Practical No-Signalling proof Randomness Amplification using Hardy paradoxes and its experimental implementation

Ravishankar Ramanathan (ravishankar.ramanathan.83@gmail.com)
The University of Hong Kong
Michal Horodecki
University of Gdansk
Hammad Anwer
Stockholm University
Stefano Pironio
Universite libre de Bruxelles
Karol Horodecki
University of Gdańsk
Marcus Grünfeld
Stockholm University
Sadiq Muhammad
Stockholm University
Mohamed Bourennane
Stockholm University
Paweł Horodecki
Technical University of Gdańsk

Article

Keywords: Device-Independent (DI) security, Hardy paradox, quantum cryptography

Posted Date: September 11th, 2020

DOI: https://doi.org/10.21203/rs.3.rs-68062/v1

Practical No-Signalling proof Randomness Amplification using Hardy paradoxes and its experimental implementation

Ravishankar Ramanathan,[1] Michał Horodecki,[2] Hammad Anwer,[3] Stefano Pironio,[1] Karol Horodecki,[4] Marcus Grünfeld,[3] Sadiq Muhammad,[3] Mohamed Bourennane,[3] and Paweł Horodecki[5,6]

[1]*Laboratoire d'Information Quantique, Université Libre de Bruxelles, Belgium*
[2]*Institute of Theoretical Physics and Astrophysics and the National Quantum Information Centre, Faculty of Mathematics, Physics and Informatics, University of Gdansk, 80-309 Gdansk, Poland.*
[3]*Department of Physics, Stockholm University, S-10691 Stockholm, Sweden*
[4]*Institute of Informatics and the National Quantum Information Centre, Faculty of Mathematics, Physics and Informatics, University of Gdansk, 80-309 Gdansk, Poland.*
[5]*Faculty of Applied Physics and Mathematics and the National Quantum Information Centre, Gdansk University of Technology, 80-233 Gdansk, Poland.*
[6]*International Centre for Theory of Quantum Technologies, University of Gdansk, 80–952 Gdansk, Poland*

Device-Independent (DI) security is the gold standard of quantum cryptography, providing information-theoretic security based on the very laws of nature. In its highest form, security is guaranteed against adversaries limited only by the no-superluminal signalling rule of relativity. The task of randomness amplification, to generate secure fully uniform bits starting from weakly random seeds, is of both cryptographic and foundational interest, being important for the generation of cryptographically secure random numbers as well as bringing deep connections to the existence of free-will. DI no-signalling proof protocols for this fundamental task have thus far relied on esoteric proofs of non-locality termed pseudo-telepathy games, complicated multi-party setups or high-dimensional quantum systems, and have remained out of reach of experimental implementation. In this paper, we construct the first practically relevant no-signalling proof DI protocols for randomness amplification based on the simplest proofs of Bell non-locality and illustrate them with an experimental implementation in a quantum optical setup using polarised photons. Technically, we relate the problem to the vast field of Hardy paradoxes, without which it would be impossible to achieve amplification of arbitrarily weak sources in the simplest Bell non-locality scenario consisting of two parties choosing between two binary inputs. Furthermore, we identify a deep connection between proofs of the celebrated Kochen-Specker theorem and Hardy paradoxes that enables us to construct Hardy paradoxes with the non-zero probability taking any value in $(0, 1]$. Our methods enable us, under the fair-sampling assumption of the experiment, to realize up to 25 bits of randomness in 20 hours of experimental data collection from an initial private source of randomness 0.1 away from uniform.

Introduction.- Device-independent (DI) cryptography [1] achieves the highest form of security in quantum cryptography, namely one where the users do not need to trust the very devices executing the cryptographic protocol. Instead, DI cryptography guarantees information-theoretic security based on the very laws of nature. Furthermore, the honest users can verify the correct execution of the cryptographic protocol and the security of their output by simple statistical tests on the devices, in the form of Bell tests for quantum non-local correlations. In its highest form, such a cryptographic protocol guarantees security based on the simplest and most fundamental law of nature, namely the rule of no-superluminal signalling of relativity. Such a high form of cryptographic security is desirable for many tasks of critical importance, but naturally comes with concomitant stringent requirements on its experimental implementation.

A paradigmatic cryptographic task is that of randomness amplification [5], namely the task of converting a source of partially random bits into one of fully uniform bits. Besides its cryptographic importance in the secure generation of private random bits (which have applications in secure encrypted communications and numerical simulations to gambling), this problem is also of foundational interest with implications for the philosophical problem of the existence of free-will [2]. The amplification of arbitrarily weak random bits into fully random ones is there thought of as the statement that the existence of any weak random physical process implying the existence of a fully random one, in other words, the existence of a complete freedom of choice. Thus, for both fundamental and practical reasons, it is of great interest to have experimentally feasible DI protocols for randomness amplification, and show their security based on the no-signalling principle.

However, all no-signalling proof DI protocols proposed so far for this fundamental task have remained out of reach of experimental implementation. They have relied on esoteric proofs of non-locality termed pseudo-telepathy games, complicated multi-party setups or high-dimensional quantum systems, placing stringent requirements on practical implementations. Therefore, the question of practical feasibility of such protocols, and the experimental realizability of any no-signaling DI protocol (for any cryptographic task even going beyond randomness amplification) has remained open.

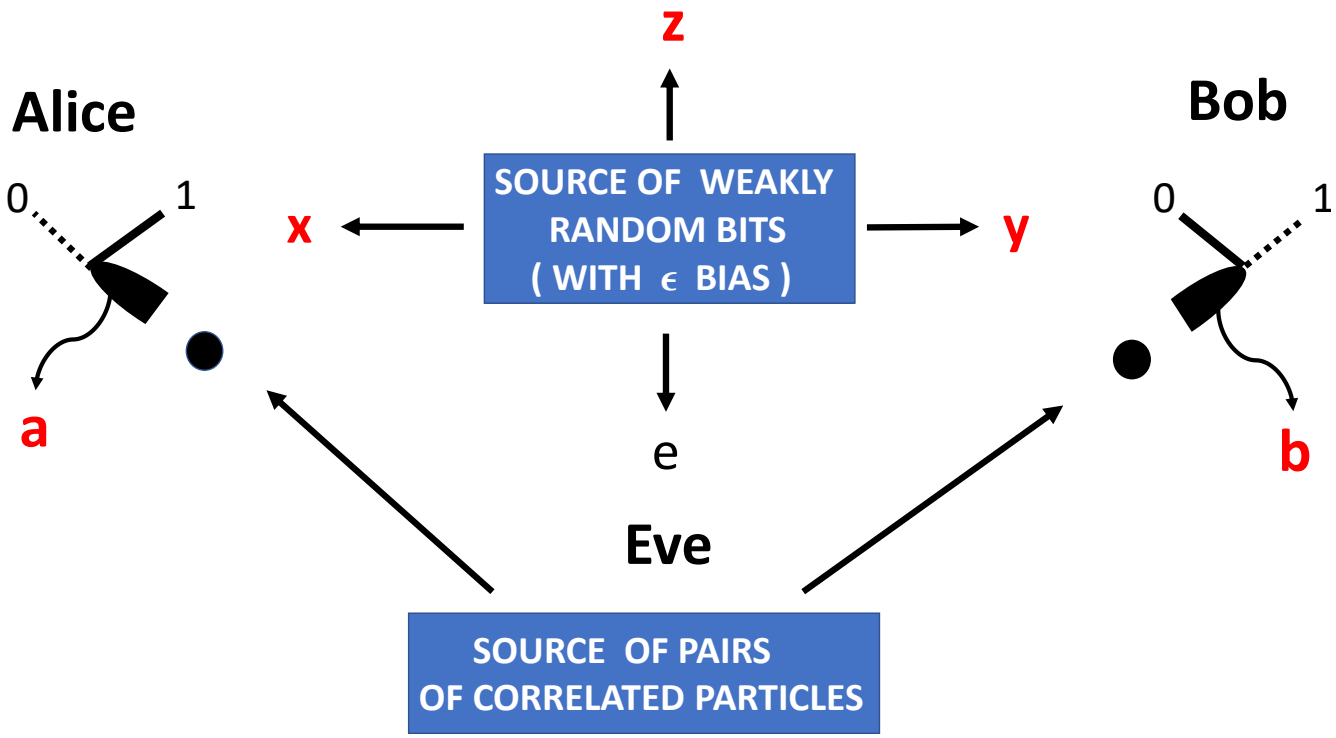

FIG. 1: *Pictorial depiction of the Device-Independent Randomness Amplification (DIRA) protocol. First step: Bell experiment with weakly random settings. An eavesdropper Eve has a source that distributes quantum particles to two parties Alice and Bob. These parties perform measurements on the received particles using apparata with two settings each, constituting the simplest possible* $(2, 2, 2)$ *Bell scenario. The choice of the settings (in each run of the experiment) is made according to bits* (x, y) *obtained from a Santha-Vazirani (SV) source of weakly random bits, which also produces further bits* z *to be fed into a randomness extractor in a subsequent step of the protocol. Eve is taken to hold some classical side information* e *about the weakly random source, as well as some no-signalling side information about the devices held by Alice and Bob. The outputs* (a, b) *produced by these devices are described by a family of probabilities* $\{P_{AB|XY}(ab|xy)\}$*. Note that in the figure, a single run of the experiment is depicted while in practice the scheme is repeated many times producing sequences of bits. The assumption here is that the SV source is private, i.e., that the bits held by Alice and Bob are unknown to Eve. The goal is to produce, out of the outcomes* (a, b) *and some further bits* z *from the SV source, a sequence of final output bits that are secure and fully random from the perspective of Eve. This is achieved by further processing of the outputs in the second step of the protocol (Fig. 2).*

In this paper, we provide the first practically feasible no-signalling proof DI protocol for randomness amplification. We do this by relating the problem of finding experimentally friendly randomness amplification schemes to the vast field of Hardy paradoxes (see Fig. **??**) and, as a consequence, present a device-independent randomness amplification protocol secure against no-signaling adversaries in the simplest experimentally feasible Bell scenario of two parties with two binary inputs. Furthermore, we show that just as proofs of the Kochen-Specker theorem give rise to pseudo-telepathy games, substructures within these proofs termed 01-gadgets give rise to Hardy paradoxes and we use them to construct Hardy paradoxes with the non-zero probability taking any value in $(0, 1]$. The inter-relationship between Hardy paradoxes and Kochen-Specker proofs, also enables us to construct customized Hardy paradoxes with interesting properties. Finally, we provide a partial characterization of the Bell scenarios in which Hardy paradoxes can be used to certify randomness against a no-signaling adversary. We illustrate the realizability of our protocol with state-of-art experimental setups by performing an experimental implementation in a quantum optical setup using polarised photons. Up to the fair-sampling assumption, this thus constitutes the first experimental realization of a DI protocol that enables a weakening of the fundamental freedom-of-choice assumption.

