



Deposited via The University of York.

White Rose Research Online URL for this paper:

<https://eprints.whiterose.ac.uk/id/eprint/194166/>

Version: Published Version

Article:

Avesani, Marco, Tebyanian, Hamid, Villoresi, Paolo et al. (2022) Unbounded randomness from uncharacterized sources. Communications Physics. 273. ISSN: 2399-3650

<https://doi.org/10.1038/s42005-022-01038-3>

Reuse

This article is distributed under the terms of the Creative Commons Attribution (CC BY) licence. This licence allows you to distribute, remix, tweak, and build upon the work, even commercially, as long as you credit the authors for the original work. More information and the full terms of the licence here:

<https://creativecommons.org/licenses/>

Takedown

If you consider content in White Rose Research Online to be in breach of UK law, please notify us by emailing eprints@whiterose.ac.uk including the URL of the record and the reason for the withdrawal request.

Unbounded randomness from uncharacterized sources

Marco Avesani¹[✉], Hamid Tebyanian¹¹, Paolo Villorosi^{1,2} & Giuseppe Vallone^{1,2,3}

Randomness is a central feature of quantum mechanics and an invaluable resource for both classical and quantum technologies. Commonly, in Device-Independent and Semi-Device-Independent scenarios, randomness is certified using projective measurements, and its amount is bounded by the quantum system's dimension. Here, we propose a Source-Device-Independent protocol, based on Positive Operator Valued Measurement (POVM), which can arbitrarily increase the number of certified bits for any fixed dimension. Additionally, the proposed protocol doesn't require an initial seed and active basis switching, simplifying its experimental implementation and increasing the generation rates. A tight lower-bound on the quantum conditional min-entropy is derived using only the POVM structure and the experimental expectation values, taking into account the quantum side-information. For symmetric POVM on the Bloch sphere, we derive closed-form analytical bounds. Finally, we experimentally demonstrate our method with a compact and simple photonic setup that employs polarization-encoded qubits and POVM up to 6 outcomes.

¹Dipartimento di Ingegneria dell'Informazione, Università degli Studi di Padova, via Gradenigo 6B, 35131 Padova, Italy. ²Istituto di Fotonica e Nanotecnologie - CNR, Via Trasea 7, 35131 Padova, Italy. ³Dipartimento di Fisica e Astronomia, Università di Padova, via Marzolo 8, 35131 Padova, Italy. ✉email: marco.avesani@unipd.it

Random numbers are necessary for many different applications, ranging from simulations to cryptography and fundamental physics tests, such as Bell tests^{1–3}. Despite its common use, the certification of randomness is a complex task. Classical processes cannot generate genuine randomness because of the determinism of classical mechanics. On the other hand, randomness is an intrinsic feature of quantum mechanics due to the probabilistic nature of its laws. However, the generation and certification of randomness, even from quantum processes, always require some assumptions⁴.

The most reliable type of certification is given by *Device-Independent* (DI) protocols⁴ where the violation of a Bell inequality can certify the randomness and privacy of the numbers without any assumption on the devices used. Despite recent demonstrations^{5–9}, DI-QRNGs are extremely demanding from an experimental point of view, and their performances also cannot satisfy the needs for practical implementation. For this reason, all current commercial QRNGs use *trusted protocols*, where both the source and measurements are trusted.

Although trusted QRNGs are high-rate, easy-to-implement and cheap, the security and privacy of the generated random numbers could be compromised. Recently, a new class of protocols, called *Semi-Device-Independent* (Semi-DI)^{10,11} have been proposed as a compromise between the DI and the trusted ones. The Semi-DI protocols work in a similar "paranoid scenario" of DI, although with few assumptions on the devices' inner working. Assumptions can be related to the dimension of the exchanged system¹², the device used for the measurement^{13–17}, the device used for the source^{18,19}, the overlap between the states²⁰ the energy^{21–27} or general apparatus imperfections²⁸. These protocols are promising, since they can provide a higher level of security with a generation rate compatible with practical needs.

Most of the DI and Semi-DI protocols employ projective measurement, limiting the maximal certification to the underlying Hilbert space's dimension. The possibility of increasing the generation rate using general measurement has recently been discussed for entangled systems in the DI scenario^{29–31}. While projective measurements can only certify up to one bit of randomness for every pair of entangled qubits, POVM can saturate the optimal bound of 2 bits³⁰. Additionally, unbounded generation is possible if repeated non-demolition measurements are performed on one of the qubits, but the protocol is not robust to noise^{32,33}. However, all of these scenarios need entanglement, which is a strong requirement and involves an increased experimental complexity.

In this work, we will consider a prepare-and-measure scenario where the coherence (or purity) of the source is the resource for the protocol. We will show that a robust unbounded randomness certification can be obtained in the Source-DI scenario when non-orthogonal POVMs are used. For a fixed dimension of Hilbert space, we demonstrate that the amount of extractable random bits scales up as $\propto \log_2(N)$ with N the number of POVM outcomes. In such a way, an infinite number of random bits can be certified for any dimension of the quantum system to be measured. In addition, the use of non-orthogonal POVMs instead of multiple projective measurements allows to implement the Source-DI protocol without an active switching of the measurement basis, but in a completely passive way. This feature greatly simplifies the experimental implementation which does not require fast electronics for the switching and can increase the generation rate, which is not limited by the switching frequency. Moreover, no additional randomness and an initial seed is required for the basis selection. We specialize our analysis for polarization qubits, considering symmetric POVM measurements. In particular, we derive tight analytical bounds for equiangular POVMs restricted on the plane of the Bloch sphere and for POVMs that correspond

to Platonic solids inscribed in the Bloch sphere. Finally, to validate our findings, we experimentally implement three equiangular measurements on a plane with 3, 4, and 6 outcomes, and the octahedron measurement with 6 outcomes, using a simple optical setup.

