

Experimental Robust Self-Testing of the State Generated by a Quantum Network

Iris Agresti,¹ Beatrice Polacchi¹,¹ Davide Poderini,¹ Emanuele Polino,¹ Alessia Suprano,¹ Ivan Šupić,² Joseph Bowles^{1,3},³ Gonzalo Carvacho,¹ Daniel Cavalcanti,^{3,*} and Fabio Sciarrino^{1,†}

¹*Dipartimento di Fisica, Sapienza Università di Roma, Piazzale Aldo Moro 5, 00185 Rome, Italy*

²*Département de Physique Appliquée, Université de Genève, 1211 Geneva, Switzerland*

³*ICFO—Institut de Ciències Fòniques, The Barcelona Institute of Science and Technology, 08860 Castelldefels, Barcelona, Spain*



(Received 21 October 2020; revised 25 March 2021; accepted 3 May 2021; published 24 June 2021)

Self-testing is a method of quantum state and measurement estimation that does not rely on assumptions about the inner working of the devices used. Its experimental realization has been limited to sources producing single quantum states so far. In this work, we experimentally implement two significant building blocks of a quantum network involving two independent sources: namely, a parallel configuration, in which two parties share two copies of a state, and a tripartite configuration, where a central node shares two independent states with peripheral nodes. Then, by extending previous self-testing techniques, we provide device-independent lower bounds on the fidelity between the generated states and an ideal target made by the tensor product of two maximally entangled two-qubit states. Given its scalability and versatility, this technique can find application in the certification of larger networks of different topologies for quantum communication and cryptography tasks and randomness generation protocols.

DOI: [10.1103/PRXQuantum.2.020346](https://doi.org/10.1103/PRXQuantum.2.020346)

I. INTRODUCTION

In the last few years, a large number of quantum resource-based protocols have been designed, with a wide range of applications. However, it is crucial, and far from trivial, to discriminate the devices that work correctly from those that do not. Indeed, two difficulties can emerge: on one hand, the task required by the user may be hard to verify, a notorious example being the boson sampling problem [1–5], and, on the other, the devices may be affected by noise and imperfections that are unknown to the user. The latter case is especially relevant for tasks aimed at being secure against possible adversaries, who could exploit such defects to obtain secret information or sabotage the operation of the devices. For instance, this is the case of private randomness generation or amplification and quantum key distribution protocols [6–21]. Hence, the ability to certify that the device is operating properly, and possibly without relying on knowledge of its internal working, is crucial for a wider application of quantum

technologies. The approach where conclusions about the correctness operation of the device are drawn only from input-output statistics, is known as the device-independent (DI) approach [22] and typically relies on the quantum violation of Bell-like inequalities [23].

A key protocol in the DI scenario is that of self-testing [24]. There, a multipartite quantum state is subjected to a number of local measurements, a procedure called a “Bell test,” and the resulting statistics alone are enough to certify the specific form of the state and measurements. For instance, the maximum violation value of $2\sqrt{2}$ in a Clauser-Horne-Shimony-Holt (CHSH) Bell test [25] certifies that the state is equivalent to a two-qubit maximally entangled state. In recent years, several self-testing protocols have been proposed to certify different states and measurements [26–41]. In this work, we present experimental demonstrations of self-testing for two types of quantum network, each featuring two independent sources: (a) a network in which the sources are placed in a parallel configuration between two parties, see Fig. 1(a) and (b) a network featuring three parties, where a central party shares a source with two peripheral parties, see Fig. 1(b). The design of our experimental setup follows the bipartite self-testing strategies recently proposed in Ref. [42], which we further adapt to the multipartite network (b). To experimentally implement the network structures, we use a flexible and versatile platform, introduced in Ref. [43], which allows one to easily change the quantum network

*daniel.cavalcanti@icfo.eu

†fabio.sciarrino@uniroma1.it

Published by the American Physical Society under the terms of the Creative Commons Attribution 4.0 International license. Further distribution of this work must maintain attribution to the author(s) and the published article’s title, journal citation, and DOI.

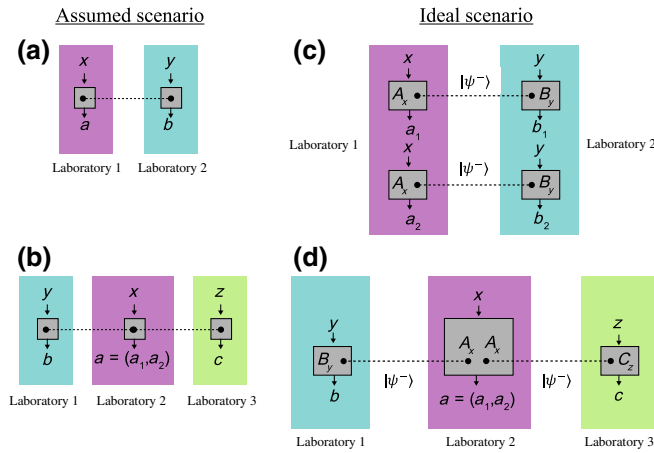


FIG. 1. Self-testing scenarios. The self-testing procedure consists in performing an experiment and analyzing the data produced without assuming a particular implementation [as in (a),(b)]; that is, by considering a black-box scenario in which we have access to only the conditional probability distributions of measurement results conditioned to measurement choices. Nothing is assumed regarding the shared quantum state and measurements in the two scenarios: (a) a scenario featuring two parties, whose outputs are labeled by a and b and whose inputs are indicated by x and y ; (b) a scenario involving three parties, whose outputs are a , b , and c and whose inputs are x , y , and z . Self-testing techniques are used to obtain the minimum fidelity between the real states produced in the experiment and the ideal situation shown in (c),(d), where the sources produce perfect maximally entangled two-qubit states (e.g., $|\psi^-\rangle$) and each party applies the local Pauli measurements to each qubit, corresponding to a maximal violation of the CHSH inequality; for example, $A_0 = \sigma_z, A_1 = \sigma_x, B_0 = C_0 = -(\sigma_x + \sigma_z)/\sqrt{2}$, and $B_1 = C_1 = (\sigma_x - \sigma_z)/\sqrt{2}$. Here we perform self-testing analysis of the state produced in two geometries: (c) a bipartite situation and (d) a tripartite scenario in which a central party shares maximally entangled states with two peripheral parties. In both cases, we aim at certifying the presence of two copies of a maximally entangled state.

topology. Precise lower bounds on the self-testing fidelity with the desired states are obtained from the experimental statistics via the SWAP method [31,41], a numerical tool based on semidefinite programming. The main novelty of our self-testing method, with respect to previous results, lies in its robustness to noise, which allows its application to real experimental data and not only to ideal statistics. Indeed, we present a strategy to tailor the adopted numerical optimization problem to the specific observed statistics and show that, under realistic experimental conditions, we can obtain nontrivial DI lower bounds on the fidelity between the actual state and ideal states. Moreover, we also indicate how to combine such a protocol with Hoeffding inequality and the Azuma-Hoeffding inequality [44–47] to device-independently quantify the confidence level of our

protocols’ results. The present techniques can, in principle, be extended to an arbitrary number of nodes and to an arbitrary target state, which makes them a promising tool for the certification of larger networks and in the implementation of quantum communication and cryptography tasks.

II. SELF-TESTING OF QUANTUM NETWORKS

In the DI scenario, the measurement devices and sources are treated as black boxes, exchanging only classical communication with external users. Suppose the users (labeled as A, B, C, \dots) share some state $\rho_{ABC\dots}$ that is unknown to them, and that they can prepare and measure the state in an independent identically distributed (IID) manner. After the experiment has been repeated many times, the users can estimate the probabilities $p(a, b, c, \dots | x, y, z, \dots)$ of obtaining measurement outcomes a, b, c, \dots if measurements x, y, z, \dots are performed. According to quantum mechanics, such probabilities are given, through the Born rule, as

$$p(a, b, c, \dots | x, y, z, \dots) = \text{Tr}(\rho_{ABC\dots} A_a^x \otimes B_b^y \otimes C_c^z \otimes \dots), \quad (1)$$

where $A_a^x, B_b^y, C_c^z, \dots$ denote the local measurement operators. We say that the probabilities $p(a, b, c, \dots | x, y, z, \dots)$ self-test the target state $|\psi'\rangle_{ABC\dots}$ if the observation of $p(a, b, c, \dots | x, y, z, \dots)$ necessarily implies the existence of a local quantum channel $\Omega[\cdot] = \Omega_A[\cdot] \otimes \Omega_B[\cdot] \otimes \Omega_C[\cdot] \dots$ such that

$$\Omega[\rho_{ABC\dots}] = |\psi'\rangle\langle\psi'|_{ABC\dots}. \quad (2)$$

Self-testing therefore certifies that the parties share the state $|\psi'\rangle_{ABC\dots}$, in the sense that there exist local operations the parties could perform to extract the state from ρ . This statement holds for *any* state ρ satisfying the condition in Eq. (1) (for some local measurements) and is thus a DI statement. As an example, it is known that for any bipartite state ρ_{AB} producing correlations resulting in the maximal quantum violation of the CHSH Bell inequality (with value $2\sqrt{2}$), there exists a channel such that $(\Omega_A \otimes \Omega_B)[\rho_{AB}] = |\psi^-\rangle\langle\psi^-|$, with $|\psi^-\rangle = \frac{1}{\sqrt{2}}(|01\rangle - |10\rangle)$ the maximally entangled singlet state.

In realistic scenarios, however, it is impossible to exactly meet the self-testing conditions in Eq. (1), not only due to experimental noise but also because the finite time of the experiment implies that one can only infer the probabilities up to a given confidence interval. For this reason, the self-testing statement has to be robust (i.e., provide information about the underlying state even when the self-testing condition is only approximately met). To do this, we focus on lower bounding the fidelity between the

extracted state and the target state, defined as follows:

$$F(\Omega[\rho_{ABC\dots}], |\psi'\rangle\langle\psi'|_{ABC\dots}) = \langle\psi'| \Omega[\rho_{ABC\dots}] |\psi'\rangle, \quad (3)$$

given the experimental statistics. That is, one proves that for any state producing the experimental statistics there exists a local channel Ω such that $F \geq f$ (for some $f \leq 1$), up to a given confidence level. Note $f = 1$ corresponds to the case of perfect self-testing given in Eq. (2). A useful method that we use for calculating such lower bounds is the SWAP method, a numerical tool based on semidefinite programming and the Navascués-Pironio-Acín (NPA) hierarchy [48,49]. In particular, this technique consists in numerically swapping part of the generated state on a dummy register to find a proper expression for the fidelity in Eq. (3) as a function of the correlation terms $p(a, b, c \dots | x, y, z \dots)$. Then, a lower bound on this fidelity can be obtained through a semidefinite-programming (SDP) optimization, over a superset of the quantum correlation set mathematically defined by level l of the NPA hierarchy. To get tighter bounds, further linear constraints can be added to the problem; for example, the observed correlations $p(a, b, c \dots | x, y, z \dots)$. Further details about this method can be found in Appendix A.

In this work, we report on the self-testing of target states that correspond to two independent sources producing maximally entangled singlet states $|\psi^-\rangle$. In detail, we focus on two scenarios, depicted in Fig. 1, which can be seen as two possible building blocks of a more complex quantum network. The first scenario features two parties (A and B) and the target state we self-test corresponds to preparing the two maximally entangled states in parallel, see Fig. 1(c). That is, we self-test the state $|\Psi\rangle_2 = |\psi^-\rangle_{A_1 B_1} \otimes |\psi^-\rangle_{A_2 B_2}$, where A_i and B_j denote local qubit Hilbert spaces of party A and party B , respectively. In the following, we refer to this scenario as *parallel self-testing*. The second structure is constituted by three parties (A , B , and C), and the target state corresponds to preparing the sources in an entanglement swapping network, see Fig. 1(d). This configuration, which is referred to as *three-party self-testing*, although investigated both theoretically and experimentally in the last few years [50–54], was implemented only very recently by use of truly independent sources [43,55] and closing the locality loophole [55]. Our target state in this scenario is therefore $|\Psi\rangle_3 = |\psi^-\rangle_{A_1, B} \otimes |\psi^-\rangle_{A_2, C}$.

Differently from the aforementioned studies, here we not only aim to certify the presence of nonclassical correlations through the violation of a suitable mathematical constraint, but our purpose is also to obtain information about the form of the state generated in the quantum network prototypes considered. Furthermore, we stress that the independence of the two sources is taken into account only to properly choose the target state, which, accordingly, displays a tensor product of two maximally entangled states,

but no assumption on this aspect is required by our protocol, which is fully DI. Therefore, the parties can, in principle, share any multipartite state, but the self-testing statements ensure they have the desired product form. It is also noteworthy that scenario (b) constitutes a particular instance of scenario (a), given that one could retrieve the parallel structure simply by allowing quantum communication between parties B and C . Therefore, the difference between the two cases investigated lies in the causal relationship between nodes B and C , which, in scenario (a) merge into a single party and in scenario (b) constitute separate parties. In mathematical terms, this reflects the requirement that in the three-party case the measurement operators performed by B and C commute.

Our self-testing protocol is inspired by Ref. [42], which presents a method for self-testing tensor products of copies of a state, while keeping the number of inputs constant. Such a method is desirable for self-testing quantum networks, since standard methods feature a number of inputs that grows exponentially with the number of copies, which becomes a relevant practical issue for larger networks. In particular, we consider scenarios in which all parties have two inputs; $x, y = 0, 1$ for scenario (a) and $x, y, z = 0, 1$ for scenario (b). The number of outputs is then given by the local Hilbert space dimension of the target state: in scenario (a) both parties have four outputs, which we write as $a = (a_1, a_2)$ and $b = (b_1, b_2)$, where a_i, b_i take values ± 1 ; in scenario (b) we have $a = (a_1, a_2)$ as before and $b = \pm 1$ and $c = \pm 1$. The measurements are chosen so that in the ideal experiment the marginal distributions provide a maximal quantum violation B of the CHSH Bell inequality. More precisely one has $B(p(a_i, b_i | x, y)) = 2\sqrt{2}$, $i = 1, 2$ for scenario (a) and $B(p(a_1, b | x, y)) = B(p(a_2, c | x, z)) = 2\sqrt{2}$ for scenario (b). Following results in Ref. [42], such distributions are known to self-test the desired target states. The measurement strategy corresponds to performing the standard CHSH measurements in parallel, which we elaborate on in the following section. More details about merging the SWAP method with the techniques from Ref. [42] can be found in Appendix A.

