Device-independent certification of two bits of randomness from one entangled bit and Gisin's elegant Bell inequality

Ole Andersson,[*] Piotr Badziąg,[†] and Irina Dumitru[‡]
Fysikum, Stockholms Universitet, S-106 91 Stockholm, Sweden

Adán Cabello[§]
Departamento de Física Aplicada II, Universidad de Sevilla, E-41012 Sevilla, Spain

(Received 30 September 2017; published 16 January 2018)

We prove that as conjectured by Acín *et al.* [Phys. Rev. A **93**, 040102(R) (2016)], two bits of randomness can be certified in a device-independent way from one bit of entanglement using the maximal quantum violation of Gisin's elegant Bell inequality. This suggests a surprising connection between maximal entanglement, complete sets of mutually unbiased bases, and elements of symmetric informationally complete positive operator-valued measures, on one side, and the optimal way of certifying maximal randomness, on the other.

DOI: 10.1103/PhysRevA.97.012314

I. INTRODUCTION

Random numbers, i.e., numbers unpredictable to anyone, play a crucial role in cryptography, algorithms, and simulation. The possibility of certifying random numbers in a device-independent (DI) way, i.e., without making any assumption about the devices used to produce them and only assuming the impossibility of superluminal communication [1–3], is a great achievement of quantum information.

All methods for DI randomness certification [1–3] require entangled pairs of systems and spacelike separated measurements whose outcomes violate one or several Bell inequalities [4] and, therefore, cannot be produced by any local realistic mechanism. The fact that entanglement and Bell inequality violation are the fundamental ingredients for DI randomness certification immediately raises two questions: (i) How many random bits can be certified from one ebit? (The *ebit* is the unit of bipartite entanglement and is defined as the amount of entanglement contained in a maximally entangled two-qubit state [5].) (ii) Which is the simplest Bell inequality, i.e., the one with the smallest number of settings, which allows for the DI certification of the maximal number of random bits? Question (i) has been answered recently. D'Ariano *et al.* [6] have proven that the maximum number of bits that can be certified in a DI way from one bit of entanglement using projective nondemolition or general demolition measurements is upper bounded by *two*, and Acín *et al.* [7] have proven analytically that this maximum can be *saturated* using a protocol based on a simultaneous maximal quantum violation of *three* Clauser-Horne-Shimony-Holt (CHSH) Bell inequalities [8]. Question (ii) is still open. Intriguingly, Acín *et al.* [7] have also conjectured on the basis of numerical evidence that observing the maximum quantum violation of a single Bell inequality called "the elegant Bell inequality" (EBI) [9] is sufficient for the DI certification of two random bits. The fact that the EBI requires fewer settings than three CHSH Bell inequalities makes this conjecture interesting and worth trying to prove analytically. In this paper, we provide such a proof.

II. THE ELEGANT BELL INEQUALITY

The EBI is a bipartite Bell inequality introduced by Gisin [9] in which one of the parties, Alice, chooses among three dichotomic measurement settings, while the other party, Bob, chooses among four dichotomic measurement settings. If the possible outcomes are ± 1 and $E_{k,l}$ denotes the mean value of the product of the outcomes of Alice's kth and Bob's lth settings, the EBI reads

$$S \equiv E_{1,1} + E_{1,2} - E_{1,3} - E_{1,4} + E_{2,1} - E_{2,2} + E_{2,3} - E_{2,4} + E_{3,1} - E_{3,2} - E_{3,3} + E_{3,4} \leqslant 6. \quad (1)$$

Its maximum quantum violation is $S = 4\sqrt{3}$ [7].

Besides the practical aspect that the EBI requires fewer settings than three CHSH Bell inequalities, there is also the exciting possibility that the answer to question (ii) would be the EBI. This would be remarkable. The adjective "elegant" in the EBI comes from the observation that its maximal quantum violation is achieved when Alice and Bob share an ebit, the eigenstates of Alice's three projective measurements form a complete set of three mutually unbiased bases (MUBs), and the eigenstates of Bob's four projective measurement can be divided into two sets, each of which defines a symmetric informationally complete positive operator-valued measure (SIC-POVM). MUBs and SIC-POVMs are two geometric structures of independent interest [10] and the fact that both might be simultaneously necessary for the optimal DI certification of maximal randomness from maximal entanglement would be quite surprising.

