Experimental test of nonclassicality with arbitrarily low detection efficiency

Alley Hameedi,[1] Breno Marques,[2] Piotr Mironowicz,[3,4] Debashis Saha,[5] Marcin Pawłowski,[5,4,*] and Mohamed Bourennane[1]

[1]*Department of Physics, Stockholm University, S-10691 Stockholm, Sweden*

[2]*Centro de Ciências Naturais e Humanas, Universidade Federal do ABC–UFABC, Santo André, Brazil*

[3]*Department of Algorithms and System Modeling, Faculty of Electronics, Telecommunications and Informatics, Gdańsk University of Technology, Gdańsk 80-233, Poland*

[4]*International Centre for Theory of Quantum Technologies, University of Gdańsk, Wita Stwosza 57, 80-308 Gdańsk, Poland*

[5]*Institute of Theoretical Physics and Astrophysics, University of Gdańsk, 80-952 Gdańsk, Poland*

(Received 26 May 2017; accepted 22 June 2020; published 21 September 2020)

We theoretically introduce and experimentally demonstrate the realization of a nonclassicality test that allows for arbitrarily low detection efficiency without invoking an extra assumption of independence of the devices. Our test and its implementation is set in a prepare-and-measure scenario with an upper limit on the classical communication capacity of the channel through which the systems are communicated. The essence for our test is the use of two preparation and two measurement devices, which are randomly paired in each round. Our work opens the possibility for experimental realizations of nonclassicality tests with off-the-shelf technology.

DOI: 10.1103/PhysRevA.102.032621

I. INTRODUCTION

Quantum information processing utilizes nonclassical resources for processing information encoded into physical systems, which are subjected to quantum mechanical laws. These quantum resources have many applications in quantum information processing ranging from cryptography [1,2] to communication complexity reduction [3].

Device-independent quantum information processing schemes have shown great promise in the estimation of critical parameters, without making any assumptions about the inner functionality of these devices. This approach comes in two main variants: fully device independent (FDI) [4] and semi device independent (SDI) [5]. FDI protocols mean that the working principles of the devices do not matter and the protocols work without assuming any internal mechanism of the devices. On the other hand, SDI protocol means that the protocols require some assumptions on the devices to be realized. In this paper, we consider the SDI approach. The assumption we make is an upper bound on the classical communication between parts of devices involved in the scenario.

No control over the communicated system renders tasks as cryptography and randomness generation impossible. Therefore, we suppose that we can find at least one parameter which describes the communication: an upper bound on the classical capacity of the channel. This assumption is the reason why the scenario is SDI.

The implementation of FDI or SDI protocols requires a test of nonclassicality to be performed, a result of which indicates that the description of the experiment is impossible through classical means. This is a necessary although not always sufficient condition. These tests include estimation of violations of Bell inequality [6], dimension witnesses [7], or success probability in a communication complexity task [8]. The important requirement, however, is that the involved parties must give a conclusive result without any additional assumptions. It is difficult in practice, mainly due to the so-called detection efficiency loophole [9], which in a nutshell states that device-independent tests of nonclassicality can only be conclusive if the detectors used in an experiment provide a detection efficiency above a certain threshold. These thresholds have been found for a variety of tests [10–15]. Unfortunately, the required efficiencies are very high and therefore difficult to obtain in practice. To our knowledge, only a few DI tests of nonclassicality have been performed thus far [16–20].

The issue can be addressed by adding extra constraints on the resources that are available to the devices. One such constraint is the requirement that the parties have no access to shared randomness. With this added assumption, it was shown [21,22] that any experimental setup with a nonzero detection efficiency can be used to prove nonclassicality. Experimental realization of protocols based on these ideas has been shown recently [23,24]. However, lack of shared randomness is a strong assumption, difficult to justify in practice. On the other hand, is seems to be relatively easy to check the classical channel capacity. It suffices to establish the type and range of parameters accessible to the sender's device and the classical capacity is bounded by the number of orthogonal states which can be prepared. This can be done by a close inspection of the hardware. Such an inspection is not trivial but overwhelmingly easier than full characterization of the device.

Here we propose a method for modification of the existing communication-based protocols, which enables us to relax this assumption. The modified protocols retain their potential to provide conclusive results for any positive detection efficiency and do not require any additional constraints. This leads to a huge increase in reliability of the tests of nonclassicality.

*dokmpa@univ.gda.pl

 ©2020 American Physical Society

Note that the assumption we need for our proposal to work is limited to classical capacity. This is important, as the quantum capacity is by far more difficult to be verified. The aim of the proposed protocol is to show an experimentally feasible way of testing that the transmitted system is quantum, no matter what its dimension.