III. EXPERIMENTAL APPARATUS

In the experimental implementation of the two scenarios of interest, we use the versatile photonic platform introduced in Ref. [43]. In detail, our three-party case can be seen as a subsystem of the five-node network implemented in such work, while we slightly change the topology of the network links to implement the parallel self-testing scenario, where both parties send and receive a system. In particular, for this latter case, in Fig. 1(c), we use two separate laboratories equipped with independent quantum state sources (Λ_1 and Λ_2 , respectively, in Fig. 2) and two measurement stations. Each measurement station is composed of a half-wave plate and a polarizing

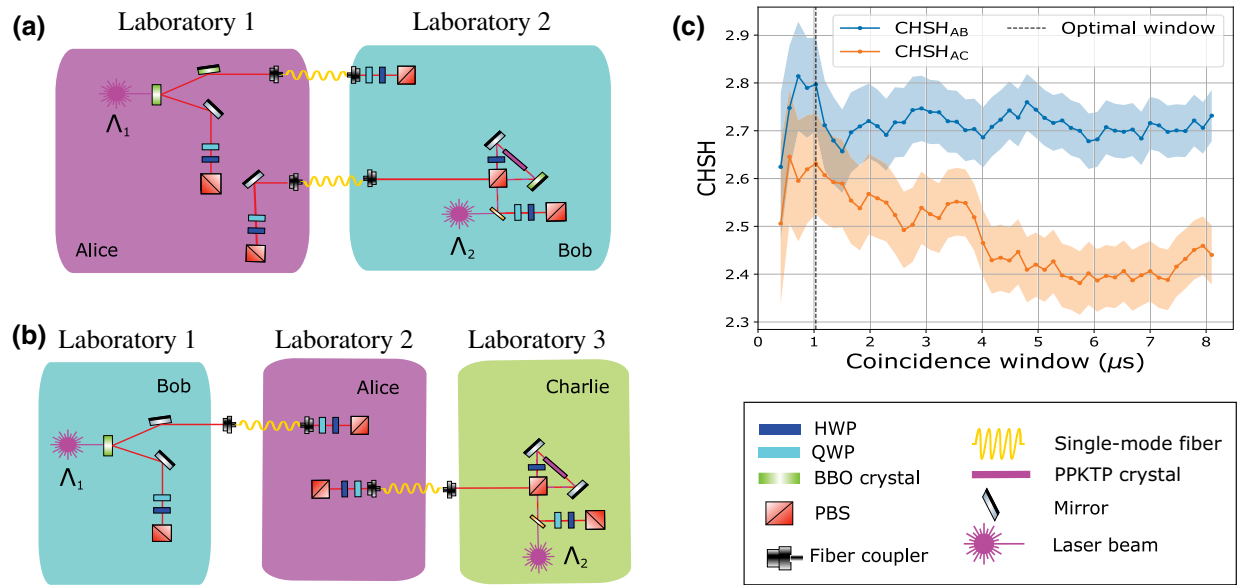


FIG. 2. Experimental apparatus and detection of fourfold coincidences. (a) Parallel self-testing scenario implementation. In this scenario, there are two laboratories, both equipped with a quantum state source and two measurement stations. The measurement stations in laboratory 1 represent Alice, while those in laboratory 2 represent Bob. Both sources generate an entangled pair of photons, and the noise model for the states of Λ_1 and Λ_2 , taking into account the presence of both white noise and colored noise, is as follows: $\rho = v|\psi\rangle\langle\psi| + (1-v)[(\lambda/2)(|01\rangle\langle 01| + |10\rangle\langle 10|) + (1-\lambda)(\mathbb{I}/4)]$, where $|\psi\rangle$ is the singlet state [56]. The noise parameters characterizing our sources are as follows: $v_1 = 0.9716$ and $\lambda_1 = 0.5004$ for Λ_1 , and $v_2 = 0.9852$ and $\lambda_2 = 0.5117$ for Λ_2 (for further details, see Appendix D). Each laboratory sends a subsystem to the other through an approximately-30-m long single-mode fiber, and keeps the other one to measure it. These fiber links reduce the overall rate of the sources by approximately 45%, due to coupling in single-mode fibers and, to a smaller extent, due to the attenuation caused by the fiber itself. Furthermore, polarization rotation occurring within the fiber, although compensated, causes residual noise of 2% or less on the visibility. The overall target state to be shared between the two parties involved in this network is the tensor product of two maximally entangled two-qubit states. (b) Tripartite scenario implementation. In this scenario, there are three laboratories, two (laboratories 1 and 3) equipped with a quantum state source and a measurement station (representing Bob and Charlie, respectively) and one with just two measurement stations, constituting Alice. The source in laboratory 1, Λ_1 , sends one photon to Bob, while Λ_2 sends one to Charlie, and both sources send the other one to Alice through an approximately-30-m-long single-mode fiber. (c) To detect the couples of two-qubit states generated by sources Λ_1 and Λ_2 , we set a coincidence window within which two twofold coincidence events must occur, to be recognized as a fourfold coincidence. The curves indicate the CHSH value of the states generated by the two sources (Λ_1 , blue curve; Λ_2 , orange curve), with the statistical uncertainty obtained considering the Poissonian distribution of the events (one standard deviation) in terms of such a fourfold coincidences window, w_2 . On one hand, w_2 should be as small as possible to approximate simultaneity between the generations of the entangled photon pairs. On the other, however, as w_2 approaches 0, the relative uncertainty on the CHSH values, and analogously on the experimental frequencies, increases. Furthermore, when the number of coincidence events is not sufficient to properly estimate the underlying statistics (i.e., for $w_2 \rightarrow 0$), the two CHSH values drop to zero and they are not relatable. Hence, as an optimal time interval, we choose the smallest one giving the highest weighted average mean of the two CHSH values, which is also characterized by a fair percentage error, to avoid a too small confidence level on the lower bounds of the fidelities (i.e., 1.033 μs). BBO, β -barium borate; HWP, half-wave plate; PBS, polarizing beam splitter; PPKTP, periodically poled potassium titanyl phosphate; QWP, quarter-wave plate.

beam splitter, which allows us to perform polarization projective measurements of the form $\cos(4\theta)\sigma_z + \sin(4\theta)\sigma_x$, where σ_x and σ_z are Pauli operators, by simply rotating the half-wave plate by the angle θ with respect to its optical axis. In the end, all the registered counts are sent to a central time tagger, which recognizes as coincidence events of distant detectors the counts occurring within a given time window. In our notation, the measurement stations in laboratory 1 represent Alice, while those in laboratory 2 represent Bob. The two laboratories are

connected through two approximately-30-m-long single-mode fibers, as shown in Fig. 2(a). The source in laboratory 1 uses a spontaneous parametric down-conversion (SPDC) of type II to generate a pair of polarization-entangled photons of wavelength $\lambda = 785$ nm through a β -barium borate crystal, which is pumped in a pulsed manner by a $\lambda = 392.5$ nm UV laser beam. In laboratory 2, we have a periodically poled potassium titanyl phosphate crystal pumped in a continuous-wave manner, which generates polarization-entangled photon pairs

at $\lambda = 808$ nm. Both sources generate a two-qubit maximally entangled state; for example, the singlet state $|\psi^-\rangle$, where the computational basis ($|0\rangle$ and $|1\rangle$) is encoded in the horizontal and vertical photon polarization states ($|H\rangle$ and $|V\rangle$), and hence $|\psi^-\rangle = (|HV\rangle - |VH\rangle)/\sqrt{2}$. At this point, both laboratories send a photon to the other one and use their measurement stations to perform projective measurements on the photon they kept and on the one they received. In detail, Alice's and Bob's operators will be those maximizing the CHSH inequality violation; that is, up to unitary transformations, $A_0 = A_0^1 \otimes A_0^2 = \sigma_z \otimes \sigma_z$ and $A_1 = A_1^1 \otimes A_1^2 = \sigma_x \otimes \sigma_x$ and $B_0 = B_0^1 \otimes B_0^2 = (\sigma_x + \sigma_z)/\sqrt{2} \otimes (\sigma_x + \sigma_z)/\sqrt{2}$, and $B_1 = B_1^1 \otimes B_1^2 = (\sigma_x - \sigma_z)/\sqrt{2} \otimes (\sigma_x - \sigma_z)/\sqrt{2}$, with superscripts indicating the source generating the subsystem.

To detect coincidence events between distant detectors, we design a software to coordinate the counters located in the different laboratories. In particular, we consider two coincidence time windows: one to detect the twofold coincidences generated by each source (set to 1.05 ns), w_1 , and the other to reveal fourfold coincidences (i.e., simultaneous twofold events occurring for both sources), indicated by w_2 . In other words, if a twofold event is registered for both sources, within w_2 , they are labeled as simultaneous and are considered as a fourfold event. The optimal value of window w_2 represents a trade-off among several requirements. Indeed, on one hand, the entangled pairs generated by the two sources should be as close as possible in time to approximate their simultaneity, even if there is no spacelike separation among the parties. On the other hand, excessively narrowing it implies that fewer coincidence events are taken into account in the analysis, since for both sources only twofold coincidences occurring close in time to another event by the other source are considered. This increases the relative uncertainty on the experimental frequencies, and analogously on the corresponding CHSH values given by the marginal probabilities, as shown in Fig. 2(c). Therefore, in our analysis, we chose the smallest w_2 value giving the highest weighted average mean of the two CHSH values, which is also characterized by a fair percentage error. In this way, we can avoid too small confidence levels on the fidelities estimated by our protocol and insufficient statistics. In particular, we take $w_2 = 1.033 \mu\text{s}$. Because of the detection efficiencies, our implementation uses the fair sampling assumption.

For the tripartite scenario implementation, depicted in Fig. 1(d) we have three laboratories. Laboratories 1 and 3 (the peripheral nodes) are constituted by a quantum state source and one measurement station each, while laboratory 2 (the central node) has two measurement stations, as shown in Fig. 2(b). The source in laboratory 1 sends one photon to Bob's measurement station and the other to Alice's, while the source in laboratory 3 sends

one photon to Alice the other one to Charlie. In this case, analogously to before, the measurement operators are as follows: $A_0 = A_0^1 \otimes A_0^2 = \sigma_z \otimes \sigma_z$ and $A_1 = A_1^1 \otimes A_1^2 = \sigma_x \otimes \sigma_x$; $B_0 = -(\sigma_x + \sigma_z)/\sqrt{2}$ and $B_1 = (\sigma_x - \sigma_z)/\sqrt{2}$; and $C_0 = -(\sigma_x + \sigma_z)/\sqrt{2}$ and $C_1 = (\sigma_x - \sigma_z)/\sqrt{2}$. From an experimental point of view, the tripartite and parallel scenarios differ in how the laboratories involved are defined. In other words, one could pass from the parallel self-testing case, represented in Fig. 2(a), to the three-party one, represented in Fig. 2(b), by considering the two measurement stations belonging to laboratory 2 as referring to separate parties with no causal relations with each other. However, in the actual implementation of the three-party scenario, such a causal requirement is enforced by putting a physical distance between the two measurement stations toward the condition of spacelike separation.

IV. RESULTS

Our main goal is to experimentally obtain lower bounds on the fidelities between the states produced and the reference states on the basis of the statistics observed through the two apparatuses shown in Figs. 2(a) and 2(b). However, we cannot simply apply the SWAP method using the raw data because, due to finite statistics, the experimental frequencies do not correspond to physically allowed correlations (e.g., they violate the no-signaling conditions) and the optimization constraints imposed by the NPA hierarchy would make the problem infeasible. Therefore, to overcome this problem, we proceed in the following way (see Appendix C for more details):

1. We use a regularization method in which we approximate the experimental frequencies f_j by probability distributions belonging to the NPA set \mathcal{Q}_4 [57], where $j = (a, b, x, y)$ or $j = (a, b, c, x, y, z)$ depending on the scenario. The solution of this method provides a no-signaling set of distributions P_j^{reg} that are guaranteed to be close to the set of quantum distributions. See Appendix C for further details.
2. We then run the SWAP SDP using P_j^{reg} as inputs.
3. The solution of this SDP provides a linear functional $d(P) = \sum_j c_j^* P_j$ (through its dual formulation), for which the value gives a lower bound on the self-testing fidelity.
4. We run another SWAP SDP, in which we do not assume the actual value of the distributions, but we impose as a constraint the experimentally obtained value of the dual functional.

