A_1(B_0 + B_1), \\ S_1 &= \frac{1}{\alpha} A_0(B_0 + B_1) - A_1(B_0 - B_1), \\ S_2 &= A_0(B_0 - B_1) - \alpha A_1(B_0 + B_1). \end{aligned} \quad (\text{A13})$$

Then we can provide two different SOS decompositions of the generalized CHSH inequalities $\mathcal{B}_{[\alpha, \beta]}$ in Eq. (A1). The first one can be given as

$$\begin{aligned} \widehat{\mathcal{B}}_{[\alpha, \beta]} &= \frac{1}{\Delta + 2\eta_{[\alpha, \beta]}} \left\{ (\alpha^2 - 1) \left[\left(\frac{\cos 2\theta}{\alpha} R_1 - R_3 \right)^2 + R_1^2 \right] + \left(\frac{\cos 2\theta}{\alpha} R_1 - \alpha R_2 - R_3 \right)^2 + \alpha^2 R_5^2 \right\} \\ &= \frac{1}{\Delta + 2\eta_{[\alpha, \beta]}} \left((\alpha^2 - 1) \left[\left[-\beta A_0 + \frac{\eta_{[\alpha, \beta]}}{\alpha^2 + 1} - A_1(B_0 - B_1) \right]^2 \right. \right. \\ &\quad \left. \left. + \left(-\frac{\eta_{[\alpha, \beta]}\alpha}{\alpha^2 + 1} A_0 + B_0 + B_1 \right)^2 \right] + [\eta_{[\alpha, \beta]} - \beta A_0 - \alpha A_0(B_0 + B_1) - A_1(B_0 - B_1)]^2 + \alpha^2 R_5^2 \right) \\ &= \frac{1}{\Delta + 2\eta_{[\alpha, \beta]}} \left((\alpha^2 - 1) \left[\left[-\beta A_0 + \frac{\eta_{[\alpha, \beta]}}{\alpha^2 + 1} - A_1(B_0 - B_1) \right]^2 + \left(-\frac{\alpha \eta_{[\alpha, \beta]}}{\alpha^2 + 1} A_0 + B_0 + B_1 \right)^2 \right] \right. \\ &\quad \left. + \widehat{\mathcal{B}}_{[\alpha, \beta]}^2 + \alpha^2 \left\{ \beta A_1 - \left[A_0(B_0 - B_1) + \frac{1}{\alpha} A_1(B_0 + B_1) \right] \right\}^2 \right) \\ &= \frac{1}{\Delta + 2\eta_{[\alpha, \beta]}} \left((\alpha^2 - 1) \left[\left[-\beta A_0 + \frac{\eta_{[\alpha, \beta]}}{\alpha^2 + 1} - A_1(B_0 - B_1) \right]^2 + \left(-\frac{\eta_{[\alpha, \beta]}\alpha}{\alpha^2 + 1} A_0 + B_0 + B_1 \right)^2 \right] \right. \\ &\quad \left. + \widehat{\mathcal{B}}_{[\alpha, \beta]}^2 + \alpha^2 (\beta A_1 - S_0)^2 \right), \end{aligned} \quad (\text{A14})$$

where $\Delta = 2(\alpha^2 - 1)\sqrt{\frac{\beta^2+4}{\alpha^2+1}}$. The second decomposition is given as

$$\begin{aligned} \widehat{\mathcal{B}}_{[\alpha,\beta]} &= \frac{\alpha^2}{\Delta + 2\eta_{[\alpha,\beta]}} \left\{ \frac{\alpha^2 - 1}{\alpha^2} \left[\left(\frac{\cos 2\theta}{\alpha} R_1 - R_3 \right)^2 + R_1^2 \right] + \left[\frac{2(\alpha^2 + 1)}{\alpha\eta_{[\alpha,\beta]}} R_1 - \frac{\beta}{2} \left(\frac{1}{\alpha} R_2 - R_3 \right) \right]^2 + \frac{1}{\alpha^2} \left(\frac{\eta_{[\alpha,\beta]}}{2} R_4 - \frac{\beta}{2} R_5 \right)^2 \right\} \\ &= \frac{\alpha^2}{\Delta + 2\eta_{[\alpha,\beta]}} \left(\frac{\alpha^2 - 1}{\alpha^2} \left\{ \left[-\beta A_0 + \frac{\eta_{[\alpha,\beta]}}{\alpha^2 + 1} - A_1(B_0 - B_1) \right]^2 + \left(-\frac{\alpha\eta_{[\alpha,\beta]}}{\alpha^2 + 1} A_0 + B_0 + B_1 \right)^2 \right\} \right. \\ &\quad + \left. \left\{ 2A_0 - \frac{\eta_{[\alpha,\beta]}}{2\alpha} (B_0 + B_1) + \frac{\beta}{2} \left[\frac{1}{\alpha} A_0(B_0 + B_1) - A_1(B_0 - B_1) \right] \right\}^2 \right. \\ &\quad + \left. \frac{1}{\alpha^2} \left\{ 2A_1 - \frac{\eta_{[\alpha,\beta]}}{2} (B_0 - B_1) + \frac{\beta}{2} [A_0(B_0 - B_1) - \alpha A_1(B_0 + B_1)] \right\}^2 \right) \\ &= \frac{\alpha^2}{\Delta + 2\eta_{[\alpha,\beta]}} \left(\frac{\alpha^2 - 1}{\alpha^2} \left\{ \left(-\frac{\eta_{[\alpha,\beta]}\alpha}{\alpha^2 + 1} A_0 + B_0 + B_1 \right)^2 + \left[-\beta A_0 + \frac{\eta_{[\alpha,\beta]}}{\alpha^2 + 1} - A_1(B_0 - B_1) \right]^2 \right\} \right. \\ &\quad + \left. \left[2A_0 - \frac{\eta_{[\alpha,\beta]}}{2\alpha} (B_0 + B_1) + \frac{\beta}{2} S_1 \right]^2 + \frac{1}{\alpha^2} \left[2A_1 - \frac{\eta_{[\alpha,\beta]}}{2} (B_0 - B_1) + \frac{\beta}{2} S_2 \right]^2 \right), \end{aligned} \tag{A15}$$

