Rapid Communications | Editors' Suggestion

Experimental nonlocality-based randomness generation with nonprojective measurements

S. Gómez,[1,2,3] A. Mattar,[4] E. S. Gómez,[1,2,3] D. Cavalcanti,[4] O. Jiménez Farías,[4] A. Acín,[4,5] and G. Lima[1,2,3]

[1]*Departamento de Física, Universidad de Concepción, 160-C Concepción, Chile*

[2]*Center for Optics and Photonics, Universidad de Concepción, 160-C Concepción, Chile*

[3]*MSI-Nucleus for Advanced Optics, Universidad de Concepción, 160-C Concepción, Chile*

[4]*ICFO-Institut de Ciencies Fotoniques, The Barcelona Institute of Science and Technology, 08860 Castelldefels, Barcelona, Spain*

[5]*ICREA-Institució Catalana de Recerca i Estudis Avançats, Lluis Companys 23, 08010 Barcelona, Spain*

(Received 9 August 2017; published 12 April 2018)

We report on an optical setup generating more than one bit of randomness from one entangled bit (i.e., a maximally entangled state of two qubits). The amount of randomness is certified through the observation of Bell nonlocal correlations. To attain this result we implemented a high-purity entanglement source and a nonprojective three-outcome measurement. Our implementation achieves a gain of 27% of randomness as compared with the standard methods using projective measurements. Additionally, we estimate the amount of randomness certified in a one-sided device-independent scenario, through the observation of Einstein-Podolsky-Rosen steering. Our results prove that nonprojective quantum measurements allow extending the limits for nonlocality-based certified randomness generation using current technology.

DOI: 10.1103/PhysRevA.97.040102

The existence of random processes, besides having philosophical consequences, has applications in many disciplines such as cryptography and simulations of physical, biological, and social phenomena. Mismatches between the modeling and the actual working of random number generators (RNGs) may lead to wrong conclusions. Quantum technologies provide a solution to this problem through device-independent (DI) randomness generation protocols [1–3] built from Bell nonlocal correlations [4,5]. To date, all implementations of DIRNGs used projective measurements on quantum bits [2,6,7], thus being limited to one random bit per round and particle. Here, we report on an optical setup providing more than one random bit per round from one entangled bit [8]. To attain this result, we implement a Bell test involving a nonprojective measurement on an entangled state of high purity. Our work demonstrates the importance of nonprojective measurements to attain the ultimate limits for DIRNG.

The standard scenario for nonlocality-based randomness generation consists of a user, who has access to two quantum measurement devices A and B, which have input choices and provide outputs [3] (see Fig. 1). The user's goal is to certify that the outcomes produced in the experiment are random. We consider the strongest definition of randomness in which the user's outcomes are demanded to be unpredictable not only to her, but to any other observer [3]. This, besides being fundamentally important, guarantees that the obtained randomness is private, a requirement for cryptographic applications [1,2,9]. In the device-independent scenario, nothing is assumed on the inner working of the measurement devices, which are treated as quantum black boxes fed with classical inputs x and y (the measurement choices) and producing classical outputs a and b (the measurement results). After collecting enough statistics, the user's description of the devices is given by the set of conditional probabilities $P(ab|xy)$.

In randomness certification protocols it is assumed that the AB state is the reduced state of a tripartite state $|\Psi\rangle_{\mathrm{ABE}}$ produced by an outsider, Eve, who holds a device E. Moreover, Eve could have prepared the measurement devices, and thus has a complete description of the measurements in A and B. The randomness in the user's outcome a for a particular measurement $x = x^*$ can be estimated through the so-called guessing probability [10,11],

$$P_{\mathrm{guess}} = \max_{\{|\Psi\rangle,\Pi_{a|x},\Pi_{b|y},\Pi_e\}} \sum_a \langle\Psi|\Pi_{a|x^*}\otimes\mathbb{I}\otimes\Pi_{e=a}|\Psi\rangle \quad (1)$$

such that

$$P(ab|xy) = \langle\Psi|\Pi_{a|x}\otimes\Pi_{b|y}\otimes\mathbb{I}|\Psi\rangle. \quad (2)$$