Using this method and a Monte Carlo simulation (assuming Poissonian statistics for the experiment) to calculate the uncertainties, we find that $F(\rho_{AB}, |\Psi\rangle_2) = 0.587 \pm 0.053$ for the parallel configuration and $F(\rho_{ABC}, |\Psi\rangle_3) = 0.863 \pm 0.032$ for the tripartite case. In detail, in Fig. 3, we

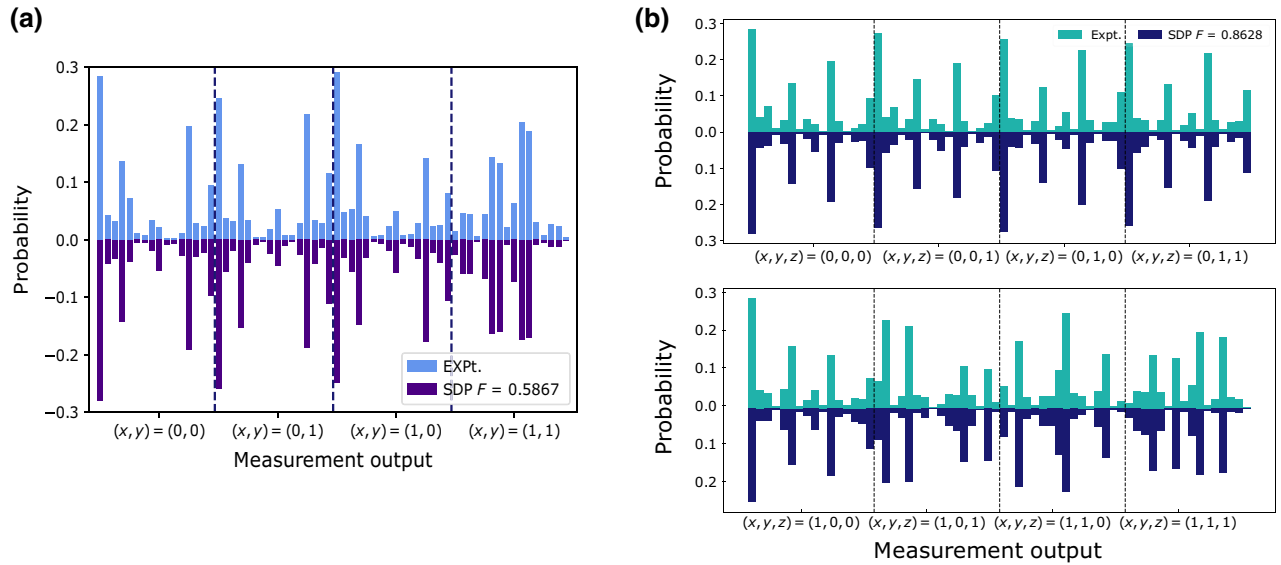


FIG. 3. Certifiable fidelities in parallel self-testing and tripartite scenarios (dual method). In the histograms shown, the upper bars correspond to the experimental frequencies of each measurement output, while the lower ones correspond to the probabilities given as a solution by the SDP optimization, with the experimental dual inequality imposed as a constraint. On the x axis, frequencies/probabilities are ordered in blocks that correspond to the possible choices of operators. (a) Parallel self-testing scenario. Indigo columns represent the experimental probabilities, divided in blocks that correspond to eight different sets of operators x and y , respectively, for Alice and Bob. Every block contains 16 columns, each corresponding to a different set of outcomes: $(a, b) = (0, 0), (0, 1), (0, 2), (0, 3), (1, 0), \dots$, with $a = 0, 1, 2, 3$ and $b = 0, 1, 2, 3$. Purple columns represent the probabilities found by the SDP, with the experimental dual inequality imposed as a constraint, and corresponding to the computed bound for the fidelity $F = 0.5867 \pm 0.053$ (the uncertainty is evaluated through Monte Carlo simulations). This result is obtained by optimization over the NPA set \mathcal{Q}_3 (for further details see Appendix A). (b) Three-party case. Turquoise columns represent the experimental probabilities obtained by gathering all our data sockets, divided in blocks that correspond to eight different sets of operators x , y , and z , respectively, for Alice, Bob, and Charlie. Every block contains 16 columns, each corresponding to a different set of outcomes: $(a, b, c) = (0, 0, 0), (0, 0, 1), (0, 1, 0), (0, 1, 1), (1, 0, 0), \dots$, with $a = 0, 1, 2, 3$ and $b, c = 0, 1$. Blue columns represent the probabilities found by the SDP, with the experimental dual inequality imposed as a constraint, and corresponding to the computed bound for the fidelity $F = 0.8628 \pm 0.032$ (analogously, uncertainty is estimated through Monte Carlo simulations). In this case, the optimization is done over the NPA set \mathcal{Q}_3 plus extramonomials of higher order (for further details see Appendix A). Both reported fidelity lower bounds are compatible, within statistical uncertainty, with those predicted considering the noise parameters that best model the states generated by our sources (for details about the noise model see Appendix D), amounting to $F = 0.631$ for the parallel case and $F = 0.830$ for the three-party case.

show the observable terms of the probability distribution given as solution obtained by the SDP run in the third step, in comparison with the experimental frequencies. Both the reported fidelity lower bounds are compatible with the values predicted considering the noise parameters that best model the states generated by our sources (for details about the noise model, see Appendix D).

A. Device-independent estimation of the uncertainty

The previous method for calculating experimental uncertainties, however, is not fully DI as it assumes a Poissonian distribution for the measurement results. We now move a step forward in removing assumptions and quantify the confidence level on the fidelity bounds by using Hoeffding inequality [44], which holds for IID variables that are in the range $(0, 1)$.

For this second method, we relax the constraint that we obtain a given value for the SDP functional $d(P)$

and impose only $d(P) \leq d^{\text{expt.}} + \tau(\epsilon)$ and $d(P) \geq d^{\text{expt.}} - \tau(\epsilon)$. In this notation, $1 - \epsilon$ constitutes the confidence level for which the observed frequencies f_j are within a range $h_j(\epsilon)$ from the real probability P_j [44]. More specifically, such intervals $h_j(\epsilon)$ amount to $\sqrt{-\ln \epsilon / 2(n_j)}$, where n_j is the number of registered counts for configuration j . At this point, by the central limit theorem [58], the linear combination of frequencies $d^{\text{expt.}}$ is characterized by Gaussian statistics, whose variance amounts to $\sigma^2 = \sum_j c_j^{*2} \text{var } y$. Furthermore, given that $\text{var } y = 1/(2n_j)$, $\tau(\epsilon)$ is chosen as follows (see Appendix E for the full derivation):

$$\tau(\epsilon)^2 = \sum_j c_j^{*2} t(\epsilon)_j^2 = -\ln(\epsilon) \sigma^2. \quad (4)$$

In the end, the confidence level for which the true value of $d(P)$ is within a range of $\tau(\epsilon)$ from $d^{\text{expt.}}$ can be easily recovered from a standard normal table, considering that this interval amounts to $\sqrt{-\ln \epsilon}$ standard deviations. In

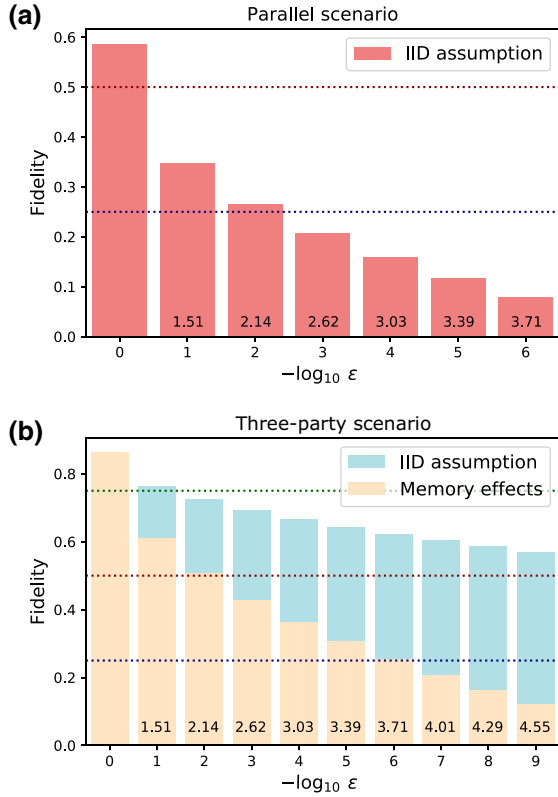


FIG. 4. Certifiable fidelities and device-independent confidence levels. We show the lower bounds on the certifiable fidelities in both of the scenarios studied as a function of the probability ϵ that for all configurations j , $f_j \notin \{P_j - t_j(\epsilon), P_j + t_j(\epsilon)\}$, where f_j are the observed frequencies, P_j are the probabilities characterizing the probability distribution underlying the experiment, and n_j are the registered counts corresponding to configuration j . To obtain such confidence levels, we firstly use Hoeffding inequality [44], which can be applied to IID variables and by which $t_j(\epsilon) = \sqrt{-\ln \epsilon / (2n_j)}$ (see Appendix E for the full derivation). Then we take a step further and consider the possible presence of memory effects, and use the Azuma-Hoeffding inequality [45–47,59], by which $t_j(\epsilon) = \sqrt{-2 \ln \epsilon / (n \times \min q^2)}$, where q is the probability distribution of the inputs and n is the total number of runs (see Appendix F for the full derivation). From those statistical uncertainties on the probabilities, we recover the confidence level on the obtained lower bounds, which amounts to $\sqrt{-\ln \epsilon}$ standard deviations of a Gaussian distribution. In (a), we report the case of parallel self-testing, for which nontrivial fidelity bounds can be found only in an IID setting (i.e., through Hoeffding inequality). In (b) we report the confidence levels of the three-party case, both in an IID setting and taking into account the possible presence of interdependencies among the experimental runs through the Azuma-Hoeffding inequality. The numbers on the bars indicate the number of standard deviations corresponding to the confidence level of such fidelities. Such confidence levels can be found in a standard normal table. The dashed lines indicate the fidelities that certify, respectively, that the state has a Schmidt number higher than or equal to 2 (blue line), 3 (red line), and 4 (green line).

Fig. 4, we show the certifiable fidelities in the two scenarios studied versus ϵ and indicate the corresponding number of standard deviations adding up to $\tau(\epsilon)$ at the bottom of the bars.

Although Hoeffding inequality allows us to drop the assumptions concerning the probability distribution underlying the experimental data, it can be applied only if the variables involved are independent and drawn from the same probability distribution (i.e., it requires the IID assumption). To go a step further and consider possible interdependencies among the experimental runs, we need to use a more sophisticated tool, that is, the Azuma-Hoeffding inequality [44–47,59], which can be applied to sequences of random variables constituting a martingale [45] and whose increment is upper bounded. It can be shown that this is the case of the frequencies registered throughout the sequence of experimental runs (see Appendix F for the full derivation) and, therefore, it is possible to bound the confidence $1 - \epsilon$ that the observed frequencies f_j are within a range $a_j(\epsilon)$ from the probability P_j , accounting for possible memory effects. Analogously to before, $a_j(\epsilon) = \sqrt{-2 \ln \epsilon / (n \times \min q^2)}$, where n is the number of registered counts, and $\text{var } y = 2 / (n \times \min q^2)$, where q is the probability distribution of the inputs. Also in this case, we obtain the lower bound on the fidelity, corresponding to the values of ϵ , imposing as an optimization constraint $d(P) \leq d^{\text{expt.}} + \tau(\epsilon)$ and $d(P) \geq d^{\text{expt.}} - \tau(\epsilon)$, with $\tau(\epsilon)$ being defined in analogy to Eq. (4). Also in this case, the considered interval $\tau(\epsilon)$ amounts to $\sqrt{-\ln \epsilon}$ standard deviations. In Fig. 4(b), the lighter bars indicate the fidelities that can be certified in the three-party case, in terms of ϵ , taking into account possible memory effects through the Azuma-Hoeffding inequality. For the parallel case it is not possible to certify nontrivial fidelity bounds (i.e., higher than 0.25) when the IID assumption is dropped.

From all the reported fidelity lower bounds, we can extrapolate a corresponding lower bound on the Schmidt number of the state [60,61]. In particular, in the cases studied, a fidelity higher than $k/4$ implies a Schmidt number higher than or equal to $k + 1$. In Fig. 4, we indicate the thresholds for a Schmidt number of 2 (blue line), 3 (red line), and 4 (green line).

V. DISCUSSION

In this work, we experimentally implement self-testing protocols in two scenarios representing two basic building blocks for quantum networks. In particular, we study a parallel self-testing scenario, in which two parties share two copies of a bipartite state, and a tripartite one, in which two bipartite states are shared among two peripheral nodes and a central one [50–55]. In these two cases, we are able to obtain lower bounds on the fidelity of

the generated states with the desired target states that demonstrate that both sources indeed produce entangled states, constituted by the tensor product of two two-qubit maximally entangled states. In detail, we find lower bounds on the Schmidt number of the states generated, certifying a Schmidt number of 2 or greater for the first case and a 3 or greater for the second case. It is noteworthy that although in the experimental implementation we use two separate and independent sources, no assumption on this aspect is required in the protocol, nor is one required on the product form of the state shared by the parties. Then we estimate the confidence level of our results in case no interdependencies are present among the experimental runs by use of Hoeffding inequality [44], and finally, for the three-party case, we take a step forward and account also for possible memory effects by using the Azuma-Hoeffding inequality [45–47,59]. We stress that the number of local measurement choices is kept constant independently of the number of quantum state copies that one aims at certifying in the parallel case [42] and is kept constant independently of the number of parties involved in extensions of the three-party case. Furthermore, from an experimental perspective, this method provides an extra significant advantage, represented by the fact that this technique requires only separable measurements. These techniques can, in principle, be extended to more complex topologies and larger networks, as well as to the case of two parties sharing more than two copies of entangled states. However, in this context, the main limitation is represented by the computational cost of semidefinite programming optimizations, which require a space memory that grows exponentially with the size of the system under consideration. This difficulty, however, can be circumvented through several approaches intended to make the calculation less demanding. In detail, from a mathematical point of view, the number of variables involved in the optimization can be reduced by finding symmetries in the objective function (see Appendix B) [62,63]. Otherwise, machine learning techniques can be used to design much faster solvers than the traditional ones, at the price of reducing the accuracy of the optimization [64]. Furthermore, the computation could be made easier by minimal assumptions on the apparatus (i.e., partially trusting specific nodes within a large network). This would allow one to make some assumptions on the form of the generated state, in particular on the presence of some tensor products, which would break the optimization problem into smaller problems that are efficiently solvable. We believe that the present tool will find applications in quantum communication, in particular in cryptographic scenarios such as quantum key distribution and blind quantum computation. In particular, quantifying how close the generated state is to a maximally entangled one can be used to bound the information that an eavesdropper could obtain by correlating a system to the one shared by the parties. Furthermore,

in the three-party scenario, if we consider the case in which the central node performs entangled measurement, correlating the systems shared by the peripheral parties, our protocol could be used to verify the quality of the entanglement swapping [34,35] by self-testing the proper target state. This can prove particularly useful in large networks to allow secure communication between distant parties. Our protocol also provides useful tools for randomness generation in quantum networks or, analogously, using qudit states. Furthermore, the fact that the number of inputs is constant, regardless of the dimension of the system, or analogously of the number of parties involved, can prove an interesting feature in randomness amplification.