For clarity, all the proofs of the Propositions and the security proof of the randomness amplification protocol are deferred to the Appendices.

Background and Statement of the problem.- The problem of randomness amplification has gained interest since the initial breakthrough work by Colbeck and Renner who showed that quantum non-local correlations enable the amplification of weak sources of specific type, a task which was shown to be impossible with purely classical resources. The model of a source of randomness is the Santha-Vazirani (SV) source [6], a model of a biased coin where the

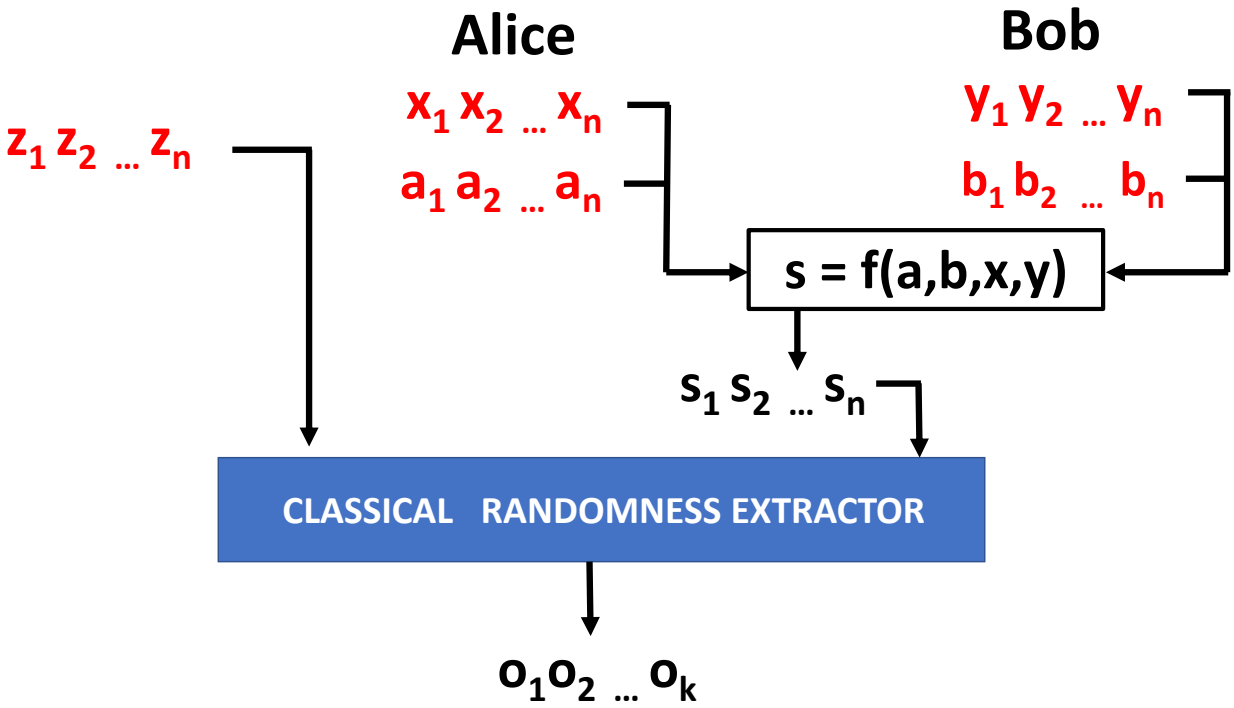

FIG. 2: *Pictorial depiction of the Device-Independent Randomness Amplification (DIRA) protocol. Second step: classical processing of the outputs of the Bell experiment. When the Bell experiment is performed as in Fig. 1, a sequence of outputs in n runs of the experiment, denoted as $\mathbf{a} = a_1, \ldots, a_n$, $\mathbf{b} = b_1, \ldots, b_n$ is obtained for inputs $\mathbf{x} = x_1, \ldots, x_n$, $\mathbf{y} = y_1, \ldots, y_n$. Alice and Bob first calculate the Bell parameter $L_n^{\epsilon}(\mathbf{a}, \mathbf{b}, \mathbf{x}, \mathbf{y})$ and verify that this is above some threshold value $\delta > 0$. They apply a hash function f to the bits $(\mathbf{a}, \mathbf{b}, \mathbf{x}, \mathbf{y})$ to obtain a bit sequence $\mathbf{s} = s_1, \ldots, s_n$ that is partially random and secure from Eve. They feed this bit sequence together with a further bit sequence $z_1, \ldots, z_n$ from the weakly random SV source to a classical randomness extractor to obtain a final output sequence $o_1, \ldots, o_k$ that is fully random and secure from Eve. The magic of the quantumness is manifested in the fact that the bits $\mathbf{s}$ happen to be decorrelated from z, which could never happen if the particles in the experiment from Fig. 1 were classical. This - quantumly originated - decorrelation is the crucial fact that makes the classical independent-source extractor work. The surprising power of the whole scenario is that the final bits stay strongly random even from the perspective of an eavesdropper who is only limited by the fundamental no-superluminal signalling principle of special relativity.*

individual coin tosses are not independent but rather the bits Y_i produced by the source obey

$$\frac{1}{2} - \epsilon \leq P(Y_i = 0 | Y_{i-1}, \ldots, Y_1) \leq \frac{1}{2} + \epsilon. \tag{1}$$

Here $0 \leq \epsilon < \frac{1}{2}$ is a parameter describing the reliability of the source, the task being to convert a source with $\epsilon < \frac{1}{2}$ into one with $\epsilon \to 0$. Since then, several works have proposed DI protocols for the task, and proven security against both quantum [14, 15] and non-signalling adversaries [8, 10, 26]. The latter paradigm, constrained by the impossibility of sending messages instantaneously (i.e., of signaling) has an appealing advantage over the paradigm with quantum adversaries. Namely, while in order to build the devices implementing the protocol, the knowledge of quantum mechanics is necessary, yet verifying whether the device provides true randomness does not require any such knowledge. Security of the randomness produced by the device can be thus verified just by experts in statistics. It is therefore desirable to develop these protocols, and to make them as feasible for implementation as possible. This practical issue goes in parallel with a fundamental one: which quantum correlations constitute the strongest and simplest source of randomness certified by impossibility of signalling.

Usually, the scheme for randomness amplification consists of two ingredients: (i) quantum correlations - whose interaction with the initial weak source of randomness generate additional quantum randomness, and (ii) a classical protocol for amplifying the obtained randomness. Regarding implementation of the scheme in practice, the first ingredient describes the quantum hardware to be built, while the second ingredient describes the needed traditional software, i.e., an algorithm to be run on a standard computer. The main technological challenge is therefore to

implement the quantum part, hence it is mandatory to make it as simple as possible.

The level of technological challenge is to a large extent related to (a) the property of each single device, and here it is desired to have the minimal number of settings and outputs, (b) the number of devices (= the number of parties needed to have quantum correlations), (c) the feasibility of implementation of the quantum states and measurements required (here, two qubit entangled states are preferred in order to achieve the high fidelities required in DI applications) (d) the quality of "raw" quantum randomness - i.e. the probability distribution of a chosen outcome (to be later amplified by the software part) should be as close as possible to the fair coin distribution $(\frac{1}{2}, \frac{1}{2})$. The ultimate bound for (a) and (b) is the Bell scenario $(2, 2, 2)$, meaning, one needs at least two devices, with each device having at least binary inputs and binary outputs (note that throughout this paper we will denote by (n, k, m) the Bell scenario with n parties, each with k inputs and m outputs per input). For typical photonic implementations, the cheapest here seems to be the number of settings, which may be increased if it could lead to better quality of raw randomness.

As yet, none of the protocols based on the simple no-signalling paradigm, has entered the regime of experimental realizability, so that the question of practical feasibility and experimental implementation of any no-signalling proof DI protocol has remained open. There are two basic problems with the present schemes of randomness amplification against a no-signaling adversary [5, 8, 10, 11, 26]. The first problem is that they have a pretty complicated quantum part: either the number of devices, the number of settings/outputs per device, or the dimensionality of quantum states and measurement required is not minimal. This implies a large level of noise, which restricts the range of parameters of the input weak source to be amplified. The simplest existing schemes are in the Bell scenarios (2,9,4) [8], and (4,2,2) [10]. These are still at the edge of the capabilities of present-day technology. And even if the technology were to reach the required level, there will always be a demand for simpler, and cheaper schemes.

The second problem is more conceptual, namely, there are no general easy methods for finding such new schemes. For instance, the scheme of [8] was obtained through extensive symbolic search. In this paper, we resolve both problems, by providing a general method of finding new schemes, as well as achieving the simplest possible scheme involving two devices each having binary inputs and outputs, which was beyond reach thus far.

Methodology.- To this end we combine three ingredients. One of them is the application of the simplest Hardy paradox, following Ref. [7] where it was shown that the Hardy paradox is a natural tool for generating randomness - namely, if the correlations exhibit Hardy paradox, then for a quantum adversary the probability of the so-called Hardy output is often bounded both from both below and from above (however it must be noted that the important problem of randomness amplification was not considered in this context). The power of using Hardy paradoxes as opposed to the pseudo-telepathy games considered so far, is illustrated in Fig. 3.

Second, we employ a novel form of Bell inequalities - ones testing so called "measurement dependent locality" (MDL) of [14, 38]. Finally, we employ a protocol of randomness amplification of [8] which turns out to be ideal to amplify randomness just by use of Hardy paradoxes.

