Quantum Information Processing (2021) 20:39
https://doi.org/10.1007/s11128-020-02948-3

Quantum randomness protected against detection loophole attacks

Piotr Mironowicz[1,2] · Gustavo Cañas[3] · Jaime Cariñe[4,5] · Esteban S. Gómez[5,6] · Johanna F. Barra[5,6] · Adán Cabello[7,8] · Guilherme B. Xavier[9] · Gustavo Lima[5,6] · Marcin Pawłowski[2,10]

Received: 6 November 2019 / Accepted: 19 November 2020 / Published online: 18 January 2021

Abstract
Device and semi-device-independent private quantum randomness generators are crucial for applications requiring private randomness. However, they are vulnerable to detection inefficiency attacks and this limits severely their usage for practical purposes. Here, we present a method for protecting semi-device-independent private quantum randomness generators in prepare-and-measure scenarios against detection inefficiency attacks. The key idea is the introduction of a blocking device that adds failures in the communication between the preparation and measurement devices. We prove that, for any detection efficiency, there is a blocking rate that provides protection against these attacks. We experimentally demonstrate the generation of private randomness using weak coherent states and standard avalanche photo-detectors.

✉ Piotr Mironowicz
piotr.mironowicz@gmail.com

1 Department of Algorithms and System Modeling, Faculty of Electronics, Telecommunications and Informatics, Gdańsk University of Technology, 80-233 Gdańsk, Poland

2 International Centre for Theory of Quantum Technologies, University of Gdansk, Wita Stwosza 63, 80-308 Gdańsk, Poland

3 Departamento de Física, Universidad del Bio-Bio, Av. Collao 1202, Concepción, Chile

4 Departamento de Ingeniería Eléctrica, Universidad Católica de la Santísima Concepción, Concepción, Chile

5 Millennium Institute for Research in Optics, Universidad de Concepción, 160-C, Concepción, Chile

6 Departamento de Física, Universidad de Concepción, 160-C, Concepción, Chile

7 Departamento de Física Aplicada II, Universidad de Sevilla, 41012 Seville, Spain

8 Instituto Carlos I de Física Teórica y Computacional, Universidad de Sevilla, 41012 Seville, Spain

9 Institutionen för Systemteknik, Linköpings Universitet, 581 83 Linköping, Sweden

10 Instytut Fizyki Teoretycznej i Astrofizyki, Uniwersytet Gdański, 80-952 Gdańsk, Poland

Keywords Detection efficiency · Quantum random number generation

1 Introduction

Private random numbers are essential for multiple applications, including, but not limited to, cryptography and digital rights management. Private random numbers are those the user is sure no one else had access to. However, random numbers produced from classical processes may be predictable and therefore not private. One solution is using quantum random number generators (QRNGs) based on the intrinsic uncertainty of quantum measurement outcomes [1]. Unfortunately, imperfections in their components can make generated numbers predictable to some extent. This may be undetected by standard randomness tests [2], and therefore exploited by an adversary [3]. The privacy of numbers obtained in QRNGs has to be proved separately [4].

A major breakthrough was the discovery of device-independent (DI) QRNGs, which permit to certify private randomness without making assumptions about the internal functioning of the devices [3]. The problem is that current DI-QRNGs require very high detection efficiencies and produce private random numbers at low rate [5].

Another approach is the semi-device-independent (SDI) QRNGs [6–8], in which no assumptions about the internal functioning of the QRNG are made, except that the dimension of the quantum system used is below a certain upper-bound. A typical SDI-QRNG consists of a device with two parts, P and M, where P prepares some quantum states that are then transmitted to M, where some quantum operations are performed producing outcomes which, after post-processing, are used as random bits. Previous works [9–13] consider SDI-QRNG protocols with the extra assumption that P and M are not correlated, which implies that P and M do not use shared randomness during the whole process of generation of random numbers. It has been shown that the presence of correlations between P and M makes DI-QRNG and SDI-QRNG protocols vulnerable to detection inefficiency attacks [14,15].

There are three possible cases in which there is shared randomness between P and M:

(i) When correlations between P and M exist before the device is used. For example, if a common seed is stored by the adversary when the devices are built. Another example is when the same environment is shared by P and M and fluctuations in electrical power or local temperature affects them equally. This problem can be avoided by employing several Ps and Ms paired randomly. Since the adversary cannot know in advance how they will be paired, then the adversary must resort to using common seed to all the parts, e.g., a synchronized timer. In this case, correlations between inputs and outputs will be observed, as discussed in [16].

(ii) When a signal sent from an external synchronizer causes correlations between P and M. This case can be avoided by invoking a standard assumption in all cryptographic schemes, namely, that P and M are inside a shielded laboratory, and thus a shared seed cannot be sent from the outside.

(iii) When P and M correlate themselves during the execution of the protocol using communication. This can occur, e.g., in the following way. If M is able to detect

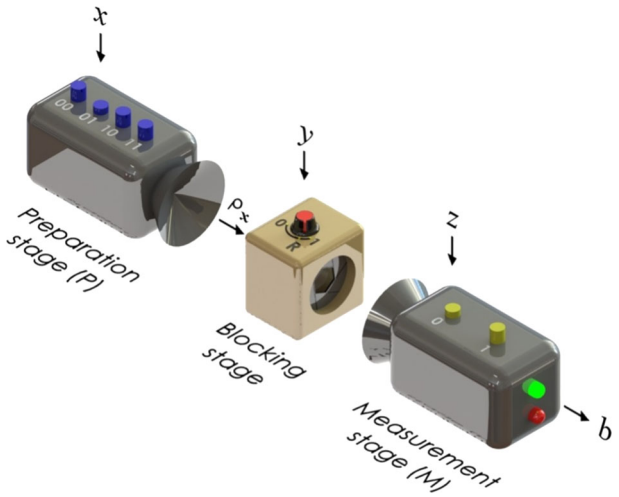

Fig. 1 (Color online) Prepare-and-measure scenario of SDI protocols with a blocker for private randomness generation. It illustrates case with $x \in X = \{00, 01, 10, 11\}$, $y \in [0, 1]$, $z \in Z = \{0, 1\}$, and $B = \{0, 1\}$, the values of $b = 0, 1$ are represented by means of a top (green) or bottom (red) light, respectively, at the final stage

all photons sent from P, then, if P decides not to send a photon for a certain round, this would be an indication for both P and M to reset their counters. In a more realistic case, when M works with imperfect detectors, this synchronization attack strategy is still possible using a longer sequence of rounds without photons to reset their counters.

In this work, we propose a private SDI-QRNG protocol which offers a protection against these last attacks and can be implemented with a very low detection efficiency. Its novelty is the introduction of a "blocker" that randomly stops the communication between the QRNG preparation and measurement stages with the purpose of destroying the correlations that may exist between them. Its relevance lies in the following features: (I) It works with inefficient detectors, as required for real-world applications. (II) No detailed knowledge of the internal functioning of the QRNG is needed. (III) The protocol works even if the adversary has introduced shared randomness between P and M. In addition, to demonstrate the practicability of the protocol, we present an experimental realization of the protocol using weak coherent states and standard avalanche photo-detectors (APDs) providing an overall detection efficiency of 6%.

2 Protocol description

Here, we overview the idea of the proposed protocol. Figure 1 shows the general scheme of SDI protocols and an extra blocker. It consists of three stages: the state preparation stage (P), the blocking stage and the measurement stage (M).

In P, a quantum system ρ_x is prepared depending on the input data $x \in X$. In the blocking stage, a blocker halts the transmitted system or allows it to go to the stage

M, depending on another random input $y \in [0, 1]$. The system is stopped if and only if $y \leq R$, where $R \in [0, 1]$ is a parameter of the blocker. In M, a random input $z \in Z$ is used to select a measurement which is then performed on the transmitted system. The outcome of the selected measurement is $b \in B \cup \{\emptyset\}$, where $b = \emptyset$ corresponds to the non-detecting events.