This quantity gives the maximum probability that E's outcome e matches the user's outcome a for measurement x^* over all possible quantum realizations, described by a tripartite quantum state $|\Psi\rangle$ and measurements $\Pi_{a|x}$, $\Pi_{b|y}$, and Π_e for devices A, B, and E, compatible with the observed distribution $P(ab|xy)$. The guessing probability can be upper bounded by semidefinite programming (SDP) techniques [10,11]. The estimated randomness can be expressed in bits through $R = -\log_2(P_{\mathrm{guess}})$. In order to guarantee some amount of randomness, the user's observed correlations must be nonlocal, that is, violate a Bell inequality. If this is not the case, they can be reproduced by a local and deterministic model and therefore $P_{\mathrm{guess}} = 1$ [3].

The main motivation of this Rapid Communication is to probe the ultimate limits for randomness certification using quantum resources. In order to observe a Bell violation between A and B, the user's state must be entangled. If the state is of two qubits and the measurements are projective, as in standard Bell experiments, one cannot certify more than one random bit from each qubit. However, this is no longer the case if one uses nonprojective measurements [8]. We report here a photonic experiment demonstrating how nonprojective measurements offer a significant advantage in a Bell scenario and allow one to certify more than one random bit from a qubit.

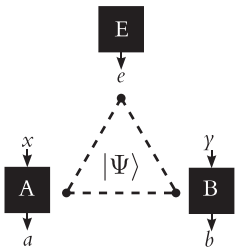

FIG. 1. Device-independent randomness generation scenario: A user applies uncharacterized measurements x and y to two devices A and B, obtaining outcomes a and b, respectively. In the experiment, the user assumes that the state of the two devices A and B is the reduced state of a pure tripartite quantum state $|\Psi\rangle$ correlated with an adversarial party, Eve, who holds device E. No further assumption is made on Eve, who could have a complete description not only of this quantum state, but also of all the measurements performed on it. In order to guess the outcomes produced in the experiment, Eve applies a measurement to her device E that produces outcomes e. Without loss of generality, this outcome can be seen as Eve's guess on the user's results.

Our experiment is similar to a standard Bell test using photons entangled in polarization [see Fig. 2(a)]. However, we need to solve two experimental challenges that make it unique with respect to previous experiments and that are crucial to achieve the certification of more than one random bit. First, we need to prepare a highly entangled state providing a very high two-photon visibility. To achieve this, we use an ultrabright spontaneous parametric down-conversion source, where a type-II nonlinear periodically poled potassium titanyl phosphate (PPKTP) crystal is pumped by a continuous-wave 405-nm laser to generate 810-nm polarization-entangled photons [13–17]. The nonlinear crystal is placed inside an intrinsically phase-stable Sagnac interferometer, which is composed of two laser mirrors, a half-wave plate (HWP), and a polarizing beam-splitter (PBS) cube. The clockwise and counterclockwise propagating modes of the generated pair of photons overlap inside the interferometer, resulting in the biphoton Bell state $|\psi^-\rangle = (|HV\rangle - |VH\rangle)/\sqrt{2}$. We carefully control the spatial and spectral modes of the generated photons. Semrock high-quality (peak transmission >90%) narrow bandpass [full width at half maximum (FWHM) of 0.5 nm] filters centered at 810 nm are used to ensure that phase-matching conditions are achieved with the horizontal and vertical polarization modes at degenerated frequencies. Then, we enforce path indistinguishability of the photon pair modes (HV and VH) by coupling the generated down-converted photons into single-mode fibers (SMFs) after being transmitted by the PBS. We also adopt high-quality polarizing optics components to ensure a polarization extinct ratio greater than $10^7 : 1$. This guarantees that the two-photon visibility is not limited by the polarization contrast of the detection apparatuses. Then, we use high-resolution coincidence field programmable gate array electronics to implement 500-ps coincidence windows, thus drastically reducing the accidental coincidence count probability to less than 10^{-5} (PerkinElmer single-photon avalanche detectors with an overall detection efficiency of 15% were used). Owing to these measures, we attain a high overall two-photon visibility of $(99.7 \pm 0.2)\%$.