Results

Randomness certification with POVM. In the prepare and measure scenario, a QRNG is composed of two systems: a source that emits a quantum state $\hat{\rho}_A$ and a measurement station. At each round, the measurement produces an outcome $K = k$ with some probability P_k .

While in the trusted scenario, both the measurement and preparation stages are trusted and characterized, in the Source-DI scenario only the measurement is trusted and characterized, while the source is considered untrusted and under the control of the eavesdropper (Eve). Trusted measurement means that the user has full control of the measurement apparatus. In particular, trusted POVM means that any adversary has no classical or quantum correlation with the measurement setup and he cannot access the Naimark extension of the POVM.

In this case, the amount of *private* randomness that can be extracted by the QRNG can be quantified by quantum conditional min-entropy³⁴, related to the guessing probability as

$$H_{\min}(X|E) = -\log_2(p_g(X|E)) \quad (1)$$

Here, the probability of correctly guessing the measurement outcome p_g is conditioned on Eve's (quantum) side information E on the system.

As discussed in ref. ¹³, if the prepared state $\hat{\rho}_A$ is pure, Eve does not have access to any quantum side information. On the contrary, if $\hat{\rho}_A$ is mixed, there is always a purification $\hat{\rho}_{AE}$ of $\hat{\rho}_A$, such that the systems A and E are correlated. Bounding the $H_{\min}(X|E)$ is then directly linked with the problem of bounding the purity of the unknown state $\hat{\rho}_A$.

In this scenario, a single projective measurement $\{\hat{P}_i\}$ cannot certify any amount of randomness^{13,35}.

A solution to this problem, proposed in ref. ¹³, uses two conjugate projective measurements \mathbb{Z} and \mathbb{X} and the Entropic Uncertainty Principle to bound the value of $H_{\min}(X|E)$. However, this approach requires the active switching of the two conjugate measurements that comes with two major drawbacks: first, the switching requires an initial source of private randomness and then requires active elements in the experimental implementation, increasing the complexity of the setup. For this protocol, the maximum value of min entropy is upper bounded by the dimension d of the measurement $H_{\min}(X|E) \leq \log_2(d)$.

In the following, we will show that the use of a single POVM $\{\hat{F}_k\}$ with $k = 1, \dots, N$ at the measurement station will solve the above issues. No initial randomness and no active devices are required; the maximum value of the min-entropy is bounded by the number of POVM elements N , but is not limited by the dimension d of the underlying Hilbert space.

Since we are working in the source-device-independent framework, we do not have assumptions on the quantum source, which can share, in general, quantum correlations with the adversary, meaning that there are no restrictions to the bipartite state $\hat{\rho}_{AE}$. On the other hand, the measurements are characterized, and the POVM operators are known, so we do not consider quantum-side information on the measurement side.

In the Methods we demonstrate the following:

Proposition 1. In the source-device independent framework with a trusted measurement device described by the POVM $\{\hat{F}_k\}$ with

$k = 1, \dots, N$, the guessing probability can be written as

$$p_g(X|E) = \max_{\{p_k, \hat{\tau}_k\}} \sum_{k=1}^N p_k \text{Tr}_A[\hat{F}_k \hat{\tau}_k] \quad (2)$$

where the normalized states $\hat{\tau}_k$ belong to the A system and the maximization is subjected to the following constraint on the states $\hat{\tau}_k$

$$\text{Tr}_A[\hat{F}_j (\sum_{k=1}^N p_k \hat{\tau}_k)] = P_j, \quad j = 1, \dots, N, \quad (3)$$

and P_j are the experimental observed probabilities.

The above constraint ensures that the states $\hat{\tau}_k$ form a decomposition of the state $\hat{\rho}'_A \equiv \sum_k p_k \hat{\tau}_k$ that has the same outcome probabilities P_j of the unknown state $\hat{\rho}_A$ when measured with the POVM $\{\hat{F}_j\}$. Differently from the common definition of p_g for classical-quantum states presented in ref. ³⁶, the above formulation is easier to calculate in scenarios where the source is untrusted.

From this definition of $p_g(X|E)$, we can see why a single projective measurement $\{\hat{\Pi}_k\}$ (that satisfies $\hat{\Pi}_i \hat{\Pi}_k = \delta_{i,k} \hat{\Pi}_k$) cannot be used to extract randomness: for every set of P_k we can choose in Eq. (2) $\hat{\tau}_k = \hat{\Pi}_k$ and $p_k = P_k$, such that $\sum_j p_j \text{Tr}[\hat{\Pi}_k \hat{\tau}_j] = P_k$ and $\text{Tr}[\hat{\Pi}_k \hat{\tau}_k] = 1$. Thus, $p_g(X|E)$ reaches unity, which means that Eve is able to guess Alice's result deterministically. On the other hand, if the POVM used by Alice have non-orthogonal elements $\hat{F}_j^N \hat{F}_k^N \neq \delta_{j,k}$ the attacker can never guess with certainty the outcome of the measurement.

Let us first consider the simple case where the equiangular three-state POVM for a qubit is used, namely:

$$\hat{F}_k^3 = \frac{2}{3} |\psi_k\rangle\langle\psi_k| \quad (4)$$

where

$$\begin{aligned} |\psi_1\rangle &= |0\rangle \\ |\psi_2\rangle &= \frac{1}{2}|0\rangle + \frac{\sqrt{3}}{2}|1\rangle \\ |\psi_3\rangle &= \frac{1}{2}|0\rangle - \frac{\sqrt{3}}{2}|1\rangle \end{aligned} \quad (5)$$

By solving the optimization problem in Eq. (2), we can calculate $H_{\min}(X|E)$ for every possible set of states $\hat{\rho}_A$ sent by the attacker.

Since the POVM elements \hat{F}_k belong to the ZX plane of the Bloch sphere, all the $\hat{\rho}_A$ that have the same projection in the ZX plane will lead to the same result. The min-entropy in function of the projection of the state $\hat{\rho}_A$ in the ZX plane are shown in Fig. 1.