The idea behind the method is quite simple. Consider a standard nonclassicality test involving one-way communication between two parties. We assume this test cannot be passed using classical resources with detectors of arbitrarily low efficiency, if the parties are not using shared randomness. Now, we want to provide a way for the test to remain conclusive even if the parties use shared randomness.

To this end, suppose we run this test with two pairs of parties performing it in parallel. However, in every round of the test, we randomly choose the pairing between senders and receivers. If the devices rely on shared randomness in their behavior, then both senders should be correlated with both receivers as they do not know to whom they are sending their messages. Yet, if this is the case, there might appear correlations in the outputs of receivers, which should not be there. If we penalize such correlations, we might end up in a situation where using shared randomness does not give any advantage.

We note that access to a source of random variables (possibly public) which are not correlated sender and receiver devices is crucial for working of the protocol. Within the paper, we use such randomness as a resource to create an experimentally feasible setup resistant to a detection efficiency loophole. This seems to be reasonable as, unless a paranoid level of certainty is assumed, it is impossible for an eavesdropper, e.g., to correlate with all publicly available sources of randomness. On the other hand, the threat that devices exploit the detection efficiency loophole is quite real.

This is, obviously, only intuitive reasoning that leads us to introducing our method. In the rest of the paper, we will show that the method indeed works for the simplest example of a communication protocol and how it can be applied in practice. We will also report the realization of a proof of principle experiment for our test of nonclassicality. We believe that this method could be applied as easily to even complex protocols, however, their study is beyond the scope of the paper. Neither do we consider the straightforward application of our method in cryptography as our aim; here is a proof of principle.

II. SEMI-DEVICE-INDEPENDENT SCENARIO

An ordinary SDI scenario involves two black boxes representing state preparation and measurement devices, see Fig. 1. The former prepares a physical system based on the input received and communicates it, via an external channel, to the latter. The measurement device returns an output after receiving the communication and an additional classical input. There are no assumptions on the internal working of the preparation and measurement devices but we do assume an upper bound on the information capacity of the system communicated between them. Here the classical information capacity of our system is one bit. We prove that the systems sent through it, necessarily, have nonclassical properties and this is realized by using a method based on a RAC. We'd like to note that these two devices are placed in a shielded laboratory, meaning they don't receive any external synchronization signals. They may share correlated classical variables but these are assumed to be uncorrelated with the inputs.

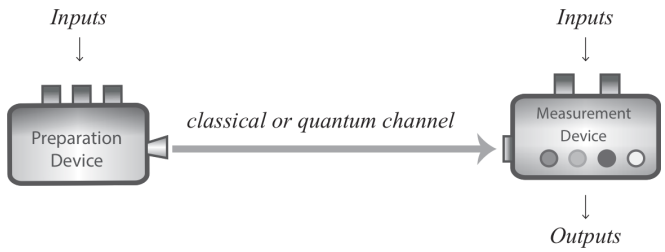

FIG. 1. Semi-device-independent implementation in a prepare-and-measure scenario. Preparation device communicates a system depending on its inputs. The message is encoded in a system with an upper bound on the dimension. The measurement device's output depends on its inputs and the received message.

The assumption on the upper bound of the communication capacity might seem difficult to justify. It is, however, much easier to inspect the components of the device responsible for encoding the information in a physical system to find its dimension, then to check if every logical circuit and bit of software does what it is supposed to do. Moreover, the SDI case has been well studied. Our method would probably work just as well with other possible constraints but as introduced here, we have chosen to analyze it in a setting which makes it easiest.

III. RANDOM ACCESS CODES

Random access code (RAC) is a communication complexity problem. In its simplest case, the sender (Alice) is given an input a consisting of two bits: a_0 and a_1. She is only allowed a single use of a communication channel which transmits systems of one classical bit capacity to send a message to the receiver (Bob). This means that the communicated system is a single bit (qubit) of information in the classical (quantum) case. The receiver, apart from the message, also receives an input $y \in \{0, 1\}$ and his task is to return one of the bits that the sender received specified by this input, i.e., a_y. If we denote the output of the receiver by b, then the success of the task is measured by the probability $P(b = a_y|a, y)$.

