Experimental Tests of Classical and Quantum Dimensionality

Johan Ahrens,[1] Piotr Badziąg,[1] Marcin Pawłowski,[2,3] Marek Żukowski,[2] and Mohamed Bourennane[1]
[1]*Department of Physics, Stockholm University, S-10691, Stockholm, Sweden*
[2]*Instytut Fizyki Teoretycznej i Astrofizyki, Uniwersytet Gdański, PL-80-952 Gdańsk, Poland*
[3]*Department of Mathematics, University of Bristol, Bristol BS8 1TW, United Kingdom*

(Received 8 October 2013; published 7 April 2014; corrected 13 October 2014)

We report on an experimental test of classical and quantum dimension. We have used a dimension witness that can distinguish between quantum and classical systems of dimensions two, three, and four and performed the experiment for all five cases. The witness we have chosen is a base of semi-device-independent cryptographic and randomness expansion protocols. Therefore, the part of the experiment in which qubits were used is a realization of these protocols. In our work we also present an analytic method for finding the maximum quantum value of the witness along with corresponding measurements and preparations. This method is quite general and can be applied to any linear dimension witness.

DOI: 10.1103/PhysRevLett.112.140401 PACS numbers: 03.65.Ud, 03.67.Mn, 42.50.Xa

Classical and quantum dimensions are fundamental quantities in information processing. In particular, security of many cryptographic schemes [1–3] crucially relies on the dimensional characteristics of the information carriers. The concept of a quantum dimension witness was first introduced for the dimension of the Hilbert space of composite systems tested locally [4]. Later, a device-independent dimension witness was introduced in [5] and the robustness of such witnesses was analyzed in [6]. More recently the device-independent dimension witnesses were realized experimentally [7,8].

Apart from testing the dimension of a system, the witnesses can also have a more practical application: semi-device-independent protocols. In these scenarios we do not make any assumptions about the devices that the parties involved are using, but we do assume an upper bound on the dimension of the systems communicated. This setting provides a good compromise between fully device-independent protocols and ones with complete knowledge of the devices because it makes implementation much easier than in the first case and provides better security than in the second. The notion of semi-device independence was introduced in [2] in the context of cryptography and was later developed for randomness expansion in [3,9,10] and for quantum state discrimination in [11]. These applications require witnesses based on quantum random access codes [12,13]. The witnesses realized in [7,8] do not have this property.

In this work we analytically study and then experimentally realize a dimension witness inspired by the Clauser-Horne-Shimony-Holt (CHSH) inequality [14]. First we derive the bounds for the classical and quantum systems of dimensions two, three, and four (the witness is saturated by a four-level system and cannot make distinction for higher dimensions). Later we describe the experimental setup and present the results. Finally, we remark on how the test for quantum dimension two, which we have conducted, would perform as a realization of a semi-device-independent Quantum Key Distribution or randomness expansion protocol.

The scenario that we consider is schematically illustrated in Fig. 1. There is a state preparer with N buttons; it emits a particle in a state ρ_x (specified by the device's supplier) when button $x \in \{1, \ldots, N\}$ is pressed. For testing, the emitted particles are sent to a measurement device, with m buttons. When button $y \in \{1, \ldots, m\}$ is pressed, the device performs measurement M_y on the incoming particle. The measurement produces outcome $b \in \{-1, +1\}$. A complete test should yield probability distributions $P(b|x, y)$ for obtaining result b in measurement M_y on state ρ_x. Suitable combinations of the experimental probabilities $P(b|x, y)$ can then be compared with the theoretical classical and quantum bounds of the dimension witness.