The SDI scheme considers P and M to be black boxes possibly built by an adversary. Their internal functioning is unknown to the user and they may even contain a malevolent agent. Still, the SDI approach assumes the following properties of the device:

1. The dimension of the transmitted system is known.
2. P and M do not receive any external signal from the adversary (i.e., the laboratory is shielded).
3. x, y, z are numbers independently produced that pass standard tests of randomness [2], but are not private. They may be produced by imperfect QRNGs or taken from a public source of random bits.

Each round of the protocol represents an event denoted by $(b|x, y, z)$. We take only the rounds with $y > R$ for our random string. We denote

$$\mathbb{P}(b|x, z) \equiv \frac{\mathbb{P}(b|x, y > R, z)}{1 - \mathbb{P}(\emptyset|x, y > R, z)}, b \in B. \tag{1}$$

To certify that the generated sequence of outputs is private and random, the user estimates the overall detection efficiency η defined as

$$\eta \equiv 1 - \sum_{x \in X} \sum_{y \in Y} \mathbb{P}_{XZ}(x, z)\mathbb{P}(\emptyset|x, y > R, z), \tag{2}$$

and the value of the so-called certificate:

$$W[\mathbb{P}] \equiv \sum_{x \in X} \sum_{y \in Y} \sum_{b \in B} \beta_{b,x,z}\mathbb{P}(b|x, z), \tag{3}$$

with $\mathbb{P}_{XZ}(x, z)$ being the probability distribution of settings in the considered case and the numbers $\beta_{b,x,z} \in \mathbb{R}$, defining a particular protocol. If $W[\mathbb{P}]$ is above a certain threshold that depends on R and η, then the random sequence generated is considered as private. Otherwise the user aborts.

In order to prove the security of the proposed solution, we consider the following characterization of the blocking and synchronization mechanism:

I. The detection efficiency does not depend on the measurement setting used by M.
II. Synchronization takes one round of communication and in this round no other information (e.g., about x) is transferred.
III. P sends synchronization signals with the same probability $\alpha \in [0, 1]$ in each round, i.e., the synchronization algorithm is memoryless.
IV. After blocking, P and M become uncorrelated until the next synchronization.

We thus consider three separate cases of runs: runs not synchronized (i.e., ones in that P and M are not correlated), runs used for synchronization and runs synchronized (and not containing the synchronization signal). In practice, it is probable that any form of synchronization will require more than, e.g., a single qubit, so the second assumption favors the adversary.

These assumptions significantly simplify the calculation of the amount of certified randomness. In a more general approach, one may consider sophisticated synchronization strategies, in which synchronization signals are being sent according to some patterns or take into account correlations which remains to some extent even after the blocking.[1]

Let c_L be the maximal value of the certificate (3) if the transmitted system is classical, and c_Q if it is quantum, for some fixed dimension. We assume $c_L < c_Q$. As mentioned above, if the detection efficiency (2) is less than 1 and the parts are synchronized, then there are strategies able to mimic higher values of the certificate (3) than allowed by quantum mechanics. Let $c_S(\eta)$ be the maximal value of the certificate (3) for a given detection efficiency η. Similarly, let c_R be the maximal value of (3) when no information is transmitted and M calculates the outcome b depending on the input z. This is the case when the transmitted system contains a synchronization signal, cf. the assumption II. We have

$$\forall_{0<\eta\leq 1} 0 \leq c_R \leq c_L < c_Q \leq c_S(\eta) \leq 1. \tag{4}$$

3 Main result: Blocking protocol theorem

A common measure of randomness generated by QRNGs is the guessing probability and, closely related, min-entropy [17,18]. For a discrete probability distribution $\mathbb{P}$, these two quantities are defined as

$$P_{guess}[\mathbb{P}] \equiv \max_{x \in \mathrm{supp}(\mathbb{P})} \mathbb{P}(x), \text{ and} \tag{5a}$$

$$H_\infty[\mathbb{P}] \equiv -\log_2 P_{guess}[\mathbb{P}], \tag{5b}$$

respectively. For a conditional distribution $\mathbb{P}_{\Phi|\Psi}$, ψ distributed with P_Ψ one [8] defines:

$$P_{guess}[\mathbb{P}_{\Phi|\Psi}] = \max_{g:\Psi\to\Phi} \left\{ \sum_{\psi\in\Psi} P_\Psi(\psi)\mathbb{P}(\boldsymbol{g}(\psi)|\psi) \right\}, \tag{6}$$

where ψ denotes all knowledge a guesser posses, possibly including, e.g., preparation and measurement settings or access to a quantum system entangled with the quantum systems used to generate $\mathbb{P}_{\Phi|\Psi}$. Further we refer to (6) as the maximal average guessing probability.

[1] For example, the internal counters of P and M differ by n rounds with some probability, depending on n and the blocking rate.

We note here that since Theorem 1 assumes that the certificate (3) constitutes a private-SDI-QRNG protocol, meaning that if no detection loophole attack occurs, then observing an experimental value $p_{\text{asyn}} > c_L$ certifies some amount of randomness greater than 0, or, in other words, the maximal average guessing probability is less than 1. The problem of construction of such protocols is beyond the scope of this papers, see e.g., [36] which deals with this topic. Here we only enumerate the required properties.

Both the sending part P and the receiving part M of the cryptographic device may be constructed by a malevolent party and no assumption regarding their internal working is made. In each run, P emits to M a particle of dimension at most d prepared using arbitrary quantum operations on a quantum system that is possibly entangled with an arbitrary large quantum state on a Hilbert space $\mathscr{H}_E$, with the latter accessible directly by the eavesdropper at any stage of the protocol. The random numbers x, y and z provided as settings to the parts of the device are assumed to be random, not known to the devices prior to the moment they are used, and the action of each of the parts in the setup is assumed not to depend on the inputs provided to other parts. For instance, it is assumed that the inputs x (provided to P) are not known to M etc. On the other hand, the inputs are all accessible to the eavesdropper. The SDI-QRNG protocol is private if under these assumption it guaranties that the output b is private, i.e., its guessing probability by the eavesdropper is less than 1.

To be more specific, a certificate $W : \mathscr{Q} \to \mathbb{R}$, see (3), constitutes a private SDI-QRNG protocol in dimension d if and only if

$$W[\mathbb{P}_{B|X,Z}] \in (c_L, c_Q] \implies P_{guess}[\mathbb{P}_{B|X,Z,E}] < 1 \tag{7}$$

for all $\{\rho_x\}_{x\in X} \subset \mathscr{P}(\mathscr{H}_A \otimes \mathscr{H}_E)$, where $\mathscr{P}(\cdot)$ is the set of all normalized states on given Hilbert space, dimensions of Hilbert spaces $\mathscr{H}_A$ and $\mathscr{H}_E$ are d and some $D \in \mathbb{N}$, respectively; E is an arbitrary finite set of size at most D; for all $\left\{M_z^b\right\}_{b\in B, z\in Z}$, where each $\{M_z^b\}_b$ is a POVM acting on $\mathscr{H}_A$; for all $\left\{N_{x,z}^e\right\}_{e\in E, x\in X, z\in Z}$, where each $\left\{N_{x,z}^e\right\}_e$ is a POVM acting on $\mathscr{H}_E$, and

$$\mathbb{P}_{B|XZ}(b|x,z) \equiv \operatorname{Tr}\left(\rho_x M_z^b \otimes \mathbb{I}_{\mathscr{H}_E}\right), \tag{8a}$$

$$\mathbb{P}_{B|XZE}(b|x,z,e) \equiv \frac{\mathbb{P}_{BE|XZ}(b,e|x,z)}{\mathbb{P}_{E|XZ}(e|x,z)}, \tag{8b}$$

where

$$\mathbb{P}_{BE|XZ}(b,e|x,z) \equiv \operatorname{Tr}\left(\rho_x M_z^b \otimes N_{x,z}^e\right), \tag{9a}$$

$$\mathbb{P}_{E|XZ}(e|x,z) \equiv \operatorname{Tr}\left(\rho_x \mathbb{I}_{\mathscr{H}_A} \otimes N_{x,z}^e\right), \tag{9b}$$

and $\mathbb{I}_\cdot$ is the identity on the relevant space.