It is possible to distinguish two different areas: the region inside the triangle (formed by the lines that connect the three $|\psi_k\rangle$), and the one outside it. Within this region, the min-entropy is constant and it reaches the minimal value of $H_{\min}(X|E) = -\log_2(2/3) \approx 0.58$. This result is in contrast with projective measurements, where a single projective measurement can never achieve $H_{\min}(X|E) > 0$. Outside this region, the min-entropy increases monotonically and reaches its maximum $H_{\min}(X|E) = 1$ for three pure states, each orthogonal to one of the states $|\psi_k\rangle$.

The reason can be intuitively understood. Consider that the state orthogonal to $|\psi_1\rangle$ is sent: the output corresponding to \hat{F}_1^3 never appears, and this result alone certifies the purity of ρ_A . On the other hand, the other two outcomes relative to \hat{F}_2^3 and \hat{F}_3^3 occur with the same probability of 0.5. Then, in this case, it behaves like an unbiased coin, and the maximum achievable randomness is 1 bit per measurement.

Exploiting the geometrical properties of the POVM we derived an analytical relation on $p_g(X|E)$ as a function of the measured

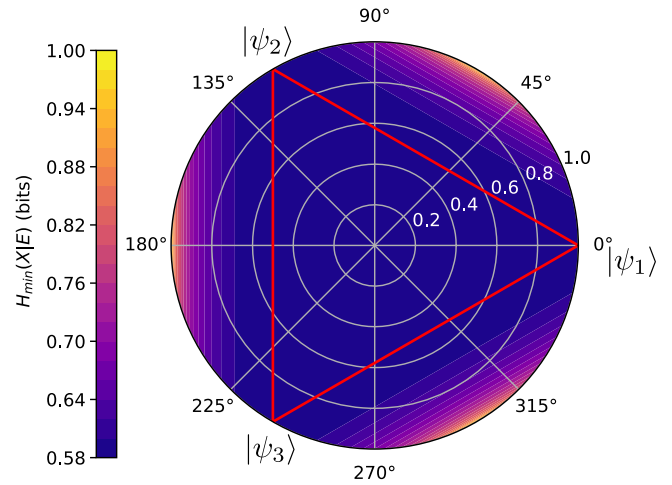


Fig. 1 Min-entropy contour plot. Contour plot of $H_{\min}(X|E)$ for the three-outcome POVM \hat{F}_k^3 in function of the projection of $\hat{\rho}_A$ in the ZX plane of the Bloch sphere. The states $|\Psi_i\rangle$ are associated to the POVM elements. For experimental probabilities inside the red triangle 0.58 bits of randomness can be certified, while for the region outside the triangle up to 1bit can be certified.

outcomes for general regular POVMs with N outcomes, as stated below.

Proposition 2. Consider the N -outcome qubit POVM $\{\hat{F}_k^N\}$ defined by

$$\hat{F}_k^N = \frac{1}{3} (\mathbb{1} + \vec{a}_k \cdot \vec{\sigma}), \quad k = 1, \dots, N \quad (6)$$

with \vec{a}_k representing the vertices of a regular polygon in the ZX plane, namely $\vec{a}_k = 1$ and $\vec{a}_k \cdot \vec{a}_{k+1} = \cos \frac{2\pi}{N}$. The measured output probabilities P_k uniquely identify a point \vec{r} in the ZX plane with coordinates (r_z, r_x) . The guessing probability $p_g(X|E)$ is given by

$$p_g = \frac{1}{N} + \frac{1}{N} \sum_k f_N(\vec{r} \cdot \vec{u}_k, \alpha) \theta(\vec{r} \cdot \vec{u}_k - \cos \alpha) \quad (7)$$

where

$$\begin{aligned} f_N(x, \alpha) &= x \cos \alpha + \sqrt{1 - x^2} \sin \alpha \\ \alpha &= \frac{\pi}{N} \end{aligned} \quad (8)$$

and \vec{u}_k the unit vectors orthogonal to the edges of the polygon.

We note that if the point \vec{r} is inside the polygon, then $p_g(X|E) = 2/N$. Otherwise, if the point \vec{r} is outside the polygon, only one term in the sum (7) is nonvanishing. From the experimental probabilities we can obtain the point \vec{r} with different methods: it is possible to employ a simple linear inversion, however, a more reliable method is to use the approach described in ref. ³⁷.

For an arbitrary set of POVM, the guessing probability can be numerically obtained by Semidefinite Optimization (SDP), as shown in the Methods.

Analytical results for regular POVMs of Eq. (7) has been compared with the numerical solutions for N up to 100. The results were calculated with respect to the statistics reproduced by $\hat{\rho}_A$ sampled from the entire Bloch sphere. The numerical and analytical methods always agreed, up to a factor smaller than the numerical tolerance.

In Fig. 2, for $N = 4, 5, 6$ and 10, we show the contour plots of the min-entropy as a function of the projection of the unknown state $\hat{\rho}_A$ in the ZX plane of the Bloch sphere. By increasing the