[*]ole.andersson@fysik.su.se
[†]piotr.badziag@gmail.com
[‡]irina.dumitru@fysik.su.se
[§]adan@us.es

Acín *et al.* [7] have proposed a strategy for proving analytically that the EBI can be used for the DI certification of two random bits from one ebit. The strategy relies on the assumption that the maximal violation of the EBI is self-testing. We have recently proven [11] that the maximal violation of the EBI is not self-testing in the sense of Refs. [12,13]. However, the conjecture still holds and we prove it through a different strategy than the one proposed in Ref. [7].

III. SCENARIO

We are interested in the following scenario. Alice has a source of systems and a measurement device with four outcomes. She uses them to perform a four-outcome measurement on each system produced by the source. The generated outcomes are apparently unpredictable, i.e., after many measurements, Alice notices that the four outcomes appear with the same frequency and follow no pattern. However, it might be that the outcomes are not so unpredictable as it seems and someone else might be able to guess the outcomes of Alice's measurements. That someone, whom we call the adversary, or Eve, could also be the manufacturer of Alice's device. This means that the device is untrusted and that Alice is therefore interested in a device-independent certification of the randomness. Here we propose two tests that Alice can perform to make sure that her device generates outputs which are completely unpredictable for everyone. The tests, if passed, certify that the local guessing probability of Eve does not exceed the minimal value 1/4. If and only if this is so, we say that Alice's measurement produces two random bits.

IV. TESTS

If we write A_4 for Alice's four-outcome POVM and model Eve's substantiated guesses as outcomes a of a local four-outcome POVM F (if Eve measures a she guesses that Alice measured a), the *local guessing probability* of Eve is

$$G = \max_F \sum_a P(a,a|A_4,F). \tag{2}$$

The sum equals the probability that Eve makes a correct guess given that Alice measures A_4 and Eve measures F. We maximize over all four-outcome POVMs that are local to Eve. The tests then certify that $G = 1/4$.

The tests involve a third party, Alice's trusted friend Bob, who has access to a second system generated simultaneously by Alice's source. The scenario is sketched out in Fig. 1.

For the tests, Alice needs three and Bob needs four measurement settings measuring local dichotomic observables. We write A_1, A_2, A_3 and B_1, B_2, B_3, B_4 for Alice's and Bob's observables, respectively, and take their outcomes to be -1 and $+1$. We also write $E_{k,l}$ for the expectation value of the products of the outcomes of Alice's kth and Bob's lth measurement and $E_{a|k,l}$ for the expectation value of Bob's lth measurement which is conditioned on the outcome of Alice's

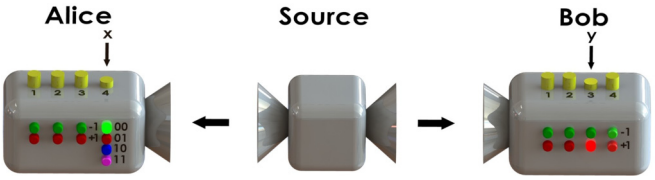

FIG. 1. The source simultaneously emits two systems, one to each side. Buttons represent possible measurements. Light bulbs represent possible outcomes. Alice and Bob wants to certify in a device-independent way that the two bits produced when Alice presses her button 4 are actually random (i.e., unpredictable even for an adversary who manufactured the devices).

kth measurement, i.e.,

$$E_{k,l} = \sum_{a,b} ab\, P(a,b|A_k,B_l), \tag{3a}$$

$$E_{a|k,l} = \sum_b b\, P(a,b|A_k,B_l). \tag{3b}$$

A test for the source. The first test is a Bell test. To pass the test, Alice's and Bob's dichotomic measurements should generate statistics indicating that the EBI is maximally violated: $S = 4\sqrt{3}$.

A test for the measurement device. A necessary requirement for $G = 1/4$ is that Alice's device generates an apparently random output, i.e., $P(a|A_4) = 1/4$ for all outcomes a. We define a family of four qubit operators $Q = \{Q_a\}$ by

$$Q_a = \gamma_a^0 \mathbb{1} + \gamma_a^1 Z + \gamma_a^2 X + \gamma_a^3 Y, \tag{4}$$

where Z, X, Y are the Pauli operators and

$$\gamma_a^0 = P(a|A_4), \tag{5a}$$

$$\gamma_a^1 = \frac{\sqrt{3}}{2}(E_{a|4,1} + E_{a|4,2}), \tag{5b}$$

$$\gamma_a^2 = \frac{\sqrt{3}}{2}(E_{a|4,1} + E_{a|4,3}), \tag{5c}$$

$$\gamma_a^3 = -\frac{\sqrt{3}}{2}(E_{a|4,2} + E_{a|4,3}). \tag{5d}$$

The second test is passed if $P(a|A_4) = 1/4$ and Q is an *extremal* four-outcome qubit POVM. Here Bob uses the same three observables B_1, B_2, B_3 used in the first test. Below we describe how to determine that Q is an extremal POVM.