Dimension of a system is defined as the number of distinguishable states. In classical information theory the states of a system are values of bits or trits and are all perfectly distinguishable. Therefore, the classical dimension of a bit is $d_c = 2$, of a trit, $d_c = 3$, and of a pair of bits, $d_c = 4$. In the quantum case the dimension d_q is simply the dimension of the Hilbert space. For our tests of the lower bounds for d_c and d_q, we utilize the dimension witnesses of the type introduced in [5]. These witnesses use as primary quantities the expectation values

$$E_{xy} = P(+1|x, y) - P(-1|x, y). \tag{1}$$

In our test we use a CHSH-inspired combination of these expectation values, which we denote D_{CHSH}. We call it CHSH inspired because it can be obtained from the CHSH inequality using the method described in [10]. It involves four states ($N = 4$) and uses two dichotomic measurements ($m = 2$),

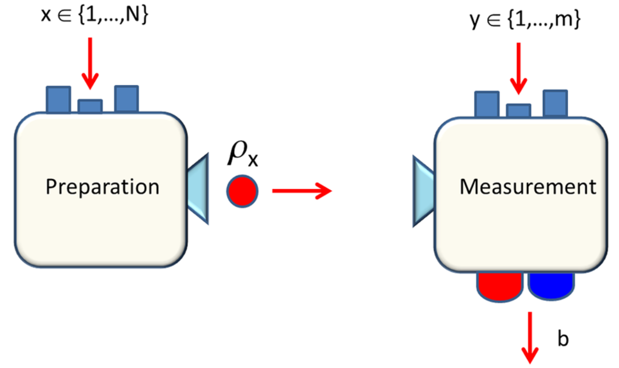

FIG. 1 (color online). Device-independent scenario for testing the minimum classical or quantum dimension. When button $x \in \{1, \ldots, N\}$ is pressed, a state preparer part of the setup, with N buttons, emits a particle in a state ρ_x. This particle is sent to a measurement device with m buttons. When button $y \in \{1, \ldots, m\}$ is pressed, the device performs measurement M_y on the particle. The measurement produces outcomes $b \in \{-1, +1\}$.

$$D_{\mathrm{CHSH}} \equiv (E_{11} + E_{12}) - (E_{21} + E_{22}) + (E_{31} - E_{32}) - (E_{41} - E_{42}) \leq \lambda_d. \tag{2}$$

The upper bound λ_d further on will be denoted as C_d and Q_d for classical and quantum cases, respectively. The subscript d denotes the dimension. Classical ensembles allow for statistical mixtures of identical or fully distinguishable states only. Quantum ensembles permit pure states, which are neither identical nor orthogonal to each other. Since classical ensembles are more restricted than quantum, one immediately notices that $C_d \leq Q_d$.

To find the classical bounds C_d, notice that, due to the linearity of D_{CHSH}, only deterministic strategies need to be considered. The preparer sends deterministic messages, but is constrained by the dimension of the system. Thus, a classical d_c dimensional system can be linked with d_c different two bit messages, each bit determining the system's behavior for a given setting y of the receiver. Each such message can be put in the form of a two-dimensional vector $\vec{v}^x$, with components $\vec{v}^x_y = \pm 1$ giving the output of the receiver, for the given message/preparation x. The classical deterministic value of (2) is

$$D_{\mathrm{CHSH}} = \vec{v}^1 \cdot (1, 1) + \vec{v}^2 \cdot (-1, -1) + \vec{v}^3 \cdot (1, -1) + \vec{v}^4 \cdot (-1, 1). \tag{3}$$

If a vector $\vec{v}^x$ is equal to the vector that enters the given scalar product with it, their product is 2. If they differ in one component, this product is 0. If they differ in two, the product is -2. Thus, if all four $\vec{v}^x$ are different, and each is equal to the vector by which it is scalarly multiplied in (3), the value of D_{CHSH} can reach 8. Thus, $d_c = 4$ implies $C_4 = 8$. If there are only three different values of $\vec{v}^x$, then at most three of the terms in (3) can be 2. Thus, $C_3 = 6$. For $d_c = 2$ we have $C_2 = 4$.