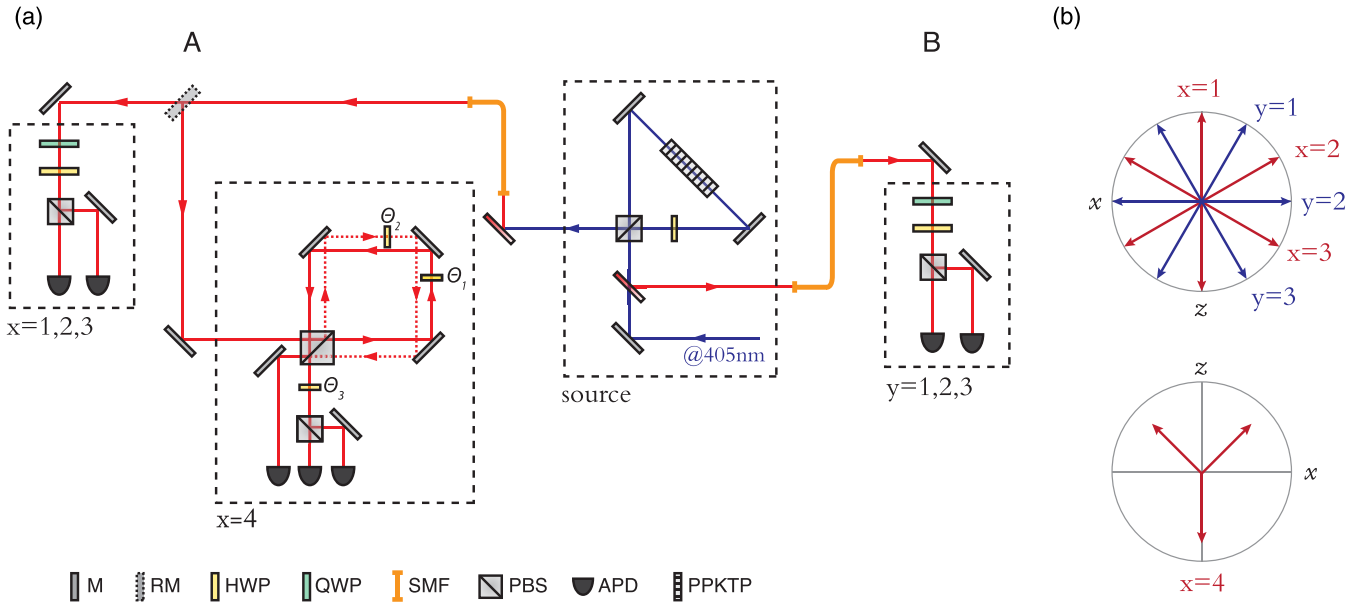

FIG. 2. (a) Our experimental setup is composed of an ultrabright parametric down-conversion source (see main text) generating a near-perfect $|\psi^-\rangle = (|HV\rangle - |VH\rangle)/\sqrt{2}$ polarization state, followed by polarization measurements in each photon. The measurements $x, y = 1,2,3$ have binary outcomes and are implemented using a quarter-wave plate (QWP), a HWP, and a PBS, followed by avalanche photodiode detectors (APDs). A removable mirror (RM) allows one to select between measurements $x = 1,2,3$ and $x = 4$. The fourth and nonprojective measurement, $x = 4$, performed by device A is implemented by a double-path Sagnac interferometer. (b) Bloch sphere representation of the measurements performed in A and B. The measurements labeled by $x, y = 1,2,3$ are given by symmetrically spaced two-outcome (projective) measurements in the x-z plane, and correspond to the settings required to maximally violate the chained Bell inequality [12]. Measurement $x = 4$ has three outcomes, corresponding to Bloch vectors equally spaced in the x-z plane.