We denote the maximal possible average guessing probability and certified randomness in an experiment with the detection efficiency η, the blocking rate R and the

observed certificate value p by $P_{guess}(R, \eta, p)$ and

$$H_\infty(R, \eta, p) \equiv -(1 - R) \times \eta \times \log_2 P_{guess}(R, \eta, p). \tag{10}$$

We provide details of these functions in" Appendix A". The main result of this work is the following:

Theorem 1 *If for a private-SDI-QRNG protocol we obtain in an experiment a value $p > c_L$, then for any detection efficiency $\eta > 0$ there exists a blocking rate R providing protection against detection loophole attacks, i.e.,*

$$\forall_{p>c_L} \forall \eta > 0 \exists_{R\in[0,1)} H_\infty(R, \eta, p) > 0. \tag{11}$$

We present the proof in "Appendix B".

4 Experiment

Our experimental implementation of the protocol with a blocker is shown schematically in Fig. 2. As the sources of x, y and z, we use three commercial QRNGs (IDQ Quantis). They passed standard tests of randomness, but no assumptions about their privacy is made.

A field programmable gate array (FPGA) in P produces an electrical synchronization signal, which also drives an acousto-optical modulator (AOM) producing attenuated optical pulses (weak coherent states) from a continuous laser operating with a center wavelength of 690 nm. These optical pulses are then sent through a sequence of four spatial light modulators (SLMs) [19]. Sets of lenses are employed to project the image of one SLM onto the next one.

The assumption that the quantum system prepared in P and measured in M is two dimensional is addressed in our experiment in the following way. The employed average photon number per optical pulse was set to $\mu = 0.66$ such that approximately 71% of the non-null pulses contain only one photon. To define the two-dimensional quantum systems, we use the linear transverse momentum degree of freedom of the photons transmitted by the SLMs [20]. This is done by projecting masks with only two paths available for the photon transmission in the liquid crystal displays of the SLMs [21–27].

The qubit state preparation in P (and the projections in M) is implemented using SLM 1 and SLM 2 [SLM 3, SLM 4 (and an APD)] working with amplitude-only and phase-only modulation, respectively [28–30]. The real and imaginary parts of the generated and measured states are set by adjusting the grey level of the pixels on the SLMs. In our demonstration, we set these states to maximize the value of $W[\mathbb{P}]$ (described in "Appendix C").

The repetition rate of the attenuated optical pulses is set to 30 Hz, which is the limit of the employed SLMs. The applied modulation in each SLM is triggered by the sync signal. An internal delay in respect to the AOM in the FPGAs is used to ensure that the SLMs in P and M are properly set by the time each optical pulse is sent. In each round,

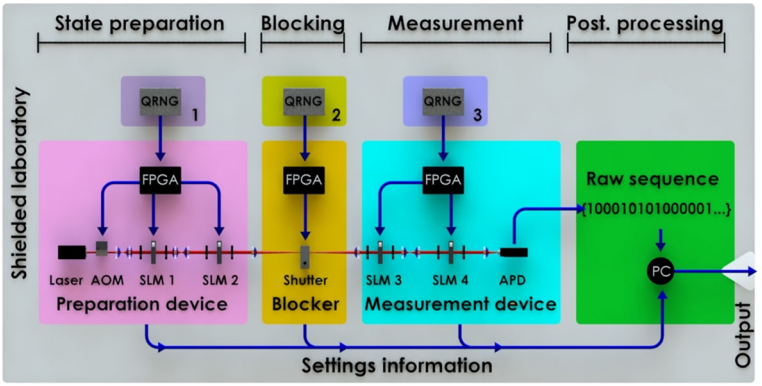

Fig. 2 (Color online) Experimental setup (see text for details)

pre-determined modulations are applied to the SLMs by their corresponding FPGAs based on the numbers produced by each QRNG. The optical blocker placed between them is a commercial shutter and is controlled by a third FPGA unit, fed by another QRNG. The blocker's electronics also receive the sync signal from P. For each round of the experiment, the blocker's FPGA unit randomly blocks the optical pulse, with an adjustable probability. The overall detection efficiency η (including losses at the measurement stage and detection probability of the single-photon detector) is 6%.

Note that the stages P, B and M rely on the sync signal, which represents the action of choosing a random input x in P, y in B and z in M. If synchronization between P and M is achieved, then an adversary's agent in M could use the sync signal to count rounds and prevent the loss of synchronization. However, this attack can easily be counteracted by the user: If he randomly sends fake signals to M between the sync signals, then synchronization will be again required for the adversary, which can be detected by the protocol.

In our implementation, a blocking rate $R = 0.99$ was employed. We obtained $W[\mathbb{P}] = 0.8425 \pm 0.0086$ with data shown in Table 1 in "Appendix C". A direct calculation using a relaxed formula for $H_\infty(R, \eta, p)$, see (50), for the considered setup shows that the key generation rate is at least 0.012 bits of min-entropy per photon passing the blocker mechanism (or 0.00012 bits per emitted photon), see "Appendix D".

5 Conclusions

We have introduced and experimentally implemented a SDI-QRNG protocol protected against attacks based on the detection loophole. In the experimental implementation, we have reported a private random bit rate generation of 0.00012 per emitted photon with a detection efficiency of 6%.

Unlike previous protocols which make the assumption that the measuring [10] or the preparing parts [11,12] are trustworthy or that there are not correlations between them [13], our protocol does not need to make any of these assumptions.

Unlike a recent protocol [31] that does not make these assumptions but requires detection efficiencies above 78% and produces relatively low randomness, our protocol works with much lower detection efficiencies and produces more randomness. For example, while the protocol in [31] produces 0.00114 bits per round, our protocol certifies 0.085 bits per emitted photon with $\eta = 0.78$ and $R = 0.3$, see "Appendix D".

We believe that our results pave the way toward a new generation of practical and secure SDI-QRNGs.

Acknowledgements This work was supported by Fondecyt 1200859, Fondecyt 1190933, Fondecyt 1190901, Fondecyt 1150101, and ANID—Millennium Science Initiative Program—ICN17_012. J.F.B. acknowledges support from Fondecyt 3170307. J.C. acknowledges support from ANID/REC/PAI77190088. A.C. acknowledges support from the Ministry of Science, Innovation and Universities (MICIU) Grant No. FIS2017-89609-P with FEDER funds, the Conserjería de Conocimiento, Investigación y Universidad, Junta de Andalucía and European Regional Development Fund (ERDF) Grant No. SOMM17/6105/UGR and the Knut and Alice Wallenberg Foundation project "Photonic Quantum Information". G.B.X. acknowledges Ceniit Linköping University and the Swedish Research Council (VR 2017-04470) for financial support. P.M. and M.P are supported by a National Science Centre (NCN) grant 2014/14/E/ST2/00020 and FNP programme First TEAM (Grant No. First TEAM/2016-1/5), and P.M. by a DS Programs of the Faculty of Electronics, Telecommunications and Informatics, Gdańsk University of Technology. The support by the Foundation for Polish Science through IRAP project co-financed by the EU within the Smart Growth Operational Programme (Contract No. 2018/MAB/5) is acknowledged. P.M. thanks Krystyna Witalewska for help during the time of writing the manuscript. The optimizations have been performed using OCTAVE [32] with SeDuMi solver [33] and YALMIP toolbox [34].

Appendix A: Guessing probability, min-entropy and randomness certification

The distribution of lengths of series of systems sent and not blocked by the blocking mechanism at a rate R is given by

$$P(R,k) = (1-R)^{k-1}R, \tag{12}$$

where $k \geq 1$ is the number of systems in a series.

Let us denote by α the ratio between the number of systems containing synchronization signal sent by P and the total number of systems sent by P, cf. the assumption III.