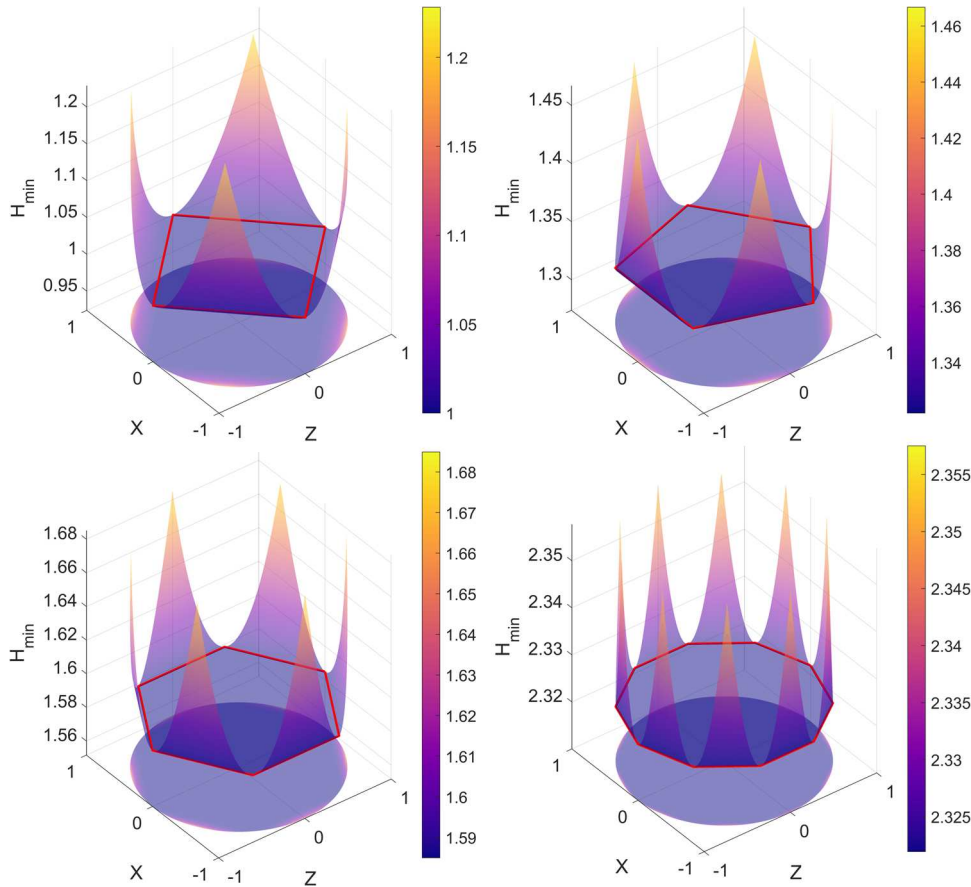


Fig. 2 Min-entropy 3D plot for different POVM outcomes. 3D plot of $H_{min}(X|E)$ in function of the projection of $\hat{\rho}_A$ in the ZX plane. The POVM considered have 4, 5, 6, 10 equispaced elements in the ZX plane. In the region inside the red lines the lower-bound of the min-entropy is reached.

number of outcomes, both the lowest and the highest $H_{min}(X|E)$ increase. From Eq. (7) we obtain:

$$M_N \equiv \max_{\vec{r}}(H_{min}(X|E)) = \log_2\left(\frac{N}{1 + \cos \alpha}\right) \quad (9)$$

$$m_N \equiv \min_{\vec{r}}(H_{min}(X|E)) = \log_2(N) - 1 \quad (10)$$

with $\alpha = \frac{\pi}{N}$. This scaling as a function of N for a qubit system and equiangular POVM on a plane is reported in Fig. 3.

The difference between M_N and m_N is given by:

$$M_N - m_N = 1 - \log_2\left(1 + \cos \frac{\pi}{N}\right) \approx \frac{\pi^2}{2N^2 \ln 2} \quad (11)$$

which becomes negligible for large N , since the distance between the POVM's elements also gets smaller.

The analytical bounds of Eq. (7) can be extended to general POVM, not restricted to a plane of the Bloch sphere. We also considered symmetric POVMs, representing platonic solids inscribed in the Bloch sphere³⁸. We show in Supplementary Method 1 that for these measurements, Eq. (9), with different values of α , correctly bounds the maximum amount of min-entropy that can be certified. In Fig. 3 we compare the scaling of such measurements with the POVM restricted to the plane.

Additionally, in Fig. 3 we show a comparison between the extractable randomness in the trusted and Source-DI scenarios. In the trusted scenario (i.e., both source and measurement trusted, without quantum correlation between the devices and the attacker), up to $\log_2 N$ bits can be certified per measurement, sending for example the completely mixed state $\hat{1}_2$.

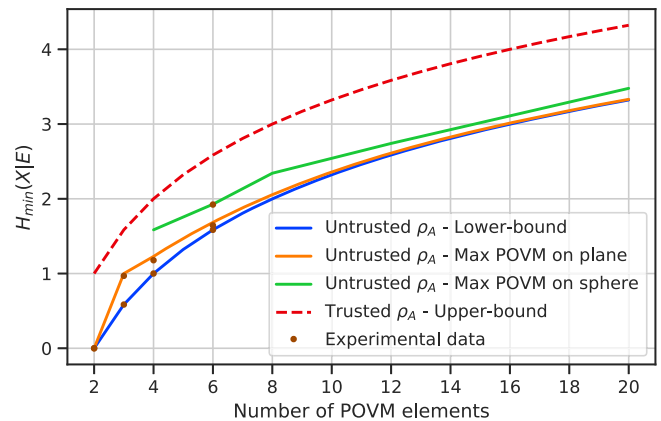


Fig. 3 Min-entropy scaling as a function of the number of POVM elements. Scaling of $H_{min}(X|E)$ as a function of N . In the untrusted scenario, we report the max and the min $H_{min}(X|E)$ for N equispaced POVM on a plane of the Bloch sphere. We also report the max $H_{min}(X|E)$ for POVM representing platonic solids inscribed in the Bloch sphere. The dashed line represents the upper-bound for the trusted model. Finally, the colored dot represent estimated min-entropy from the experimental data. The error bars represent the standard deviation of the mean but they are smaller than the symbols of the datapoints.