We show that the three ingredients combined together result in a qualitative advance in the case of a no-signaling adversary - the possibility of randomness amplification in $(2, 2, 2)$ (the protocol is depicted in Figures 1 and 2). We further analyse which Hardy paradoxes can be used for randomness amplification, and prove that any Hardy paradox with 2 settings for one party and arbitrary $n \geq 2$ settings for the other party gives rise to a randomness amplification scheme.

Remarkably, in the simplest $(2, 2, 2)$ case, we show that for every input, half of the outputs has probability bounded from above and from below. This allows for huge simplification of the original protocol of Ref. [8], resulting in dramatic improvement of noise tolerance.

These findings provide additional motivation for the community developing Hardy type paradoxes [3, 4, 25, 33], to search for new ones, tailored to randomness amplification scheme. Indeed, as a side product of our investigation, we also relate the generation of Hardy paradoxes to proofs of the Kochen-Specker theorem. In particular, we show that substructures within these proofs termed as 01-gadgets in [19] directly give rise to Hardy paradoxes. We then use this connection to solve an open problem in the design of such paradoxes, by generating Hardy paradoxes where the non-zero probability takes all values in the range $(0, 1]$.

Our results once more show that quantum information is "applied philosophy" [22]: the field of Hardy-type paradoxes, developed initially as a fancy way of proving that Nature violates local-realism, can be directly related to practical issues, providing a qualitative jump in the randomness amplification technology. For other applications of Hardy paradoxes for cryptographic tasks see [23].

Bell inequalities for the task of randomness amplification.- In the task of device-independent randomness amplification (DIRA) against no-signaling adversaries, inequalities where quantum theory allows to reach the no-signaling limit have been considered to be of prime importance. Beginning with Colbeck and Renner's use of the Braunstein-Caves chained Bell inequality in [5], successive works have used versions of the GHZ paradox [10, 26] or two-player pseudo-telepathy games [8]. A failure to reach the no-signaling limit implies that there exists some bias ϵ of the source for which the observed Bell violation can be simulated with classical boxes, leading to an adversarial attack strategy [21]. A central aim of this work is to bring DIRA closer to practical realization, by reducing the number of inputs.

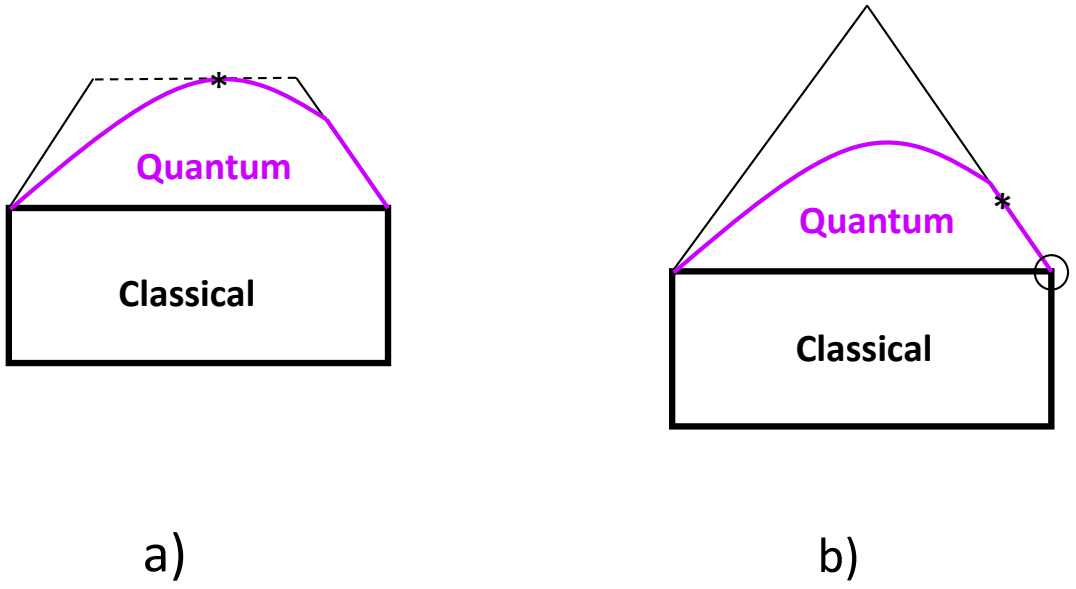

FIG. 3: *A novelty of the present approach that enables practical implementation. The convex sets of statistical behaviors* $\{P_{A,B|X,Y}(a,b|x,y)\}$ *obtainable in Bell experiments using classical, quantum and general no-signalling correlations are depicted here. The quantum correlations outside the classical set enable violation of a Bell inequality. Thus far, it was believed that randomness amplification schemes against no-signalling adversaries required quantum correlations that reached a "pure" no-signalling boundary as in the figure (a) above. These "pseudo-telepathic" correlations (depicted by the dashed line in (a)) met the stringent requirement that their convex decomposition admitted no classical fraction. However, such a stringent requirement was only possible in Bell scenarios with many inputs and outputs and high-dimensional quantum systems making them completely infeasible for practical experimental implementation. A novelty in this paper is the identification that much simpler quantum correlations that violate Hardy paradoxes, i.e., which only reach "partial" no-signalling boundaries as in figure (b) above, can still enable DIRA against a general no-signalling adversary. Crucially, our protocol enables the application of these correlations to the task, despite the fact that these correlations admit a significant classical fraction, denoted by the circle* $\circ$*, when considered as a convex mixture of general no-signalling behaviors. Furthermore, the special Hardy behaviors such as the point denoted by (*) in the figure (b), are already realizable in the simplest possible* $(2,2,2)$ *Bell scenario of two parties choosing two binary inputs, which corresponds to simple polarization-entangled photon experiments that are realized everyday in photonic laboratories with high fidelities. It is noteworthy that the pseudo-telepathic part of the boundary is well-known to not exist in this simple case, as illustrated in (b).*

To this end, we present a DIRA protocol based on Hardy paradoxes, which are proofs of non-locality with a similar flavour to pseudo-telepathy games, in that they also impose the probability of a particular subset of events to be zero.

Hardy's original paradox [3, 4] was regarded by Mermin to be the "simplest form of Bell's theorem" [31]. In the $(2,2,2)$ Bell scenario, the two parties Alice and Bob choose between two inputs X, Y taking values $x, y \in \{0,1\}$ respectively, and obtain outcomes A, B taking values $a, b \in \{0,1\}$ respectively. The observed probability distribution of their outputs conditioned upon the inputs is then denoted by $P_{\mathrm{A,B|X,Y}}(a,b|x,y)$. In this scenario, the paradox is formulated by the following four constraints:

$$\begin{aligned} \text{(i)}\ P_{\mathrm{A,B|X,Y}}(0,1|0,1) &= 0, \\ \text{(ii)}\ P_{\mathrm{A,B|X,Y}}(1,0|1,0) &= 0, \\ \text{(iii)}\ P_{\mathrm{A,B|X,Y}}(0,0|1,1) &= 0, \\ \text{(iv)}\ P_{\mathrm{A,B|X,Y}}(0,0|0,0) &> 0. \end{aligned} \tag{2}$$

While classically, it is simple to verify that conditions (i)-(iii) impose the probability of the "Hardy output" to be zero, i.e., $P_{\mathrm{A,B|X,Y}}(0,0|0,0) = 0$, there exist a suitable two-qubit non-maximally entangled state and dichotomic

measurements such that all four conditions are obeyed. Explicitly, Alice and Bob perform on the shared state

$$|\psi_\theta\rangle = \frac{1}{\sqrt{1+\cos(\theta)^2}}\left[\cos(\theta)\left(|01\rangle+|10\rangle\right)+\sin(\theta)|11\rangle\right], \tag{3}$$

measurements in the bases

$$\begin{aligned} &\{|0\rangle,|1\rangle\} \quad \text{for } x,y=1,\\ &\{\sin\theta|0\rangle-\cos\theta|1\rangle,\cos\theta|0\rangle+\sin\theta|1\rangle\} \ \text{ for } x,y=0. \end{aligned} \tag{4}$$

The constraints (i)-(iv) are satisfied for any value $0<\theta<\pi/2$, and the optimal value of $P_{\mathrm{A,B|X,Y}}(0,0|0,0)$ ($=\frac{5\sqrt{5}-11}{2}\approx 0.09$) is achieved at $\theta=\arccos\left(\sqrt{\frac{\sqrt{5}-1}{2}}\right)$. Hardy's paradox is thus a proof of "non-locality without inequalities". Yet it is also a probabilistic proof, in the sense that the difference between classical and quantum worlds in the paradox lies in the possibility of occurrence of some type of events.

Hardy paradoxes and randomness certification.- Since the discovery of the original Hardy paradox in the $(2,2,2)$ Bell scenario, the paradoxes have been intensively studied and various extensions have been proposed [9, 33, 36], especially with a view to boost the probability of the Hardy output. In [7] it was noted that the Hardy paradox is especially suited to reveal intrinsic randomness of quantum statistics. Namely, the authors show (in the case of quantum adversary) that the Hardy output is a source of so-called min-entropy, identifying thereby a natural source of Bell inequalities dedicated for randomness generation. Note here, that while the Hardy paradox is termed a paradox without inequalities, in the presence of noise it becomes a Bell inequality (similar to how Kochen-Specker paradoxes in contextuality are tested in labs by means of Cabello-type inequalities [28]).

On the other hand, one can notice that the Bell inequality used in a DIRA protocol of Ref. [8] – which allowed for the first time to amplify arbitrarily weak randomness by use of two devices – can be seen as a variant of Hardy paradox, and the Hardy's output probability is used as a source of min-entropy needed for obtaining randomness.

Last but not least, recently a concept of measurement dependent locality inequalities appeared, which is suitable for randomness amplification problems.

Combining the above concepts, we will show in this paper that a DIRA protocol can be constructed starting from any Hardy paradox that certifies randomness against a no-signaling adversary for arbitrary initial ϵ. Before present this main result, let us discuss a couple of important questions that arise in this regard. Firstly, it is interesting to see if all Hardy paradoxes certify randomness against a no-signaling adversary. Secondly, it is important to understand how far the probability of the Hardy output can be boosted.