For the quantum bounds, the relevant measuring operators for $d = 2$ and $d = 3$ must obey the following:

Lemma 1. To find the maximal quantum value of any linear dimension witness, based on binary outcomes, given by

$$W_D = \sum_{x=1}^{N} \sum_{y=1}^{m} \sum_{s=\pm 1} K_{(x,y,s)} P(s|x, y), \tag{4}$$

where $K_{(x,y,s)}$ are some real coefficients, it is sufficient to consider only pure states and projective measurements.

Proof. Since any mixed state is as a convex combination (probabilistic mixture) of pure ones, the value of the part of a dimension witness corresponding to such a state is equal to a probabilistic average of the values for the pure states. Therefore, it cannot be greater than the largest value entering this sum. Thus, the maximal value is achieved for pure states. We only need to prove that projective measurements are sufficient. The most general form of measurement is a positive operator value measurement (POVM). If there are only two outcomes, a POVM measurement consists of a pair of positive operators that sum up to identity. We denote them $\mathcal{O}^y_+$ and $\mathcal{O}^y_- = \mathbb{1} - \mathcal{O}^y_+$. Obviously, $\mathcal{O}^y_+$ and $\mathcal{O}^y_-$ commute. Thus, they can be simultaneously diagonalized. Therefore, we can write them as $\mathcal{O}^y_- = \sum_{j=1}^{d} c^y_j |j\rangle\langle j|$ and $\mathcal{O}^y_+ = \sum_{j=1}^{d} (1 - c^y_j)|j\rangle\langle j|$, where $|j\rangle$'s form the diagonalizing basis (d is the dimension of the system). Obviously, $0 \leq c_i \leq 1$. The probability of obtaining outcome $s = \pm 1$ when measuring a system in pure state ψ_x is $P(s|x, y) = \langle \psi_x | \mathcal{O}^y_s | \psi_x \rangle$, where $|\psi_x\rangle$ is the quantum state sent by the preparer.

The dimension witness is a sum of terms corresponding to different measurements. Such terms corresponding to a specific measurement setting y are given by

$$\sum_x K(x, y, +1) \langle \psi_x | \mathcal{O}^y_+ | \psi_x \rangle + \sum_x K(x, y, -1) \langle \psi_x | \mathcal{O}^y_- | \psi_x \rangle = k_0 + \sum_j c_j k_j. \tag{5}$$

The coefficients k_0 and k_j can be easily calculated, but their actual values are irrelevant. What is relevant is the fact that the final formula is linear in c_i's. The maximal value of this expression is reached when c_j's reach their boundary values, i.e., are equal to 1 or 0. In all such cases, $\mathcal{O}^y_\pm$ are projectors. Q.E.D.

Projective dichotomic measurements for any dimension of eigenvalues ± 1 are represented by operators of the form

$$M_i = \mathbb{1} - 2|m_i\rangle\langle m_i|, \tag{6}$$

where $\mathbb{1}$ denotes the identity matrix. In both cases of dimensions two and three, and just two dichotomic operators ($i = 1, 2$), one can always find such a specific basis in which the states linked with eigenvalues -1 can be put as

$$|m_{1,2}\rangle = \cos\left(\frac{\theta}{2}\right)|1\rangle \mp \sin\left(\frac{\theta}{2}\right)|2\rangle. \tag{7}$$

In the case of qutrits, this is so because $|m_i\rangle$ span a two-dimensional subspace, and one can define the basis state $|0\rangle$ as being orthogonal to it. Moreover, the expectation value of D_{CHSH} can be written as

$$\langle\psi_1|(M_1+M_2)|\psi_1\rangle - \langle\psi_2|(M_1+M_2)|\psi_2\rangle + \langle\psi_3|(M_1-M_2)|\psi_3\rangle - \langle\psi_4|(M_1-M_2)|\psi_4\rangle. \tag{8}$$

The optimization can thus be reduced to finding the maximum of the sum of the differences between the maximum and minimum eigenvalues of M_1+M_2 and M_1-M_2 with

$$M_1+M_2 = 2[\mathbb{1} - (1+\cos\theta)|1\rangle\langle 1| - (1-\cos\theta)|2\rangle\langle 2|] \tag{9}$$

and

$$M_1-M_2 = 4\cos\left(\frac{\theta}{2}\right)\sin\left(\frac{\theta}{2}\right)[|1\rangle\langle 2| + |2\rangle\langle 1|]. \tag{10}$$