VI. METHODS

A. Experimental details

For the experimental setups in Fig. 2, the pump laser beam for source 1, with $\lambda = 392.5$ nm, is produced by a second harmonic generation process from a Ti:sapphire mode-locked laser with a repetition rate of 76 MHz. Photon pairs entangled in the polarization degree of freedom are generated by type-II SPDC in 2-mm-thick β -barium borate crystals. Source 2 uses a continuous-wave diode laser with wavelength $\lambda = 404$ nm, which pumps a 20-mm-thick periodically poled potassium titanyl phosphate crystal inside a Sagnac interferometer to generate photon pairs using a type-II degenerate SPDC process. The photons generated in both the sources are filtered with regard to wavelength and spatial mode by use of narrowband interference filters and single-mode fibers, respectively.

B. Coincidence counting

The photon detection events are collected and timed by a different time-tagger device for each party, located in the corresponding laboratory [43]. For each 1 s of data acquisition, the events are sent to a central server, along with a random clock signal shared between all the time taggers, which is used to synchronize the timestamps of events relative to different devices. To filter out part of the noise, the raw data are first preprocessed by our keeping only double-coincidence events for each photon source, using a narrow coincidence window of 1.05 ns. Then the fourfold coincidence events between the two sources are counted every time one such double coincidence event is recorded for each source in a window of approximately 1.033 μ s.

ACKNOWLEDGMENTS

This work was supported by the John Templeton Foundation via Q-CAUSAL Grant No. 61084, by the Ministero dell’Istruzione, dell’Università e della Ricerca via project PRIN 2017 “Taming complexity via QUantum Strategies a Hybrid Integrated Photonic approach” (QUSHIP) ID

2017SRNBRK, and by the Regione Lazio program “Progetti di Gruppi di ricerca” Legge Regionale no. 13/2008 (SINFONIA project, protocol no. 85-2017-15200) via LazioInnova SpA. I.A. acknowledges La Sapienza University of Rome for a grant for joint research projects for the mobility no. 2289/2018 protocol no. 50074. D.C. acknowledges support from the Government of Spain (Ramon y Cajal fellowship, FIS2020-TRANQI and Severo Ochoa CEX2019-000910-S), Fundació Cellex, Fundació Mir-Puig, Generalitat de Catalunya (CERCA, AGAUR SGR 1381), ERC AdG CERQUITE, and the Swiss National Science Foundation (Starting Grant DIAQ and NCCR QSIT).

APPENDIX A: BOUND ON THE FIDELITY BETWEEN THE STATE GENERATED BY A QUANTUM NETWORK AND A TARGET

In this section, we describe in further detail the self-testing approach we use in this work, which was firstly introduced in Ref. [31], and which can be applied when experimental imperfections do not allow one to reach the maximal quantum violation of a causal constraint, such as the CHSH inequality. In this case, the violation reveals the presence of nonclassical correlations, but it does not single out the system producing it. However, through the techniques introduced in Ref. [31], it is possible to establish a lower bound on the fidelity between the target state and the unknown generated quantum state with use of the NPA hierarchy [48,49].

We consider the simplest quantum scenario, with one source of a bipartite entangled system and two parties (Alice and Bob) performing two-output local measurements on a given subsystem, according to an input $(x, y) \in (0, 1)$. The figure of merit for self-testing of a two-qubit maximally entangled state is the CHSH inequality, but, if the maximal violation extent is not achieved, for instance, due to experimental imperfections, the test is inconclusive.

Hence, we can use the following protocol: First, we use, as a figure of merit, the fidelity with a target state $|\psi_{\text{target}}\rangle$, defined as follows:

$$F(\rho_{AB}, |\psi_{\text{target}}\rangle) = \langle \psi_{\text{target}} | \rho_{AB} | \psi_{\text{target}} \rangle. \quad (\text{A1})$$

However, without making assumptions on the dimension of the generated state, this fidelity is not properly defined; therefore, to have a fully device-independent protocol, we can use the SWAP operator [31]. As a first step, we consider an ancillary register, defined on a Hilbert space of the same dimension as that of the target, and we trust that each system is prepared in the dummy state (i.e., $|0\rangle$). In our case we take $\dim(\mathcal{H}_{\text{target}}) = 2$. Then we define the local operator $S = S_{AA'} \otimes S_{BB'}$, where $S_{AA'} = U_{AA'} V_{AA'}$, where

$$U_{AA'} = \mathbb{I} \otimes |0\rangle_{A'} \langle 0|_{A'} + O_1^A \otimes |1\rangle_{A'} \langle 1|_{A'}, \quad (\text{A2})$$

and

$$V_{AA'} = \frac{\mathbb{I} + O_0^A}{2} \otimes \mathbb{I}^{A'} + \frac{\mathbb{I} - O_0^A}{2} \otimes \sigma_x^{A'}, \quad (\text{A3})$$

and analogously for Bob (B). These operations are unitary if both O_0 and O_1 are unitary and Hermitian. Through this operator, we aim to swap part of the state ρ_{AB} , which is seen as a black box, onto the ancillary register, and ρ_{SWAP} has the following form:

$$\rho_{\text{SWAP}} = \text{Tr}_{AB}[S(\rho_{AB} \otimes |00\rangle \langle 00|)S^\dagger]. \quad (\text{A4})$$

Once we have S explicitly in terms of $O_0^{A,B}$ and $O_1^{A,B}$, the entries of ρ_{SWAP} , from the partial trace in Eq. (A4), are given by linear combinations of correlation terms from the set $c = [c_{\mathbb{I}} = \text{Tr}(\rho_{AB}\mathbb{I}), c_{O_0^A} = \text{Tr}(\rho_{AB}O_0^A), \dots, c_{O_0^A O_1^A O_0^B} = \text{Tr}(\rho_{AB}O_0^A O_1^A O_0^B)]$.

Hence, we can solve the following SDP:

$$\begin{aligned} f &= \min \langle \psi_{\text{target}} | \rho_{\text{SWAP}} | \psi_{\text{target}} \rangle \\ &\text{subject to } c \in \mathcal{Q}_l, \\ &c_{O_0^A O_0^B} + c_{O_0^A O_1^B} + c_{O_1^A O_0^B} - c_{O_1^A O_1^B} = \mathcal{I}_{\text{CHSH}}, \end{aligned} \quad (\text{A5})$$

where \mathcal{Q}_l is a set that includes the set of quantum correlations and that corresponds to the l th level of the NPA hierarchy. In this way, by simply evaluating the CHSH inequality on the generated state, and setting it as a constraint in the problem in Eq. (A5), we can lower-bound the fidelity with the target state. To obtain higher bounds, we can add further constraints; for instance, if the statistics correspond to isotropic black boxes, we could add constraints of the following kind:

$$c_{O_0^A O_0^B} = c_{O_1^A O_0^B} = c_{O_0^A O_1^B} = -c_{O_1^A O_1^B}.$$

A better lower bound can be obtained giving the full statistics to the SDP, solving

$$\begin{aligned} &\text{given } p(a, b|x, y), \\ f &= \min \langle \psi_{\text{target}} | \rho_{\text{SWAP}} | \psi_{\text{target}} \rangle \\ &\text{subject to } c \in \mathcal{Q}_n. \end{aligned} \quad (\text{A6})$$

The bound on the certifiable fidelity, considering a generated state $\rho_{AB} = v|\psi\rangle\langle\psi| + (1-v)\mathbb{I}/2$, is plotted in Fig. 5 as a function of the visibility v (dotted curve). This method is general and can be extended to more parties and different network topologies by choosing the operators O_0 and O_1 according to the target state, although general methods have been introduced for the case in which one simply has some distributions $p(a, b|x, y)$ and wishes to guess what involved state and measurements are [41].

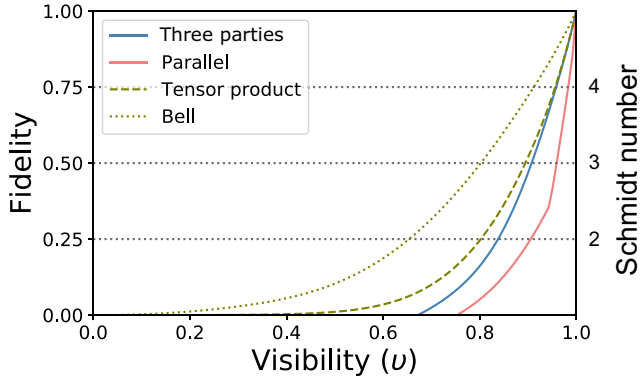


FIG. 5. Certifiable fidelities in the three-party and parallel self-testing scenarios. The minimum fidelity certifiable with our protocol, in the simple CHSH scenario (dotted curve) [31], in the three-party scenario (blue curve) and in the scenario of two parties sharing two singlets; that is, the parallel self-testing scenario (red curve) [42]. The dashed curve represents the fidelity bound that would be obtained through the assumption that the state generated by the network is made of a tensor product of two quantum states, each shared between two parties (i.e., in a semi-device-independent setting). In the Bell case, the target state is a two-qubit maximally entangled state, $|\psi\rangle$, while in the other cases, the target is a product of two two-qubit maximally entangled states $|\psi\rangle_{A_1B} \otimes |\psi\rangle_{A_2C}$ (three-party scenario) and $|\psi\rangle_{A_1B_1} \otimes |\psi\rangle_{A_2B_2}$ (parallel self-testing scenario). The fidelities are plotted in terms of the visibilities of the generated states. In particular, we consider that in the CHSH case, the generated state would have the following form: $\rho_{AB} = \nu|\psi\rangle\langle\psi| + (1-\nu)\mathbb{I}/4$. In the three-party case, $\rho_{ABC} = \rho_{A_1B} \otimes \rho_{A_2C}$, with $\rho_{A_1B} = \rho_{A_2C} = \nu|\psi\rangle\langle\psi| + (1-\nu)\mathbb{I}/4$. In the parallel self-testing case, analogously, $\rho_{AB} = \rho_{A_1B_1} \otimes \rho_{A_2B_2}$, with $\rho_{A_1B_1} = \rho_{A_2B_2} = \nu|\psi\rangle\langle\psi| + (1-\nu)\mathbb{I}/4$. The horizontal dotted gray lines correspond to $k/4$, with $k \in (1, 2, 3)$, and indicate the thresholds over which the fidelity guarantees a Schmidt number (and therefore an entanglement dimension) higher than $k+1$ (i.e., 2, 3, and 4, respectively).

1. The SWAP method for parallel self-testing

In the first part of our experiment, we use this protocol for a scenario involving two independent sources Λ_1 and Λ_2 generating singlets and two parties performing four-output local measurements on the subsystem they get according to an input $(x, y) \in (0, 1)$. Both observers own dummy states with total dimension equal to the one of the target Hilbert spaces, whose dimension ($\dim(\mathcal{H}_{\text{target}})$) amounts to 4, so Alice will have $|00\rangle_{A'_1A'_2}$, similarly to Bob. The fidelity to be bounded takes the form

$$F(\rho_{A_1B_1B_2A_2}, |\psi_{\text{target}}\rangle) = \langle \psi_{\text{target}} | \rho_{A_1B_1B_2A_2} | \psi_{\text{target}} \rangle, \quad (\text{A7})$$

where the target state is $|\psi_{\text{target}}\rangle = |\bar{\psi}\rangle \otimes |\bar{\psi}\rangle$ and $|\bar{\psi}\rangle$ is defined as

$$|\bar{\psi}\rangle = \cos \frac{\pi}{8} |\psi^-\rangle + \sin \frac{\pi}{8} |\psi^+\rangle, \quad (\text{A8})$$

which is maximally entangled and therefore equivalent to $|\psi^-\rangle$ up to local unitaries. The state in Eq. (A8) is chosen for simplicity of notation since this state reaches $\mathcal{I}_B = 2\sqrt{2}$ for the operators

$$O_0^A = \bar{A}_0 = \bar{B}_0 = \sigma_z, \quad O_1^A = \bar{A}_1 = \bar{B}_1 = \sigma_x. \quad (\text{A9})$$

Such operators are then inserted in the expression for the operators U and V defined in Eqs. (A2) and Eq. (A3), where σ_x and σ_z are Pauli operators. Then Alice and Bob perform a swap between the dummy states on their ancillary register and the subsystem they receive, and the ρ_{SWAP} density matrix takes the following form:

$$\rho_{\text{SWAP}} = \text{Tr}_{A_1B_1A_2B_2} [S(\rho_{A_1B_1A_2B_2} \otimes |0000\rangle\langle 0000|)S^\dagger], \quad (\text{A10})$$

where the SWAP operator is defined as $S = S_{A_1A'_1} \otimes S_{B_1B'_1} \otimes S_{A_2A'_2} \otimes S_{B_2B'_2}$. We write the complete expression for the SWAP operator performed by Alice $S_{AA'} = S_{A_1A'_1} \otimes S_{A_2A'_2}$, which is analogous to that performed by Bob:

$$S_{AA'} = S_{A_1A'_1} \otimes S_{A_2A'_2} = U_{A_1A'_1A_2A'_2} V_{A_1A'_1A_2A'_2}. \quad (\text{A11})$$

Since the operators U and V act on subsystems of dimension 2, Alice and Bob can get four possible outcomes from their measurements, and this can be described by defining $A_1^{AB} = \sum_{\{x,y\} \in \{0,1\} \times \{0,1\}} (-1)^{Ax+By} \Pi_{A_1}^{2x+y}$, where $\{A, B\} \in \{0, 1\}$ and $\Pi_{A_x}^a$ is the projector on the eigenspace corresponding to the eigenvalue ($a = 0, 1, 2, 3$) of operator A_x .