In answering the first question, we observe that any no-signaling box in the (2,2,2) Bell scenario that satisfies conditions (i) - (iv) of the original Hardy paradox also satisfies $P_{A,B|X,Y}(0,0|0,0)\leq\frac{1}{2}$. This is due to the fact that the only non-local no-signaling extremal box in this scenario is the Popescu-Rohrlich (PR) box (up to relabeling of parties, inputs and outputs) whose entries are in $\{0,\frac{1}{2}\}$, [40] and any box that satisfies conditions (i) - (iii) is a convex mixture of a PR box and classical boxes which have $P_{A,B|X,Y}(0,0|0,0)=0$. This therefore implies partial randomness in the outputs for the input $(0,0)$ in any no-signaling box. Specifically, assigning bit value 0 to the output pair $(0,0)$ and bit value 1 to the output pairs $(0,1),(1,0),(1,1)$, one obtains a partially random bit S of the form $0<P_{S|X,Y}(s=0|0,0)\leq\frac{1}{2}$. We will have more to say about the randomness in this particular scenario in Section IE of the Appendix. We now consider whether such a phenomenon is generic to all Hardy paradoxes, i.e., is it the case that every two-party Hardy paradox which certifies that $P_{A,B|X,Y}(a^*,b^*|x^*,y^*)>0$ also guarantees that $P_{A,B|X,Y}(a^*,b^*|x^*,y^*)<1$?

In Section IIC of the Appendix, we show (in Proposition **??**) that this is the case when both parties have binary outputs $|\mathcal{A}|=|\mathcal{B}|=2$. We then move to the case when Alice measures 2 observables and Bob measures $n>2$ observables, each with an arbitrary number of outputs, and show in Prop. **??** of Section **??** that in this case the probability of the Hardy output is bounded as $P_{A,B|X,Y}(a^*,b^*|x^*,y^*)\leq\frac{n-1}{n}$, again giving rise to partial randomness. Finally, we consider the case where both parties measure more than two observables with more than two outputs each, i.e., $|\mathcal{A}|=|\mathcal{B}|=m>2$. In this case, we show in Section **??** that for all $m>2$, there exist Hardy paradoxes such that $0<P^q_{A,B|X,Y}(a^*,b^*|x^*,y^*)<1$ and yet $P^{ns}_{A,B|X,Y}(a^*,b^*|x^*,y^*)=1$. In other words, in this case, even though the probability of the Hardy output is strictly bounded below 1 in quantum theory, there exist no-signaling boxes that achieve the value 1 while satisfying the same Hardy constraints. Therefore, in using paradoxes with more than two outputs for device-independent randomness certification, a linear programming check is needed in each specific instance to ensure that the Hardy probability is strictly bounded below 1. We now proceed to answer the second interesting question as to how far the Hardy output probability can be boosted, and relate this problem to a class of local contextuality sets recently studied in [19, 20].

Protocol I

1. The ϵ-SV source is used to choose the measurement settings (x_i, y_i) for n runs on a single device consisting of two components. The device produces output bits $x = (a_i, b_i)$ with $i \in \{1, \ldots, n\}$.
2. The parties perform an estimation of the violation of a measurement-dependent locality inequality from the Hardy paradox by computing the empirical average $L_n^{\epsilon}(\mathbf{a}, \mathbf{b}, \mathbf{x}, \mathbf{y}) := \frac{1}{n} \sum_{i=1}^{n} w_i(\epsilon) B_{\mathrm{H}}(a_i, b_i, x_i, y_i)$. The protocol is aborted unless $L_n^{\epsilon}(\mathbf{a}, \mathbf{b}, \mathbf{x}, \mathbf{y}) \geq \delta$ for fixed constant $\delta > 0$.
3. Conditioned on not aborting in the previous step, the parties apply an independent source extractor [29, 30] to the sequence of outputs from the device and further n bits from the SV source.

FIG. 4: Protocol for device-independent randomness amplification using the two-party Hardy paradox.

Generating new Hardy paradoxes using contextuality.- Several improvements on the probability of the Hardy output have been proposed in the literature [9, 25, 33]. A "ladder paradox" was introduced in [9] in the $(2, k, 2)$ scenario of two parties, each choosing from k binary inputs. In the limit of a large number of inputs ($k \to \infty$), the Hardy probability was shown to approach 0.5, with the corresponding state getting close to the maximally entangled state. An extension to two qudit systems for $d > 2$ considered in [33] makes use of the following conditions in the $(2, 2, d)$ scenario: $P_{A,B|X,Y}(a < b|1, 0) = 0$, $P(b < a|0, 0) = 0$, $P(a < b|0, 1) = 0$ and $P(a < b|1, 1) > 0$. While classically it is easy to see that the above conditions cannot be satisfied simultaneously, it was numerically verified that in quantum theory the maximum value of the non-zero probability in this case is ≈ 0.417 for large d. The occurrence of the original Hardy paradox as a universal sub-structure within the Hardy paradoxes in $(2, k, 2)$ and $(2, 2, d)$ Bell scenarios was studied by Mansfield and Fritz in [24]. In [25], Mančinska and Vidick proposed a generalization of Hardy's paradox, increasing the probability of the Hardy output to the entire interval $(0, 1]$, but at the expense of a large number of outputs and increasing dimensionality of the shared quantum state. More precisely they showed that in the $(2, 2, 2^d)$ scenario, the probability of the Hardy output can be boosted to $1-(1-p_Q^*)^d$ where $p_Q^* = \frac{5\sqrt{5}-11}{2}$, so that infinite dimensional states are required to achieve the entire interval $(0, 1]$. In this paper, we relate the field of Hardy paradoxes to so-called 01-gadgets - basic ingredients of the Kochen-Specker paradox [19, 20]. In particular, we show how to construct Hardy paradoxes using these local contextuality proofs to achieve the entire interval $(0, 1]$ using a finite number of inputs, and as few as four outputs, with a shared two-ququart maximally entangled state. The details of the construction are shown in Section IIF in the Appendix. It is well-known that proofs of the Kochen-Specker theorem give rise to pseudo-telepathy games [16, 17], and we now find that in a foundational analogy, the so-called gadget substructures within these proofs similarly lead to Hardy paradoxes neatly connecting these domains of study. We now outline a generic procedure to design DIRA protocols against no-signaling adversaries using Hardy paradoxes.

A generic procedure to obtain DIRA protocols using Hardy paradoxes.-

(a) Given a Hardy paradox, identify the pair of Hardy settings (x^*, y^*), and Hardy output (a^*, b^*).

(b) obtain the maximal quantum value probability $P_{\mathrm{A,B|X,Y}}(a^*, b^*|x^*, y^*)$ denoted by p_Q^*.

(c) Use linear programming to find the maximal no-signaling value of the probability $P_{\mathrm{A,B|X,Y}}(a^*, b^*|x^*, y^*)$ denoted by p_{NS}^*.

(d) Check for each input if at least one of the output probabilities is bounded strictly below unity. This can be verified using linear programming.

(e) If item (d) applies, use the software part Protocol I (Fig. 4). If not, apply the software part Protocol II (Fig. 11 stated in Section I of the Appendix.

Remark. The linear programming part is replacing the semidefinite programming used in works such as [7] for a quantum adversary.

Note that as we show in Section IE of the Appendix, the condition in item (d) directly applies in the (2,2,2) scenario without resorting to linear programming, i.e., we establish for each input in this scenario, strict and achievable bounds on the output probabilities.

Randomness amplification in the simplest (2,2,2) Bell scenario.- We exemplify the procedure by means of the simplest Hardy paradox in the experimentally feasible (2,2,2) Bell scenario, with the security proof provided in Appendix I. The Protocol I of Fig. 4 for extracting randomness from Hardy paradoxes is a modification of the protocol we designed in [8]. In that protocol, the honest parties were required to perform two tests: one for the Hardy constraints such as (i)-(iii) from Eq.(2), and a second test corresponding to constraint (iv). This second test served to

lower bound the value of the Hardy output $P_{\mathrm{A,B|X,Y}}(a^*, b^*|x^*, y^*)$ in a linear number of runs. In the modified Protocol I proposed above, we combine these two tests into a single test estimating the violation of a *measurement-dependent locality inequality* (see Section IF of the Appendix) first introduced in [38]. The proof of security is appropriately modified [8, 10] and is sketched with the particular parameters of the simplest (2,2,2) Hardy paradox in Section I and Section IV of the Appendix. In particular, when the test is passed (i.e., the measurement-dependent locality quantity is observed to satisfy $L_n^{\epsilon}(\mathbf{a}, \mathbf{b}, \mathbf{x}, \mathbf{y}) \geq \delta$ for some $\delta > 0$), we certify that the outputs constitute a min-entropy source of linear min-entropy h_{box} given by (see Appendix IV A for the derivation of this expression)

$$h_{box} \geq \max_{\delta_{Az},\kappa} \Bigg[\frac{n}{4} \min \Bigg\{ -\left(\frac{\delta - \delta_{Az} - \kappa}{\frac{1}{16} - \kappa}\right) \log_2 \left(1 - \frac{\kappa}{2(\frac{1}{4} - \epsilon^2)^2}\right), \log_2(e) \frac{\delta_{Az}^2}{4} \Bigg\} - \frac{3}{4} \Bigg] \tag{5}$$

for parameters $0 < \delta_{Az} < \delta$ and $0 < \kappa < \delta - \delta_{Az}$. Feeding these bits together with some further bits from SV source into a randomness extractor [41], and following an analogous proof to [8, 10], we obtain $\Omega(n^{1/4})$ bits that are guaranteed to be secure under the strong universal composability criterion. The universally composable security parameter d_c given by [39]

$$d_c := \sum_{o,e} \max_{w} \sum_{z} \left| P_{O,Z,E|W,ACC}(o, z, e|w, ACC) - \frac{1}{|O|} P_{Z,E|W,ACC}(z, e|w, ACC) \right|, \tag{6}$$

is shown to satisfy

$$d_c \times P(\mathrm{ACC}) \leq 2^{-\Omega(n^{1/4})}, \tag{7}$$

where $P(\mathrm{ACC})$ denotes the probability with which the test in the protocol is passed.