For $d=2$, the Hilbert space is spanned by vectors $|1\rangle$ and $|2\rangle$. This gives

$$M_1+M_2 = 2\,\cos(\theta)[|2\rangle\langle 2| - |1\rangle\langle 1|] \tag{11}$$

and

$$M_1-M_2 = 2\,\sin(\theta)[|1\rangle\langle 2| + |2\rangle\langle 1|], \tag{12}$$

and without loss of generality one can choose $\cos(\theta)\geq 0$ and $\sin(\theta)\geq 0$. This fixes the optimal states to

$$|\psi_1\rangle = |2\rangle, \tag{13a}$$

$$|\psi_2\rangle = |1\rangle, \tag{13b}$$

$$|\psi_3\rangle = \frac{1}{\sqrt{2}}(|1\rangle + |2\rangle), \tag{13c}$$

$$|\psi_4\rangle = \frac{1}{\sqrt{2}}(|1\rangle - |2\rangle), \tag{13d}$$

and reduces the optimization to finding the maximum value of $4(\cos(\theta)+\sin(\theta))\leq 4\sqrt{2}$. The bound is achieved for $\theta=\pi/4$. Thus the qubit bound for D_{CHSH} is $Q_2 = 4\sqrt{2}\sim 5.66$.

For $d=3$, the Hilbert space is spanned by vectors $|0\rangle$ and $|1\rangle$ and $|2\rangle$, and the sum M_1+M_2 is

$$M_1+M_2 = 2[|0\rangle\langle 0| + \cos(\theta)(|2\rangle\langle 2| - |1\rangle\langle 1|)]. \tag{14}$$

Thus the optimal $|\psi_1\rangle$ becomes $|0\rangle$. Determination of the bound of D_{CHSH} for qutrits is thus reduced to the maximization of $(2+2\cos\theta+4\sin\theta)\leq 2(1+\sqrt{5})$, which is achieved for $\tan(\theta)=2$. Thus the qutrit bound for D_{CHSH} is $Q_3 = 2(1+\sqrt{5})\sim 6.47$.

Note that due to our lemma, if a qubit enters our device, for example, then measurements of degenerate dichotomic observables of dimension larger than two constitute POVM measurements on a qubit (by Naimark theorem). Thus, in such a case the qubit limit in the inequality cannot be violated.

In general, the dimension testing protocol could be put as follows. A state preparer claims that his/her systems are of certain classical or quantum dimension, and the emitted systems are tested with observables selected in such a way that they are compatible with the claim. If, for example, the claim is that the system is qutrit, and the bound for qubits is violated, then the system is of a higher dimension than two. If the value is close to the bound for qutrits, we can safely conclude that the system has such a dimension as declared, and imperfections do not allow perfect saturation of the bound. Of course the system may be of even higher dimensionality, and in a more noisy state. Thus we effectively test the minimal dimension of the system provided by the preparer.

Let us now move to our experimental realization of the dimension indicator.

The preparer uses a preparation device (see the preparation device frame in Fig. 2), which encodes the information in four basis states: $|1\rangle\equiv|V,a\rangle$, $|2\rangle\equiv|H,a\rangle$, $|3\rangle\equiv|V,b\rangle$, and $|0\rangle\equiv|H,b\rangle$, where (H) and (V) are horizontal and vertical polarization photonic modes, respectively, and (a and b) are two spatial photonic modes. Any qutrit state can be written as $\alpha|H,a\rangle+\beta|V,a\rangle+\gamma|H,b\rangle$, and any qubit state can be represented by $\alpha|H,a\rangle+\beta|V,a\rangle$. The photonic states were prepared by