The use of RACs in quantum information was mentioned already in Ref. [25] and the interest in them has been present ever since [26–28]. In fact, most SDI protocols are based on RAC [5,29,30] and, depending on the targeted application, different figures of merit can be used, e.g., average success probability $S_{\mathrm{av}} = \frac{1}{8}\sum_{a,y} P(b = a_y|a, y)$ [5,29,30]; worst case $S_{\mathrm{wc}} = \min_{a,y} P(b = a_y|a, y)$ [26]; or even the whole set $\{P(b = a_y|a, y)\}_{a,y}$ [23]. Regardless of the chosen figure of merit, quantum communication allows us to reach values that are not possible for classical resources, thereby making RACs a good choice for a test of nonclassicality. For example, the maximum average success probability when one bit is communicated is 0.75 while with one qubit it can reach 0.85.

Like other tests of nonclassicality, RACs are also vulnerable to the detection efficiency loophole [9], which leaves

MOST WIEDZY Downloaded from mostwiedzy.pl

them inconclusive if the detectors frequently fail to register incoming particles. The critical detection efficiency depends on the particularities of the test: the choice of the figure of merit and the corresponding treatment of the experimental rounds with no particle registered. In our work, we choose the most generic approach for the latter case where we make our devices return a random number whenever a detector fails to register a particle. This artificially makes the effective efficiency to be 100% as we observe an outcome in every round. This does, however, lead to a decrease in the maximal success probability for the quantum case. For a given maximum Q of the quantum theory, the detectors registering particles in η fraction of the rounds can yield the largest success probability,

$$Q_\eta = \eta Q + (1-\eta)\frac{1}{2}, \tag{1}$$

tending to $\frac{1}{2}$ as $\eta \to 0$. The classical value does not increase, allowing us to find the η required for the quantum theory to be able to provide an advantage. However, the critical η is usually very high and extremely difficult to reach in practice. Our goal is to propose a test with η arbitrarily close to 0. From (1), we see that it is possible if we can design a test with the maximal classical value reduced to $1/2$. This is the bound for the worst-case success probability if no shared randomness is available to the communicating parties [21]. As mentioned, we need tasks with such a property as a starting point for our method. This, together with its simplicity, makes RAC a perfect candidate.

IV. PROBABILITY POLYTOPES

The considerations above are specific to RACs. However, they can be generalized to different tests of nonclassicality using the framework of probability polytopes [7]. Consider a set of conditional probability distributions $p(\vec{x}|\vec{y})$ arising in an experiment, where $\vec{x}$ denotes the set of outcomes of all the devices in a single round of the experiment and $\vec{y}$ the inputs. Let $\vec{p}$ be a vector whose elements correspond to conditional probabilities for every combination of $\vec{x}$ and $\vec{y}$. $\vec{p}$ can characterize the behavior of any devices employing any strategy. While testing these devices, e.g., if they violate Bell inequalities, we often look at the linear combinations of probabilities $p(\vec{x}|\vec{y})$. Such tests can also be represented by a vector, $\vec{t}$, living in the same space as $\vec{p}$. The quantitative outcome of the test is the scalar product $\vec{t}\cdot\vec{p}$.

The average success probability of a RAC, $S_{\mathrm{av}} = \frac{1}{8}\sum_{a,y} P(b = a_y|a, y)$, is an example of such a test. The vector $\vec{t}_{\mathrm{RAC}}$ corresponding to it has 16 elements because there are that many combinations of a, b, and y. These elements are equal to $\frac{1}{8}$ whenever the corresponding variables satisfy $b = a_y$ and 0 otherwise. When a single bit is communicated, then for every possible classical protocol we have $S_{\mathrm{av}} = \vec{t}_{\mathrm{RAC}}\cdot\vec{p}_{\mathrm{cl}} \leqslant 0.75$.

For classical devices, the set of allowed probability distributions $\vec{p}_{\mathrm{cl}}$ is a polytope. Its vertices correspond to deterministic strategies. Every other strategy can be considered as a convex combination of deterministic ones and corresponds to a point inside this polytope. The set of quantum distributions is much harder to characterize and, instead of faces, usually is bounded by smooth curved surfaces. This set is, typically, strictly larger than the classical polytope but their dimensions are usually the same. However, it is not always true [31] and these are the cases that we find the most interesting. Whenever this happens, there exists a vector $\vec{t}_0$ perpendicular to the subspace spanned by classical probabilities, i.e., $\forall_{\vec{p}_{\mathrm{cl}}}\ \vec{t}_0\cdot\vec{p}_{\mathrm{cl}} = 0$, and there exists a quantum probability distribution $\vec{p}_{qm}$ such that $\vec{t}_0\cdot\vec{p}_{qm} = Q \neq 0$.