Experiment.- In our experiment, the physical qubits are single-photon polarization states and the computational basis corresponds to the horizontal (H) and vertical (V) polarization, i.e., $|H\rangle \equiv |0\rangle$ and $|V\rangle \equiv |1\rangle$. To produce the state in Eq.(3), an ultraviolet pump laser at $390nm$ was focused onto two beta barium borate (BBO) crystals places placed in cross-configuration to produce photon pairs emitted into two spatial modes "a" and "b" through a type-I Spontaneous Parametric Down-Conversion (SPDC) process. Two crystals were used for compensation of longitudinal and transversal walk-offs. The emitted photons were coupled into single-mode optical fibers and passed through a narrow-bandwidth interference filter to secure well-defined spatial and spectral emission modes (see Fig. 5). To observe the desired state, we have used a half wave plate (HWP) oriented at 27.86 degrees and placed after the output fiber coupler in each of the two modes. The polarization measurement was performed using HWPs and polarizing beam splitters followed by single photon detectors. We have performed the full state tomography and we have obtained the desired state with very high fidelity of $F = 0.997 \pm 0.001$ where the fidelity is given by $F = \langle\psi_\theta|\rho_{\mathrm{exp}}|\psi_\theta\rangle$, of the experimentally prepared state ρ_{exp} with respect to the optimal ψ_θ. For the Hardy test, the settings of Alice and Bob (for $x, y = 1$) and (for $x, y = 0$) 4 were implemented with a help of a HWP oriented at the angle for 64.09 and 0 degrees respectively. The average rate of the two photon counting coincidence events was 10^5 per second and the measurement time for each setting was 5 hours (giving a total of 20 hours of experimental data collection).

During each measurement, the total number of coincidence counts for Alice and Bob's settings ($x = 0, y = 0$), ($x = 0, y = 1$), ($x = 1, y = 0$), and ($x = 1, y = 1$) were 1.90×10^9, 1.91×10^9, 1.91×10^9, and 1.93×10^9 respectively. The obtained joint probability $P_{AB,XY}(ab, xy)$ and corresponding errors (standard deviations in the estimated probabilities) for $a, b = \{0, 1\}$ the outputs of Alice and Bob's measurements respectively and $x, y = \{0, 1\}$, Alice and Bob's settings respectively are listed in the table I . In particular the probabilities $P_{\mathrm{AB,XY}}(00, 00) = 0.022668 \pm 0.000035$, $P_{\mathrm{AB,XY}}(01, 01) = 0.000384 \pm 0.000004$, $P_{\mathrm{AB,XY}}(10, 10) = 0.000363 \pm 0.000004$,and $P_{\mathrm{AB,XY}}(00, 11) = 0.000203 \pm 0.000003$. For further details on the experimental setup and results see Appendix III.

Final output randomness from the experimental data.- The detailed analysis of the final output randomness, obtained by applying the randomness extractor to the min-entropy from the device and further bits from the SV source, is performed in Appendix IV. With respect to the specific randomness extractor from [41] that we apply here, our experimental data allows for the production of $k(\epsilon, t)$ bits of final output randomness, where

$$k(\epsilon, t) = \frac{g(\delta_{exp}, \epsilon, n)n - (t + 3)}{2}, \tag{8}$$

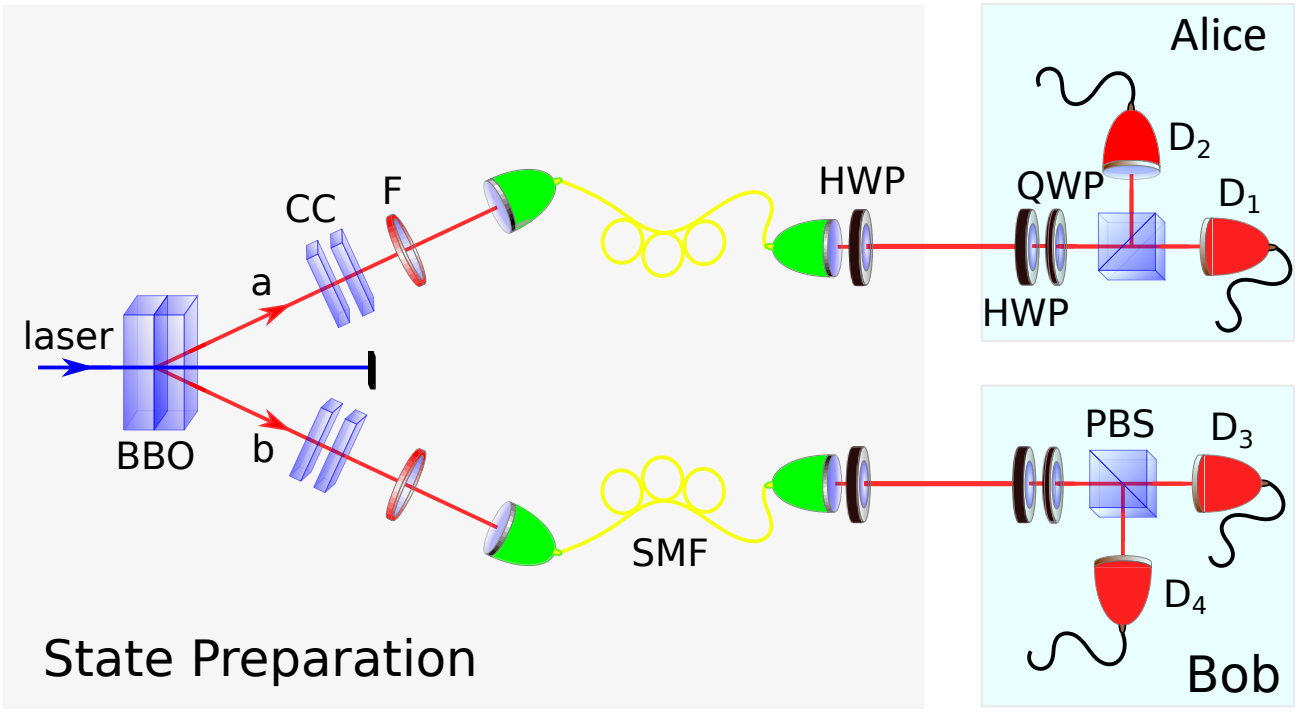

FIG. 5: Preparation and measurement setup. A UV pump laser at $390nm$ was focused onto two beta barium borate (BBO) crystals places in cross-configuration to produce photon pairs emitted into two spatial modes "a" and "b" through type-I SPDC process. To remove any spatial, temporal or spectral distinguishability between the photons we use a pair of YVO_4 crystals (CC), narrow-bandwidth filters (F) ($\lambda = 1$ nm), and coupling into single-mode fibers (SMF). To prepare the state 3, the photon polarizations in each mode are rotated through a half wave plate (HWP). Alice's and Bob's measurements were performed using a HWP, a quarter wave plate (QWP), a polarizing beam splitter (PBS) and single-photon avalanche photodiodes $D_i (i = \{1, 2, 3, 4\})$.

for experimentally obtained MDL value δ_{exp}, experimental number of runs n and a security parameter $t > 0$. The distribution $\{q_i\}, i = 1, \ldots, 2^k$ of the final $k(\epsilon, t)$ output bits satisfies

$$q_i \leq \frac{1}{2^k}\left(1 + 2^{-t}\right). \tag{9}$$

The explicit form of the function $g(\delta_{exp}, \epsilon, n)$, encapsulating the details of the protocol including also the experimental data, is provided in the Appendix IV. Exemplary data showing the number of output bits $k(\epsilon, t)$ as a function of the initial ϵ from the SV source are shown in the Fig. (6) for particular values of the security parameter t ($t = 5, 10, 100$, with the final bits deviating from uniform by 2^{-t-1}). One can see that the state-of-art experimental setups are able to achieve the parameters required for reasonable randomness production by our protocol. It must be stressed that, up to the fair-sampling assumption, this is the first time ever that any device-independent protocol secure against a no-signalling adversary has been implemented in the lab, since all previous schemes had stringent requirements far beyond the scope of any experimental technology known to date.

Conclusions.- In this paper, we have shown a generic application of Hardy paradoxes to a scheme of device-independent randomness amplification secure against general no-signaling adversaries. Remarkably, the Hardy paradox allows for experimentally friendly parameters in the simplest (2,2,2) Bell scenario, providing the first practically feasible device-independent application against a no-signaling adversary. We have illustrated this feasibility with help of the routine two-photon experiment, achieving the satisfactory rates. This is the first time, when such an illustration is provided, since the previous protocols were out of reach of the state-of-art technology.