With these definitions, the expressions for the operators U and V have the following forms:

$$U_{A_{1,2}A'_{1,2}} = A_1^{00} \otimes |00\rangle\langle 00| + A_1^{01} \otimes |01\rangle\langle 01| \\ + A_1^{10} \otimes |10\rangle\langle 10| + A_1^{11} \otimes |11\rangle\langle 11|, \quad (\text{A12})$$

$$V_{A_{1,2}A'_{1,2}} = \Pi_{A_0}^0 \otimes \mathbb{I} + \Pi_{A_0}^1 \otimes (\mathbb{I} \otimes \sigma_x) \\ + \Pi_{A_0}^2 \otimes (\sigma_x \otimes \mathbb{I}) + \Pi_{A_0}^3 \otimes (\sigma_x \otimes \sigma_x). \quad (\text{A13})$$

After finding the complete expression for ρ_{SWAP} , the next step is to solve the semidefinite program defined in Eq. (A6), where probabilities $p(a_1, b_1|x, y)$ and $p(a_2, b_2|x, y)$ are given as optimization constraints. We need to use the full $p(a, b|x, y)$ statistics as an optimization constraint instead of using the CHSH violations given by the marginal statistics $p(a_1, b_1|x, y)$ and $p(a_2, b_2|x, y)$, not only to obtain higher fidelity bounds but also because the sole extension of the two quantum violations would not be sufficient to guarantee that the two parties are actually sharing the tensor product of two two-qubit quantum states. For instance, the simultaneous maximum violation

of the two CHSH inequalities could occur in a scenario where Alice and Bob share only a single copy of a two-qubit maximally entangled state and get, as the outcome, a single bit repeated (i.e., $a_1 = a_2$ and $b_1 = b_2$). In this situation, the marginal CHSH violations would make our fidelity optimization output trivial fidelity bounds. Concerning the choice of the NPA hierarchy level to be used in the optimization, we need to take into account that all of the correlation terms adding up to the objective function must be contained within the Γ matrix, which is imposed to be positive semidefinite in our optimization. In detail, for level k of the NPA, $\Gamma_{ij} = \text{Tr}(S_j^\dagger S_i \rho)$, where S is the set of all of the operator products featuring k terms (for further details, see Appendix B) [48,49]. Hence, the correlation terms of highest degree that will appear within Γ at level k will be of order $2k$; for example, if $k = 2$ and two parties are involved, $c_{A_x A_x^* B_y B_y^*} = \text{Tr}(\rho_{A_1 B_1 A_2 B_2} A_x A_x^* B_y B_y^*)$. Therefore, for the parallel scenario, it is sufficient to choose \mathcal{Q}_n with $n = 3$ (i.e., the NPA hierarchy [48,49] at level 3) since the correlation term with the highest degree appearing in the fidelity is of order 6; that is, $c_{A_0 A_1 A_0 B_0 B_1 B_0} = \text{Tr}(\rho_{A_1 B_1 A_2 B_2} A_0 A_1 A_0 B_0 B_1 B_0)$. It would also be desirable, in order to get higher fidelity bounds, to reach even higher levels of the hierarchy, but the optimization would become more demanding on a computational level. The bound on the certifiable fidelity, considering a generated state $\rho_{A_1,2 B_1,2} = \rho_{A_1 B_1} \otimes \rho_{A_2 B_2}$, where $\rho_{A_1 B_1} = \rho_{A_2 B_2} = v|\psi\rangle\langle\psi| + (1-v)\mathbb{I}/d$, is plotted in Fig. 5 as a function of the visibility v (blue curve). The bound on the certifiable fidelity can be translated into a bound on the entanglement dimension of the state, and in our case, a fidelity higher than $k/4$ certifies a Schmidt number higher than or equal to $k + 1$ [60,61]. These fidelity thresholds are indicated in Fig. 5 by the horizontal dotted lines.

2. The SWAP method for the three-party scenario

We now consider the case in which the states generated by sources Λ_1 and Λ_2 are sent to three parties (Alice, Bob, and Charlie) that perform local measurements according to an input $(x, y, z) \in (0, 1)$. In detail, Bob and Charlie perform two-output local measurements on their subsystem, generated by sources Λ_1 and Λ_2 , respectively, while Alice performs four-output local measurements on the subsystem generated by both sources. In such a scenario, self-testing can be achieved for a state product of two-qubit maximally entangled states by performing either two separate CHSH tests or a bilocality test [52–54] when observing the maximum violation. However, if we violate the classical bound but we do not observe the maximum violation extent or we want to self-test another state, these tests are not conclusive. Therefore, we wish to bound the fidelity between the generated state and the target state;

that is,

$$F(\rho_{A_1 B_1 A_2 C}, |\psi_{\text{target}}\rangle) = \langle \psi_{\text{target}} | \rho_{A_1 B_1 A_2 C} | \psi_{\text{target}} \rangle, \quad (\text{A14})$$

where the target is a state product of $|\bar{\psi}\rangle$, defined in Eq. (A8). To test the state, the participants each own an ancillary register with a dummy state of dimension 2 for Alice and 1 for Bob and Charlie. As in the previous case, the parties perform the swap, and the resulting ρ_{SWAP} density matrix takes the form

$$\rho_{\text{SWAP}} = \text{Tr}_{A_1 B_1 A_2 C} [S(\rho_{A_1 B_1 A_2 C} \otimes |0000\rangle\langle 0000|) S^\dagger]. \quad (\text{A15})$$

The SWAP operator is defined as $S = S_{A_1 A_1'} \otimes S_{B B'} \otimes S_{A_2 A_2'} \otimes S_{C C'}$, Alice's one having dimension 2 and thus defined as in Eqs. (A12) and (A13), and Bob and Charlie's having dimension 1 and thus defined as in Eqs. (A2) and (A3).

In this case, the choice of the NPA hierarchy level should work analogously to what we saw in the previous paragraph; that is, we should take the highest-order terms within the objective (I), and the minimum level k required for the optimization would be $k = l/2$ (or $k = \lceil l/2 \rceil + 1$ if $l/2$ is not an integer). Therefore, for the three-party case, the correlation terms of highest order display the product of nine operators—that is, $c_{A_0 A_1 A_0 B_0 B_1 B_0 C_0 C_1 C_0} = \text{Tr}(\rho_{A_1 B_1 A_2 B_2} A_0 A_1 A_0 B_0 B_1 B_0 C_0 C_1 C_0)$ —so level 5 would be necessary. Unfortunately, this results in a too demanding optimization problem, so our choice is to stop at level 3, as in the parallel case, and add only the necessary extraterms of higher order. Indeed, not all of the operator products combinations appear in the fidelity expression constituting the objective.

The bound on the certifiable fidelity, considering a generated state $\rho_{A_1,2 B C} = \rho_{A_1 B} \otimes \rho_{A_2 C}$, where $\rho_{A_1 B} = \rho_{A_2 C} = v|\psi\rangle\langle\psi| + (1-v)\mathbb{I}/d$, is plotted in Fig. 5 as a function of the visibility v (red curve). The bound on the certifiable fidelity can be translated into a bound on the entanglement dimension of the state, and in our case, a fidelity higher than $k/4$ certifies a Schmidt number higher than or equal to $k + 1$ [60,61]. These fidelity thresholds are indicated in Fig. 5 by the horizontal dotted lines.

APPENDIX B: NPA HIERARCHY

In this section we discuss the Navascués-Pironio-Acín hierarchy, first introduced in Ref. [48], which is an efficient tool to solve optimization problems over the set \mathcal{Q} of all quantum states and measurements of arbitrary dimension.

We consider the case of two parties, Alice and Bob, sharing a state ρ and performing local measurements that, without loss of generality, we consider to be projectors, indicated with E_α and E_β , respectively, for Alice and Bob. The properties of the projection operation are as follows: (i) $\sum_\mu E_\mu = I$ and (ii) $E_\mu E_\nu = \delta_{\mu,\nu}$ for E_μ and E_ν

belonging to the same measurement, and (iii) $[E_\alpha, E_\beta] = 0$, namely, projectors belonging respectively to Alice and Bob commute with each other. We assume that for a given probability distribution $P_{\alpha\beta}$ there exist a quantum state ρ and a set $\{E_\mu\}$ of projection operations such that

$$P_{\alpha\beta} = \text{Tr}(\rho E_\alpha E_\beta). \quad (\text{B1})$$

The implications from this assumption give necessary conditions that must hold for the set $\{E_\mu\}$.

We consider the matrix Γ defined as follows:

$$\Gamma_{ij} = \sum_j \text{Tr}(S_i^\dagger S_j \rho), \quad (\text{B2})$$

where $\mathcal{S} = \{S_1, S_2, \dots, S_n\}$ is the set made by all the operators of the form $E_\alpha E_\beta E_{\alpha'}$ or $\sum_\alpha c_\alpha E_\alpha$. It can be shown [48] that for Γ , together with Hermiticity, the following linearity conditions hold:

$$\sum_{ij} c_{ij} \Gamma_{ij} = 0 \quad (\text{B3})$$

$$\text{if } \sum_{ij} c_{ij} S_i^\dagger S_j = 0,$$

$$\begin{aligned} \sum_{ij} c_{ij} \Gamma_{ij} &= \sum_{\alpha\beta} d_{\alpha\beta} P_{\alpha\beta} \\ \text{if } \sum_{ij} c_{ij} S_i^\dagger S_j &= \sum_{\alpha\beta} d_{\alpha\beta} E_\alpha E_\beta. \end{aligned} \quad (\text{B4})$$

In addition, Γ is positive semidefinite:

$$\Gamma \succeq 0. \quad (\text{B5})$$

It follows that if for some set \mathcal{S} it is not possible to find a Γ matrix with the aforesaid properties, we must conclude that the probability distribution $P_{\alpha\beta}$ cannot be reproduced through local measurements on a quantum state. Additionally, if a set \mathcal{S} can be written as linear combinations of operators in another set \mathcal{S}' , the conditions imposed by \mathcal{S}' are at least as constraining as the ones imposed by \mathcal{S} , and the set \mathcal{S}_m of all possible products of m projectors generates by linear combinations all the operators that are linear combinations of products of m' projectors, with $m' \leq m$ [48].

Hence, given a set of projectors $\{E_\mu\}$, the NPA method allows us to build in a hierarchical way all the conditions (i.e., the sets \mathcal{S}) to be satisfied to certify the *quantumness* of a given probability distribution. The hierarchy is based on constructing sets \mathcal{S}_n made up of products of the given operators until degree n : for instance, we can first consider the set containing just the projectors of the two parties, Alice and Bob, which we indicate by $\mathcal{S}_1 = \{E_\alpha, E_\beta\}$. If the

conditions stated in Eqs. (B3)–(B5) hold, we can go on and verify the constraints imposed by the set $\mathcal{S}_2 = \{E_\mu E_\nu\}$, made up of all the products of the operators $\{E_\alpha, E_\beta\}$, and then iterate the process until some condition fails, or until the set \mathcal{S}_n is sufficiently large to represent all the conditions we need to check.

For a concrete example, we consider Alice performing measurements $X = 1, 2$ and Bob performing measurements $Y = 3, 4$, where each measurement yields one of the two possible outcomes $\{a, b\} \in \{+1, -1\}$. We also define the correlation functions $C_{XY} = \sum_{ab} abP(a, b|X, Y)$ and the marginal quantities $C_X = \sum_a aP(a, b|X, Y)$ and $C_Y = \sum_b bP(a, b|X, Y)$. The test of the NPA hierarchy corresponding to the first level (i.e., $n = 1$) is built on the set $\mathcal{S}_1 = \{X_1, X_2, Y_1, Y_2\}$, and the Γ matrix has the following form:

$$\Gamma = \begin{pmatrix} 1 & C_1 & C_2 & C_3 & C_4 \\ & 1 & u & C_{13} & C_{14} \\ & & 1 & C_{23} & C_{24} \\ & & & 1 & w \\ & & & & 1 \end{pmatrix}, \quad (\text{B6})$$

where the lower symmetric part has been elided (remember that Γ is Hermitian), and the entries u and w correspond to the correlation terms involving noncommuting measurements (both belonging to Alice or Bob). These entries are thus indeterminate and can be adjusted by use of a semidefinite program to get a SDP Γ matrix if the other correlations $\{C_X, C_Y, C_{XY}\}$ are quantum [48].

1. Application to SDP characterization in parallel self-testing

In the parallel self-testing scenario the function to be minimized—that is, the fidelity defined in Eq. (A7)—is a linear combination of correlation terms containing products of two (one for Alice and one for Bob) to six (three each) operators. To minimize such a function on a quantum set, we need to impose these terms to be the entries of one positive semidefinite Γ matrix, and given that, as shown in the previous example, level 1 of the hierarchy considers constraints on correlation terms up to degree 2, in our case it is necessary to build the hierarchy up to level 3, at least. To do so, we use the PYTHON library first introduced in Ref. [65], which allows one to set both the objective function to be optimized and the level of the relaxation, and then to solve the SDP problem with the optimization program MOSEK [66].