The gap between the trusted and the untrusted bounds is never larger than 1 bit, for any ρ_A , meaning that the price to pay for the increased security of the Source-DI certification is at most 1 bit per measurement. The results indicate that in the asymptotic limit

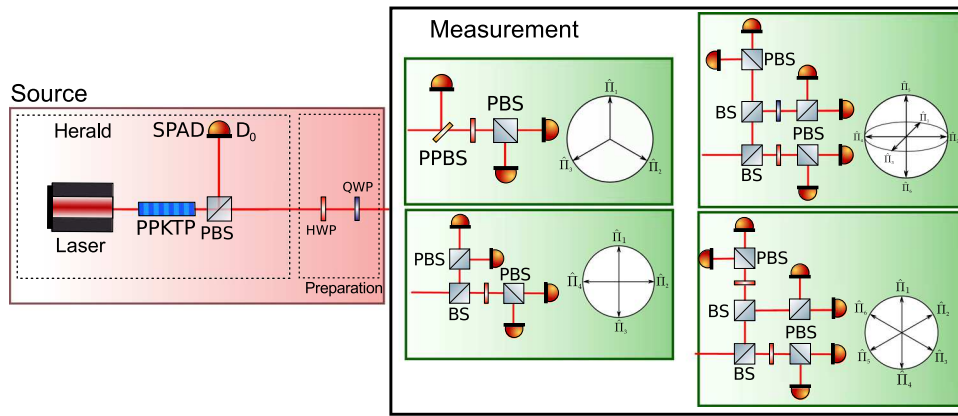


Fig. 4 Experimental setup. An heralded single photon source made from a Periodically Poled Potassium Titanyl Phosphate (PPKTP) crystal in a Sagnac interferometer, generates single photons at 808 nm. After the polarizing beam splitter (PBS), the heralded photon is prepared in any desired polarization by using an Half-Wave Plate (HWP) and a Quarter-Wave Plate (QWP). The photon is then measured using Single Photon Avalanche Diodes (SPAD) with four different POVM configurations with 3, 4, and 6 outcomes. The coincidences between the heralding photon detector D_0 and the detectors in the measurement station are recorded by a timetagger on a PC.

$N \rightarrow \infty$ the min-entropy tends to $H_{min}(X|E) \rightarrow \infty$, showing that unbounded randomness can be certified even from quantum systems with finite dimension d , including qubits.

Finally, we would like to highlight several advantages of the proposed protocol over previous discrete variable source-DI protocols^{13,35,39,40}. In addition to the increased $H_{min}(X|E)$ per measurement, the protocol allows for an important simplification of the experimental setup. Indeed, the non-orthogonal POVMs considered in this work can be implemented with only passive optical element. On the contrary, previous protocols based on Quantum State Tomography³⁵ or the Entropic Uncertainty Principle^{13,39,40} require an active and random switching of the measurement basis. The active switching requires fast electronics to implement it in real-time during the execution of the protocol and is often the main factor limiting the speed of the QRNG⁴⁰. Moreover, basis switching requires an initial random seed for random selection of the basis and consumes part of the produced randomness after the start of the protocol, lowering the final generation rate. In contrast, the protocol presented in this work does not require any initial seed for the implementation of the protocol.

Experimental implementation. To test the certification protocol with a proof-of-principle experiment, we developed a simple optical setup that employs a heralded single-photon source and four different POVM configurations. The preparation and measurement exploit the polarization degree of freedom of single photons. A schematic representation of the setup is shown in Fig. 4. The heralded source is composed of a continuous-wave laser at 404 nm, which optically pumps a 30 mm long Periodically Poled Potassium Titanyl Phosphate crystal. This configuration produces photon pairs at 808 nm through type-II collinear-phase-matching spontaneous parametric down-conversion.

The photons are deterministically separated by a polarizing beam splitter (PBS), and the detection of a photon at D_0 (see Fig. 4) heralds the presence of the single photon $|H\rangle_s$, which is sent to the preparation stage.

Here a Half Wave Plate (HWP) and a Quarter Wave Plate (QWP) are used to prepare the photon in any required polarization. The photon is then sent to Alice’s measurement. Taking into account filtering and finite SPAD efficiency, we obtain a heralded photon generation rate of ≈ 10 kHz.

We decided to implement the protocol using a heralded single-photon source in order to reduce the contribution of dark counts

and background noise. However, since we work in the Source-DI scenario, no assumptions are made on the source or on the channel losses and any implementation can be used.

The POVM $\{\hat{F}_k^N\}$ used by Alice are N -output measurement in the two-dimensional Hilbert space of photon polarization. The optical implementation of such POVM can be realized by using interferometric setups (as in ref. 41); however, this technique requires high precision in the alignment and offers low temporal stability. For this reason, we decided to follow the approach presented in⁴², which does not require any interferometric scheme.

In the three outcomes equiangular POVM \hat{F}_k^3 , shown in Fig. 4, the photon passes through a Partially Polarizing Beam Splitter (pPBS), which reflects with probability $2/3$ the state $|V\rangle$, while fully transmits $|H\rangle$.

Thus, detecting the reflected photons implements the first POVM element $\hat{F}_1^3 = \frac{2}{3}|V\rangle\langle V|$. The transmitted part is instead measured in the diagonal basis, implementing the remaining operators \hat{F}_2^3 and \hat{F}_3^3 (see ref. 42 for more detail).

The POVM with four and six outcomes can be implemented in a similar way, and they only require standard BS, PBS and waveplates.