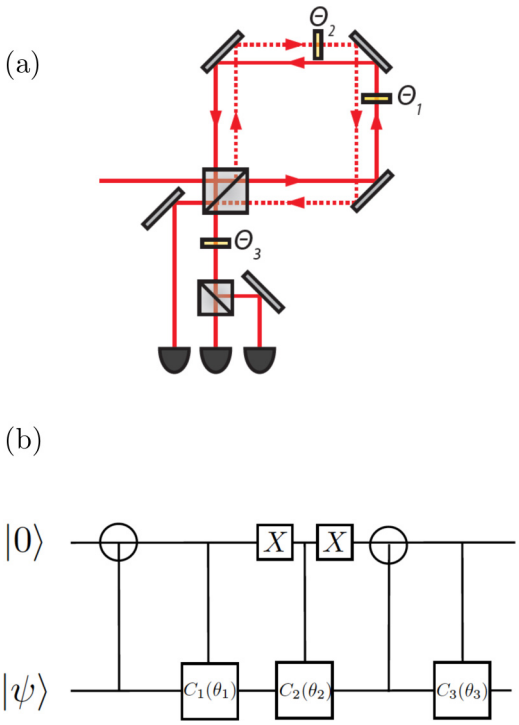

FIG. 3. (a) The Sagnac interferometer used to implement the three-outcome POVM. (b) shows the corresponding quantum circuit.

Last, we resort to an active power control system to stabilize the pump beam incident power. This minimizes signaling in the recorded data as the marginal counts are kept stable over the entire data acquisition procedure.

Second, and contrary to standard Bell tests, our experiment consists not only of projective measurements, but involves a nonprojective measurement defined by a positive-operator-valued measure (POVM). Indeed, while device B applies three projective measurements (labeled by $y = 1,2,3$), device A can implement three projective measurements ($x = 1,2,3$) plus a POVM measurement ($x = 4$) of three outcomes. All projective measurements are implemented by usual polarization analyzers. The nonprojective measurement used in our experiment consists of three outcomes, associated with POVM elements $\Pi_i = \frac{2}{3}|\psi_i\rangle\langle\psi_i|$, where

$$\begin{aligned} |\psi_0\rangle &= |V\rangle, \\ |\psi_1\rangle &= -\tfrac{1}{2}(|V\rangle + \sqrt{3}|H\rangle), \\ |\psi_2\rangle &= -\tfrac{1}{2}(|V\rangle - \sqrt{3}|H\rangle). \end{aligned} \tag{3}$$

This measurement is obtained in our setup by coherently coupling to additional spatial modes through the Sagnac intereferometer in Fig. 3(a).

We consider the polarization basis for the single photon $\{|H\rangle,|V\rangle\}$ and two spatial modes $\{|0\rangle,|1\rangle\}$ created by the polarizing beam splitter (PBS) which defines the Sagnac interferometer. The action of the interferometer can be better understood by the quantum circuit in Fig. 3(b): A single photon with polarization $|\psi\rangle$ enters through port $|0\rangle$ of the PBS and populates the spatial modes according to

$$\begin{aligned} |H\rangle|0\rangle &\to |H\rangle|0\rangle, \\ |V\rangle|0\rangle &\to |V\rangle|1\rangle. \end{aligned} \tag{4}$$

The input port $|1\rangle$ is fed with vacuum, but an analogous analysis of its working completes the specification of the controlled-NOT (CNOT) gate implemented by the PBS. Once inside the interferometer, half-wave plates at angles θ_1 and θ_2 rotate polarization depending on the spatial mode of the photon. That is, internal half-wave plates implement controlled operations $C_1(\theta_1)$ controlled by the state $|0\rangle$ and $C_2(\theta_2)$. A new passage through the same PBS implements a second CNOT gate controlled by the polarization. Finally, we insert a half-wave plate on output mode $|0\rangle$ at θ_3 implementing the controlled operation $C_3(\theta_3)$.