Consider again the case with an experiment reaching $\vec{p}_{qm}$ if we had perfect detectors. If no particles are registered, we again assign a random outcome. Since returning a random outcome is also a classical strategy, the vector corresponding to the probability distribution observed in the experiment is $\vec{p}_\eta = \eta\vec{p}_{qm} + (1-\eta)\vec{p}_{\mathrm{cl}}$ and for $\eta > 0$ the outcome of the test will be equal to $\eta^Q > 0$, since by assumption $\vec{p}_{qm} > 0$ and $\vec{p}_{\mathrm{cl}} = 0$. Therefore, it pays off to look for experimental setups which have different dimensions of the corresponding quantum and classical sets.

We will see that the two approaches, looking for a game with classical success probability $\frac{1}{2}$ and for setups with different classical and quantum set dimensions, are complementary. The former provides us with an intuitive candidate in the form of a parallel RAC that we describe in the next section. However, what we need from it is only the structure of the experiment, i.e., the number of parties and their inputs and outputs, communication paths, and the quantum protocol. The proof that the experiment with the given structure provides us a robust test given by the latter and in the test itself no reference to RACs is necessary.

V. PARALLEL RANDOM ACCESS CODING

We define parallel RAC as a task in which two pairs of senders and receivers perform RAC in parallel but in each round they are paired randomly. Additionally, the devices do not have access to information about the pairing in any given round. This situation is illustrated in Fig. 1. The inputs to preparation device P^i are denoted by a^i and y^i for the measurement devices, M^i, $i = 0, 1$. The choice of pairing is denoted by a random variable x. If $x = 0$, information from P^0 goes to M^0 and from P^1 to M^1. Whereas for $x = 1$, P^0 communicates with M^1 and P^1 with M^0. We state that the nth receiver (i.e., measuring device) is successful if $b^n = a^{n\oplus x}_{y^n}$, where n is either 0 or 1.

There exist $2^{16} = 65\,536$ different deterministic strategies. Because of symmetries between some of them (e.g., joint negation of messages of both Alices connected with negation of the reaction of both Bobs), these strategies relate to 30 496 different points in conditional probability space,

$$P\big(b_0^{\mathrm{out}}, b_1^{\mathrm{out}}\big|a_{0,0}, a_{0,1}, a_{1,0}, a_{1,1}, c, b_0, b_1\big), \tag{2}$$

where b_i^{out} refers to the outcome of ith Bob, $a_{i,j}$ to jth bit of ith Alice, c determines which Alice is sending to which Bob, and b_i is the input of i th Bob.

Since there are four different possible outcomes, $(b_0^{\mathrm{out}}, b_1^{\mathrm{out}})$, and $2^7 = 128$ different possible inputs $(a_{0,0}, a_{0,1}, a_{1,0}, a_{1,1}, c, b_0, b_1)$, the points in this probability space can be represented as vectors forming a simplex in $4\times 128 = 512$ dimensional linear space. It reveals that this simplex is embeded in 125 dimensional subspace (i.e., there are only 125 linearly independent vectors among 30 496 points). Let P^{sub} be the projector onto that subspace.

MOST WIEDZY Downloaded from mostwiedzy.pl

Let $P^{\max}$ be the vector in 512 space related to the optimal quantum strategies maximizing the probability of correct guesses of both Bobs. If we project the vector $P^{\max}$ on P^{sub}, then we obtain a Bell operator $B_{1,1}^{2s2r}$ given by

$$B_{k,l}^{2s2r} \equiv \sum_{\substack{a_{0,0},\, a_{0,1}\\ a_{1,0},\, a_{1,1}=0,1\\ b_0,\, b_1}} \delta_{b_0\oplus b_1,k}\,\delta_{a_{0,0}\oplus a_{0,1}\oplus a_{1,0}\oplus a_{1,1},l} \times \left[\sum_{b_0^{\text{out}},b_1^{\text{out}}=0,1} (-1)^{s_0+s_1} P\big(b_0^{\text{out}}, b_1^{\text{out}}\big|a_{0,0}, a_{0,1}, a_{1,0}, a_{1,1}, c, b_0, b_1\big)\right], \tag{3}$$

where s_i is the binary indicator success of ith Bob. Let $p = \frac{1}{2}(1+\frac{\sqrt{(2)}}{2})$ be the maximal probability of success of a 2 to 1 quantum random access code. It is easy to see that for each nonzero term in the outer summation, the maximum value is $p^2+(1-p)^2-2p(1-p)=0.5$, and there are 32 such terms, giving Tsirelon bound 16. The values obtained in the experiment are $B_{0,0}^{2s2r}=0.1797$, $B_{0,1}^{2s2r}=0.1792$, $B_{1,0}^{2s2r}=0.1728$, and $B_{1,1}^{2s2r}=0.1721$.