where Δ is defined the same as in (A14).

Hence, we complete the SOS decompositions for $\widehat{\mathcal{B}}_{[\alpha,\beta]}$ such that $\widehat{\mathcal{B}}_{[\alpha,\beta]} = \sum_i P_i^\dagger P_i$ and P_i are the polynomial functions of A_x and B_y . The existence of SOS decompositions (A14) and (A15) implies that any state $|\psi\rangle$ and operators A_x and B_y achieving the maximal quantum bound $\eta_{[\alpha,\beta]}$ will result in $P_i|\psi\rangle = 0$. In particular, we are interested in the following four terms:

$$P1|\psi\rangle = \widehat{\mathcal{B}}_{[\alpha,\beta]}|\psi\rangle, \tag{A16a}$$

$$P2|\psi\rangle = (\beta A_1 - S_0)|\psi\rangle, \tag{A16b}$$

$$P3|\psi\rangle = \left[2A_0 - \frac{\eta_{[\alpha,\beta]}}{2\alpha} (B_0 + B_1) + \frac{\beta}{2} S_1 \right] |\psi\rangle, \tag{A16c}$$

$$P4|\psi\rangle = \left[2A_1 - \frac{\eta_{[\alpha,\beta]}}{2} (B_0 - B_1) + \frac{\beta}{2} S_2 \right] |\psi\rangle, \tag{A16d}$$

which can be linearly combined to form the operators

$$(Z_A - Z_B)|\psi\rangle = 0, \tag{A17a}$$

$$[\sin\theta X_A(\mathbb{I} + Z_B) - \cos\theta X_B(\mathbb{I} - Z_A)]|\psi\rangle = 0 \tag{A17b}$$

in the case of yielding the maximal quantum bound. The algebraic relations (A17a) and (A17b) established by the SOS decompositions (A14) and (A15) are necessarily satisfied by any quantum state and observables achieving the maximal quantum bound. Moreover, they are important for the self-testing of partially entangled states $|\psi\rangle = \cos\theta|00\rangle + \sin\theta|11\rangle$ using the isometry circuit.

[1] J. F. Clauser, M. A. Horne, A. Shimony, and R. A. Holt, Proposed Experiment to Test Local Hidden-Variable Theories, *Phys. Rev. Lett.* **23**, 880 (1969).
 [2] N. Brunner, D. Cavalcanti, S. Pironio, V. Scarani, and S. Wehner, Bell nonlocality, *Rev. Mod. Phys.* **86**, 419 (2014).
 [3] A. Acín, N. Brunner, N. Gisin, S. Massar, S. Pironio, and V. Scarani, Device-Independent Security of Quantum Cryptography against Collective Attacks, *Phys. Rev. Lett.* **98**, 230501 (2007).
 [4] U. Vazirani, and T. Vidick, Fully Device-Independent Quantum Key Distribution, *Phys. Rev. Lett.* **113**, 140501 (2014).
 [5] 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, and C. Monroe, Random numbers certified by Bell's theorem, *Nature (London)* **464**, 1021 (2010).
 [6] Y. Liu *et al.*, Device-independent quantum random-number generation, *Nature (London)* **562**, 548 (2018).
 [7] T. Moroder, J.-D. Bancal, Y.-C. Liang, M. Hofmann, and O. Gühne, Device-Independent Entanglement Quantification