In a given series of transmitted systems of length k, the average number of photons before the first synchronizing system within that series is

$$\begin{aligned} F_{\text{asyn}}(\alpha,k) &= \left[\sum_{i=0}^{k} i(1-\alpha)^i\alpha\right] + k(1-\alpha)^k \\ &= \frac{1-\alpha}{\alpha}\left(1-(1-\alpha)^k\right). \end{aligned} \tag{13}$$

Using (13), we get that the probability that a particular photon received by M is not synchronized is

$$\begin{aligned} P_{\text{asyn}}(R,\alpha) &= \sum_{k=1}^{\infty} P(R,k)\frac{F_{\text{asyn}}(\alpha,k)}{k} \\ &= \frac{1-\alpha}{\alpha}\frac{R}{1-R}\ln\left(\frac{\alpha+R-\alpha R}{R}\right), \end{aligned} \tag{14}$$

for $\alpha > 0$ and $P_{\text{asyn}}(R,0) = 1$. Directly from the definition of α, the probability that the received system is a synchronization signal is

$$P_{\text{sig}}(R,\alpha) = \alpha. \tag{15}$$

The probability that a received system is synchronized and not carrying a synchronization signal is

$$P_{\text{syn}}(R,\alpha) = 1 - P_{\text{asyn}}(R,\alpha) - P_{\text{sig}}(R,\alpha), \tag{16}$$

for $\alpha > 0$ and $P_{\text{syn}}(R,0) = 0$. One can easily calculate that $\forall_{\alpha\in[0,1]} \lim_{R\to 1^-} P_{\text{syn}}(R,\alpha) = 0$. Let us define $F_{\text{syn}}(R) \equiv \max_{\alpha\in[0,1]} P_{\text{syn}}(R,\alpha)$. Then,

$$\lim_{R\to 1^-} F_{\text{syn}}(R) = 0. \tag{17}$$

If $\mathbb{P}$ is a mixture of distributions $\mathbb{P}_i$ with frequencies $\{\omega_i\}$, $\sum_i \omega_i = 1$, and an eavesdropper is *aware* which distribution i occurs, we have $P_{guess}[\mathbb{P}] \equiv \sum_i \omega_i P_{guess}[\mathbb{P}_i]$.

Let us consider separately runs of the protocol without synchronization (abbreviated as "asyn"), runs containing synchronization signal (abbreviated as "sig") and synchronized runs without the signal (abbreviated as "syn").

Let $P^{\text{asyn}}_{guess}(p,\eta)$, $P^{\text{sig}}_{guess}(p,\eta)$, $P^{\text{syn}}_{guess}(p,\eta)$ be functions providing upper bounds on the maximal average guessing probabilities, p_{asyn}, p_{sig}, p_{syn} be the average values of the certificate (3), and η_{asyn}, η_{sig}, η_{syn} be the detection efficiencies (2), in the respective runs. These values cannot be observed individually by a user, but each of them has impact on the observed values of (3) and (2).

Let $\mathbf{p} \equiv (p_{\text{asyn}}, p_{\text{sig}}, p_{\text{syn}})$ and $\equiv (\eta_{\text{asyn}}, \eta_{\text{sig}}, \eta_{\text{syn}})$. Note that $p_{\text{asyn}} \le c_Q$, $p_{\text{sig}} \le c_R$ and $p_{\text{syn}} \le c_S(\eta_{\text{syn}})$. Let $\mathscr{M} \equiv \{\text{asyn}, \text{sig}, \text{syn}\}$, $\bar{\eta} \equiv \sum_{i\in\mathscr{M}} \eta_i P_i(R,\alpha)$, and $\omega_i \equiv \frac{\eta_i P_i(R,\alpha)}{\bar{\eta}}$ for $i \in \mathscr{M}$, thus $\sum_{i\in\mathscr{M}} \omega_i = 1$.

Let us also define

$$P^{\text{fun}}_{guess}(R,\alpha,\mathbf{p},) \equiv \sum_{i\in\mathscr{M}} \omega_i P^i_{guess}(p_i,\eta_i), \tag{18a}$$

$$p^{\text{fun}}(R,\alpha,\mathbf{p},) \equiv \sum_{i\in\mathscr{M}} \omega_i p_i, \tag{18b}$$

$$\eta^{\text{fun}}(R,\alpha,) \equiv \bar{\eta}. \tag{18c}$$

Using the above expression, we can give the following upper bounds on the maximal average guessing probability for the blocking parameter R, the observed value p of the certificate (3) and the observed value η of the detection efficiency (2):

$$\begin{aligned} P_{guess}(R,\eta,p) \equiv \quad & \underset{\substack{\alpha\in[0,1]\\ \eta_{\text{asyn}},\eta_{\text{sig}},\eta_{\text{syn}}\in[0,1]\\ p_{\text{asyn}}\in[0,c_Q]\\ p_{\text{sig}}\in[0,c_R]\\ p_{\text{syn}}\in[0,c_S(\eta_{\text{syn}})]}}{\text{maximize}} && P^{\text{fun}}_{guess}\,(R,\alpha,\mathbf{p},) \\ & \text{subject to} && p^{\text{fun}}\,(R,\alpha,\mathbf{p},) = p, \\ & && \eta^{\text{fun}}\,(R,\alpha,) = \eta. \end{aligned} \tag{19}$$

Note that the constraints can be equivalently rewritten as $\sum_{i\in\mathscr{M}} \eta_i P_{guess}(R,\alpha) = \eta p$ and $\bar{\eta} = \eta$, and these forms are used in "Appendix B".

Since (19) involves (18a) to perform maximization, we need explicit formulae for $P^i_{guess}(p_i,\eta_i), i \in \mathscr{M}$. Since "sig" runs are deterministic, we have $P^{\text{sig}}_{guess}(p_{\text{sig}},\eta_{\text{sig}}) \equiv 1$. $P^{\text{asyn}}_{guess}(p_{\text{asyn}},\eta_{\text{asyn}})$ is a guessing probability of an eavesdropper not exploiting the detection loophole, thus it doesn't depend on η_{asyn}. We provide analysis for this function in this section below. The function $P^{\text{syn}}_{guess}(p_{\text{syn}},\eta_{\text{syn}})$ has to be developed independently for different formulae for the certificate (3), as this depends on a particular form of detection loophole attack.

Let us now consider a private SDI-QRNG protocol given by some certificate of a form (3) in some fixed dimension. For some $p \in (c_L, c_Q]$, we have the following formula for $P^{\text{asyn}}_{guess}(p,\eta)$:

$$\begin{aligned} \underset{\{\rho_x\},\{M^b_z\},\{N^e_{x,z}\},\boldsymbol{g}}{\text{maximize}} \quad & P_{guess}[\mathbb{P}_{B|XZE}] \\ \text{subject to} \quad & W[\mathbb{P}_{B|XZ}] = p. \end{aligned} \tag{20}$$

Without restricting the power of an eavesdropper, we may assume that

$$\mathbb{P}_{E|XZ}(e|x,z) = \mathbb{P}_E(e), \tag{21}$$

i.e., the probability of the result e does not depend on x and z. This can be obtained using proper extension of $\mathscr{H}_E$, or providing some additional "idle" information to an extended set E.

From (6), it follows that when $\{\rho_x\}$, $\{M^b_z\}$ and $\{N^e_{x,z}\}$ are fixed, then for an eavesdropper having access to $\mathscr{H}_E$ the optimal guessing function $\boldsymbol{g} : X \times Z \times E \to B$ is

$$\boldsymbol{g}(x,z,e) = \text{argmax}_b \mathbb{P}(b|x,z,e), \tag{22}$$

i.e., a function returning a most probable result b for each x, z and e.