Since the tests only require an analysis of the measurement statistics and assume nothing about either the devices used to generate this statistics or the measurement device used by Eve, they ensure that the randomness generated by Alice is genuine and device-independent.

The simplest scenario that passes the two tests is the following. Suppose that Alice and Bob share two qubits in the singlet state,

$$|\phi_+\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle). \tag{6}$$

If Alice measures three dichotomic observables which correspond to the Pauli observables

$$A_1 = Z, \quad A_2 = X, \quad A_3 = Y, \tag{7}$$

and Bob measures four observables which correspond to

$$B_1 = \frac{1}{\sqrt{3}}(Z + X - Y),\ B_3 = \frac{1}{\sqrt{3}}(-Z + X + Y), \quad (8a)$$

$$B_2 = \frac{1}{\sqrt{3}}(Z - X + Y),\ B_4 = \frac{1}{\sqrt{3}}(-Z - X - Y), \quad (8b)$$

then the EBI is maximally violated, which means the first test is passed. Furthermore, if Alice measures the four-outcome POVM A_4 whose elements correspond to the four linearly independent unit rank projectors

$$A_{1|4} = \frac{1}{4}\left[\mathbb{1} - \frac{1}{\sqrt{3}}(Z + X + Y)\right], \quad (9a)$$

$$A_{2|4} = \frac{1}{4}\left[\mathbb{1} - \frac{1}{\sqrt{3}}(Z - X - Y)\right], \quad (9b)$$

$$A_{3|4} = \frac{1}{4}\left[\mathbb{1} + \frac{1}{\sqrt{3}}(Z - X + Y)\right], \quad (9c)$$

$$A_{4|4} = \frac{1}{4}\left[\mathbb{1} + \frac{1}{\sqrt{3}}(Z + X - Y)\right], \quad (9d)$$

then Q defined by Eq. (4) equals A_4, which is extremal according to the discussion in Sec. VI. The requirement $P(a|A_4) = 1/4$ is also satisfied and, hence, the second test is also fulfilled.

V. PROOF

We now prove that for any quantum state $|\psi\rangle$ generated by Alice's source and shared with Bob and Eve, and for any A_1, A_2, A_3, A_4 local to Alice, B_1, B_2, B_3, B_4 local to Bob, and F local to Eve, if the two tests have been passed, then $\sum_a P(a,a|A_4,F) = 1/4$ and therefore $G = 1/4$.

In Ref. [11], we have shown that a maximal violation of the EBI implies the existence of an isometry $\Phi = \Phi_A \otimes \Phi_B \otimes \mathbb{1}_E$,

$$\begin{aligned}\Phi : \mathcal{H}_A \otimes \mathcal{H}_B \otimes \mathcal{H}_E &\to (\mathcal{H}_A \otimes \mathcal{H}_2) \otimes (\mathcal{H}_B \otimes \mathcal{H}_2) \otimes \mathcal{H}_E \\ &= (\mathcal{H}_A \otimes \mathcal{H}_B \otimes \mathcal{H}_E) \otimes (\mathcal{H}_2 \otimes \mathcal{H}_2),\end{aligned} \quad (10)$$

such that $\Phi(|\psi\rangle) = |\chi\rangle \otimes |\phi_+\rangle$ for some $|\chi\rangle$ in $\mathcal{H}_A \otimes \mathcal{H}_B \otimes \mathcal{H}_E$ and such that

$$\begin{aligned}\Phi(B_1|\psi\rangle) = \frac{1}{\sqrt{3}}\{&|\chi\rangle \otimes [\mathbb{1} \otimes (Z + X)|\phi_+\rangle] \\ &- J|\chi\rangle \otimes (\mathbb{1} \otimes Y|\phi_+\rangle)\},\end{aligned} \quad (11a)$$