Furthermore, we answered interesting questions arising with regard to Hardy paradoxes and randomness certification. We have shown that Hardy paradoxes with binary outputs, and those with two observables for one party

TABLE I: The obtained joint number of coincidence counts $n_{AB,XY}(ab,xy)$ (in multiples of 10^6), joint probabilities $P_{AB,XY}(ab,xy)$ and corresponding errors (standard deviations in the estimated probabilities) for $a,b = \{0,1\}$ the outputs of Alice and Bob's measurements respectively and or $x,y = \{0,1\}$, Alice and Bob's settings respectively

(ab,xy)	**Counts** 10^6	**Probabilities**	**Error**
$(00,00)$	173.54	0.022668	0.000035
$(01,00)$	284.78	0.037198	0.000045
$(10,00)$	301.86	0.039430	0.000046
$(11,00)$	1143.84	0.149410	0.000095
$(00,01)$	459.53	0.060024	0.000058
$(01,01)$	2.94	0.000384	0.000004
$(10,01)$	257.02	0.033572	0.000043
$(11,01)$	1190.90	0.155556	0.000097
$(00,10)$	479.39	0.062619	0.000059
$(01,10)$	270.59	0.035345	0.000044
$(10,10)$	2.78	0.000363	0.000004
$(11,10)$	1162.20	0.151788	0.000096
$(00,11)$	1.56	0.000204	0.000003
$(01,11)$	715.59	0.093471	0.000073
$(10,11)$	754.50	0.098554	0.000075
$(11,11)$	454.88	0.059417	0.000057

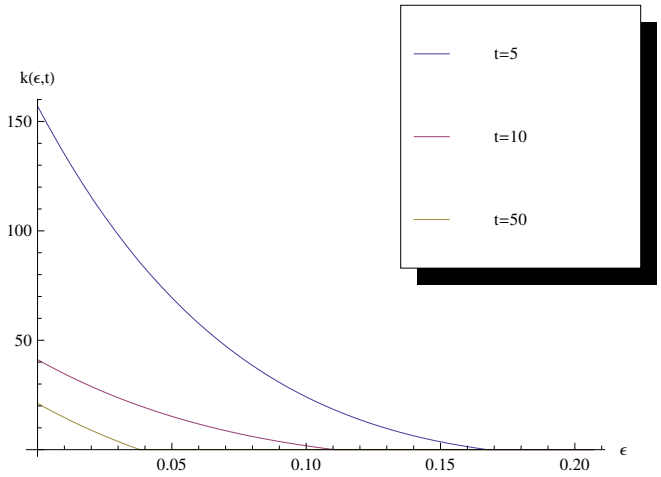

FIG. 6: The number of output bits $k(\epsilon,t)$ versus ϵ for three values of security parameter t (recall that the final k bits deviate from uniform by 2^{-t-1}).

allow for generic randomness certification against no-signaling adversaries, while more general Bell scenarios require specific linear programming checks. Moreover, we have shown that just as Kochen-Specker sets give rise to two-player pseudo-telepathy games, subsets within the KS proofs provide a systematic method to construct Hardy paradoxes. We use this to solve an open problem showing the existence of Hardy paradoxes with finite numbers of inputs and outputs for which the non-zero Hardy probability takes any value in the interval $(0,1]$.

An interesting open question is to optimize the construction of Hardy paradoxes to obtain the DIRA scheme with highest min-entropy rate, under constant noise-tolerance. A similar question arises to find the minimal Hardy paradox (with minimum input, output parameters) that allows the probability of the Hardy output to take all values in $(0,1]$. An important question in general DIRA schemes is to relax the assumption of independence between source and device which has so far been employed in all finite-device randomness amplification schemes against no-signaling adversaries [11].

Acknowledgements.- R.R. acknowledges support from the research project "Causality in quantum theory: foundations and applications" of the Fondation Wiener-Anspach and from the Interuniversity Attraction Poles 5 program of

the Belgian Science Policy Office under the grant IAP P7-35 photonics@be. This work is supported by the Start-up Fund 'Device-Independent Quantum Communication Networks' from The University of Hong Kong. This work was supported by the National Natural Science Foundation of China through grant 11675136, the Hong Kong Research Grant Council through grant 17300918, and the John Templeton Foundation through grants 60609, Quantum Causal Structures, and 61466, The Quantum Information Structure of Spacetime (qiss.fr). MH and PH are supported by the John Templeton Foundation. The opinions expressed in this publication are those of the authors and do not necessarily reflect the views of the John Templeton Foundation. M.H. is also supported by the National Science Centre, Poland, grant OPUS 9. 2015/17/B/ST2/01945. KH acknowledges support from the grant Sonata Bis 5 (grant number: 2015/18/E/ST2/00327) from the National Science Centre. S.P. is a Research Associate of the Fonds de la Recherche Scientifique (F.R.S.-FNRS). We acknowledge support from the EU Quantum Flagship project QRANGE.

---

[1] S. Pironio et al. "Random numbers certified by Bell's theorem". Nature **464**, 1021 (2010).

[2] W. Myrvold, *Philosophical Issues in Quantum Theory*, in: https://plato.stanford.edu/entries/qt-issues/

[3] L. Hardy. Quantum mechanics, local realistic theories, and Lorentz-invariant realistic theories. Phys. Rev. Lett., **68**(20):2981 (1992).

[4] L. Hardy. *Nonlocality for two particles without inequalities for almost all entangled states*. Phys. Rev. Lett., **71**(11):1665 (1993).

[5] R. Colbeck and R. Renner. *Free randomness can be amplified*. Nat. Phys. **8**, 450 (2012), arXiv:1105.3195 (2011).

[6] M. Santha and U. V. Vazirani. *Generating quasi-random sequences from slightly-random sources*. In Proc. of the 25th IEEE Symp. on Found. of Comp. Sci. (FOCS-84), 434 (1984).

[7] Hong-Wei Li, Marcin Pawlowski, Ramij Rahaman, Guang-Can Guo, Zheng-Fu Han, *Device and semi-device independent random numbers based on non-inequality paradox*, Phys. Rev. A 92, 022327 (2015), arXiv:1402.1850 (2014).

[8] R. Ramanathan, F. G. S. L. Brandão, K. Horodecki, M. Horodecki, P. Horodecki and H. Wojewódka. *Randomness amplification against no-signaling adversaries using two devices*. Phys. Rev. Lett. **117**, 230501 (2016), arXiv:1504.06313 (2015).

[9] D. Boschi, S. Branca, F. De Martini, and L. Hardy. *Ladder proof of nonlocality without inequalities: Theoretical and experimental results*. Phys. Rev. Lett., **79**(15):2755 (1997).

[10] F. G. S. L. Brandão, R. Ramanathan, A. Grudka, K. Horodecki, M. Horodecki, P. Horodecki, T. Szarek, H. Wojewódka. *Robust Device-Independent Randomness Amplification with Few Devices*. Nat. Comm. **7**, 11345 (2016), arXiv:1310.4544 (2013).

[11] H. Wojewódka, F. G. S. L. Brandão, A. Grudka, M. Horodecki, K. Horodecki, P. Horodecki, M. Pawłowski, R. Ramanathan. *Amplifying the randomness of weak sources correlated with devices*. IEEE Trans. on Inf. Theory. Vol. PP, Issue 99 (2017), arXiv:1601.06455, (2016).

[12] A. Panconesi and A. Srinivasan, Randomized distributed edge coloring via an extension of the Chernoff-Hoeffding bounds. SIAM Journal on Computing **26**, 350 (1997).

[13] A. Cabello, S. Severini and A. Winter. *Graph-Theoretic Approach to Quantum Correlations*. Phys. Rev. Lett. **112**, 040401 (2014), arXiv:1401.7081 (2014).

[14] M. Kessler, R. Arnon-Friedman. *Device-independent Randomness Amplification and Privatization*. arXiv:1705.04148 (2017).

[15] K.-M. Chung, Y. Shi, and X. Wu. *Physical Randomness Extractors: Generating Random Numbers with Minimal Assumptions*. arXiv:1402.4797 (2014).

[16] G. Brassard, A. Broadbent and A. Tapp. *Quantum Pseudo-Telepathy*. Found. of Phys., vol. **35**, 11, 1877 (2005), arXiv:quant-ph/0407221 (2014).

[17] R. Renner and S. Wolf. *Quantum pseudo-telepathy and the Kochen-Specker theorem*. In Proc. Int. Symp. Inf. Theory, pp. 322-329 (2004).

[18] R. Ramanathan and P. Horodecki. *Necessary and sufficient conditions for state-independent measurement contextual scenarios*. Phys. Rev. Lett. **112**, 040404 (2014), arXiv:1212.5933 (2012).

[19] R. Ramanathan, M. Rosicka, K. Horodecki, S. Pironio, M. Horodecki and P. Horodecki. *Gadget structures in proofs of the Kochen-Specker theorem*. arXiv:1807.00113 (2018).

[20] A. Cabello, J. R. Portillo, A. Solis and K. Svozil *Minimal true-implies-false and true-implies-true sets of propositions in noncontextual hidden variable theories*. Phys. Rev. A **98**, 012106 (2018), arXiv:1805.00796 (2018).

[21] A. Grudka, K. Horodecki, M. Horodecki, P. Horodecki, M. Pawłowski, and R. Ramanathan. *Free randomness amplification using bipartite chain correlations*. Phys. Rev. A **90**, 032322 (2014), arXiv:1303.5591 (2013).

[22] The term coined by Marek Zukowski.

[23] R. Rahaman, M. Wiesniak and M. Zukowski. *Quantum Byzantine Agreement via Hardy correlations and entanglement swapping*. Phys. Rev. A 92, 042302 (2015), arXiv:1408.1540 (2014).

[24] S. Mansfield and T. Fritz. *Hardy's Non-locality Paradox and Possibilistic Conditions for Non-locality*. Found. of Phys., Vol 42, No. 5, 709 (2012), arXiv:1105.1819 (2011).

[25] L. Mančinska and T. Vidick. *Unbounded entanglement can be needed to achieve the optimal success probability*. In: Esparza J., Fraigniaud P., Husfeldt T., Koutsoupias E. (eds) Automata, Languages, and Programming. ICALP 2014. Lecture Notes in Computer Science, vol 8572. Springer, Berlin, Heidelberg (2014), arXiv:1402.4145, (2014).

[26] R. Gallego, L. Masanes, G. de la Torre, C. Dhara, L. Aolita and A. Acin. *Full randomness from arbitrarily deterministic events*. Nature Communications 4, 2654 (2013), arXiv:1210.6514 (2012).

[27] R. K. Clifton. *Getting Contextual and Nonlocal Elements-of-Reality the Easy Way.* American Journal of Physics, **61**: 443 (1993).

[28] A. Cabello. *Experimentally testable state-independent quantum contextuality*. Phys. Rev. Lett. **101**, 210401 (2008), arXiv:0808.2456 (2008).

[29] B. Chor and O. Goldreich, Unbiased bits from sources of weak randomness and probabilistic communication complexity. SIAM Journal on Computing, 17(2): 230 (1988).

[30] E. Chattopadhyay and D. Zuckerman, Explicit two-source extractors and resilient functions. Electronic colloquium on computational complexity. Revision 1 of Report No. 119 (2015).

[31] N. D. Mermin, Am. J. Phys. **62**, 880 (1994).

[32] A. M. Gleason. *Measures on the Closed Subspaces of a Hilbert Space.* Journal of Mathematics and Mechanics **6**, 885 (1957).