Using no-signaling $\mathbb{P}_{B|XZ}(b|x,z) = \sum_{e\in E} \mathbb{P}_{BE|XZ}(b,e|x,z)$ and (21), we get

$$\mathbb{P}_{B|XZ}(b|x,z) = \sum_e \mathbb{P}_{BE|XZ}(b,e|x,z) = \sum_e \mathbb{P}_E(e)\mathbb{P}_{B|XZE}(b|x,z,e). \tag{23}$$

Thus, we can rewrite (20) as

$$\begin{aligned} \underset{\{\rho_x\},\{M_z^b\},\{N_{x,z}^e\},\boldsymbol{g}}{\text{maximize}} \quad & \sum_e \mathbb{P}_E(e) \sum_{x,z} \mathbb{P}_{XZ}(x,z)\mathbb{P}_{B|XZE}(\boldsymbol{g}(x,z,e)|x,z,e) \\ \text{subject to} \quad & \sum_e \mathbb{P}_E(e) \sum_{b,x,z} \beta_{b,x,z}\mathbb{P}_{B|XZE}(b|x,z,e) = p. \end{aligned} \tag{24}$$

Obviously, $\sum_e \mathbb{P}_E(e) = 1$ and the probability distribution is obtained by quantum measurements, see (9b). We can relax the latter constraint and replace $\mathbb{P}_E(e)$ with nonnegative coefficients c_e, with $\sum_e c_e = 1$. Then (20) can be relaxed as

$$\begin{aligned} G(p) \equiv \quad \underset{\{c_e\},\{p_e\}}{\text{maximize}} \quad & c_e g(p_e,e) \\ \text{subject to} \quad & c_e \geq 0, \sum_e c_e = 1, \\ & p_e \in [c_L, c_Q], \sum_e c_e p_e = p, \end{aligned} \tag{25}$$

where cf. (8),

$$\begin{aligned} g(p_e,e) \equiv \quad \underset{\substack{\{\rho_{x|e}\},\{M_{z|e}^b\},\\ \boldsymbol{g}(\cdot,\cdot,e):X\times Z\to B}}{\text{maximize}} \quad & \sum_{x,z} \mathbb{P}_{XZ}(x,z)\mathbb{P}_{B|XZe}(\boldsymbol{g}(x,z,e)|x,z) \\ \text{subject to} \quad & \mathbb{P}_{B|XZe}(b|x,z) \equiv \mathrm{Tr}\left[\rho_{x|e}M_{z|e}^b\right] \\ & \sum_{b,x,z} \beta_{b,x,z}\mathbb{P}_{B|XZe}(b|x,z) = p_e. \end{aligned} \tag{26}$$

Appendix B: Proof of the blocking protocol theorem

From (19), it follows that to have $P_{guess}(R,\eta,p) = 1$ we need

$$P_{guess}^{\text{asyn}}(p_{\text{asyn}},\eta_{\text{asyn}}) = 1, \text{ or} \tag{27a}$$

$$\omega_{\text{asyn}} = 0. \tag{27b}$$

For (27a) to hold, we need $p_{\text{asyn}} \leq c_L$.

Now, assuming $p_{\text{asyn}} \leq c_L$, and using $p_{\text{sig}} \leq c_L$, we relax the constraints in the optimization problem (19):

$$c_L \times (\omega_{\text{asyn}} + \omega_{\text{sig}}) + P_{\text{syn}}(R, \alpha) \geq \eta p, \tag{28a}$$

$$\omega_{\text{asyn}} + \omega_{\text{sig}} \leq \eta. \tag{28b}$$

Using (28) and the theorem's assumption $p > c_L$, we get

$$P_{\text{syn}}(R, \alpha) \geq \eta \times (p - c_L) \equiv \epsilon > 0. \tag{29}$$

From (17), we know there exists $R < 1$ such that $P_{\text{syn}}(R, \alpha) < \epsilon$. The contradiction with $p_{\text{asyn}} \leq c_L$ shows that (27a) cannot be satisfied for all R.

What remains for the proof is to show that also (27b) is not true. To show this considers the following relaxation of constraints in (19):

$$c_Q \omega_{\text{asyn}} + c_R \omega_{\text{sig}} + F_{\text{syn}}(R) \geq \eta p, \tag{30}$$

and (28b). Substituting the latter into (30), we get

$$\omega_{\text{asyn}} \geq \frac{\eta \times (p - c_R) - F_{\text{syn}}(R)}{c_Q - c_R}. \tag{31}$$

Since, for some blocking rate $R < 1$, the value of $F_{\text{syn}}(R)$ is arbitrary small and $p - c_R > 0$, we see that also (27b) is not satisfied. Therefore, there exists a blocking rate R such that $P_{guess}(R, \eta, p) < 1$.

Appendix C: Randomness of 2 → 1 quantum random access code

A common example [6,35,36] of a certificate (3) is based on the so-called $2 \rightarrow 1$ quantum random access code [37,38] in dimension 2:

$$W^{2\rightarrow 1}\left[\mathbb{P}_{B|XZ}\right] \equiv \frac{1}{8} \sum_{x \in X} \sum_{z \in Z} \mathbb{P}_{B|XZ}(b = x_z|x, z), \tag{32}$$

with $X = \{00, 01, 10, 11\}$, $Z = \{0, 1\}$, $B = \{0, 1\}$. Results of our experimental implementation of this QRAC are shown in Table 1.

To calculate the maximal average guessing probability and min-entropy in the proposed protocol, we performed optimization over the set of all probability distributions allowed by quantum mechanics using the see-saw technique [39,40] of semi-definite

Table 1 Observed experimental probabilities $\mathbb{P}(b|x,z)$ with error bars

$z=0$	$b=0$	$b=1$
$x=00$	$\mathbf{0.850016 \pm 0.026011}$	0.149984 ± 0.007815
$x=01$	$\mathbf{0.858255 \pm 0.029392}$	0.141745 ± 0.008488
$x=10$	0.145144 ± 0.007938	$\mathbf{0.854856 \pm 0.027039}$
$x=11$	0.146975 ± 0.007632	$\mathbf{0.853025 \pm 0.025767}$
$z=1$	$b=0$	$b=1$
$x=00$	$\mathbf{0.813494 \pm 0.020024}$	0.186506 ± 0.007073
$x=01$	0.148772 ± 0.006703	$\mathbf{0.851228 \pm 0.022439}$
$x=10$	$\mathbf{0.820518 \pm 0.020665}$	0.179482 ± 0.007086
$x=11$	0.161361 ± 0.006431	$\mathbf{0.838639 \pm 0.020305}$

The bold values refer to QRAC successes (their maximal possible average value is $0.5 + \frac{\sqrt{2}}{4} \approx 0.85355$). Please note that experimental losses, together with the average photon number per pulse μ, do affect the observed success probabilities reported here. However, as we have demonstrated recently [24], in a QRAC the decrease in the average success probability is only linear in the term μ (where represents the losses). Thus, the effect of multiphoton events while using $\mu = 0.66$, and an overall detection efficiency of 6% is minimal. This can be corroborated by noting that the obtained results are close to the ideal one

programming [41] and computed $g(p_e, e)$ from (26) with:

$$\begin{aligned} &\underset{\{\rho_x\},\{M_z^b\},\tilde{\boldsymbol{g}}:X\times Z\to B}{\text{maximize}} \quad \frac{1}{8}\sum_{x,z} P(\tilde{\boldsymbol{g}}(x,z)|x,z) \\ &\text{subject to} \quad \frac{1}{8}\sum_{x,z} P(x_z|x,z) = p_e, \\ &P(b|x,z) = \mathrm{Tr}\left(\rho_x M_b^z\right), \end{aligned} \tag{33}$$

where $\{\rho_x\} = \{\rho_{00}, \rho_{01}, \rho_{10}, \rho_{11}\}$ are states, $\{M_z^b\} = \{\{M_0^0, M_1^0\}, \{M_0^1, M_1^1\}\}$ are measurements on a Hilbert space of dimension 2, and $\tilde{\boldsymbol{g}}$ is a possible guessing strategy when x and z are known. We took $\mathbb{P}_{XZ}(x,z) = \frac{1}{|X||Z|} = \frac{1}{8}$. In this case, $c_L = \frac{3}{4}$ and $c_Q = \frac{1}{2} + \frac{\sqrt{2}}{4} \approx 0.8536$. The result of the optimization as a function of p_e is shown in Fig. 3. From (25), we conclude the following formula for $G(p)$:

$$G(p) = \frac{\frac{1}{2} + \frac{\sqrt{2}}{4} - 1}{\frac{1}{2} + \frac{\sqrt{2}}{4} - \frac{3}{4}} \times \left(p - \frac{3}{4}\right) + 1 = -\sqrt{2} \times \left(p - \frac{3}{4}\right) + 1. \tag{34}$$

Now, we give the explicit formula for $P_{guess}^{\mathrm{syn}}(p_{\mathrm{syn}}, \eta_{\mathrm{syn}})$ for the considered protocol. M is allowed not to click in $1-\eta$ part of rounds, and using detection efficiency loophole it can mimic a higher value of the certificate (32). The method is the following.