The total unitary transformation which couples polarization with spatial modes is given

$$U = C_3(\theta_3) \cdot \text{CNOT} \cdot C_2(\theta_2) \cdot C_1(\theta_1) \cdot \text{CNOT}. \tag{5}$$

The coupling matrix (5) followed by detection in spatial modes defines a family of POVMs in polarization parametrized by θ_1, θ_2, and θ_3. In order to obtain this extremal POVM we chose the settings $\theta_1 = 0, \theta_2 = 2\sin\sqrt{2/3}$, and $\theta_3 = \pi/2$. With these settings, the effect of U on the states $\{|\psi_0\rangle,|\psi_1\rangle,|\psi_2\rangle\}$ of Eq. (4) is

$$\begin{aligned} |\psi_0\rangle &\to \sqrt{1/6}|0\rangle|H\rangle + \sqrt{1/6}|0\rangle|V\rangle + \sqrt{2/3}|1\rangle|V\rangle, \\ |\psi_1\rangle &\to \sqrt{2/3}|0\rangle|H\rangle + \sqrt{1/6}|0\rangle|V\rangle + \sqrt{1/6}|1\rangle|V\rangle, \\ |\psi_2\rangle &\to \sqrt{1/6}|0\rangle|H\rangle + \sqrt{2/3}|0\rangle|V\rangle + \sqrt{1/6}|1\rangle|V\rangle. \end{aligned} \tag{6}$$

By inserting a PBS in the outcome mode $|0\rangle$ we obtain the three outcome ports with the measurement statistics defining the desired POVM.

We also notice that in our work we invoke the fair-sampling assumption [5], which we use to discard the no-detection events. This assumption is highly debatable in DI cryptographic applications, in which two distant users are connected by a channel whose losses can be simulated by an eavesdropper. But note that it is less critical in DIRNG protocols in which the two devices are in the same location and under the control of an honest user.

Using the estimated visibilities we first run a numerical search to find measurements that maximize the amount of randomness generated in our scenario. This search led us to the measurement settings shown in Fig. 2(b). By implementing these measurements we obtained a collection of observed experimental frequencies $f(ab|xy)$. The raw data obtained from measurements are available in Ref. [18]. Retrieving the amount of randomness from these data is not straightforward because the probability distributions $P(ab|xy)$ obtained upon normalizing these frequencies are ill defined due to the finite statistics regime intrinsic to any implementation. For instance, they do not satisfy the no-signaling conditions (satisfied in quantum mechanics) defined by $\sum_b P(ab|xy) = \sum_b P(ab|xy')$ (no signaling from B to A) and $\sum_a P(ab|xy) = \sum_a P(ab|x'y)$ (no signaling from A to B). In order to circumvent this problem we use the following steps. From the experimental frequencies $f(ab|xy)$ we generated a set of no-signaling probability distributions $P_{NS} = \{P_{NS}(ab|xy)\}$ through the Collins-Gisin parametrization of the space of probabilities [19]. By considering marginal probabilities $P(a|x,y=1)$ and $P(b|x=1,y)$, the Collins-Gisin representation enforces the no-signaling constraints of P by dropping all probabilities involving the

last outcome of all measurements. For instance, for the POVM that has three outcomes, the probability $P_{NS}(a=3,b|xy)$ is implicitly set by imposing $P_{NS}(a=3,b|xy) = P(a=3|x, y=1) - P(a=2,b|xy) - P(a=1|xy)$. With P_{NS} we run the semidefinite (SDP) program proposed in Refs. [10,11], that provides an upper bound to the guessing probability (1),