In the deterministic model, each Alice receives a four-dimensional input (a setting) and returns a binary output, so each Alice has $2^4=16$ deterministic strategies. Similarly, each Bob get a four-dimensional input (message and setting) and outputs a binary result. Thus, in our setting, there exist 2^{16} deterministic strategies. They are spanning a 125-dimensional subspace. Now we need to choose a vector corresponding to the test that we are going to perform. We choose it to be parallel to the line connecting the point $\vec{p}_{qm}$ corresponding to the probabilities that would arise in the perfect quantum experimental realization of RAC and its projection onto the classical subspace. It gives rise to the following figure of merit:

$$T = \sum_{a_0^0\oplus a_0^1\oplus a_1^0\oplus a_1^1=1}\ \sum_{y^0\neq y^1}\ \sum_{b^0,b^1,x} \times s_0 s_1 p(b^0, b^1|a^0, a^1, y^0, y^1, x), \tag{4}$$

where s_0 and s_1 are success indicators of the two receivers. $s_n=1$ when $b^n = a_{y^n}^{n\oplus x}$ and -1 otherwise. Note there is no obvious relation between T and average or worst case success probability in RAC. This code was only a step necessary to find the number of inputs and outputs for each of the parties, defining the space and point $\vec{p}_{qm}$. However, it is still quite straightforward to turn T into a game with classical average success probability of $\frac{1}{2}$ simply by changing each coefficient in T from -1 to 0, i.e., we replace $s_0 s_1$ with Kronecker's delta δ_{s_0,s_1} and get

$$T' \equiv \sum_{a_0^0\oplus a_0^1\oplus a_1^0\oplus a_1^1=1}\ \sum_{y^0\neq y^1}\ \sum_{b^0,b^1,x} \times \delta_{s_0,s_1} p(b^0, b^1|a^0, a^1, y^0, y^1, x). \tag{5}$$

T' describes average success probability in a game in which success is defined by having $s_0=s_1$. If $T=0$, then $T'=\frac{1}{2}$, therefore it is a game with classical average success probability $\frac{1}{2}$.

One way to view T' is as a parallel RAC with a promise on the distribution of the inputs, expressed by the fact that the sums in T' do not include every possible combination of input variables. Another important aspect is that the parties win a round of the game not if they successfully guess the desired bit as in a typical RAC but when their successes are correlated, i.e., they either both guess correctly or both fail. However, it's easy to see that using the same states as measurements as in a standard RAC, the parties can beat the classical bound. It suffices to notice that the optimal strategy in that protocol gives success probability $p_s=\frac{1}{2}+\frac{1}{2\sqrt{2}}$ for every input. If the same states and measurements are used in this game, one will obtain $T'=p_s^2+(1-p_s)^2=\frac{3}{4}$.

From now on, one can stop thinking about RACs and consider only T. Its classical value is 0 and the theoretical maximal quantum value is 16 corresponding to the point $\vec{p}_{qm}$. Therefore, our result is a general property of a probability space corresponding to a parallel test with a certain number of inputs and outcomes rather than of RACs.

We leave as an open question whether the same (i.e., that classical polytope has lower dimension than the quantum region) holds for spaces corresponding to tests with different than binary numbers of inputs and outcomes. This seems plausible and it is this conjecture which is behind our optimism regarding the possibility of applying the same method in different scenarios. Now we describe our experimental realization to obtain an experimentally measured value of T.

The experiment requires three assumptions:

(1) The system that leaves the laboratory of each sender has information encoded in the Hilbert space dimension of 2.

(2) The devices don't have the access to the information about the party they are communicating with in the given round of the experiment.

(3) The inputs of all the parties are chosen at random.

In our experiment, we measured each combination of settings for 20 seconds before moving to the other, therefore the final assumption was not satisfied. This is because it was intended as a proof of principle and choosing random settings for each round would considerably extend the already long measurement time. In practical applications based on this setup, that assumption cannot be omitted.

VI. EXPERIMENTAL DEMONSTRATION

Our experimental realization is shown in Fig. 3. Any qubit state can be prepared by a suitably oriented half-wave plate, HWP(θ_0) and HWP(θ_1) for P_0 and P_1, respectively. We used a heralded single photon source from a spontaneous parametric down-conversion process at 780 nm. For the four experimentally prepared qubit states, the HWP settings for both θ_0 and θ_1 correspond to 0°, 45°, and ±22.5°. We have also added an extra HWP in each device to assure the same polarization in both paths.