If $\eta \leq \frac{1}{2}$, then the malevolent vendor can use the following strategy for all inputs. P is encoding one bit from the input, x_0 or x_1 with equal ratio. The choice which bit

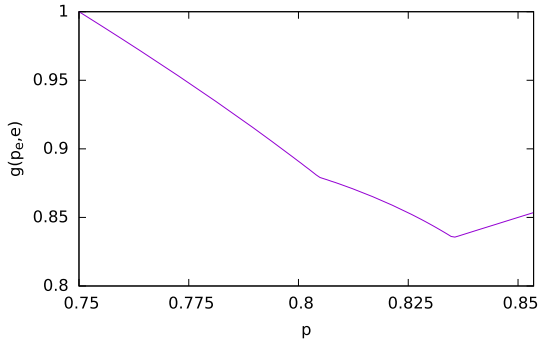

Fig. 3 (Color online) Maximal average guessing probability for a certificate (32) based on $2 \to 1$ quantum random access code obtained using see-saw technique with the formula (33). The function is not differentiable at points relating to changes of the optimal guessing function $\boldsymbol{g} : X \times Z \to B$, which are $\boldsymbol{g}_1(x_0, x_1, z) = x_0$, $\boldsymbol{g}_2(x_0, x_1, z) = x_0 \cdot x_1 \vee x_1 \cdot z$ and $\boldsymbol{g}_3(x_0, x_1, z) = x_z$ (reading from the left of the plot)

to encode is guided by shared randomness. If the input z matches the encoded bit, M measures the qubit and satisfies the certificate (32) with probability 1. Otherwise M outputs $\emptyset$. An upper bound on the maximal average guessing probability is given by:

$$\begin{aligned} P^{2\to 1}_{guess}\left(R, \eta, \alpha, p_{\text{asyn}}, q, \eta_{\text{asyn}}, \eta_{\text{syn}}\right) &\equiv_{[\eta_{\text{syn}} \le \frac{1}{2}]} \omega_{\text{asyn}} G(p_{\text{asyn}}) + \omega_{\text{sig}} + \omega_{\text{syn}} \\ &= 1 - \omega_{\text{asyn}}\sqrt{2}\left(p_{\text{asyn}} - \frac{3}{4}\right) = 1 - \frac{\sqrt{2}}{\eta}\eta_{\text{asyn}} P_{\text{asyn}}(R, \alpha) \times \left(p_{\text{asyn}} - \frac{3}{4}\right). \end{aligned} \tag{35}$$

If $\eta > \frac{1}{2}$ then in $2(1-\eta)$ part of rounds P uses the above encoding strategy and the device attains $W^{2\to 1}[\mathbb{P}] = 1$. In the remaining $2\eta - 1$ part of rounds, P and M use the states and measurements referring to the value of the certificate (32) equal to some $q \in [c_L, c_Q]$. The observed average value of the certificate in such a strategy is

$$p_{\text{syn}} = \frac{1}{\eta_{\text{syn}}}\left[(2\eta_{\text{syn}} - 1)q + (1 - \eta_{\text{syn}})\right] = 2q - 1 + \frac{1-q}{\eta_{\text{syn}}}. \tag{36}$$

The detection loophole allows to achieve the value of (36) up to $\frac{2\eta+\sqrt{2}-1}{2\sqrt{2}\eta} \le 1$ with $q = c_Q$. Thus,

$$c_S(\eta) = \min\left(\frac{2\eta + \sqrt{2} - 1}{2\sqrt{2}\eta}, 1\right). \tag{37}$$

The value of (36) equals $p_{\text{syn}} \leq c_S(\eta_{\text{syn}})$ if and only if $q = \frac{\eta_{\text{syn}}(1+p_{\text{syn}})-1}{2\eta_{\text{syn}}-1}$. The maximal average guessing probability is then upper bounded by

$$\begin{aligned}\tilde{G}(p_{\text{syn}}, \eta_{\text{syn}}) &\equiv \frac{2\eta_{\text{syn}}-1}{\eta_{\text{syn}}} \times G\left(\frac{\eta_{\text{syn}}(1+p_{\text{syn}})-1}{2\eta_{\text{syn}}-1}\right) + \frac{1-\eta_{\text{syn}}}{\eta_{\text{syn}}} \\ &= -\sqrt{2}p_{\text{syn}} + 1 + \frac{\sqrt{2}}{2} + \frac{\sqrt{2}}{4\eta_{\text{syn}}},\end{aligned} \tag{38}$$

or, equivalently,

$$\begin{aligned}\bar{G}(q, \eta_{\text{syn}}) &\equiv \frac{2\eta_{\text{syn}}-1}{\eta_{\text{syn}}} \times G(q) + \frac{1-\eta_{\text{syn}}}{\eta_{\text{syn}}} \\ &= \frac{1}{\eta_{\text{syn}}} \times \left[-\sqrt{2}q \times (2\eta_{\text{syn}}-1) - \frac{3\sqrt{2}}{4}\right] + \frac{3\sqrt{2}}{2} + 1,\end{aligned} \tag{39}$$

and is lower than 1 if and only if $p_{\text{syn}} > \frac{1}{2} + \frac{1}{4\eta_{\text{syn}}}$ or, equivalently, $q > \frac{3}{4}$. Using this, we get that an upper bound on the maximal average guessing probability is in this case given by

$$\begin{aligned}&P_{guess}^{2\to 1}\left(R, \eta, \alpha, p_{\text{asyn}}, q, \eta_{\text{asyn}}, \eta_{\text{syn}}\right) \equiv_{[\eta_{\text{syn}} > \frac{1}{2}]} \omega_{\text{asyn}} G(p_{\text{asyn}}) + \omega_{\text{sig}} \\ &\quad + \omega_{\text{syn}} \bar{G}(q, \eta_{\text{syn}}) \\ &= 1 - \sqrt{2} \times \left[\omega_{\text{asyn}} \times \left(p_{\text{asyn}} - \frac{3}{4}\right) + \frac{2\eta_{\text{syn}}-1}{\eta_{\text{syn}}} \times \omega_{\text{syn}} \times \left(q - \frac{3}{4}\right)\right] \\ &= 1 - \frac{\sqrt{2}}{\eta} \times \left[\eta_{\text{asyn}} P_{\text{asyn}}(R, \alpha)\left(p_{\text{asyn}} - \frac{3}{4}\right) + (2\eta_{\text{syn}}-1) P_{\text{syn}}(R, \alpha)\left(q - \frac{3}{4}\right)\right].\end{aligned} \tag{40}$$

Let us now give an explicit formula for an upper bound on the maximal average guessing probability, see (19), in this scenario. Let us define, cf. (36),

$$(36), p_{\text{syn}}^{\text{fun}}(q, \eta_{\text{syn}}) \equiv \begin{cases} 2q - 1 + \frac{1-q}{\eta_{\text{syn}}} & \text{for } \eta_{\text{syn}} > \frac{1}{2}, \\ 1 & \text{for } \eta_{\text{syn}} \leq \frac{1}{2}. \end{cases} \tag{41}$$