and Related Applications, *Phys. Rev. Lett.* **111**, 030501 (2013).
 [8] J. Bowles, I. Šupić, D. Cavalcanti, and A. Acín, Device-Independent Entanglement Certification of All Entangled States, *Phys. Rev. Lett.* **121**, 180503 (2018).
 [9] D. Mayers, and A. Yao, Self testing quantum apparatus, *Quantum Inf. Comput.* **4**, 4 (2004).
 [10] V. Scarani, The device-independent outlook on quantum physics, *Acta Phys. Slovaca* **62**, 4 (2013).
 [11] I. Šupić and J. Bowles, Self-testing of quantum systems: A review, *Quantum* **4**, 337 (2020).
 [12] J. Barrett, and N. Gisin, How Much Measurement Independence Is Needed to Demonstrate Nonlocality? *Phys. Rev. Lett.* **106**, 100406 (2011).
 [13] S. Popescu and D. Rohrlich, Which states violate Bell's inequality maximally? *Phys. Lett. A* **169**, 411 (1992).
 [14] C. Bamps and S. Pironio, Sum-of-squares decompositions for a family of Clauser-Horne-Shimony-Holt-like inequalities and their application to self-testing, *Phys. Rev. A* **91**, 052111 (2015).

- [15] A. Coladangelo, K. T. Goh, and V. Scarani, All pure bipartite entangled states can be self-tested, *Nat. Commun.* **8**, 15485 (2017).
- [16] K. F. Pál, T. Vértesi, and M. Navascués, Device-independent tomography of multipartite quantum states, *Phys. Rev. A* **90**, 042340 (2014).
- [17] Y. Wang, X. Wu, and V. Scarani, All the self-testings of the singlet for two binary measurements, *New J. Phys.* **18**, 025021 (2016).
- [18] M. McKague, Self-testing graph states, [arXiv:1010.1989](https://arxiv.org/abs/1010.1989).
- [19] X. Wu, C. Yu, T. H. Yang, H. N. Le, and V. Scarani, Robust self-testing of the three-qubit W state, *Phys. Rev. A* **90**, 042339 (2014).
- [20] X. Li, Y. Cai, Y. Han, Q. Wen, and V. Scarani, Self-testing using only marginal information, *Phys. Rev. A* **98**, 052331 (2018).
- [21] X. Li, Y. Wang, Y. Han, S. Qin, F. Gao, and Q. Wen, Self-testing of symmetric three-qubit states, *IEEE J. Sel. Areas Commun.* **38**, 589 (2020).
- [22] J. Kaniewski, Analytic and Nearly Optimal Self-Testing Bounds for the Clauser-Horne-Shimony-Holt and Mermin Inequalities, *Phys. Rev. Lett.* **117**, 070402 (2016).
- [23] X. Li, Y. Wang, Y. Han, S. Qin, and F. Gao, Analytic robustness bound for self-testing of the singlet with two binary measurements, *J. Opt. Soc. Am. B* **36**, 457 (2019).
- [24] T. Coopmans, J. Kaniewski, and C. Schaffner, Robust self-testing of two-qubit states, *Phys. Rev. A* **99**, 052123 (2019).
- [25] J. D. Bancal, M. Navascués, V. Scarani, T. Vértesi, and T. H. Yang, Physical characterization of quantum devices from non-local correlations, *Phys. Rev. A* **91**, 022115 (2015).
- [26] X. Wu, J. D. Bancal, M. McKague, and V. Scarani, Device independent parallel self-testing of two singlets, *Phys. Rev. A* **93**, 062121 (2016).
- [27] M. McKague, T. H. Yang, and V. Scarani, Robust self-testing of the singlet, *J. Phys. A* **45**, 455304 (2012).
- [28] A. Coladangelo, Parallel self-testing of (tilted) EPR pairs via copies of (tilted) CHSH and the magic square game, *Quantum Inf. Comput.* **17**, 9 (2017).
- [29] M. Coudron and A. Natarajan, The parallel-repeated magic square game is rigid, [arXiv:1609.06306](https://arxiv.org/abs/1609.06306).
- [30] M. McKague, Self-testing in parallel with CHSH, *New J. Phys.* **18**, 045013 (2016).
- [31] S. Wagner, J.-D. Bancal, N. Sangouard, and P. Sekatski, Device-independent characterization of quantum instruments, *Quantum* **4**, 243 (2020).
- [32] A. Acín, S. Massar, and S. Pironio, Randomness versus Nonlocality and Entanglement, *Phys. Rev. Lett.* **108**, 100402 (2012).
- [33] T. Lawson, N. Linden, and S. Popescu, Biased nonlocal quantum games, [arXiv:1011.6245](https://arxiv.org/abs/1011.6245).
- [34] M. Navascués, S. Pironio, and A. Acín, A convergent hierarchy of semidefinite programs characterizing the set of quantum correlations, *New J. Phys.* **10**, 073013 (2008).
- [35] A. Maitra, G. Paul, and S. Roy, Device-independent quantum private query, *Phys. Rev. A* **95**, 042344 (2017).
- [36] Y.-G. Yang, S.-J. Sun, P. Xu, and J. Tian, Flexible protocol for quantum private query based on B92 protocol, *Quantum Inf. Process.* **13**, 805 (2014).