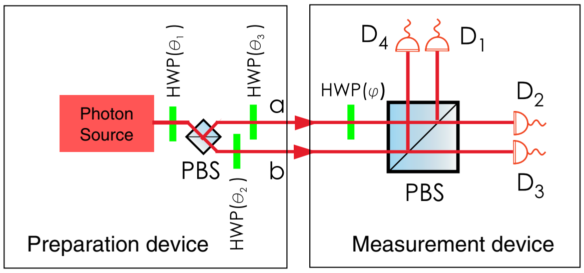

FIG. 2 (color online). Experimental setup for a witness testing classical and quantum dimensions.The state preparer is a single photon source emitting horizontally polarized photons that, after passing through three half-wave plates (HWP) suitably oriented at angles θ_i (with $i=1,2,3$), are prepared in the required states. Information is encoded in horizontal and vertical polarizations, and in two spatial modes. The probabilities needed for the dimension witnesses D_{CHSH} are obtained from the number of detections in the detectors D_i, after properly adjusting the orientation φ of the half-wave plate on the measurement side of the setup.

three suitably oriented half-wave plates HWP(θ_1), HWP(θ_2), and HWP(θ_3), such that

$$|\psi\rangle = \sin(2\theta_1)\sin(2\theta_3)|H,a\rangle - \sin(2\theta_1)\cos(2\theta_3)|V,a\rangle + \cos(2\theta_1)\cos(2\theta_2)|H,b\rangle + \cos(2\theta_1)\sin(2\theta_2)|V,b\rangle. \quad (15)$$

Thus, by adjusting the orientation angles θ_i of the HWP (θ_i), we can produce any of the required states. In the experiment, classical sets (bits, trits, quarts) consisted of states that were perfectly distinguishable or identical.

The tester can use a different operational approach but with a single measurement device, depending on the claim of the preparer, and test whether the bounds are violated. To implement M_i, the HWP is set in such a way that the eigenstate $|m_i\rangle$, which corresponds to the -1 eigenvalue, can give a click only in detector D_1.

The internal functioning of the measurement device is as follows: it consists of one adjustable HWP(φ) and one polarization beam splitter (PBS). If the input state is the eigenstate with negative eigenvalue, the polarization in mode a will first be rotated by HWP(φ) to obtain the state $\beta'|V,a\rangle$. When the PBS splits the polarization modes of the two spatial modes, this will give a click in detector D_1. All the tests are exactly the same, up to a half-wave plate rotation. To test the qubit, M_1 and M_2 correspond to setting the half-wave plate to an angle $\varphi = 11.25°$ and $\varphi = 78.75°$, respectively. To test the qutrit, M_1 and M_2 correspond to setting the half-wave plate to an angle $\varphi = 15.86°$ and $\varphi = 74.14°$, respectively.

For qubit states, $P(+1|x,y)$ and $P(-1|x,y)$ were estimated from the number of detections in D_2 and D_1, respectively. For qutrit states, the values of $P(+1|x,y)$ and $P(-1|x,y)$ were obtained from the number of detections in D_2 and D_3, and in D_1, respectively. When the preparer claimed classical sets, the measurement settings of the tester were reduced to arranging the detectors so that they clicked with the negative eigenvalue upon receiving a photon in a particular basis state: $|0\rangle \rightarrow D_3$, $|1\rangle \rightarrow D_1$, $|2\rangle \rightarrow D_2$, and $|3\rangle \rightarrow D_4$.

Our single-photon source was weak coherent light from a diode laser emitting at 780 nm. The laser was attenuated so that the two-photon coincidences were negligible. Our single-photon detectors (D_i, $i = 1, 2, 3, 4$) were silicon avalanche photodiodes with detection efficiency $\eta_d = 0.55$ and a dark counts rate $R_d \simeq 400$ Hz.

The detectors D_i produced output transistor-transistor logic signals of 4.1 V (with duration of 41 ns). The dead time of the detectors was 50 ns. All single counts were registered using multichannel coincidence logic with a time window of 1.7 ns.