The four-outcome POVM \hat{F}_k^4 is realized in the following way: a 50:50 BS reflects and transmits the photons with equal probability, then in the reflected path a PBS measures in the \mathbb{Z} basis, while in the transmitted path the HWP at $\frac{\pi}{8}$ followed by the PBS, performs a measurement in the \mathbb{X} basis. Accordingly, the four POVM elements $\{\hat{F}_k^4\} = \{\frac{1}{4}|H\rangle\langle H|, \frac{1}{4}|+\rangle\langle +|, \frac{1}{4}|V\rangle\langle V|, \frac{1}{4}|-\rangle\langle -|\}$ are realized. Similarly, for the six-outcome POVM on the plane \hat{F}_k^6 , a BS with transmissivity $\frac{2}{3}$ followed by a BS with transmissivity $\frac{1}{2}$, creates three different optical paths where the probability of detecting a photon is $\frac{1}{3}$. Later, one path is measured directly along with the \mathbb{Z} basis with a

PBS, implementing the elements $\hat{F}_{1,4}^6 = \frac{1}{6}|H\rangle\langle H|, \frac{1}{6}|V\rangle\langle V|$. In the second arm, an HWP at $\frac{\pi}{12}$ before the PBS implements the elements $\hat{F}_{2,5}^6 = \frac{1}{6}(\frac{\sqrt{3}}{2}|H\rangle + \frac{1}{2}|V\rangle)(\frac{\sqrt{3}}{2}\langle H| + \frac{1}{2}\langle V|), \frac{1}{6}(\frac{1}{2}|H\rangle - \frac{\sqrt{3}}{2}|V\rangle)(\frac{1}{2}\langle H| - \frac{\sqrt{3}}{2}\langle V|)$. Similarly, in the third arm, an HWP at $\frac{\pi}{6}$ before the PBS implements the elements: $\hat{F}_{3,6}^6 = \frac{1}{6}(\frac{1}{2}|H\rangle + \frac{\sqrt{3}}{2}|V\rangle)(\frac{1}{2}\langle H| + \frac{\sqrt{3}}{2}\langle V|), \frac{1}{6}(\frac{\sqrt{3}}{2}|H\rangle - \frac{1}{2}|V\rangle)(\frac{\sqrt{3}}{2}\langle H| - \frac{1}{2}\langle V|)$. Finally, the implementation of the six-outcome POVM \hat{S}^6 is similar to the previous one. One of the HWP is now rotated at $\frac{\pi}{8}$ while the other HWP is replaced with a QWP at $\frac{\pi}{4}$. In this way, each arm measures along one of the $\mathbb{X}, \mathbb{Y}, \mathbb{Z}$

bases, implementing the following POVM elements $\{\hat{S}_k^6\} = \{\frac{1}{6}|H\rangle\langle H|, \frac{1}{6}|+\rangle\langle +|, \frac{1}{6}|L\rangle\langle L|, \frac{1}{6}|V\rangle\langle V|, \frac{1}{6}|-\rangle\langle -|, \frac{1}{6}|R\rangle\langle R|\}$.

After the polarization measurements, the photons are collected by multimode fibers and detected by Silicon SPAD (Excelitas SPCM-NIR).

The electrical signals generated by the SPADs are registered by a Time-to-Digital Converter with a resolution of 81 ps, which streams the data to a PC. On the PC, we keep only the timetags that are inside a coincidence window of 1ns between the heralding detector and any other detector.

Experimental results. In this section we describe the results of our experimental run. For each of the four measurement configurations described in the previous section, we prepare four different quantum states ρ_A and we evaluate the corresponding min-entropy $H_{\min}(X|E)_a$ in the asymptotic limit. The states are chosen in order to maximize or minimize the min-entropy. However, since the protocol assumes uncharacterized light, we do not use any information about the preparation for the actual estimation of the randomness in the system.

For each run of the protocol, we use the heralded source to prepare the state, and we record the number of coincidences between the heralding detector D_0 and any other detector D_1-D_N , associated to a particular POVM element. Then the total number of events per detector N_k is directly converted to a probability $p_k = \frac{N_k}{\sum_i N_i}$ of the occurrence of a particular POVM element \hat{F}_k .

For a typical run of the experiment, we acquire a total number N_{tot} of 10^7 coincidence events. However, since the prepared states are (almost) pure, the finite statistics could lead to non-physical quantum states, similarly to what happens for quantum state tomography^{43,44}. To enforce a physical reconstruction, we use the constrained maximum-likelihood estimation technique presented in ref.³⁷ to retrieve a physical state $\tilde{\rho}_A$ compatible with the measured statistics p_k . The asymptotic min-entropy $H_{\min}(X|E)_a$ has been calculated using both the numerical methods presented in Methods and the analytical expression given by Eq. (7) (or its general version given in Eq. S25) for the reconstructed state $\tilde{\rho}_A$.

The results are shown graphically in Fig. 3, while the estimated $\tilde{\rho}_A$ and $H_{\min}(X|E)_a$ are reported in the Supplementary Methods 3, in particular in the Supplementary Tables I, II, III, IV. As we can see, the experimental data confirm the expected scalings up to $N=6$, for both the maximum and minimum of the $H_{\min}(X|E)$. Considering the heralded photon generation rate of ≈ 10 kHz of our source, depending on the specific configuration implemented and the obtained min-entropy, the random generation rate is between 5 and 20 kbps.

Although the theoretical lower bound was always experimentally achievable (up to numerical precision), the maximum of the $H_{\min}(X|E)$ could not be achieved exactly. This effect is due to the limited accuracy in the preparation of the ρ_A state and the unavoidable dark counts in \hat{F}_k due to accidental coincidences.

In the present proof-of-principle experiment, we considered a perfect POVM as defined above. However, any experimental measurement device is subject to imperfection. To deal with the experimental realization of POVM subjected to errors, we could recall that our results are completely general and they can be applied to any POVM. Therefore, since the measurement device is trusted, it is possible to characterize all the imperfections of the beam-splitters, polarizing beam-splitters, single-photon detectors and other elements. To perform this characterization of the implemented POVM, Quantum Measurement Tomography (QMT) can be used⁴⁵. After these characterizations a well-defined POVM is obtained. While for "symmetric" POVM such as (6) it is possible to find analytic results, for generic POVM it is possible to use the numerical tools illustrated in Methods to

evaluate the conditional min-entropy. In this way, by using the QMT and the numerical tools, it is possible to bound the min-entropy not only for SIC-POVM and ideal measurements, but also for any general non-ideal measurement, greatly simplifying the experimental requirements and increasing the robustness of the protocol.