The choice of the two communication paths is made in a region R, which consists of two polarization beam splitters

MOST WIEDZY Downloaded from mostwiedzy.pl

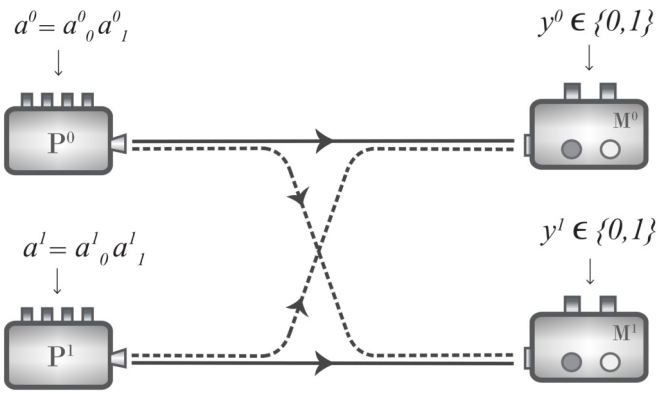

FIG. 2. Parallel RAC scenario consisting of two preparation devices, P^0 and P^1, and two measurement devices, M^0 and M^1. The pairing choice between the senders and receivers devices depends on the value of random variable x. Here, the solid line corresponds to $x = 0$, and the dotted line to $x = 1$.

(PBSs) and six HWPs, and by properly adjusting the HWP orientation angles, we choose the pairing of the devices. Note that we do not consider the region R a device for the purposes of our analysis. Another option would be simply to connect senders and receivers by fibers randomly each round. This would leave R empty but greatly increase the duration of the experiment.

The measurement devices consist of an interferometric setup, one adjustable HWP(φ_0) and HWP(φ_1) for M_0 and M_1 respectively along with twoPBSs and two single-photon detectors ($D_{ij}, i = 0, 1; j = 1, 2$) for each device M_j. The success probabilities are estimated from the number of detections in the detectors D_{ij}, after properly adjusting the orientation φ_j of the HWP in each of the measurement devices M_0 and M_1. In our experiment, the two used HWP settings are 11.25° and 78.75°, respectively.

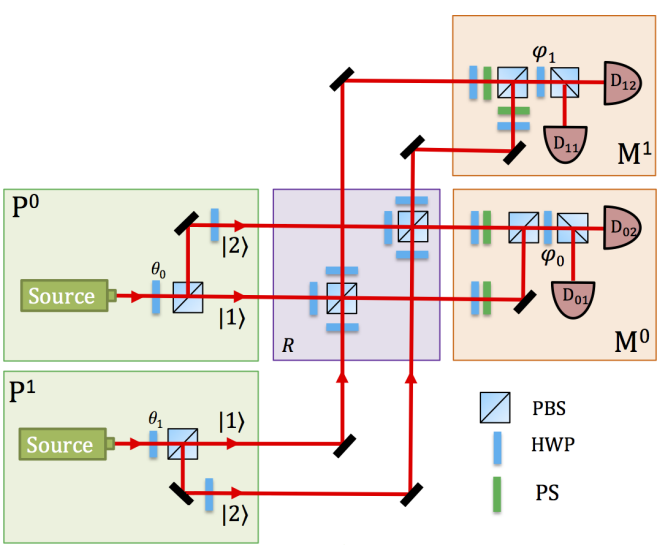

FIG. 3. Experimental setup. Information is encoded into two spatial-photonic modes. The preparation devices P_i ($i = 0, 1$) consist of a heralded single photon source that emits horizontally polarized photons which, after passing through a half-wave plate (HWP) oriented at an angle θ_i, can be prepared in the required protocol states. The measurement devices M_i consist of a HWP oriented at an angle φ_i, polarization beam splitter (PBS), single photon detectors D_{ij}. The pairing of the preparation and measurement devices is performed with help of adjustable HWP plates and PBSs.

Considering the parallel RAC scenario in Fig. 2, when $x = 0$, the state prepared in P^0 (P^1) is measured in the receiver M^0 (M^1), whereas for $x = 1$, the state prepared in P^0 (P^1) is measured in the receiver M^1 (M^0). In this proof-of-principle experimental demonstration, the values of HWP(θ_0) and HWP(θ_1) on the preparation sides and HWP(φ_0) and HWP(φ_1) on the measurement sides were preselected rather than a randomized selection. However, a randomized selection between the setting choice can be implemented by mounting all the corresponding wave plates on motorized stages.

Our single-photon detectors ($D_{ij}, i = 0, 1; j = 1, 2$) were fiber-coupled silicon avalanche photodiodes (APDs) with effective detection efficiency $\eta_d = 0.55$ (with 0.85 fiber coupling and 0.65 for APD efficiency) and dark count rate $R_d \simeq 300$ Hz. The detectors D_{ij} 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.