We have

$$\begin{aligned}P_{guess}(R, \eta, p) \leq \underset{\substack{\alpha\in[0,1] \\ \eta_{\text{asyn}}, \eta_{\text{sig}}, \eta_{\text{syn}} \in [0,1] \\ p_{\text{asyn}}, q \in [\frac{3}{4}, c_Q]}}{\text{maximize}} & P_{guess}^{2\to 1}\left(R, \eta, \alpha, p_{\text{asyn}}, q, \eta_{\text{asyn}}, \eta_{\text{syn}}\right) \\ \text{subject to} \quad & q^{\text{fun}}\left(R, \alpha, p_{\text{asyn}}, q, \right) \geq p, \\ & \eta^{\text{fun}}\left(R, \alpha, \right) = \eta,\end{aligned} \tag{42}$$

where q^{fun}, cf. (18b) is given by

$$\begin{aligned} q^{\text{fun}}\left(R,\alpha,p_{\text{asyn}},q,\right) &\equiv p_{\text{asyn}}\omega_{\text{asyn}}+\frac{1}{2}\omega_{\text{sig}}+p^{\text{fun}}_{\text{syn}}(q,\eta_{\text{syn}})\omega_{\text{syn}} \\ &= p_{\text{asyn}}\eta_{\text{asyn}}\frac{P_{\text{asyn}}(R,\alpha)}{\eta}+\frac{1}{2}\eta_{\text{sig}}\frac{P_{\text{sig}}(R,\alpha)}{\eta}+\eta_{\text{syn}}p^{\text{fun}}_{\text{syn}}(q,\eta_{\text{syn}})\frac{P_{\text{syn}}(R,\alpha)}{\eta} \end{aligned} \tag{43}$$

Let us denote

$$\begin{aligned} x &\equiv \eta\omega_{\text{asyn}}=\eta_{\text{asyn}}P_{\text{asyn}}(R,\alpha), \\ y &\equiv \eta\omega_{\text{syn}}=\eta_{\text{syn}}P_{\text{syn}}(R,\alpha). \end{aligned} \tag{44}$$

Now, use the constraint $\eta^{\text{fun}}\left(R,\alpha,\right)=\eta$, or, equivalently, $\eta_{\text{sig}}P_{\text{sig}}(R,\alpha)=\eta-x-y$, to eliminate η_{sig}. We separate further analysis in two cases.

In the case with $\eta_{\text{syn}}\in[0,\frac{1}{2}]$, we have $y\leq\frac{1}{2\eta}P_{\text{syn}}(R,\alpha)$. Let us denote for this case $z^{-}\equiv x\times\left(p_{\text{asyn}}-\frac{3}{4}\right)$. Then, (42) transforms to

$$P^{-}_{guess}(R,\eta,p)\leq \underset{\substack{\alpha\in[0,1]\\(x,y,z^{-})\in A^{-}(R,\eta,p,\alpha)}}{\text{maximize}} \quad 1-\frac{\sqrt{2}}{\eta}z^{-}, \tag{45}$$

where $A^{-}(R,\eta,p,\alpha)\subseteq\mathscr{R}^3$ is defined by the following linear constraints:

$$\begin{aligned} &0\leq x\leq P_{\text{asyn}}(R,\alpha), \\ &0\leq y\leq\frac{1}{2}P_{\text{syn}}(R,\alpha), \\ &0\leq z^{-}\leq\left(c_q-\frac{3}{4}\right)\times x, \\ &\eta-P_{\text{sig}}(R,\alpha)\leq x+y\leq\eta, \\ &\eta\times\left(p-\frac{1}{2}\right)-\frac{1}{4}x-\frac{1}{2}y\leq z^{-}. \end{aligned} \tag{46}$$

In the case with $\eta>\frac{1}{2}$, we have $y\geq\frac{1}{2}P_{\text{syn}}(R,\alpha)$. Let us now denote

$$z^{+}\equiv x\times\left(p_{\text{asyn}}-\frac{3}{4}\right)+(2y-P_{\text{syn}}(R,\alpha))\times\left(q-\frac{3}{4}\right). \tag{47}$$

As in the previous case, (42) transforms to

$$P^{+}_{guess}(R,\eta,p)\leq \underset{\substack{\alpha\in[0,1]\\(x,y,z^{+})\in A^{+}(R,\eta,p,\alpha)}}{\text{maximize}} \quad 1-\frac{\sqrt{2}}{\eta}z^{+}, \tag{48}$$

where $A^{+}(R,\eta,p,\alpha)\subseteq\mathscr{R}^3$ is defined by the following linear constraints:

$$\begin{aligned}
&0\leq x\leq P_{\text{asyn}}(R,\alpha),\\
&\frac{1}{2}P_{\text{syn}}(R,\alpha)\leq y\leq P_{\text{syn}}(R,\alpha),\\
&0\leq z^{+}\leq\left(c_Q-\frac{3}{4}\right)\times\left[x+2y-P_{\text{syn}}(R,\alpha)\right],\\
&\eta-P_{\text{sig}}(R,\alpha)\leq x+y\leq\eta,\\
&\eta\times\left(p-\frac{1}{2}\right)-\frac{1}{4}x-\frac{1}{4}P_{\text{syn}}(R,\alpha)\leq z^{+}.
\end{aligned}\tag{49}$$

It is easy to see that, for fixed $\alpha\in[0,1]$, the internal optimization in (45) and (48) is a linear program. Thus, we derive the following formula for $P_{guess}(R,\eta,p)$ for this scenario:

$$P_{guess}(R,\eta,p)\leq\max\left(P^{-}_{guess}(R,\eta,p),P^{+}_{guess}(R,\eta,p)\right),\tag{50}$$

with $P^{\pm}_{guess}(R,\eta,p)\equiv 0$ if $A^{\pm}=\emptyset$.

Appendix D: Direct calculations of the experimental randomness

We take the experimental value $p=0.8425$ and $\eta=0.06$ for $R=0.99$, as used in the setup. From our calculations of (45) and (48), it follows that the maximal average guessing probability is obtained for $\alpha=0.499$. In that case, $\eta_{\text{asyn}}=0.11880$, $\eta_{\text{sig}}=0$ and $\eta_{\text{syn}}=0.5$. We have $\omega_{\text{asyn}}=0.98951$, $\omega_{\text{sig}}=0$ and $\omega_{\text{syn}}=0.01049$ with $p_{\text{asyn}}=0.84083$ and $p_{\text{syn}}=1$. This gives $G(0.84083)=0.87155$. Direct calculation of (35) gives

$$0.98951\times 0.87155+0+0.01049\approx 0.87289,\tag{51}$$

and thus $-\log_2(0.87289)\approx 0.19612$. Since only $(1-R)\times\eta=0.0006$ emitted photons are detected, the generation ratio of min-entropy is

$$H_{\infty}(0.99,0.06,0.8425)\approx 0.00012.\tag{52}$$

Analogous calculations for $R=0.3$, $\eta=0.78$, and optimal $\alpha=0.157$. This gives $P_{\text{asyn}}(R,\alpha)=0.71827$, $P_{\text{sig}}(R,\alpha)=0.157$, $P_{\text{syn}}=0.12473$ with $\eta_{\text{asyn}}=0.99912$, $\eta_{\text{sig}}=0$, $\eta_{\text{syn}}=0.5$. Here $p_{\text{asyn}}=0.82881$ and $p_{\text{syn}}=1$, giving $G(0.82881)=0.88854$. From this, it follows that $\omega_{\text{asyn}}=0.92004$, $\omega_{\text{sig}}=0$, and $\omega_{\text{syn}}=0.07996$. Direct calculation gives

$$0.92004\times 0.88854+0+0.07996=0.89745,\tag{53}$$

and

$$H_\infty(0.3, 0.78, 0.8425) \approx -0.7 \times 0.78 \times \log_2(0.89745) \approx 0.08523. \quad (54)$$