Considering that Alice and Bob each own eight projector operators, indicated by Π_{A/B_x}^a , where $a = \{0, 1, 2, 3\}$ are the possible eigenvalues, and $x \in (0, 1)$, and given also property (i) of the projection operation, yielding $\Pi_{A/B_x}^3 = \mathbb{I} - (\Pi_{A/B_x}^0 + \Pi_{A/B_x}^1 + \Pi_{A/B_x}^2)$, at level 1 the \mathcal{S}_1 set contains the following 12 elements: $\Pi_{A_0}^0, \Pi_{A_0}^1, \Pi_{A_0}^2, \Pi_{A_1}^0,$

$\Pi_{A_1}^1, \Pi_{A_1}^2, \Pi_{B_0}^0, \Pi_{B_0}^1, \Pi_{B_0}^2, \Pi_{B_1}^0, \Pi_{B_1}^1,$ and $\Pi_{B_1}^2$. Given also that the number of the Γ entries grows with the level of the relaxation and with the number of operators involved, and decreases with the number of allowed substitutions, namely, if entry $\Gamma_{ij} = \Pi_{A_0}^0 \times \Pi_{A_0}^0 \times \Pi_{B_1}^0$ and entry $\Gamma_{i'j'} = \Pi_{A_0}^0 \times \Pi_{B_1}^0$, then the two are the same variable, due to property (ii) of the projection operation, the total number of variables concerned in this optimization problem is 22 602.

However, it is possible to further reduce this quantity by noticing that our objective function is symmetric under exchange of parties $A \leftrightarrow B$, and that this transformation keeps also the Γ matrix unchanged. In particular, we add to the aforementioned substitutions those of the kind

$$\begin{aligned}
 \Pi_{A_0}^a &: \Pi_{B_0}^a, \\
 \Pi_{A_1}^a &: \Pi_{B_1}^a, \\
 \Pi_{A_0}^a \times \Pi_{A_1}^{a'} &: \Pi_{B_0}^a \times \Pi_{B_1}^{a'}, \\
 \Pi_{A_0}^a \times \Pi_{B_1}^{a'} &: \Pi_{A_1}^{a'} \times \Pi_{B_0}^a, \\
 \Pi_{A_0}^a \times \Pi_{A_1}^{a'} \times \Pi_{B_0}^{a''} &: \Pi_{A_0}^{a''} \times \Pi_{B_0}^a \times \Pi_{B_1}^{a'}, \\
 &\dots,
 \end{aligned} \tag{B7}$$

where we take care to respect the commutation rules of Alice and Bob's operators when defining the left-hand side and the right-hand side of each substitution.

2. Application to SDP characterization in the tripartite scenario

We now consider the scenario in which Alice shares one singlet with Bob and another with Charlie. Here the fidelity to be bounded is the one in Eq. (A14), which contains correlation terms of at least three (one for each party) and at most nine (three for each party) operators. In this case, level 1 of the hierarchy is built over the following set containing ten projection operators: $\mathcal{S}_{bilo} = \{\Pi_{A_0}^0, \Pi_{A_0}^1, \Pi_{A_0}^2, \Pi_{A_1}^0, \Pi_{A_1}^1, \Pi_{A_1}^2, \Pi_{B_0}^0, \Pi_{B_1}^0, \Pi_{C_0}^0, \Pi_{C_1}^0\}$. At the minimum required level (i.e., level 5) the problem would be too computationally requiring for a normal computer. To simplify the problem, it is possible to stop at level 3 of the hierarchy by considering all the monomials with degree higher than 6 appearing in the objective function as *extramonomials*. In this way, not all the possible product combinations of the operators are taken into account as variables for correlation terms of degree greater than 6, and only those given as extramonomials are taken into account. The number of variables for the optimization is, considering also the standard substitutions due to the projection properties, 10 115. Besides this, it is possible to further reduce the number of the Γ entries by using, again, the symmetries of the objective function. This time, the symmetry holds for the exchange of the peripheral parties (i.e., Bob and Charlie, $B \leftrightarrow C$) and swapping the second

and third outputs of the central party (i.e., $01 \leftrightarrow 10$). By considering this symmetry when setting the list of the substitutions, the number of SDP variables decreases to 7670, while the time for the optimization decreases from 136.28 to 78.16 s.

APPENDIX C: FREQUENCY REGULARIZATION AND DEFINITION OF THE DUAL EQUALITY CONSTRAINT

The NPA hierarchy is just one of several examples of theoretical tools taking into account the full quantum distribution for device-independent characterization, which all share the common assumption of no signaling. However, because of finite statistics, raw distributions obtained by the experimental frequencies generally do not satisfy this condition, to the extent that it is almost always impossible to use raw data with these methods. In Ref. [57], a general tool called the ‘‘device-independent least-squares method’’ is introduced, which can be used to estimate the no-signaling probability distribution belonging to a superset of the quantum correlation set, \mathcal{Q}_I , which is the closest to the experimental frequencies in terms of a norm-2 distance ($\|\vec{f} - \vec{P}\|_2$). In particular, we indicate with \vec{f} the experimental frequencies and P is the probability distribution satisfying the no-signaling condition. We briefly state the no-signaling condition: a distribution of probability $P(a, b|x, y)$ is nonsignaling if the following two relations are simultaneously satisfied:

$$\begin{aligned}
 P(a|x, y) &\equiv \sum_b P(a, b|x, y) = P(a|x, y') \text{ for all } a, x, y, y', \\
 P(b|x, y) &\equiv \sum_a P(a, b|x, y) = P(b|x', y) \text{ for all } b, y, x, x'.
 \end{aligned} \tag{C1}$$

In detail, this technique is shown in Ref. [57] to be equivalent to performing a projection $P_{\Pi}(\vec{f})$ of \vec{f} onto an affine subspace \mathcal{N} of \mathbb{R}^{16} (16 is the dimension of the frequency vector in a simple CHSH two-party scenario), which contains only \vec{P} s satisfying the no-signaling condition, followed by the minimization of the norm-2 distance between P_{Π} and \mathcal{Q} .

Formally, the method amounts to finding the unique minimizer of the least-squares problem

$$\vec{P}_{LS}(\vec{f}) = \operatorname{argmin}_{\vec{P} \in \mathcal{Q}} \|\vec{f} - \vec{P}\|_2, \tag{C2}$$

where when the quantum set \mathcal{Q} is approximated by a superset relaxation \mathcal{Q}_I that admits a semidefinite programming characterization through the NPA hierarchy. The problem in Eq. (C2) can be cast as a SDP, although the norm-2 distance is not a linear function in the following formulation, using the characterization of positive semidefinite matrices

via their Shur complement:

$$\begin{aligned} & \operatorname{argmin}_{\vec{P} \in \mathcal{Q}_l} \quad s \\ & \text{subject to } \begin{pmatrix} s\mathbb{I} & \vec{f} - \vec{P} \\ \vec{f}^T - \vec{P}^T & s \end{pmatrix} \succeq 0 \quad (\text{C3}) \\ & \text{and } \Gamma \succeq 0, \end{aligned}$$

where \mathbb{I} is the identity matrix having the same dimension of the column vector \vec{f} , and Γ is defined as in Eq. (B6), depending on the NPA hierarchy level chosen. Indeed, by Theorem 7.7.7 in Ref. [67],

$$s - (\vec{f}^T - \vec{P}^T) \frac{\mathbb{I}}{s} (\vec{f} - \vec{P}) \succeq 0. \quad (\text{C4})$$

Given that $(\vec{f}^T - \vec{P}^T)(\vec{f} - \vec{P}) = \|\vec{f} - \vec{P}\|_2^2$, Eq. (C4) is equivalent to

$$s^2 \succeq \|\vec{f} - \vec{P}\|_2^2, \quad (\text{C5})$$

and hence $s \geq \|\vec{f} - \vec{P}\|_2$.

This problem involves only an objective function and matrix constraints that are linear in the SDP variables s and \vec{P} and in the variables of the Γ matrix, and is shown [57] to be unique and totally equivalent to the one defined in Eq. (C2).

At this point, the probability distribution \vec{P} obtained is input into the SDP as linear constraints on the moments of the Γ matrix, as described in Eq. (A6), where the p are the regularized probabilities.

Now consider that given $C \in \mathcal{M}^n$, $A_i \in \mathcal{M}^n$, $i = 1, 2, \dots, m$, and $b \in \mathcal{R}^m$, the semidefinite programming problem is to find a matrix $X \in \mathcal{M}^n$ for the following optimization problem:

$$\begin{aligned} & \inf \quad C \cdot X \\ & \text{subject to } A_i \cdot X = b_i \mid i = 1, \dots, m \mid X \succeq 0, \end{aligned} \quad (\text{C6})$$

which individuates the *primal* solution to the problem (i.e., searches for the minimum solution from above). The corresponding dual problem can be written as

$$\begin{aligned} & \sup \quad b^T y \\ & \text{subject to } \sum_i y_i A_i + S = C \mid S \succeq 0. \end{aligned} \quad (\text{C7})$$

Here $y \in \mathcal{R}^m$ and $S \in \mathcal{M}^n$ constitute the solution of the dual problem; namely, the best approximation of the result from below that coincides with the primal due to strong duality. The objective function of the dual problem, $b^T y$, is in our case a linear combination of the regularized frequencies $\sum_i^m c_i P_i$. At this point, we take the dual solution

of the SDP (namely, the vector of coefficients y) and evaluate the linear combination $D_{\text{expt.}} = b_{\text{expt.}}^T y$ by putting as $b_{\text{expt.}}$ the observed frequencies. In the end, this new linear combination of the matrix moment is given as the equality constraint to a new SDP, which finally gives our device-independent estimation of the minimal certifiable fidelity, as follows:

$$\begin{aligned} & f = \min \langle \psi_{\text{target}} \mid \rho_{\text{SWAP}} \mid \psi_{\text{target}} \rangle \\ & \text{subject to } c \in \mathcal{Q}_l, \quad (\text{C8}) \\ & c^T y = b_{\text{expt.}}^T y. \end{aligned}$$

This method allows one to extract an experimental lower bound on the fidelity directly from the experimental data and not from the regularized data, avoiding a possible over-estimation of it. For the NPA level of the hierarchy used in the data regularization, we choose to consider level 4 to avoid to selecting a probability distribution not belonging to the level used in the fidelity lower bound optimizations (i.e., 3 for the parallel case and 3 plus extraterms for the three-party case), which would result in an infeasible optimization problem.

APPENDIX D: NOISE MODEL

In Appendix A, we report the theoretical fidelity lower bounds corresponding to different state visibilities according to the following noise model, taking into account only white noise (i.e., isotropic depolarization):

$$\rho_v = v |\psi\rangle\langle\psi| + (1-v) \frac{\mathbb{I}}{4}, \quad (\text{D1})$$

where ρ_v is the state generated by one of the two sources. Furthermore, both sources are assumed to be characterized by the same noise parameter v . Hence, the model of the overall generated state is the following: $\rho_v^{AB} = \rho_v^{A_1 B_1} \otimes \rho_v^{A_2 B_2}$ (for the parallel case) and $\rho_v^{ABC} = \rho_v^{AB} \otimes \rho_v^{AC}$ (for the three-party case). This model is used to have an overview of the robustness of the proposed self-testing protocol, but despite its usefulness, it is not appropriate as a model of our experimental conditions.

Hence, to design a noise model that better represents the states generated by our sources, we need to take into account also the presence of colored noise (i.e., depolarization along a preferred direction), which is typical of SDPC sources of type II [56]:

$$\rho_\lambda = \lambda |\psi\rangle\langle\psi| + \frac{1-\lambda}{2} (|01\rangle\langle 01| + |10\rangle\langle 10|). \quad (\text{D2})$$

Moreover, we consider that there could be errors in the rotation of the wave plates belonging to the parties' measurement stations—that is, $\mathcal{O}'_A = U(\phi)^\dagger \mathcal{O}_A U(\phi)$,

etc.—and the fact that the two sources can have different visibilities.

Therefore, overall, our noise model is as follows:

$$\rho_{\lambda v} = v|\psi\rangle\langle\psi| + (1-v) \times \left(\frac{\lambda}{2}(|01\rangle\langle 01| + |10\rangle\langle 10|) + (1-\lambda)\frac{\mathbb{I}}{4} \right), \quad (\text{D3})$$

and the total states generated by the networks have the following form:

$$\rho_{\lambda_1, 2, v_1, 2}^{AB} = \rho_{\lambda_1, v_1}^{A_1 B_1} \otimes \rho_{\lambda_2, v_2}^{A_2 B_2}, \quad (\text{D4})$$

$$\rho_{\lambda_1, 2, v_1, 2}^{ABC} = \rho_{\lambda_1, v_1}^{A_1 B} \otimes \rho_{\lambda_2, v_2}^{A_2 C}. \quad (\text{D5})$$

The noise parameters that best explain our experimental observations are estimated by minimizing the distance between the theoretical probability distribution predicted by the noise model, $p_{\text{mod}}(a, b|x, y)$ or $p_{\text{mod}}(a, b, c|x, y, z)$, and the experimental frequencies, $f(a, b|x, y)$ or $f(a, b, c|x, y, z)$. In detail, we define the total distance as

$$d(p, f) = \frac{1}{8} \sum_{a, b, x, y} |p(a, b|x, y) - f(a, b|x, y)|, \quad (\text{D6})$$

$$d(p, f) = \frac{1}{16} \sum_{a, b, x, y} |p(a, b, c|x, y, z) - f(a, b, c|x, y, z)|, \quad (\text{D7})$$

where Eq. (D6) refers to the parallel case and Eq. (D7) refers to the three-party one. The noise parameters corresponding to our experimental conditions are $v_1 = 0.9716$, $\lambda_1 = 0.5004$, $v_2 = 0.9852$, and $\lambda_2 = 0.5117$, giving $d_{\text{parallel}} = 0.100$ and $d_{\text{three-party}} = 0.103$. A comparison between the experimental frequencies and the noise-predicted ones is shown in Fig. 6. With such parameters, the predicted fidelities for the parallel scenario and for the three-party scenario are, 0.631 and 0.830, respectively, both of which are compatible, within approximately one standard deviation, with the experimental values (i.e., 0.587 ± 0.053 and 0.863 ± 0.032).