Under the i.i.d. condition, it is possible to exploit the numerical approach presented in the Methods to include finite-size effects. To obtain bounds without the I.I.D assumption, several approaches are possible. A simple, but non-tight method would be to bound the guessing probability without constraints. In this way, the min-entropy would be minimized over all the possible quantum states, not only the ones compatible with the observed statistics. We detail this approach in Supplementary Methods 2. However, this method is not tight, since it always bounds the min-entropy with the lowest possible value obtainable by that specific POVM, regardless of the output statistics. To obtain tighter bound without the I.I.D assumption it is possible to exploit the newly developed Entropy Accumulation Theorem (EAT)⁴⁶ or Quantum Probability Estimation⁴⁷. As an example, if the EAT is chosen, it is possible to follow the construction detailed in⁴⁸, where a min-tradeoff function for the EAT is built from the single-round quantum conditional min-entropy. Using that framework it is possible to obtain the (accumulated) smooth conditional min-entropy for n rounds without the I.I.D assumption. A similar approach can be done for QPE, as, for example, in ref.²⁸. The full inclusion of finite-size effects by the EAT is out of the scope of this work and will be investigated in our future research.

Conclusion

We have presented a protocol for the generation of random numbers from quantum measurement based on the Source-Device-Independent scenario: no assumptions are included in the source of quantum states, while the measurement device is fully trusted and characterized. We have shown that the amount of extractable random bits scales up as $\propto \log_2(N)$ when the measurement is performed by a N -outcome POVM. Thus, an infinite number of random bits can be certified for any dimension of the quantum system to be measured. We derived an analytical bound for the estimation of the extractable randomness using symmetric POVM on the Bloch sphere. Our findings were validated experimentally by implementing several POVMs in the polarization space of single photons with a simple optical setup. Compared to previous DV Source-DI protocols, the one presented here allows for a passive implementation without an active switching of the measurement basis. This feature greatly simplifies the experimental implementation, which does not require fast electronics for the switching and can increase the generation rate, which is not limited by the switching frequency. Moreover, no additional randomness and an initial seed is required for the basis selection.

Note added: After the completion/submission of this manuscript, we became aware of a similar work which also considers Source-DI randomness generation with POVM measurements⁴⁹.

Methods

Source-DI guessing probability: proof of Proposition 1. The framework we are considering is a QRNG whose output is obtained by measuring a quantum system A with a POVM $\{\hat{F}_j\}$ obtaining the observed probabilities P_j . Since the system A may have correlation with the adversary E , as shown in ref.⁵⁰, the probability of guessing the output of the QRNG is given by

$$p_g(X|E) = \sum_{a=1}^M P(a) \max_j [p(j|a)] \quad (12)$$

where $j = 0, \dots, d-1$ are the possible classical outcomes of the QRNG, a is the state (possibly quantum) held by the adversary Eve, M is an arbitrary integer,

$p(j|a)$ the probability of guessing j when the state a is prepared, $P(a)$ the probability of preparing the state a .

In the source-device-independent scenario, we may assume that Eve can arbitrarily prepare the joint state of the AE system $\hat{\rho}_{AE}^a$, while the measurement POVMs $\{\hat{F}_j\}$ on Alice's side are trusted. Since the E system is arbitrary, any quantum state $\hat{\rho}_{AE}^a$ prepared with probability $P(a)$ can also be seen as the post-measurement state obtained after a generalized measurement \hat{E}_a in a bipartite system ρ_{AE} , namely

$$\hat{\rho}_{AE}^a = \frac{\hat{E}_a \rho_{AE} \hat{E}_a^\dagger}{P(a)}, \quad P(a) = \text{Tr}_{AE}[\hat{E}_a \rho_{AE} \hat{E}_a^\dagger] \quad (13)$$

By defining the POVM $\hat{M}_a = \hat{E}_a^\dagger \hat{E}_a$ the above guessing probability can be written in complete generality as

$$p_g(X|E) = \max_{\{P(a), \hat{\rho}_{AE}^a\}} \sum_{a=1}^M P(a) \max_j \text{Tr}_{AE}[(\hat{F}_j \otimes \hat{1}) \hat{\rho}_{AE}^a] \quad (14)$$

$$= \max_{\{M(a), \hat{\rho}_{AE}^a\}} \sum_{a=1}^M P(a) \max_j \frac{\text{Tr}_{AE}[(\hat{F}_j \otimes \hat{M}_a) \hat{\rho}_{AE}^a]}{P(a)} \quad (15)$$

The maximization over $\{P(a), \hat{\rho}_{AE}^a\}$ is constrained to be compatible with the experimental outcomes on Alice's side given by $P_j = \text{Tr}_A[\hat{F}_j \hat{\rho}_A]$ where $\hat{\rho}_A = \sum_a P(a) \text{Tr}_E[\hat{\rho}_{AE}^a]$ is the reduced state on A subsystem. By tracing the E system, the above expression can be written in terms of states on A , defined by

$$\text{Tr}_E[\hat{\rho}_{AE}^a] = \hat{\rho}_a^A \Rightarrow \text{Tr}_{AE}[(\hat{F}_j \otimes \hat{1}) \hat{\rho}_{AE}^a] = \text{Tr}_A[\hat{F}_j \text{Tr}_E[\hat{\rho}_{AE}^a]] = \text{Tr}_A[\hat{F}_j \hat{\rho}_a^A] \quad (16)$$

where $\hat{\rho}_a^A$ is a normalized state. We note that, by the above definition, the reduced state on the A system can be written as $\hat{\rho}_A = \sum_a P(a) \hat{\rho}_a^A$. Therefore, the guessing probability can be written only by using states and measurement in the A subsystem as

$$p_g(X|E) = \max_{\{P(a), \hat{\rho}_a^A\}} \sum_{a=1}^M P(a) \max_j \text{Tr}_A[\hat{F}_j \hat{\rho}_a^A] \quad (17)$$

where the maximization over $\{P(a), \hat{\rho}_a^A\}$ is constrained to $\text{Tr}_A[\hat{F}_j (\sum_a P(a) \hat{\rho}_a^A)] = P_j$. The above equation has a simple physical interpretation: by using the optimal measurement strategy on the state ρ_{AE} , the eavesdropper effectively prepares, on Alice's side, the states $\hat{\rho}_a^A$ with probabilities $P(a)$. The states $\hat{\rho}_a^A$ and probabilities $P(a)$ are constrained to reproduce the experimental measured probabilities P_j . When the eavesdropper prepares the state $\hat{\rho}_a^A$ her guessing probability is $p(j|a) = \max_j \text{Tr}[\hat{F}_j \hat{\rho}_a^A]$, namely she guessed the output with maximum output probability. Equation (17), averaging and maximizing over all the different prepared states, represents the optimization of her strategy.