$$\begin{aligned}\Phi(B_2|\psi\rangle) = \frac{1}{\sqrt{3}}\{&|\chi\rangle \otimes [\mathbb{1} \otimes (Z - X)|\phi_+\rangle] \\ &+ J|\chi\rangle \otimes (\mathbb{1} \otimes Y|\phi_+\rangle)\},\end{aligned} \quad (11b)$$

$$\begin{aligned}\Phi(B_3|\psi\rangle) = \frac{1}{\sqrt{3}}\{&|\chi\rangle \otimes [\mathbb{1} \otimes (-Z + X)|\phi_+\rangle] \\ &+ J|\chi\rangle \otimes (\mathbb{1} \otimes Y|\phi_+\rangle)\},\end{aligned} \quad (11c)$$

$$\begin{aligned}\Phi(B_4|\psi\rangle) = \frac{1}{\sqrt{3}}\{&|\chi\rangle \otimes [\mathbb{1} \otimes (-Z - X)|\phi_+\rangle] \\ &- J|\chi\rangle \otimes (\mathbb{1} \otimes Y|\phi_+\rangle)\}.\end{aligned} \quad (11d)$$

Here, $\mathcal{H}_A$, $\mathcal{H}_B$, and $\mathcal{H}_E$ are the Hilbert spaces of Alice, Bob, and Eve, $\mathcal{H}_2$ is a two-dimensional Hilbert space with a computational basis $\{|0\rangle, |1\rangle\}$, the state $|\phi_+\rangle$ is the two-qubit singlet state defined in Eq. (6), and J is an involution (i.e., J^2 is the identity) on the support of $\Phi_B \otimes \mathbb{1}_E$ which commutes with every operator local to Eve.

On the support of Φ_A, each $A_{a|4}$, i.e., the element of A_4 corresponding to outcome a, can be represented by an operator R_a acting on $\mathcal{H}_A \otimes \mathcal{H}_2$. If we expand R_a as

$$R_a = R_a^0 \otimes \mathbb{1} + R_a^1 \otimes Z + R_a^2 \otimes X + R_a^3 \otimes Y, \quad (12)$$

where each R_a^k is a Hermitian operator on $\mathcal{H}_A$, then

$$\gamma_a^0 \equiv \langle\psi|A_{a|4}|\psi\rangle = \langle\chi|R_a^0|\chi\rangle, \quad (13a)$$

$$\gamma_a^1 \equiv \frac{\sqrt{3}}{2}\langle\psi|A_{a|4}(B_1 + B_2)|\psi\rangle = \langle\chi|R_a^1|\chi\rangle, \quad (13b)$$

$$\gamma_a^2 \equiv \frac{\sqrt{3}}{2}\langle\psi|A_{a|4}(B_1 + B_3)|\psi\rangle = \langle\chi|R_a^2|\chi\rangle, \quad (13c)$$

$$\gamma_a^3 \equiv -\frac{\sqrt{3}}{2}\langle\psi|A_{a|4}(B_2 + B_3)|\psi\rangle = \langle\chi|R_a^3 J|\chi\rangle. \quad (13d)$$

The family of operators $Q = \{Q_a\}$ on $\mathcal{H}_2$ defined by

$$Q_a = \gamma_a^0\mathbb{1} + \gamma_a^1 Z + \gamma_a^2 X + \gamma_a^3 Y \quad (14)$$

forms an extremal four-outcome POVM by the second test.

The operator J is diagonalizable with eigenvalues -1 and $+1$. We write $J_\pm$ for the orthogonal projections onto its ± 1 eigenspaces. Also, inspired by Acín *et al.*, we define normalized states $|\varphi_{\pm,a}\rangle$ by

$$|\varphi_{\pm,a}\rangle = J_\pm F_a|\chi\rangle/\sqrt{q_{\pm,a}}. \quad (15)$$

Then,

$$\begin{aligned}\gamma_a^k &= \sum_{a'}\langle\chi|F_{a'}J_+R_a^kJ_+F_{a'}|\chi\rangle + \langle\chi|F_{a'}J_-R_a^kJ_-F_{a'}|\chi\rangle \\ &= \sum_{a'} q_{+,a'}\langle\varphi_{+,a'}|R_a^k|\varphi_{+,a'}\rangle + q_{-,a'}\langle\varphi_{-,a'}|R_a^k|\varphi_{-,a'}\rangle \\ &\equiv \sum_{a'} q_{+,a'}\beta_a^{k;+,a'} + q_{-,a'}\beta_a^{k;-,a'},\end{aligned} \quad (16)$$