APPENDIX E: BOUNDING THE CONFIDENCE LEVEL ON THE FIDELITY BY USE OF Hoeffding Inequality

Hoeffding inequality [44] is a very useful tool when there is a need to estimate uncertainties on experimental probabilities, taking into account finite statistics. It asserts that given n independent random variables X_1, \dots, X_n , defined in $[0, 1]$, with the following mean, expected value, and variance:

$$S = (X_1 + X_2 + \dots + X_n),$$

$$\bar{X} = S/n,$$

$$\mu = E[\bar{X}] = E[S/n],$$

$$\sigma^2 = \text{var } y/n.$$

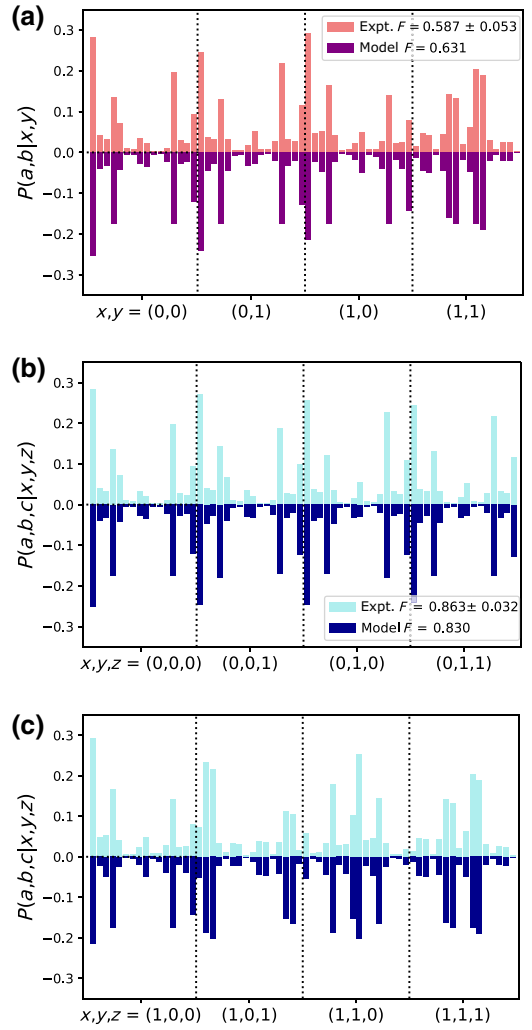


FIG. 6. Noise theoretical model. The histograms show a comparison between the experimentally observed frequencies and the probability distributions that are expected by the noise model of the state generated by the sources involved. In particular, we consider each source to generate the state $\rho_{\lambda v} = v|\psi\rangle\langle\psi| + (1-v)[(\lambda/2)(|01\rangle\langle 01| + |10\rangle\langle 10|) + (1-\lambda)(\mathbb{I}/4)]$, which is affected both by an isotropic depolarization (white noise) and by a specific direction (colored noise). The fraction of the latter is given by the parameter λ , while v is the overall state visibility. Hence, the state generated in the network will be $\rho_{\lambda_1, 2, v_1, 2}^{AB} = \rho_{\lambda_1, v_1}^{A_1 B_1} \otimes \rho_{\lambda_2, v_2}^{A_2 B_2}$ in the parallel case and $\rho_{\lambda_1, 2, v_1, 2}^{ABC} = \rho_{\lambda_1, v_1}^{A_1 B} \otimes \rho_{\lambda_2, v_2}^{A_2 C}$ in the three-party case. The noise parameters characterizing our state are as follows: $v_1 = 0.9716$, $\lambda_1 = 0.5004$, $v_2 = 0.9852$, and $\lambda_2 = 0.5117$, and according to such a model, the predicted fidelity lower bounds for the parallel and three-party scenarios are 0.631 and 0.830, respectively, both compatible within 1.5 standard deviations with the experimental values; that is, 0.587 ± 0.053 (a) and 0.863 ± 0.032 (b).

Then the following inequality holds for $0 \leq t \leq 1 - \mu$:

$$\epsilon = \Pr(\bar{X} - \mu \geq t) \leq e^{-2nt^2}, \quad (\text{E1})$$

where t depends on the arbitrary confidence interval ϵ assigned to the variable $y = \bar{X} - \mu$ according to $t(\epsilon) = \sqrt{-\ln \epsilon / (2n)}$.

From this bound, it is possible to extract information about the effects of finite statistics on the estimation of the dual constraint, described in Appendix C. We consider the worst-case scenario of Hoeffding inequality (E1); that is, $\epsilon = e^{-2nt^2}$. The right-hand side of this equality corresponds to 1 minus the cumulative distribution of the variable y ; namely:

$$P\{y \geq t\} = \int_t^\infty P(y) dy = e^{-2nt^2}, \quad t > 0. \quad (\text{E2})$$

For the fundamental theorem of calculus, the probability distribution function $P(y)$ for $y > 0$ can be obtained by differentiating 1 minus Eq. (E2), thus yielding

$$P(y) = \frac{d(1 - e^{-2ny^2})}{dy} = 4nye^{-2ny^2}, \quad (\text{E3})$$

which is a well-defined, positive and normalized distribution of probability for $y > 0$. For the case $y < 0$, Hoeffding inequality still holds symmetrically [44], leading to the following upper bound for $t > 0$:

$$\Pr(-\bar{X} + \mu \geq t) = e^{-2nt^2}. \quad (\text{E4})$$

This means that we can consider the two-sided variant of Hoeffding bound relative to the absolute value of the variable y ,

$$\Pr(|\bar{X} - \mu| \geq t) = 2e^{-2nt^2}, \quad (\text{E5})$$

by defining the normalized probability distribution over all real values of y , which is $P(y) = 2n|y|e^{-2ny^2}$ and whose variance is defined as $\text{var } y = 1/(2n)$. For the central limit theorem, a linear combination $\sum_{k=1}^N a_k y_k$ of N such independent, finite variance variables has a Gaussian distribution characterized by the following variance:

$$\sigma_{\text{Gauss}}^2 = \sum_{k=1}^N a_k^2 (\text{var } y_k) = \sum_{k=1}^N a_k^2 / (2n).$$

Since the experimental value of the dual d_{exp} is actually a linear combination of the experimental frequencies, its probability distribution can be approximated by a Gaussian, and we can estimate that the experimental dual lies

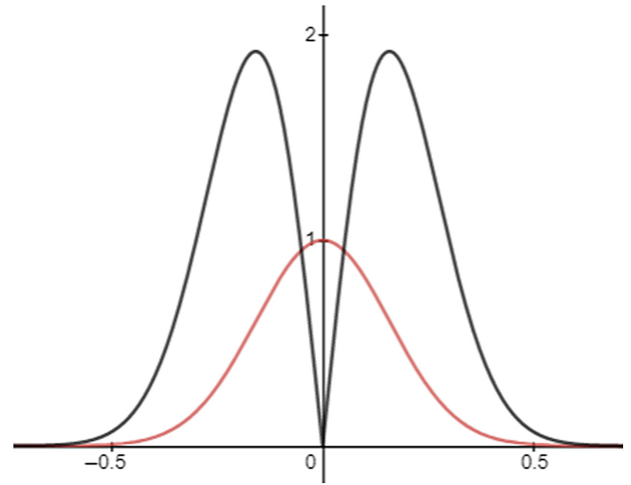


FIG. 7. Hoeffding distribution function. The black curve represents the normalized probability distribution of the variable $y = \bar{X} - \mu > 0$, $P(y) = 2n|y|e^{-2ny^2}$, while the red curve represents 1 minus the cumulative probability of such a distribution; that is, the probability that y lies outside the range $[0, t]$, given by Hoeffding inequality [44]. Since for the case $y < 0$ Hoeffding inequality holds symmetrically and hence $P(y) = P(-y)$, the probability that y lies outside the range $[-t, t]$ amounts to $P(|y| \geq t, t > 0) = \int_{-\infty}^{-t} -2nye^{-2ny^2} dy + \int_t^{\infty} 2nye^{-2ny^2} dy = e^{-2nt^2}$. The variance of the black function is $\text{var } y = 1/(2n)$. We use the variance of this distribution to compute the statistical uncertainty on the constraint $c^T(y)$ of the problem given by Eq. (C8) by asserting that it lies inside the interval $d_{\text{expt.}} - \tau(\epsilon) \leq c^T y \leq d_{\text{expt.}} + \tau(\epsilon)$ with a probability that can be recovered from a standardized normal table, considering that such an interval amounts to $\sqrt{-\ln \epsilon}$ standard deviations.

within the following interval:

$$d_{\text{expt.}}(f) - \tau(\epsilon) \leq d(p) \leq d_{\text{expt.}}(f) + \tau(\epsilon), \quad (\text{E6})$$

where

$$\tau^2(\epsilon) = \sum_{k=1}^N a_k^2 t_k^2(\epsilon) = -\ln(\epsilon)\sigma^2, \quad (\text{E7})$$

having defined $\sigma^2 = \sum_{k=1}^N a_k^2 \text{var } y_k$, with a confidence level that can be computed from a standardized normal table considering that such an interval amounts to $\sqrt{-\ln \epsilon}$ standard deviations.

APPENDIX F: ACCOUNTING FOR POSSIBLE MEMORY EFFECTS THROUGH THE AZUMA-HOEFFDING INEQUALITY

Hoeffding inequality [44], as explained in Appendix E, allows us to find a confidence level for our fidelity results without making assumptions on the statistics underlying the experiment. However, this method still requires

the assumption that the variables involved are independent of each other and drawn from the same probability distribution; namely, the so-called IID assumption.

To drop such an assumption and take into account possible memory effects throughout the experiment, which may cause interdependencies among the runs, we can use a different approach: the Azuma-Hoeffding inequality [45–47,59]. The application of such an inequality requires that the random variables involved in our process constitute a martingale [45]; namely, a stochastic process in which the expected value of an observation at some time k , conditioned on all the previous observations up to a earlier time k' , is equal to the observation at that earlier time. This feature implies that martingales, under some circumstances, behave like the sum of independent variables.

Here we describe how this approach works for the three-party case (the parallel one is analogous).

In our case, the random variables we consider are as follows:

$$C_i(a, b, c|x, y, z) = \frac{\chi(a_i = a, b_i = b, c_i = c, x_i = x, y_i = y, z_i = z)}{q(x, y, z)}, \quad (\text{F1})$$

where $q(x, y, z)$ is the input probability distribution and $\chi(e)$ is the indicator function for event e ; that is, if event e occurs, $\chi(e) = 1$, otherwise $\chi(e) = 0$. The relation between $C_i(a, b, c|x, y, z)$ and our frequencies $f(a, b, c|x, y, z)$ is as follows:

$$f(a, b, c|x, y, z) = \frac{1}{n} \sum_{i=1}^n C_i(a, b, c|x, y, z), \quad (\text{F2})$$

where n is the total number of runs. Then the probabilities after n runs of the experiment and considering the eventual presence of memory effects amount to

$$p^n(a, b, c|x, y, z) = \frac{1}{n} \sum_{i=1}^n C_i(a, b, c|x, y, z, W_i), \quad (\text{F3})$$

where $W_i = (a^{i-1}, b^{i-1}, c^{i-1}, x^{i-1}, y^{i-1}, z^{i-1})$, implying that in Eq. (F3), we are taking into account all of the runs before the n th run. If we take variable $Z^k(a, b, c|x, y, z) = \sum_{i=1}^k |C_i(a, b, c|x, y, z) - C(W_i)|$, where $C(W_i) = E[C_i|W_i]$, the sequence of Z^k is a martingale with respect to the sequence of W^i . In detail, it constitutes a *Doob martingale* [68] because $E[Z^k] < \infty$ and $W^i \subset W^j$ if $i < j$.