$$P_{\text{guess}} = \max_{\{P(abe|xy)\}} P(a=e|x^*), \tag{7}$$

such that

$$P(ab|xy) = \sum_e P(a,b,e|x,y) \quad \forall a,b,x,y, \tag{8}$$

$$P(abe|xy) \geqslant 0 \quad \forall a,b,e,x,y, \tag{9}$$

$$\sum_{abe} P(abe|xy) = 1 \quad \forall x,y, \tag{10}$$

$$\{P(a,b,e|x,y)\}_{a,b,e,x,y} \in \mathcal{Q}_2. \tag{11}$$

This expression gives the maximum probability that Eve's outcomes match Alice's, given that the distributions observed are marginals of a joint tripartite distribution with Eve. The last constraint means that the joint distributions lie in the set $\mathcal{Q}_2$, an outer approximation to the set of quantum probability distributions $\mathcal{Q}$ proposed in Ref. [20]. The solution of this SDP optimization provides a linear function $S(P)$ whose value is a lower bound on the amount of randomness of any set of distributions P. We finally rewrite S in terms of expected values and use it to estimate the amount of randomness in our experiment. The errors of the recorded probabilities are calculated assuming fair samples from Poissonian distributions and Gaussian error propagation. We note that our statistical analysis considers the asymptotic limit of many experimental runs. A more detailed statistical method considering finite statistics [2,7,21,22] is beyond the scope of this work.

After these steps we were able to certify

$$R^{\text{DI}}_{\text{POVM}} = 1.18 \pm 0.08 \tag{12}$$

bits of randomness per use of the devices. As a matter of comparison we also performed the same analysis in the case where Alice and Bob use only the projective measurements $x,y = 1,2,3$ and randomness is obtained from the setting $x=1$. In this case, $R^{\text{DI}}_{\text{proj}} = 0.93 \pm 0.08$. Thus, the addition of a three-outcome nonprojective measurement provided a gain of 27% of randomness.

In our setup, we can also certify randomness in a semidevice-independent scenario in which device B is assumed to be fully characterized. In this scenario, randomness can be certified by the presence of quantum steering [23], a situation where box A is still treated as a black box with inputs x and outputs a, while B is assumed to be able to make tomography of the conditional states $\rho^B_{a|x}$. The information the user has in this situation can be summarized in the set of unnormalized quantum sates $\{\sigma^B_{a|x}\}_{a,x}$, where $\sigma^B_{a|x} = p(a|x)\rho^B_{a|x}$. Notice that, in order to obtain a set $\{\sigma^B_{a|x}\}_{a,x}$ that satisfies the no-signaling conditions $\sum_a \sigma^B_{a|x} = \sum_a \sigma^B_{a|x'}$, we also need to resort to the distributions P_{NS} obtained through the Collins-Gisin parametrization. Given the knowledge of $\{\sigma_{a|x}\}_{a,x}$, Alice and Bob can estimate the amount of randomness in Alice's outcomes through the following semidefinite program [24],

$$P_{\text{guess}}(x^*) = \max_{\{\sigma^e_{a|x}\}} \text{Tr} \sum_e \sigma^e_{a=e|x^*} \tag{13}$$

such that

$$\sum_e \sigma^e_{a|x} = \sigma_{a|x} \quad \forall a,x, \tag{14}$$

$$\sum_a \sigma^e_{a|x} = \sum_a \sigma^e_{a|x'} \quad \forall e,x,x', \tag{15}$$

$$\sigma^e_{a|x} \geqslant 0 \quad \forall a,x,e. \tag{16}$$

Once more, the solution to this program gives a linear function (a quantum steering inequality) of the experimental data that can be used to calculate the guessing probability and appropriate errors. The amount of randomness can be calculated in a similar manner as in (1) [24] and, in this case, we were able to certify $R^{\text{St}}_{\text{POVM}} = 1.27 \pm 0.14$.

In the context of certified RNG protocols, our work is relevant both from a fundamental and applied perspective, as it demonstrates how the more general class of nonprojective quantum measurements allows extending the limits for nonlocality-based certified randomness generation using current technology. In the scenario of device-independent quantum information processing, we show that a gain of 27% in the rate of random bit string generation is possible. In the case of semidevice-independent RNG protocols, we demonstrate that this gain can be improved to 36%.