for $k = 0,1,2$, and

$$\begin{aligned}\gamma_a^3 &= \sum_{a'}\langle\chi|F_{a'}J_+R_a^3J_+F_{a'}|\chi\rangle - \langle\chi|F_{a'}J_-R_a^3J_-F_{a'}|\chi\rangle \\ &= \sum_{a'} q_{+,a'}\langle\varphi_{+,a'}|R_a^3|\varphi_{+,a'}\rangle - q_{-,a'}\langle\varphi_{-,a'}|R_a^3|\varphi_{-,a'}\rangle \\ &\equiv \sum_{a'} q_{+,a'}\beta_a^{3;+,a'} - q_{-,a'}\beta_a^{3;-,a'}.\end{aligned} \quad (17)$$

Here we have, without loss of generality, assumed that F is projective. Next, define four-outcome qubit POVMs $R^{\pm,a'} = \{R_a^{\pm,a'}\}$ as

$$R_a^{+,a'} = \beta_a^{0;+,a'}\mathbb{1} + \beta_a^{1;+,a'}Z + \beta_a^{2;+,a'}X + \beta_a^{3;+,a'}Y, \quad (18a)$$

$$R_a^{-,a'} = \beta_a^{0;-,a'}\mathbb{1} + \beta_a^{1;-,a'}Z + \beta_a^{2;-,a'}X - \beta_a^{3;-,a'}Y. \quad (18b)$$

From Eqs. (16) and (17) follow that $Q_a = \sum_{\pm,a'} q_{\pm,a'}R_a^{\pm,a'}$, which is a convex decomposition of Q. Since Q is extremal,

$R_a^{\pm,a'} = Q_a$ and, hence, $\beta_a^{k;\pm,a'} = \gamma_a^k$ for all a'. In particular, $\beta_a^{0;\pm,a} = \gamma_a^0 = 1/4$ for all a. Now,

$$\begin{aligned}\sum_a P(a,a|A_4,F) &= \sum_a \langle\psi|A_{a|4}F_a|\psi\rangle \\ &= \sum_a \langle\chi|R_a^0 F_a|\chi\rangle \\ &= \sum_a \langle\chi|F_a J_+ R_a^0 J_+ F_a|\chi\rangle \\ &\quad + \langle\chi|F_a J_- R_a^0 J_- F_a|\chi\rangle \\ &= \sum_a q_{+,a}\beta_a^{0;+,a} + q_{-,a}\beta_a^{0;-,a} \\ &= 1/4. \end{aligned} \tag{19}$$

Since we have not assumed anything about Eve's measurement, this proves that $G = 1/4$.

VI. EXTREMAL QUBIT POVMs

POVMs of a fixed number of outcomes form a convex set. Its extremal elements are those that cannot be written as nontrivial convex combinations of other POVMs. D'Ariano *et al.* [6] have classified all extremal POVMs with discrete output sets. According to this classification, a four-outcome qubit POVM is extremal if, and only if, it consists of four linearly independent one-dimensional projectors. The elements of Q defined by Eq. (4) are one-dimensional projectors provided that $\mathrm{tr}\, Q_a > 0$ and $\det Q_a = 0$. The former condition is satisfied if $P(a|A_4) > 0$ and the latter condition is satisfied if

$$\begin{aligned}(E_{a|4,1} + E_{a|4,2})^2 + (E_{a|4,1} + E_{a|4,3})^2 \\ + (E_{a|4,2} + E_{a|4,3})^2 = \tfrac{4}{3}P(a|A_4)^2,\end{aligned} \tag{20}$$

for all a. Moreover, the projectors are linearly independent provided the vectors $[\gamma_a^0\ \gamma_a^1\ \gamma_a^2\ \gamma_a^3]^T$ are linearly independent, where the γ_a^ks are defined as in Eq. (5). Given that $\gamma_a^0 = P(a|A_4) = 1/4$ for all a, this is equivalent to the condition that the matrix of conditional expectation values,

$$\begin{bmatrix} E_{1|4,1} & E_{1|4,2} & E_{1|4,3} \\ E_{2|4,1} & E_{2|4,2} & E_{2|4,3} \\ E_{3|4,1} & E_{3|4,2} & E_{3|4,3} \end{bmatrix}, \tag{21}$$

has full rank.