[33] J-L. Chen, A. Cabello, Z-P. Xu, H-Yi. Su, C. Wu, L. C. Kwek. *Hardy's Paradox for High-Dimensional Systems: Beyond Hardy's Limit*. Phys. Rev. A **88**, 062116 (2013), arXiv:1308.4468 (2013).

[34] N. S. Jones and L. Masanes. *Interconversion of Nonlocal Correlations*. Phys. Rev. A **72**, 052312 (2005), arXiv:quant-ph/0506182 (2005).

[35] J. Barrett and S. Pironio. *Popescu-Rohrlich Correlations as a Unit of Nonlocality.* Phys. Rev. Lett. 95, 140401 (2005), arXiv:quant-ph/0506180 (2005).

[36] S. Abramsky, C. M. Constantin and S. Ying. *Hardy is (almost) everywhere: nonlocality without inequalities for almost all entangled multipartite states*. Information and Computation vol. **250**, 3 (2016), arXiv:1506.01365 (2015).

[37] P. M. Cohn. *Basic algebra: groups, rings, and fields*. Springer (2003).

[38] G. Pütz, D. Rosset, T. J. Barnea, Y.-C. Liang and N. Gisin. *Arbitrarily small amount of measurement independence is sufficient to manifest quantum nonlocality*. Phys. Rev. Lett. **113**, 190402 (2014), arXiv:1407.5634, (2014).

[39] C. Portmann and R. Renner. *Cryptographic security of quantum key distribution*. arXiv:1409.3525 (2014).

[40] S. Popescu and D. Rohrlich. *Nonlocality as an axiom*. Foundations of Physics. 24 (3): 379 (1994).

[41] Ran Raz. *Extractors with weak random seeds*. STOC '05: Proceedings of the thirty-seventh annual ACM symposium on Theory of computing May 2005, pages 11–20, https://doi.org/10.1145/1060590.1060593

Figures

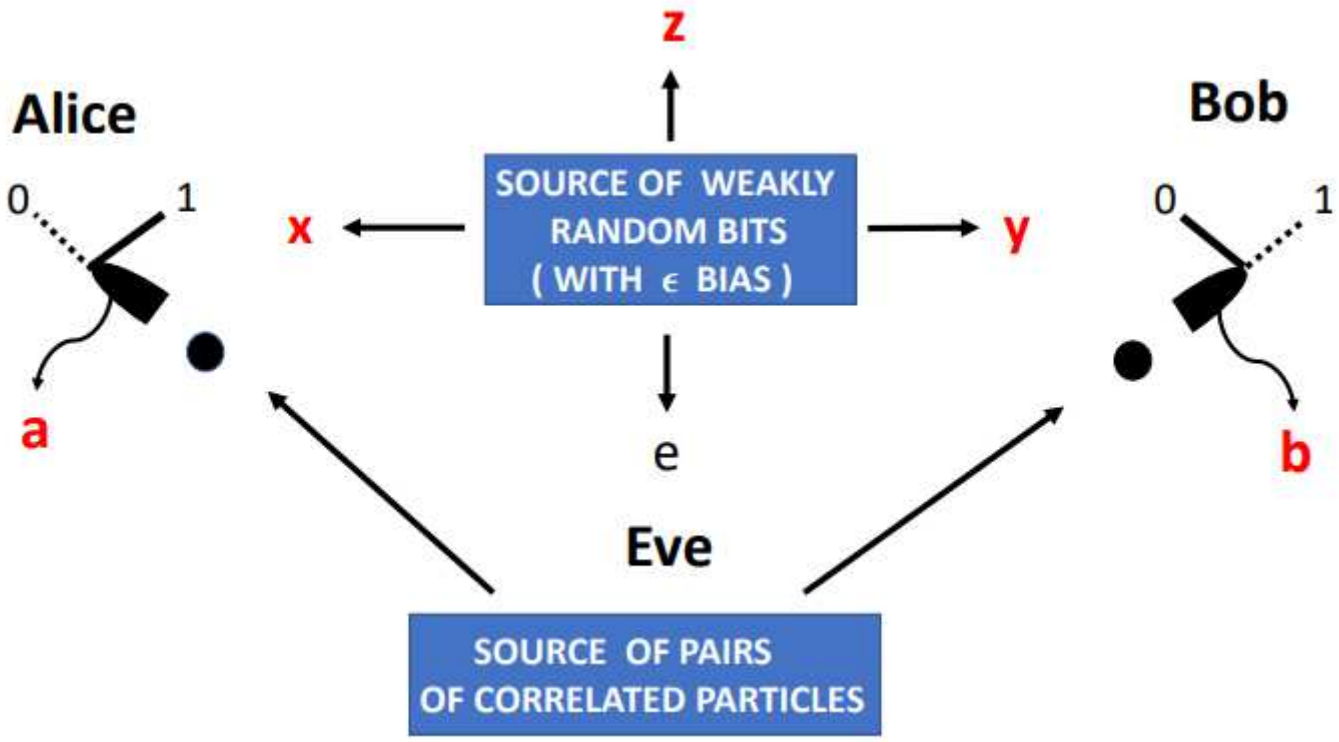

Figure 1

Pictorial depiction of the Device-Independent Randomness Amplification (DIRA) protocol. First step: Bell experiment with weakly random settings. An eavesdropper Eve has a source that distributes quantum particles to two parties Alice and Bob. These parties perform measurements on the received particles using apparata with two settings each, constituting the simplest possible (2, 2, 2) Bell scenario. The choice of the settings (in each run of the experiment) is made according to bits (x, y) obtained from a Santha-Vazirani (SV) source of weakly random bits, which also produces further bits z to be fed into a randomness extractor in a subsequent step of the protocol. Eve is taken to hold some classical side information e about the weakly random source, as well as some no-signalling side information about the devices held by Alice and Bob. The outputs (a, b) produced by these devices are described by a family of probabilities {PAB|XY (ab|xy)}. Note that in the figure, a single run of the experiment is depicted while in practice the scheme is repeated many times producing sequences of bits. The assumption here is that the SV source is private, i.e., that the bits held by Alice and Bob are unknown to Eve. The goal is to produce, out of the outcomes (a, b) and some further bits z from the SV source, a sequence of final output bits that are secure and fully random from the perspective of Eve. This is achieved by further processing of the outputs in the second step of the protocol (Fig. 2).

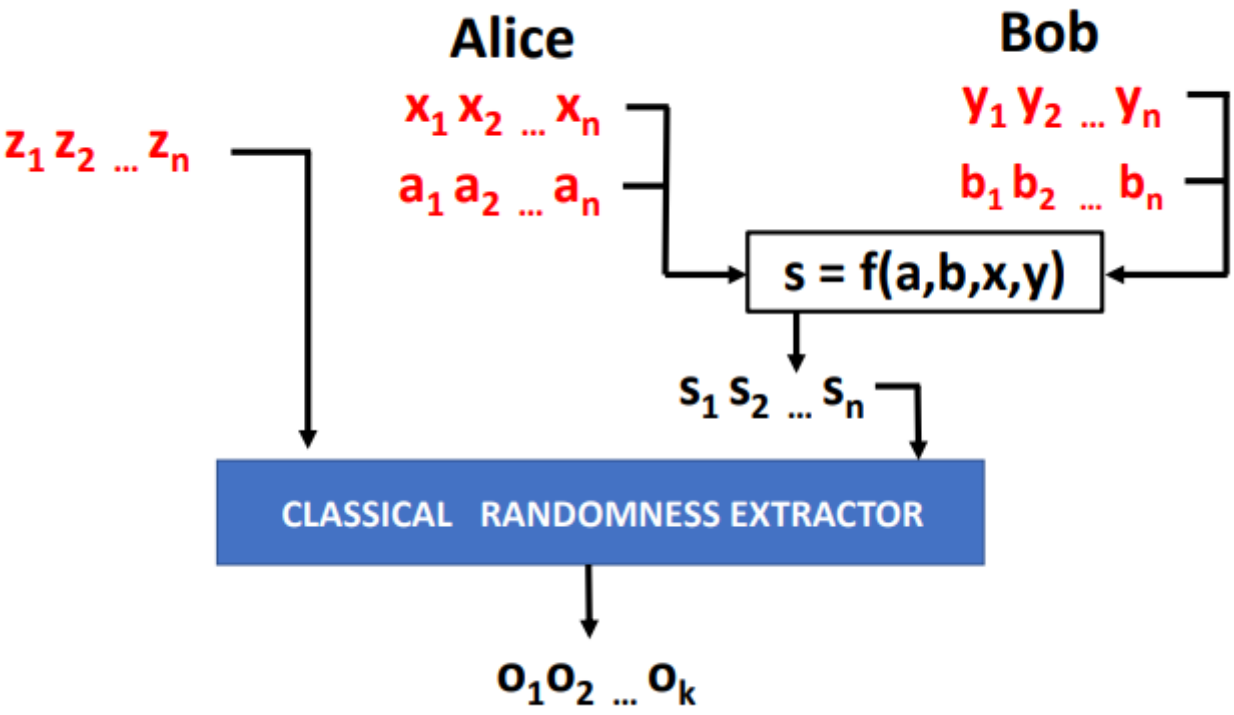

Figure 2

Pictorial depiction of the Device-Independent Randomness Amplification (DIRA) protocol. Second step: classical processing of the outputs of the Bell experiment. When the Bell experiment is performed as in Fig. 1, a sequence of outputs in n runs of the experiment, denoted as a = a1, . . . , an, b = b1, . . . , bn is obtained for inputs x = x1, . . . , xn, y = y1, . . . , yn. Alice and Bob first calculate the Bell parameter L n(a, b, x, y) and verify that this is above some threshold value δ > 0. They apply a hash function f to the bits (a, b, x, y) to obtain a bit sequence s = s1, . . . , sn that is partially random and secure from Eve. They feed this bit sequence together with a further bit sequence z1, . . . , zn from the weakly random SV source to a classical randomness extractor to obtain a final output sequence o1, . . . , ok that is fully random and secure from Eve. The magic of the quantumness is manifested in the fact that the bits s happen to be decorrelated from z, which could never happen if the particles in the experiment from Fig. 1 were classical. This - quantumly originated - decorrelation is the crucial fact that makes the classical independent-source extractor work. The surprising power of the whole scenario is that the final bits stay strongly random even from the perspective of an eavesdropper who is only limited by the fundamental no-superluminal signalling principle of special relativity.