We thank A. Cabello, T. Vértesi, and M. Pawlowski for discussions. This work was supported by the Ramón y Cajal fellowship, Spanish MINECO (QIBEQI FIS2016-80773-P and Severo Ochoa SEV-2015-0522), the AXA Chair in Quantum Information Science, Generalitat de Catalunya (SGR875 and CERCA Programme), Fundació Privada Cellex, Fondecyt 1160400, CONICYT PFB08-024, and Milenio RC130001. E.S.G. acknowledges support from Fondecyt 11150325. S.G. acknowledges CONICYT.

[1] R. Colbeck, Ph.D. thesis, University of Cambridge, 2006 (unpublished).

[2] S. Pironio, A. Acín, S. Massar, B. de la Giroday, D. Matsukevich, P. Maunz, S. Olmschenk, D. Hayes, L. Luo, T. Manning *et al.*, Nature (London) **464**, 1021 (2010).

[3] A. Acín and L. Masanes, Nature (London) **540**, 213 (2016).

[4] J. S. Bell, Physics **1**, 195 (1964).

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

[6] B. G. Christensen, K. T. McCusker, J. B. Altepeter, B. Calkins, T. Gerrits, A. E. Lita, A. Miller, L. K. Shalm, Y. Zhang, S. W. Nam *et al.*, Phys. Rev. Lett. **111**, 130406 (2013).

[7] P. Bierhorst, E. Knill, S. Glancy, A. Mink, S. Jordan, A. Rommal, Y.-K. Liu, B. Christensen, S. W. Nam, and L. K. Shalm, arXiv:1702.05178.

[8] A. Acín, S. Pironio, T. Vértesi, and P. Wittek, Phys. Rev. A **93**, 040102(R) (2016).
[9] R. Colbeck and A. Kent, J. Phys. A: Math. Theor. **44**, 095305 (2011).
[10] O. Nieto-Silleras, S. Pironio, and J. Silman, New J. Phys. **16**, 013035 (2014).
[11] J.-D. Bancal, L. Sheridan, and V. Scarani, New J. Phys. **16**, 033011 (2014).
[12] P. M. Pearle, Phys. Rev. D **2**, 1418 (1970).
[13] T. Kim, M. Florentino, and F. N. C. Wong, Phys. Rev. A **73**, 012316 (2006).
[14] F. N. C. Wong, J. H. Shapiro, and T. Kim, Laser Phys. **16**, 1517 (2006).
[15] A. Fedrizzi, T. Herbst, A. Poppe, T. Jennewein, and A. Zeilinger, Opt. Express **15**, 15377 (2007).
[16] D. Ljunggren and M. Tengner, Phys. Rev. A **72**, 062301 (2005).
[17] E. S. Gómez, S. Gómez, P. González, G. Cañas, J. F. Barra, A. Delgado, G. B. Xavier, A. Cabello, M. Kleinmann, T. Vértesi *et al.*, Phys. Rev. Lett. **117**, 260401 (2016).
[18] https://github.com/mattarcon2tes/MoreThanOneBit.
[19] D. Collins and N. Gisin, J. Phys. A: Math. Gen. **37**, 1775 (2004).
[20] M. Navascués, S. Pironio, and A. Acín, Phys. Rev. Lett. **98**, 010401 (2007).
[21] Y. Zhang, S. Glancy, and E. Knill, Phys. Rev. A **84**, 062118 (2011).
[22] P.-S. Lin, D. Rosset, Y. Zhang, J.-D. Bancal, and Y.-C. Liang, Phys. Rev. A **97**, 032309 (2018).
[23] H. M. Wiseman, S. J. Jones, and A. C. Doherty, Phys. Rev. Lett. **98**, 140402 (2007).
[24] E. Passaro, D. Cavalcanti, P. Skrzypczyk, and A. Acín, New J. Phys. **17**, 113010 (2015).