The goals of the experiments were to obtain the maximum qubit violation of the bit bound $D_{\mathrm{CHSH}}(\mathrm{bit}) = C_2 = 4$, the maximum trit violation of the qubit bound $D_{\mathrm{CHSH}}(\mathrm{qubit}) = Q_2 = 5.66$, and the maximum qutrit violation of the trit bound $D_{\mathrm{CHSH}}(\mathrm{trit}) = C_3 = 6$. We prepared four qutrit states and performed $m = 2$ dichotomic measurements which maximize D_{CHSH}. The last experiment was a D_{CHSH} test on quarts, the maximum quart violation of the qutrit bound $D_{\mathrm{CHSH}}(\mathrm{qutrit}) = Q_3 = 6.47$. For this we prepared four fully distinguishable quart states the D_{CHSH}, and the results were very close to the algebraic bound $D_{\mathrm{CHSH}} = C_4 = 8$.

All our experimental results are summarized in Table I. The experimental values are in very good agreement with the theoretical predictions. This clearly demonstrates that we are able to determine the minimum dimension of a supplied set of states. The errors were deduced from propagated Poissonian counting statistics of the raw detection events, the limited precision of the settings of the polarization components (HWP plates), and the imperfection of the polarizing beam splitters. The number of detected single photons was about 1.5×10^5 per second, and the ratio of coincidences to singles was less than 2×10^{-4}. The measurement time for each experiment was 30 s. All the results and their corresponding errors are listed in Table 1.

As we have previously stated, the witness D_{CHSH} plays a crucial role in semi-device-independent quantum key distribution and randomness expansion. In [2] it has been used as a certificate for the security of quantum key distribution. The protocol there assumed that the communicated system was a qubit, and this has been the only assumption made about the devices. The value of D_{CHSH} for qubits obtained in our experiment would imply a secure key rate of 5.18% or 6.67% if we had made an additional assumption that the dark counts observed are not controlled by a potential eavesdropper. The derivation of these values is based on results from [15,16] given in the Supplemental Material [17].

The witness D_{CHSH} has been first used as a certificate for semi-device randomness expansion in [3] and the bounds on the amount of min-entropy generated with it have been improved in [10]. The amount of min-entropy generated by a round of protocol with qubits for the values observed in

TABLE I. Experimental results of the dimension witness tests. D_{th}, D_{exp}, and D^b_{exp} represent the theoretical, raw experimental, and dark counts corrected experimental values of the dimension witness bounds, respectively. ΔD_p, ΔD_d, and ΔD_T are the errors due to the limited precision of the settings of the polarization components and the imperfections of the polarization splitting, the propagated Poissonian counting statistics of the raw detection events and the total errors, respectively.

Inequality bound	D_{th}	D_{exp}	D^b_{exp}	ΔD_p	ΔD_d	ΔD_T
$D_{\mathrm{CHSH}}(\mathrm{bit})$	4	3.94	3.98	0.08	0.010	0.08
$D_{\mathrm{CHSH}}(\mathrm{qubit})$	5.66	5.51	5.56	0.12	0.008	0.12
$D_{\mathrm{CHSH}}(\mathrm{trit})$	6	5.90	5.96	0.13	0.010	0.13
$D_{\mathrm{CHSH}}(\mathrm{qutrit})$	6.47	6.44	6.50	0.14	0.009	0.14
$D_{\mathrm{CHSH}}(\mathrm{quart})$	8	7.88	7.94	0.16	0.010	0.16

our experiment can be read from Fig. 4 in [10] (note that T_2 used there is equal to $\frac{1}{2}D_{\mathrm{CHSH}}$). For $D_{\mathrm{CHSH}} = 5.51$ it is 0.0595, and for $D_{\mathrm{CHSH}} = 5.56$ it reaches 0.0820.