For each choice of settings a^0, a^1, y^0, y^1, x, we registered an average of 222 528 clicks, where 3104 have the four-photon coincidence, meaning that both photon sources in P^0 and P^1 were heralded. Only the runs that have both photons heralded together contribute for the value of T, for all other (when one or no photon is heralded) $\sum_{b^0,b^1} s_0 s_1 p(b^0, b^1|a^0, a^1, y^0, y^1, x) = 0$, where we considered that for these rounds a random value was assigned to the outcomes. If we consider only the run when we measured four-photon coincidence and fair sampling, we have $T = 14.74 \pm 1.56$. Now, considering the detector efficiency and all runs, we obtain $T = 3.16 \pm 0.33 \times 10^{-3}$, witnessing the system nonclassicality.

VII. CONCLUSION

The nonclassicality test that we have introduced and experimentally demonstrated allows for arbitrarily low detection efficiency without invoking extra assumptions such as independence of the devices. This opens up the possibility for constructing SDI protocols based on this test, which can be easily realized with today's technology.

ACKNOWLEDGMENTS

This work is supported by FNP grant First TEAM, NCN Grant No. 2014/14/E/ST2/00020, Swedish Research Council (VR), Knut and Alice Wallenberg Foundation, DS Programs of the Faculty of Electronics, Telecommunications and Informatics, Gdańsk University of Technology, and the Brazilian funding agencies CNPq and CAPES. The International Centre for Theory of Quantum Technologies project is carried out within the International Research Agendas Programme of the Foundation for Polish Science cofinanced by the European Union from funds of the Smart Growth Operational Programme, Axis IV: Increasing the Research Potential (Measure 4.3).

MOST WIEDZY Downloaded from mostwiedzy.pl

[1] C. H. Bennett and G. Brassard, Quantum key distribution and coin tossing, *in Proceedings of IEEE International Conference on Computers, Systems, and Signal Processing, Bangalore, India* (IEEE, New York, 1984), pp. 175–179.

[2] A. K. Ekert, Quantum Cryptography Based on Bell's Theorem, Phys. Rev. Lett. **67**, 661 (1991).

[3] H. Buhrman, R. Cleve, and W. van Dam, Quantum entanglement and communication complexity, SIAM J. Comput. **30**, 1829 (2001).

[4] A. Acin, N. Brunner, N. Gisin, S. Massar, Pironio, and V. Scarani, Device-Independent Security of Quantum Cryptography Against Collective Attacks, Phys. Rev. Lett. **98**, 230501 (2007).

[5] M. Pawłowski and N. Brunner, Semi-device-independent security of one-way quantum key distribution, Phys. Rev. A **84**, 010302(R) (2011).

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

[7] R. Gallego, N. Brunner, C. Hadley, and A. Acín, Device-Independent Tests of Classical and Quantum Dimensions, Phys. Rev. Lett. **105**, 230501 (2010).

[8] J. Ahrens, P. Badziag, M. Pawłowski, M. Żukowski, and M. Bourennane, Experimental Tests of Classical and Quantum Dimensionality, Phys. Rev. Lett. **112**, 140401 (2014).

[9] P. Pearle, Hidden-variable example based upon data rejection, Phys. Rev. D **2**, 1418 (1970).

[10] P. H. Eberhard, Background Level and Counter Efficiencies Required for a Loophole-Free Einstein-Podolsky-Rosen Experiment, Phys. Rev. A **47**, R747 (1993).

[11] S. Massar, Nonlocality, closing the detection loophole, and communication complexity, Phys. Rev. A **65**, 032121 (2002).

[12] A. Cabello, D. Rodriguez, and I. Villanueva, Necessary and Sufficient Detection Efficiency for the Mermin Inequalities, Phys. Rev. Lett. **101**, 120402 (2008).

[13] H.-W. Li, Z.-Q. Yin, M. Pawłowski, G.-C. Guo, and Z.-F. Han, Detection efficiency and noise in a semi-device-independent randomness-extraction protocol, Phys. Rev. A **91**, 032305 (2015).

[14] M. Dall'Arno, E. Passaro, R. Gallego, and A. Acín, Robustness of device-independent dimension witnesses, Phys. Rev. A **86**, 042312 (2012).

[15] A. Dutta, M. Pawłowski, and M. Żukowski, Detection-efficiency loophole and the Pusey-Barrett-Rudolph theorem, Phys. Rev. A **91**, 042125 (2015).