At this point, since the range of variation of our martingale is bounded by $|C_i(a, b, c|x, y, z) - C(W_i)| \leq 1/\min(q(x, y, z))$, we can apply the Azuma-Hoeffding

inequality [45–47,59] as follows:

$$\epsilon = P\left(\sum_{i=1}^n |C_i(a, b, c|x, y, z) - C(W_i)| \geq t^*\right) \leq e^{-p}, \quad (\text{F4})$$

where

$$p = \min(q(x, y, z))^2 \frac{t^{*2}}{2n}. \quad (\text{F5})$$

By our taking $t^* = nt$, Eq. (F4) becomes

$$\epsilon = P\left(\frac{1}{n} \sum_{i=1}^n |C_i(a, b, c|x, y, z) - C(W_i)| \geq t\right) \leq e^{-p^*}, \quad (\text{F6})$$

where

$$p^* = \frac{n \times \min(q(x, y, z))^2 t^2}{2}. \quad (\text{F7})$$

Given that, as previously mentioned, our experimental frequencies are given by $f(a, b, c|x, y, z) = \sum_{i=1}^n (1/n) C_i(a, b, c|x, y, z)$, we can use an approach analogous to the one we followed in the case of Hoeffding inequality to conclude that such variables are distributed according to the following probability distribution: $P(y) \sim (n/2) |y| e^{-[n \times \min(q(x, y, z))^2 y^2 / 2]}$, with variance $\text{var } y = 2/[n \times \min(q(x, y, z))^2]$. For the central limit theorem, a linear combination $\sum_{k=1}^n a_k y_k$ of n variables characterized by such a distribution follows a Gaussian distribution with the following variance:

$$\sigma_{\text{Gauss}} = \sum_{k=1}^n a_k^2 \text{var } y_k = \sum_{k=1}^n a_k^2 \frac{2}{n \times \min(q(x, y, z))^2}. \quad (\text{F8})$$

Since the experimental value of the dual d_{exp} is actually a linear combination of the experimental frequencies, its probability distribution can be approximated by a Gaussian, and we can estimate that the experimental dual lies within the following interval:

$$d_{\text{expt.}}(f) - \tau(\epsilon) \leq d(p) \leq d_{\text{expt.}}(f) + \tau(\epsilon), \quad (\text{F9})$$

with a confidence level that can be computed from a standardized normal table considering that such an interval

amounts to $\sqrt{-\ln \epsilon}$ standard deviations, with

$$\tau^2(\epsilon) = \sum_{k=1}^N a_k^2 t_k^2(\epsilon) = -\ln(\epsilon)\sigma^2. \quad (\text{F10})$$

- [1] S. Aaronson and A. Arkhipov, in *Proceedings of the Forty-Third Annual ACM Symposium on Theory of Computing* (ACM, New York, 2011), p. 333.
- [2] M. A. Broome, A. Fedrizzi, S. Rahimi-Keshari, J. Dove, S. Aaronson, T. C. Ralph, and A. G. White, Photonic boson sampling in a tunable circuit, *Science* **339**, 794 (2013).
- [3] J. B. Spring, B. J. Metcalf, P. C. Humphreys, W. S. Kolthammer, X.-M. Jin, M. Barbieri, A. Datta, N. Thomas-Peter, N. K. Langford, D. Kundys, *et al.*, Boson sampling on a photonic chip, *Science* **339**, 798 (2013).
- [4] M. Tillmann, B. Dakić, R. Heilmann, S. Nolte, A. Szameit, and P. Walther, Experimental boson sampling, *Nat. Photonics* **7**, 540 (2013).
- [5] A. Crespi, R. Osellame, R. Ramponi, D. J. Brod, E. F. Galvao, N. Spagnolo, C. Vitelli, E. Maiorino, P. Mataloni, and F. Sciarrino, Integrated multimode interferometers with arbitrary designs for photonic boson sampling, *Nat. Photonics* **7**, 545 (2013).
- [6] 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).
- [7] R. Ramanathan, F. Brandão, K. Horodecki, M. Horodecki, P. Horodecki, and H. Wojewódka-Ściażko, Randomness Amplification under Minimal Fundamental Assumptions on the Devices, *Phys. Rev. Lett.* **117**, 230501 (2016).
- [8] R. Colbeck and R. Renner, Free randomness can be amplified, *Nat. Phys.* **8**, 450 (2012).
- [9] R. Gallego, L. Masanes, G. de la Torre, C. Dhara, L. Aolita, and A. Acín, Full randomness from arbitrarily deterministic events, *Nat. Commun.* **4**, 2654 (2013).
- [10] C. A. Miller and Y. Shi, Robust protocols for securely expanding randomness and distributing keys using untrusted quantum Devices, *J. ACM* **63**, 33:1 (2016).
- [11] F. G. S. L. Brandão, R. Ramanathan, A. Grudka, K. Horodecki, M. Horodecki, P. Horodecki, T. Szarek, and H. Wojewódka, Realistic noise-tolerant randomness amplification using finite number of devices, *Nat. Commun.* **7**, 11345 (2016).
- [12] U. V. Vazirani and T. Vidick, [ArXiv:1111.6054](https://arxiv.org/abs/1111.6054) (2011).
- [13] Y. Liu, *et al.*, High-Speed Device-Independent Quantum Random Number Generation Without a Detection Loop-hole, *Phys. Rev. Lett.* **120**, 010503 (2018).
- [14] U. Vazirani and T. Vidick, Fully Device-Independent Quantum Key Distribution, *Phys. Rev. Lett.* **113**, 140501 (2014).
- [15] K.-M. Chung, Y. Shi, and W. Xiaodi, [ArXiv:1402.4797](https://arxiv.org/abs/1402.4797) (2014).
- [16] F. Dupuis, O. Fawzi, and R. Renner, [ArXiv:1607.01796](https://arxiv.org/abs/1607.01796) (2016).
- [17] R. Arnon-Friedman and R. Renner, de Finetti reductions for correlations, *J. Math. Phys.* **56**, 052203 (2015).
- [18] L. Shen, J. Lee, L. P. Thinh, J.-D. Bancal, A. Cerè, A. Lamas-Linares, A. Lita, T. Gerrits, S. W. Nam, V. Scarani, and C. Kurtsiefer, Randomness Extraction from Bell Violation with Continuous Parametric Down-Conversion, *Phys. Rev. Lett.* **121**, 150402 (2018).
- [19] M. Kessler and R. Arnon-Friedman, [ArXiv:1705.04148](https://arxiv.org/abs/1705.04148) (2017).
- [20] J.-D. Bancal, L. Sheridan, and V. Scarani, More randomness from the same data, *New J. Phys.* **16**, 033011 (2014).
- [21] P. Bierhorst, E. Knill, S. Glancy, Y. Zhang, A. Mink, S. Jordan, A. Rommal, Y.-K. Liu, B. Christensen, S. W. Nam, M. J. Stevens, and L. K. Shalm, Experimentally generated randomness certified by the impossibility of superluminal signals, *Nature* **556**, 223 (2018).
- [22] S. Pironio, V. Scarani, and T. Vidick, Focus on device independent quantum information, *New J. Phys.* **18**, 100202 (2016).
- [23] N. Brunner, D. Cavalcanti, S. Pironio, V. Scarani, and S. Wehner, Bell nonlocality, *Rev. Mod. Phys.* **86**, 419 (2014).
- [24] I. Šupić and J. Bowles, Self-testing of quantum systems: a review, *Quantum* **4**, 337 (2020).
- [25] 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).
- [26] D. Mayers and A. Yao, [ArXiv:quant-ph/0307205](https://arxiv.org/abs/quant-ph/0307205) (2003).
- [27] Y. Wang, X. Wu, and V. Scarani, All the self-testings of the singlet for two binary measurements, *New J. Phys.* **18**, 025021 (2016).
- [28] 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).
- [29] I. Šupić, R. Augusiak, A. Salavrakos, and A. Acín, Self-testing protocols based on the chained bell inequalities, *New J. Phys.* **18**, 035013 (2016).
- [30] J. Kaniewski, Self-testing of binary observables based on commutation, *Phys. Rev. A* **95**, 062323 (2017).
- [31] T. H. Yang, T. Vértesi, J.-D. Bancal, V. Scarani, and M. Navascués, Robust and Versatile Black-Box Certification of Quantum Devices, *Phys. Rev. Lett.* **113**, 040401 (2014).
- [32] J. Kaniewski, Analytic and Nearly Optimal Self-Testing Bounds for the Clauser-Horne-Shimony-Holt and Mermin Inequalities, *Phys. Rev. Lett.* **117**, 070402 (2016).
- [33] A. Coladangelo, K. T. Goh, and V. Scarani, All pure bipartite entangled states can be self-tested, *Nat. Commun.* **8**, 15485 (2017).
- [34] I. Šupić, A. Coladangelo, R. Augusiak, and A. Acín, Self-testing multipartite entangled states through projections onto two systems, *New J. Phys.* **20**, 083041 (2018).
- [35] M. O. Renou, J. Kaniewski, and N. Brunner, Self-Testing Entangled Measurements in Quantum Networks, *Phys. Rev. Lett.* **121**, 250507 (2018).
- [36] P. Sekatski, J.-D. Bancal, S. Wagner, and N. Sangouard, Certifying the Building Blocks of Quantum Computers from Bell's Theorem, *Phys. Rev. Lett.* **121**, 180505 (2018).
- [37] A. Rocchetto, S. Aaronson, S. Severini, G. Carvacho, D. Poderini, I. Agresti, M. Bentivegna, and F. Sciarrino,

- Experimental learning of quantum states, *Sci. Adv.* **5**, eaau1946 (2019).
- [38] J. Bowles, I. Šupić, D. Cavalcanti, and A. Acín, Self-testing of pauli observables for device-independent entanglement certification, *Phys. Rev. A* **98**, 042336 (2018).
- [39] S. Gómez, A. Mattar, I. Machuca, E. Gómez, D. Cavalcanti, O. J. Fariás, A. Acín, and G. Lima, Experimental investigation of partially entangled states for device-independent randomness generation and self-testing protocols, *Phys. Rev. A* **99**, 032108 (2019).
- [40] S. Breiner, A. Kalev, and C. A. Miller, [ArXiv:1806.04744](https://arxiv.org/abs/1806.04744) (2018).
- [41] J.-D. Bancal, M. Navascués, V. Scarani, T. Vértesi, and T. H. Yang, Physical characterization of quantum devices from nonlocal correlations, *Phys. Rev. A* **91**, 022115 (2015).
- [42] I. Šupić, D. Cavalcanti, and J. Bowles, [ArXiv:1909.12759](https://arxiv.org/abs/1909.12759) (2019).
- [43] D. Poderini, I. Agresti, G. Marchese, E. Polino, T. Giordani, A. Suprano, M. Valeri, G. Milani, N. Spagnolo, G. Carvacho, *et al.*, Experimental violation of n-locality in a star quantum network, *Nat. Commun.* **11**, 1 (2020).
- [44] W. Hoeffding, Probability inequalities for sums of bounded random Variables, *J. Am. Stat. Assoc.* **58**, 13 (1963).
- [45] G. S. Grimmett, *et al.*, *Probability and Random Processes* (Oxford University Press, Oxford, 2020).
- [46] N. Alon and J. H. Spencer, *The Probabilistic Method* (John Wiley & Sons, Hoboken, New Jersey, USA, 2004).
- [47] K. Azuma, Weighted sums of certain dependent random variables, *Tohoku Math. J. Section Ser.* **19**, 357 (1967).
- [48] M. Navascués, S. Pironio, and A. Acín, Bounding the Set of Quantum Correlations, *Phys. Rev. Lett.* **98**, eid010401 (2007).
- [49] M. Navascués, S. Pironio, and A. Acín, A convergent hierarchy of semidefinite programs characterizing the set of quantum correlations, *New J. Phys.* **10**, eid073013 (2008).
- [50] C. Branciard, N. Gisin, and S. Pironio, Characterizing the Nonlocal Correlations Created via Entanglement Swapping, *Phys. Rev. Lett.* **104**, 170401 (2010).
- [51] C. Branciard, D. Rosset, N. Gisin, and S. Pironio, Bilocal versus nonbilocal correlations in entanglement-swapping experiments, *Phys. Rev. A* **85**, 032119 (2012).
- [52] G. Carvacho, F. Andreoli, L. Santodonato, M. Bentivegna, R. Chaves, and F. Sciarrino, Experimental violation of local causality in a quantum network, *Nat. Commun.* **8**, 14775 (2017).
- [53] D. J. Saunders, A. J. Bennet, C. Branciard, and G. J. Pryde, Experimental demonstration of nonbilocal quantum correlations, *Sci. Adv.* **3**, e1602743 (2017).
- [54] F. Andreoli, G. Carvacho, L. Santodonato, M. Bentivegna, R. Chaves, and F. Sciarrino, Experimental bilocality violation without shared reference frames, *Phys. Rev. A* **95**, 062315 (2017).
- [55] Q.-C. Sun, Y.-F. Jiang, B. Bai, W. Zhang, H. Li, X. Jiang, J. Zhang, L. You, X. Chen, Z. Wang, *et al.*, Experimental demonstration of non-bilocality with truly independent sources and strict locality constraints, *Nat. Photonics* **13**, 687 (2019).
- [56] A. Cabello, A. Feito, and A. Lamas-Linares, Bell's inequalities with realistic noise for polarization-entangled photons, *Phys. Rev. A* **72**, 052112 (2005).
- [57] P.-S. Lin, D. Rosset, Y. Zhang, J.-D. Bancal, and Y.-C. Liang, Device-independent point estimation from finite data and its application to device-independent property estimation, *Phys. Rev. A* **97**, 032309 (2018).
- [58] C. Bini, *Lezioni di Statistica per la Fisica Sperimentale* (Edizioni Nuova Cultura, Rome, 2011).
- [59] S. Pironio, *et al.*, Random numbers certified by Bell's theorem, *Nature* **464**, 1021 (2010).
- [60] V. P. Gupta, P. Mandayam, and V. Sunder, in *Lecture Notes in Physics* (Berlin, 2015), chap. 2, p. 33.
- [61] R. Fickler, R. Lapkiewicz, M. Huber, M. P. Lavery, M. J. Padgett, and A. Zeilinger, Interface between path and orbital angular momentum entanglement for high-dimensional photonic quantum information, *Nat. Commun.* **5**, 1 (2014).
- [62] A. Tavakoli, D. Rosset, and M.-O. Renou, Enabling Computation of Correlation Bounds for Finite-Dimensional Quantum Systems via Symmetrization, *Phys. Rev. Lett.* **122**, 070501 (2019).
- [63] K. Gatermann and P. A. Parrilo, Symmetry groups, semidefinite programs, and sums of squares, *J. Pure Appl. Algebra* **192**, 95 (2004).
- [64] T. Kriváchy, Y. Cai, J. Bowles, D. Cavalcanti, and N. Brunner, [ArXiv:2011.05785](https://arxiv.org/abs/2011.05785) (2020).
- [65] P. Wittek, Algorithm 950, *ACM Trans. Math. Softw. (TOMS)* **41**, 1 (2015).
- [66] MosekApS, <https://docs.mosek.com/9.0/pythonapi/install-interface.html> (2019).
- [67] R. A. Horn and C. R. Johnson, *Matrix Analysis* (Cambridge University Press, Cambridge, 2012).
- [68] J. L. Doob, Regularity properties of certain families of chance variables, *Trans. Am. Math. Soc.* **47**, 455 (1940).