In summary, we have experimentally determined lower bounds for the dimension of several ensembles of physical systems in a device-independent way. For the tests we utilized a dimension witnesses device inspired by the structure of the CHSH inequality, which has a direct application in semi-device-independent quantum key distribution and randomness expansion. Note that the presented single device is universal for all studied dimensions from $d_{c/q} = 2$ to $d_{c/q} = 4$. In the witness device we used optimal measurements for the given dimension. We applied them to sets of photonic bits, qubits, trits, qutrits, and quarts. Our results demonstrate that CHSH-inspired dimension witnesses can be utilized to test classical and quantum dimensions of sets of physical states generated in externally supplied, potentially defective devices, and that one can distinguish between classical and quantum sets of states of a given dimension. We also discussed the efficiency of the semi-device-independent protocols based on our witness using the values reached in our experiment. The approach can be generalized to tests of systems of higher dimensions. This can be done in several ways, some of which will be presented in forthcoming papers.

M. P. would like to thank Ryszard Weinar for discussions and Piotr Mironowicz for supplying the raw data from [10]. J. A., P. B., and M. B. are supported by the Swedish Research Council (VR), the Linnaeus Center of Excellence ADOPT. M. P. is supported by the TEAM program of the Foundation for Polish Science (FNP), UK EPSRC, NCN Grant No. 2013/08/M/ST2/00626, and QUASAR (ERA-NET CHIST-ERA 7FP UE). M. Z. is supported by an Ideas Plus Program MNiSW (IdP2011 000361). M. B. is supported by the European Research Council, Grant QOLAPS.

[1] A. Acín, N. Gisin, and L. Masanes, Phys. Rev. Lett. **97** 120405 (2006).

[2] M. Pawłowski and N. Brunner, Phys. Rev. A **84**, 010302 (2011).

[3] H.-W. Li, Z.-Q. Yin, Y.-C. Wu, X.-B. Zou, S. Wang, W. Chen, G.-C. Guo, and Z.-F. Han, Phys. Rev. A **84**, 034301 (2011).

[4] N. Brunner, S. Pironio, A. Acin, N. Gisin, A. Méthot, and V. Scarani, Phys. Rev. Lett. **100**, 210503 (2008).

[5] R. Gallego, N. Brunner, C. Hadley, and A. Acín, Phys. Rev. Lett. **105**, 230501 (2010).

[6] M. DallArno, E. Passaro, R. Gallego, and A. Acín, Phys. Rev. A **86**, 042312 (2012).

[7] J. Ahrens, P. Badziag, A. Cabello, and M. Bourennane, Nat. Phys. **8**, 592 (2012).

[8] M. Hendrych, R. Gallego, M. Micuda, N. Brunner, A. Acín, and J. P. Torres, Nat. Phys. **8**, 588 (2012).

[9] H.-W. Li, M. Pawłowski, Z.-Q. Yin, G.-C. Guo, and Z.-F. Han, Phys. Rev. A **85**, 052308 (2012).

[10] H.-W. Li, P. Mironowicz, M. Pawłowski, Z.-Q. Yin, Y.-C. Wu, S. Wang, W. Chen, H.-G. Hu, G.-C. Guo, and Z.-F. Han, Phys. Rev. A **87**, 020302(R) (2013).

[11] N. Brunner, M. Navascues, and T. Vrtesi, Phys. Rev. Lett. **110**, 150501 (2013).

[12] S. Wehner, M. Christandl, and A. C. Doherty, Phys. Rev. A **78**, 062112 (2008).

[13] A. Ambainis, A. Nayak, A. Ta-Shma, and U. Vazirani, J. Assoc. Comput. Mach. **49**, 496 (2002).

[14] J. F. Clauser, M. A. Horne, A. Shimony, and R. A. Holt, Phys. Rev. Lett. **23**, 880 (1969).

[15] I. Csiszar and J. Körner, IEEE Trans. Inf. Theory **24**, 339 (1978).

[16] M. Pawłowski and A. Winter, Phys. Rev. A **85**, 022331 (2012).

[17] See Supplemental Material at http://link.aps.org/supplemental/10.1103/PhysRevLett.112.140401 for the derivation of the key rates given in the text.