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

[17] 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, N. Brunner, C. C. W. Lim, N. Gisin, and P. G. Kwiat, Detection-Loophole-Free Test of Quantum Nnonlocality, and Applications, Phys. Rev. Lett. **111**, 130406 (2013).

[18] B. Hensen, H. Bernien, A. E. Drasau, A. Reiserer, N. Kalb, M. S. Blok, J. Ruitenberg, R. F. L. Vermeulen, R. N. Schouten, A. Cabello *et al.*, Loophole-free Bell inequality violation using electron spins separated by 1.3 kilometres, Nature **526**, 682 (2015).

[19] M. Giustina, M. A. M. Versteegh, S. Wengerowsky, J. Handsteiner, A. Hochrainer, K. Phelan, F. Steinlechner, J. Kofler, J.-A. Larsson, C. Abellan, W. Amaya, V. Pruneri, M. W. Mitchell, J. Beyer, T. Gerrits, A. E. Lita, L. K. Shalm, S. W. Nam, T. Scheidl, R. Ursin, B. Wittmann, and A. Zeilinger, Significant-Loophole-Free Test of Bell's Theorem with Entangled Photons, Phys. Rev. Lett. **115**, 250401 (2015).

[20] L. K. Shalm, E. Meyer-Scott, B. G. Christensen, P. Bierhorst, M. A. Wayne, M. J. Stevens, T. Gerrits, S. Glancy, D. R. Hamel, M. S. Allman, K. J. Coakley, S. D. Dyer, C. Hodge, A. E. Lita, V. B. Verma, C. Lambrocco, E. Tortorici, A. L. Migdall, Y. Zhang, D. R. Kumor, W. H. Farr, F. Marsili, M. D. Shaw, J. A. Stern, C. Abellan, W. Amaya, V. Pruneri, T. Jennewein, M. W. Mitchell, P. G. Kwiat, J. C. Bienfang, R. P. Mirin, E. Knill, and S. W. Nam, A Strong Loophole-Free Test of Local Realism, Phys. Rev. Lett. **115**, 250402 (2015).

[21] M. Dall'Arno, E. Passaro, R. Gallego, M. Pawłowski, and A. Acín, Detection loophole attacks on semi-device independent quantum protocols, Quantum Inf. Comput. **15**, 0037 (2015).

[22] J. Bowles, M. T. Quintino, and N. Brunner, Certifying the Dimension of Classical and Quantum Systems in a Prepare-and-Measure Scenario with Independent Devices, Phys. Rev. Lett. **112**, 140407 (2014).

[23] G. Cañas, J. Cariñe, E. S. Gómez, J. F. Barra, A. Cabello, G. B. Xavier, G. Lima, and M. Pawłowski, Experimental quantum randomness generation invulnerable to the detection loophole, arXiv:1410.3443; S. Pironio, Lifting Bell inequalities, J. Math. Phys. **46**, 062112 (2005).

[24] T. Lunghi, J. B. Brask, C. C. W. Lim, Q. Lavigne, J. Bowles, A. Martin, H. Zbinden, and N. Brunner, A self-Testing Quantum Random Number Generator, Phys. Rev. Lett. **114**, 150501 (2015).

[25] S. Wiesner, Conjugate coding, SIGACT News **15**, 78 (1983).

[26] A. Ambainis, A. Nayak, A. Ta-Shma, and U. Vazirani, Dense quantum coding and quantum finite automata, J. ACM **49**, 496 (2002).

[27] A. Ambainis, D. Leung, L. Mancinska, and M. Ozols, Quantum random access codes with shared randomness, submitted as M.S. thesis at University of Waterloo by M.O., 2008.

[28] A. Tavakoli, A. Hameedi, B. Marques, and M. Bourennane, Quantum Random Access Codes Using Dingle *d*-Level Systems, Phys. Rev. Lett. **114**, 170502 (2015).

[29] H.-W. Li, Z.-Q. Yin, Y.-C. Wu, X.-B. Zou, S. Wang, W. Chen, G.-C. Guo, and Z.-F. Han, Semi-device independent random number expansion without entanglement, Phys. Rev. A **84**, 034301 (2011).

[30] H.-W. Li, M. Pawłowski, Z.-Q. Yin, G.-C. Guo, and Z.-F. Han, Detection efficiency and noise in a semi-device-independent randomness-extraction protocol, Phys. Rev. A **85**, 052308 (2012).

[31] L. Clemente and J. Kofler, No Fine Theorem for Macrorealism: Limitations of the Leggett-Garg Inequality, Phys. Rev. Lett. **116**, 150401 (2016).

MOST WIEDZY Downloaded from mostwiedzy.pl