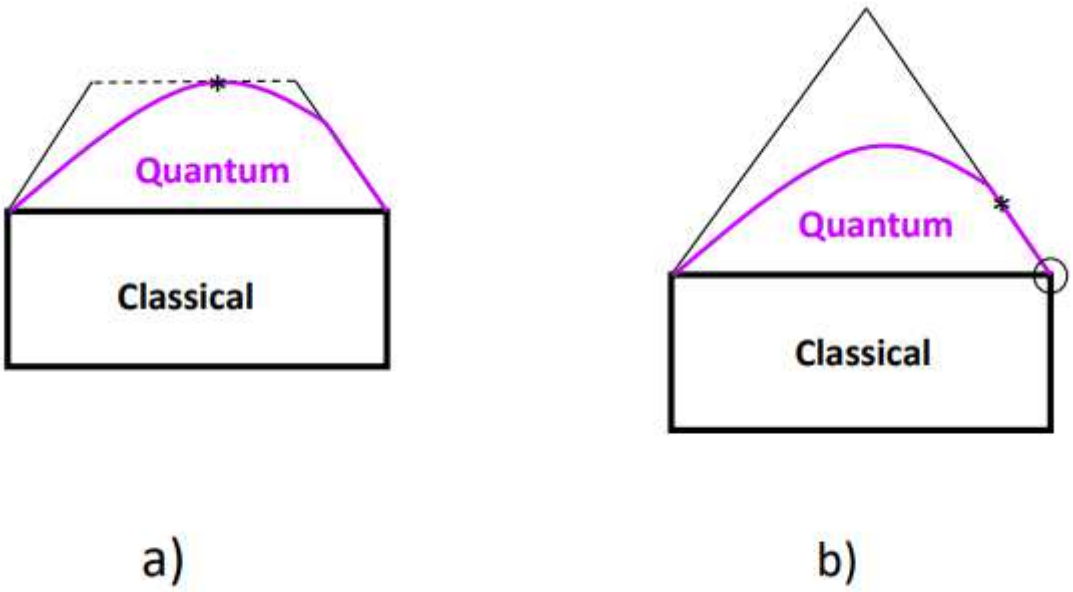

Figure 3

A novelty of the present approach that enables practical implementation. The convex sets of statistical behaviors {PA,B|X,Y (a, b|x, y)} obtainable in Bell experiments using classical, quantum and general no-signalling correlations are depicted here. The quantum correlations outside the classical set enable violation of a Bell inequality. Thus far, it was believed that randomness amplification schemes against no-signalling adversaries required quantum correlations that reached a “pure” nosignalling boundary as in the figure (a) above. These “pseudo-telepathic” correlations (depicted by the dashed line in (a)) met the stringent requirement that their convex decomposition admitted no classical fraction. However, such a stringent requirement was only possible in Bell scenarios with many inputs and outputs and high-dimensional quantum systems making them completely infeasible for practical experimental implementation. A novelty in this paper is the identification that much simpler quantum correlations that violate Hardy paradoxes, i.e., which only reach “partial” no-signalling boundaries as in figure (b) above, can still enable DIRA against a general no-signalling adversary. Crucially, our protocol enables the application of these correlations to the task, despite the fact that these correlations admit a significant classical fraction, denoted by the circle □, when considered as a convex mixture of general no-signalling behaviors. Furthermore, the special Hardy behaviors such as the point denoted by (*) in the figure (b), are already realizable in the simplest possible (2, 2, 2) Bell scenario of two parties choosing two binary inputs, which corresponds to simple polarization-entangled photon experiments that are realized everyday in photonic laboratories with high fidelities. It is noteworthy that the pseudo-telepathic part of the boundary is well-known to not exist in this simple case, as illustrated in (b).

Protocol I

1. The ϵ-SV source is used to choose the measurement settings (x_i, y_i) for n runs on a single device consisting of two components. The device produces output bits $x = (a_i, b_i)$ with $i \in \{1, \ldots, n\}$.
2. The parties perform an estimation of the violation of a measurement-dependent locality inequality from the Hardy paradox by computing the empirical average $L_n^\epsilon(\mathbf{a}, \mathbf{b}, \mathbf{x}, \mathbf{y}) := \frac{1}{n}\sum_{i=1}^{n} w_i(\epsilon) B_{\mathrm{H}}(a_i, b_i, x_i, y_i)$. The protocol is aborted unless $L_n^\epsilon(\mathbf{a}, \mathbf{b}, \mathbf{x}, \mathbf{y}) \geq \delta$ for fixed constant $\delta > 0$.
3. Conditioned on not aborting in the previous step, the parties apply an independent source extractor [29, 30] to the sequence of outputs from the device and further n bits from the SV source.

Figure 4

Protocol for device-independent randomness amplification using the two-party Hardy paradox.

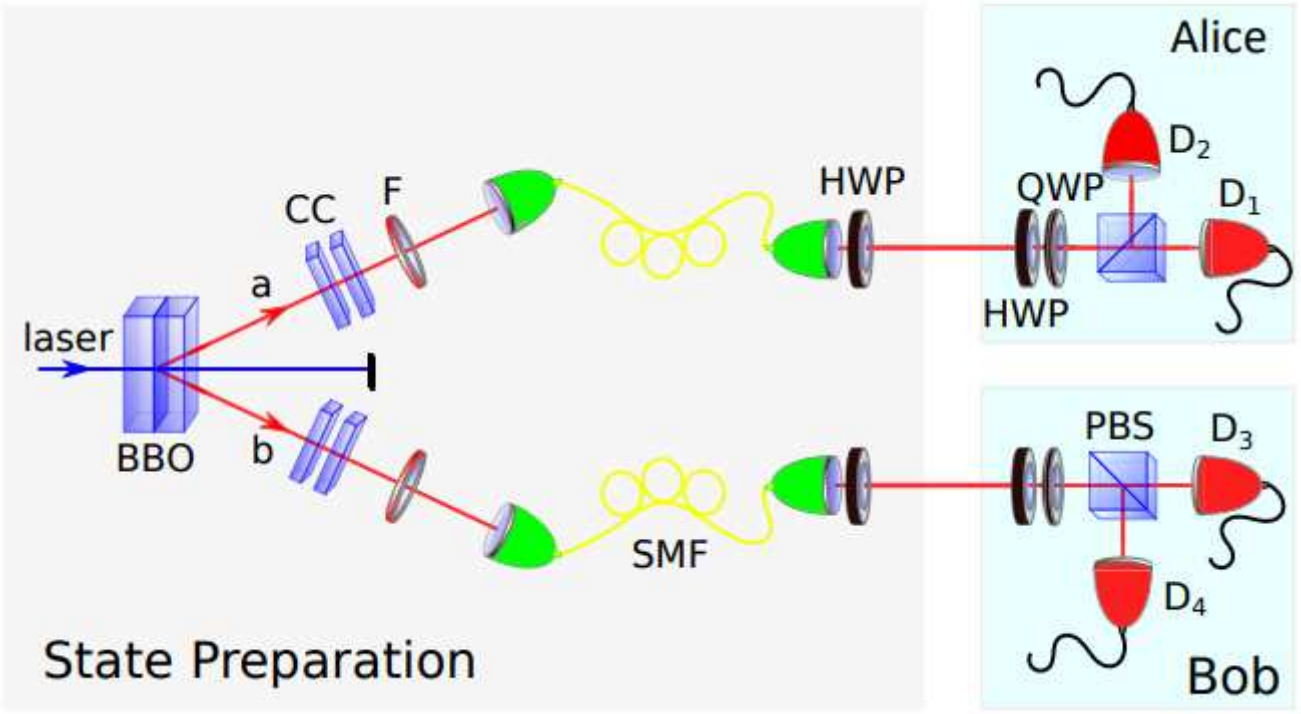

Figure 5

Preparation and measurement setup. A UV pump laser at 390nm was focused onto two beta barium borate (BBO) crystals places in cross-configuration to produce photon pairs emitted into two spatial modes ”a” and ”b” through type-I SPDC process. To remove any spatial, temporal or spectral distinguishability between the photons we use a pair of Y V O4 crystals (CC), narrow-bandwidth filters (F) (λ = 1 nm), and coupling into single-mode fibers (SMF). To prepare the state 3, the photon polarizations in each mode are rotated through a half wave plate (HWP). Alice’s and Bob’s measurements were performed using a HWP, a quarter wave plate (QWP), a polarizing beam splitter (PBS) and single-photon avalanche photodiodes Di(i = {1, 2, 3, 4}).

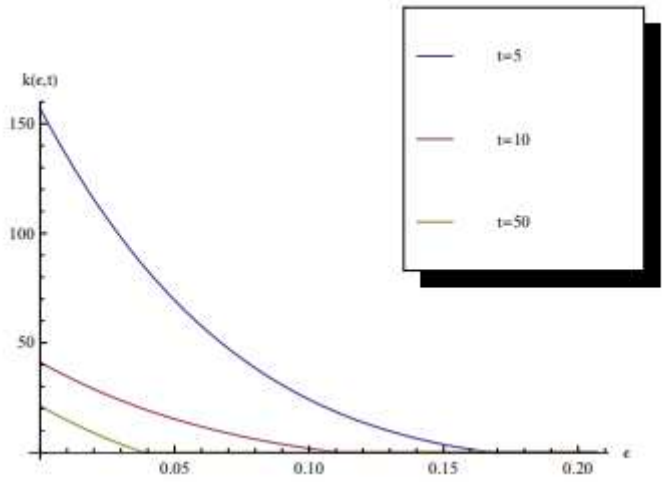

Figure 6

The number of output bits k(, t) versus for three values of security parameter t (recall that the final k bits deviate from uniform by 2−t−1).

Supplementary Files

This is a list of supplementary files associated with this preprint. Click to download.

- RandomnessAmpSIv1.pdf