VII. CONCLUSIONS

We have proven that as conjectured by Acín *et al.* in Ref. [7], the maximal quantum violation of the elegant Bell inequality can be used to certify, in a device-independent way, two bits of randomness from one ebit. This demonstrates how fundamental tools in quantum information, namely, an ebit, a complete set of qubit MUBs, and the elements of qubit SIC-POVMs, are connected to maximal randomness. An open question is whether a certification similar to ours would be possible with fewer measurement settings. If not, this would sharpen the elegance of the protocol and strengthen the surprising connection between complete sets of MUBs and SIC-POVM elements, on one side, and optimal maximal randomness from maximal entanglement, on the other.

Concerning the practical aspects of randomness generation, it should be mentioned that violating different Bell inequalities is not equally costly in terms of statistics [14,15]. Moreover, to certify device-independent generation of more that one random bit from an ebit, it is often better to use a three-outcome POVM rather than a four-outcome POVM since the former is generally more robust against imperfections in the experimental setup [16].

ACKNOWLEDGMENTS

We thank Ingemar Bengtsson for fruitful discussions and for proposing improvements to the text. We also thank Gustavo Cañas for his help with Fig. 1. A.C. acknowledges support from Project No. FIS2014-60843-P, "Advanced Quantum Information" (MINECO, Spain), with FEDER funds, the FQXi Large Grant "The Observer Observed: A Bayesian Route to the Reconstruction of Quantum Theory," and the project "Photonic Quantum Information" (Knut and Alice Wallenberg Foundation, Sweden).

[1] R. Colbeck, Quantum and relativistic protocols for secure multi-party computation, Ph.D. thesis, University of Cambridge, 2006; arXiv:0911.3814.

[2] S. Pironio, A. Acín, S. Massar, A. Boyer de la Giroday, D. N. Matsukevich, P. Maunz, S. Olmschenk, D. Hayes, L. Luo, T. A. Manning, and C. Monroe, Random numbers certified by Bell's theorem, Nature (London) **464**, 1021 (2010).

[3] A. Acín and L. Masanes, Certified randomness in quantum physics, Nature (London) **540**, 213 (2016).

[4] J. S. Bell, On the Einstein Podolsky Rosen Paradox, Physics **1**, 195 (1964).

[5] S. Popescu and D. Rohrlich, The joy of entanglement, in *Introduction to Quantum Computation and Information*, edited by H. Lo, S. Popescu, and T. Spiller (World Scientific, New York, 1998), p. 29.

[6] G. M. D'Ariano, P. L. Presti, and P. Perinotti, Classical randomness in quantum measurements, J. Phys. A: Math. Gen. **38**, 5979 (2005).

[7] A. Acín, S. Pironio, T. Vértesi, and P. Wittek, Optimal randomness certification from one entangled bit, Phys. Rev. A **93**, 040102(R) (2016).

[8] 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).

[9] N. Gisin, Bell inequalities: Many questions, a few answers, in *Quantum Reality, Relativistic Causality, and Closing the Epistemic Circle: Essays in Honour of Abner Shimony*, edited by W. C. Myrvold and J. Christian, The Western Ontario Series in Philosophy of Science Vol. 73 (Springer, Netherlands, 2009), p. 125.

[10] W. K. Wootters, Quantum measurements and finite geometry, Found. Phys. **36**, 112 (2006).

[11] O. Andersson, P. Badziąg, I. Bengtsson, I. Dumitru, and A. Cabello, Self-testing properties of Gisin's elegant Bell inequality, Phys. Rev. A **96**, 032119 (2017).

[12] M. McKague and M. Mosca, Generalized self-testing and the security of the 6-state protocol, in *Theory of Quantum Computation, Communication, and Cryptography*, edited by W. van Dam, V. M. Kendon, and S. Severini, Lecture Notes in Computer Science Vol. 6519 (Springer, Berlin, 2010), p. 113.

[13] M. McKague, Quantum information processing with adversarial devices, Ph.D. thesis, University of Waterloo, 2010; arXiv:1006.2352.

[14] A. Peres, Bayesian analysis of Bell inequalities, Fortschr. Phys. **48**, 531 (2000).

[15] R. D. Gill, Statistics, causality and Bell's theorem, Statist. Sci. **29**, 512 (2014).

[16] S. Gómez, A. Mattar, E. S. Gómez, D. Cavalcanti, O. Jiménez Farías, A. Acín, and G. Lima, Experimental nonlocality-based randomness generation with non-projective measurements, arXiv:1711.10294.