References

1. Rarity, J.G., Owens, P.C.M., Tapster, P.R.: Quantum random-number generation and key sharing. J. Mod. Opt. **41**, 2435 (1994)
2. National Institute of Standards and Technology. Computer Security Division. Computer Security Resource Center
3. Colbeck, R.: Quantum and Relativistic Protocols for Secure Multi-Party Computation. Ph.D. Thesis, Cambridge University. arXiv:0911.3814v2 (2009)
4. Pironio, S., Massar, S.: Security of practical private randomness generation. Phys. Rev. A **87**, 012336 (2013)
5. Pironio, S., Acín, A., Massar, S., Boyer de la Giroday, A., Matsukevich, D.N., Maunz, P., Olmschenk, S., Hayes, D., Luo, L., Manning, T.A., Monroe, C.: Random numbers certified by Bell's theorem. Nature **464**, 1021 (2010)
6. Pawłowski, M., Brunner, N.: Semi-device-independent security of one-way quantum key distribution. Phys. Rev. A **84**, 010302 (2011)
7. Li, H.-W., Pawłowski, M., Yin, Z.-Q., Guo, G.-C., Han, Z.-F.: Semi-device-independent randomness certification using $n \rightarrow 1$ quantum random access codes. Phys. Rev. A **85**, 052308 (2012)
8. Mironowicz, P., Tavakoli, A., Hameedi, A., Marques, B., Pawłowski, M., Bourennane, M.: Increased certification of semi-device independent random numbers using many inputs and more post-processing. New J. Phys. **18**, 065004 (2016)
9. Lunghi, T., Brask, J.B., Lim, C.C.W., Lavigne, Q., Bowles, J., Martin, A., Zbinden, H., Brunner, N.: Self-testing quantum random number generator. Phys. Rev. Lett. **114**, 150501 (2015)
10. Cao, Z., Zhou, H., Ma, X.: Loss-tolerant measurement-device-independent quantum random number generation. New J. Phys. **17**, 125011 (2015)
11. Cao, Z., Zhou, H., Yuan, X., Ma, X.: Source-independent quantum random number generation. Phys. Rev. X **6**, 011020 (2016)
12. Marangon, D.G., Vallone, G., Villoresi, P.: Source-device-independent ultrafast quantum random number generation. Phys. Rev. Lett. **118**, 060503 (2017)
13. Brask, J.B., Martin, A., Esposito, W., Houlmann, R., Bowles, J., Zbinden, H., Brunner, N.: Megahertz-rate semi-device-independent quantum random number generators based on unambiguous state discrimination. Phys. Rev. Appl. **7**, 054018 (2017)
14. Dall'Arno, M., Passaro, E., Gallego, R., Pawłowski, M., Acín, A.: Detection loophole attacks on semi-device-independent quantum and classical protocols. Quant. Inf. Comput. **15**, 37 (2015)
15. Acín, A., Cavalcanti, D., Passaro, E., Pironio, S., Skrzypczyk, P.: Necessary detection efficiencies for secure quantum key distribution and bound randomness. Phys. Rev. A **93**, 012319 (2016)
16. Hameedi, A., Marques, B., Mironowicz, P., Saha, D., Pawłowski, M., Bourennane, M.: Experimental test of nonclassicality with arbitrarily low detection efficiency. Phys. Rev. A **102**, 032621 (2020)
17. Renner, R.: Security of Quantum Key Distribution. arXiv:quant-ph/0512258 (2005)
18. Koenig, R., Renner, R., Schaffner, C.: The operational meaning of min- and max-entropy. IEEE Trans. Inf. Theory **55**, 4337 (2009)
19. Grier, D.G.: A revolution in optical manipulation. Nature **424**, 810 (2003)
20. Lima, G., Vargas, A., Neves, L., Guzmán, R., Saavedra, C.: Manipulating spatial qudit states with programmable optical devices. Opt. Express **17**, 10688 (2009)
21. Neves, L., Lima, G., Gómez, J.A., Monken, C.H., Saavedra, C., Pádua, S.: Generation of entangled states of qudits using twin photons. Phys. Rev. Lett. **94**, 100501 (2005)
22. Goyeneche, D., Cañas, G., Etcheverry, S., Gómez, E.S., Xavier, G.B., Lima, G., Delgado, A.: Five measurement bases determine pure quantum states on any dimension. Phys. Rev. Lett. **115**, 090401 (2015)
23. Cañas, G., Etcheverry, S., Gómez, E.S., Saavedra, C., Xavier, G.B., Lima, G., Cabello, A.: Experimental implementation of an eight-dimensional Kochen–Specker set and observation of its connection with the Greenberger–Horne–Zeilinger theorem. Phys. Rev. A **90**, 012119 (2014)

24. Aguilar, E.A., Farkas, M., Martínez, D., Alvarado, M., Cariñe, J., Xavier, G.B., Barra, J.F., Cañas, G., Pawłowski, M., Lima, G.: Certifying an irreducible 1024-dimensional photonic state using refined dimension witnesses. Phys. Rev. Lett. **120**, 230503 (2018)
25. Solís-Prosser, M.A., Fernándes, M.F., Jiménez, O., Delgado, A., Neves, L.: Experimental minimum-error quantum state discrimination in high dimensions. Phys. Rev. Lett. **118**, 100501 (2017)
26. Marques, B., Matoso, A.A., Pimenta, W.M., Gutiérrez-Esparza, A.J., Santos, M.F., Pádua, S.: Experimental simulation of decoherence in photonics qudits. Sci. Rep. **5**, 16049 (2017)
27. Torres-Ruiz, F.A., Lima, G., Delgado, A., Pádua, S., Saavedra, C.: Decoherence in a double-slit quantum eraser. Phys. Rev. A **81**, 042104 (2010)
28. Lima, G., Neves, L., Guzmán, R., Gómez, E.S., Nogueira, W.A.T., Delgado, A., Vargas, A., Saavedra, C.: Experimental quantum tomography of photonic qudits via mutually unbiased basis. Opt. Express **19**, 3542 (2011)
29. Etcheverry, S., Cañas, G., Gómez, E.S., Nogueira, W.A.T., Saavedra, C., Xavier, G.B., Lima, G.: Quantum key distribution session with 16-dimensional photonic states. Sci. Rep. **3**, 2316 (2013)
30. Moreno, I., Velásquez, P., Fernandez-Pousa, C.R., Sánchez-López, M.M., Mateos, F.: Jones matrix method for predicting and optimizing the optical modulation properties of a liquid-crystal display. J. Appl. Phys. **94**, 3697 (2003)
31. Liu, Y., Yuan, X., Li, M.H., Zhang, W., Zhao, Q., Zhong, J., Cao, Y., Li, Y.-H., Chen, L.-K., Li, H., Peng, T., Chen, Y.-A., Peng, C.-Z., Shi, S.-C., Wang, Z., You, L., Ma, X., Fan, J., Zhang, Q., Pan, J.-W.: High-speed device-independent quantum random number generation without a detection loophole. Phys. Rev. Lett. **120**, 010503 (2018)
32. Eaton, J.W., Bateman, D., Hauberg, S., Wehbring, R.: GNU Octave Version 4.2.0 Manual: A High-Level Interactive Language for Numerical Computations. http://www.gnu.org/software/octave/doc/interpreter (2016)
33. Sturm, J.F.: Using SeDuMi 1.02, a MATLAB toolbox for optimization over symmetric cones. Optim. Methods Softw. **11**, 625 (1999)
34. Löfberg, J.: YALMIP: a toolbox for modeling and optimization in MATLAB. In: IEEE International Symposium on Computer Aided Control Systems Design (2004). IEEE, New York, p. 284
35. Li, H.-W., Yin, Z.-Q., Wu, Y.-C., Zou, X.-B., Wang, S., Chen, W., Guo, G.-C., Han, Z.-F.: Semi-device-independent random-number expansion without entanglement. Phys. Rev. A **84**, 034301 (2011)
36. Mironowicz, P., Li, H.W., Pawłowski, M.: Properties of dimension witnesses and their semi-definite programming relaxations. Phys. Rev. A **90**, 022322 (2014)
37. Ambainis, A., Nayak, A., Ta-Shma, A., Vazirani, U.: Dense quantum coding and quantum finite automata. J. ACM **49**, 496 (2002)
38. Ambainis, A., Leung, D., Mancinska, L., Ozols, M.: Quantum random access codes with shared randomness. arXiv:0810.2937 (2008)
39. Werner, R.F., Wolf, M.M.: Bell inequalities and entanglement. Quantum Info. Comput. **1**, 1 (2001)
40. Pál, K.F., Vértesi, T.: Maximal violation of a bipartite three-setting, two-outcome Bell inequality using infinite-dimensional quantum systems. Phys. Rev. A **82**, 022116 (2010)
41. Vandenberghe, L., Boyd, S.: Semidefinite programming. SIAM Rev. **38**, 49 (1996)