Now we can simplify the above expression. For a given decomposition $\mathcal{E} \equiv \{P(a), \hat{\rho}_a^A\}$ we can group the indices $a = 1, \dots, M$ into the N disjoint subset $S_k(\mathcal{E})$, with $k = 1, \dots, N$. The subset $S_k(\mathcal{E})$ includes all indices a so that $\text{Tr}[\hat{F}_j \hat{\rho}_a^A]$ is maximized for $j = k$. Therefore,

$$p_g(X|E) = \max_{\{P(a), \hat{\rho}_a^A\}} \sum_{k=1}^N \sum_{a \in S_k(\mathcal{E})} P(a) \max_j \text{Tr}_A[\hat{F}_j \hat{\rho}_a^A] \quad (18)$$

$$= \max_{\{p_k, \hat{\tau}_k^A\}} \sum_{k=1}^N p_k \text{Tr}_A[\hat{F}_k \hat{\tau}_k^A] \quad (19)$$

where we defined $\hat{\tau}_k^A = \sum_{a \in S_k(\mathcal{E})} P(a) \hat{\rho}_a^A / p_k$ and $p_k = \sum_{a \in S_k(\mathcal{E})} P(a)$. We note that since $\sum_a P(a) \hat{\rho}_a^A = \sum_k \sum_{a \in S_k(\mathcal{E})} P(a) \hat{\rho}_a^A = \sum_k p_k \hat{\tau}_k^A$ the constraints on the normalized states $\hat{\rho}_a^A$ can be rewritten as

$$P_j = \text{Tr}[\hat{F}_j (\sum_k p_k \hat{\tau}_k^A)], \quad j = 1, \dots, N. \quad (20)$$

The proposition is thus demonstrated.

We can also relate our relation to a standard expression typically used for QRNG derived for classical-quantum states (see ref. 36). In the framework considered in ref. 36, a joint state ρ_{AE} is measured on the A subsystem by obtaining the classical-quantum state $\hat{\rho}_{XE} = \sum_j P_j |j\rangle_X \langle j| \otimes \sigma_E^j$ where P_j are the output probabilities after the POVM $\{\hat{F}_j\}$, X represents a classical system encoding the outputs and σ_E^j are the resulting states on the E system after the measurement. Eve can perform arbitrary measurements on her quantum system to maximize the guessing probability of Alice's outcomes. The guessing probability is then defined as $p_g(X|E) = \max_{\{\hat{M}_k\}} \sum_{j=1}^N P_j \text{Tr}_E[\hat{M}_j \sigma_E^j]$ where \hat{M}_k is a POVM on the E subsystem. In the source-device-independent framework, the initial state $\hat{\rho}_{AE}$ is not defined, so we need to optimize also over the possible state σ_E^j compatible with the observed statistic. Now we show that the above expression is equivalent to (18). By repeating the reasoning leading to (18) from (17), we can rewrite eq. (14) without the internal

maximization as

$$p_g(X|E) = \max_{\{\hat{M}_k, \hat{\rho}_{AE}\}} \sum_{k=1}^N \text{Tr}_{AE}[(\hat{F}_k \otimes \hat{M}_k) \hat{\rho}_{AE}] \quad (21)$$

where the maximization over $\hat{\rho}_{AE}$ is constrained to satisfy the observed statistic, namely $P_j = \text{Tr}_{AE}[(\hat{F}_j \otimes \hat{1}) \hat{\rho}_{AE}]$. Due to the above constraint, we can define the normalized states

$$\hat{\sigma}_E^k = \frac{1}{P_k} \text{Tr}_A[(\hat{F}_k \otimes \hat{1}) \hat{\rho}_{AE}] \quad (22)$$

such that the guessing probability can be written as

$$p_g(X|E) = \max_{\{\hat{M}_k, \hat{\sigma}_E^k\}} \sum_{k=1}^N P_k \text{Tr}_E[\hat{M}_k \hat{\sigma}_E^k] \quad (23)$$

that is the expression mentioned above and typically used to define the guessing probability for QRNG (see discussion after eq. (17) in ref. 36). Therefore eqs. (23) and (18) are completely equivalent and they represent the guessing probability evaluated by considering the E or A subsystem respectively.

We note that the two scenarios considered above both correspond to start from a joint state $\hat{\rho}_{AE}$ and perform measurement \hat{F}_k on Alice's side and measurement \hat{M}_k on Eve's side. If we consider performing first Alice's measurement, the post-measurement state is given by $\hat{\rho}_{XE} = \sum_k P_k |k\rangle_X \langle k| \otimes \sigma_E^k$. If we consider to perform first the Eve's measurement, the post-measurement state is given by $\hat{\rho}_{AY} = \sum_k p_k \hat{\tau}_k^A \otimes |k\rangle_Y \langle k|$ where Y is a classical system in which Eve's encode her results. The two equivalent expressions (18) and (23) for the guessing probability are obtained by considering, respectively, the post-measurement state $\hat{\rho}_{AY}$ or $\hat{\rho}_{XE}$.

Numerical tools for bounding the $H_{\min}(X|E)$ with arbitrary POVM. In this section we introduce a numerical tool based on Semidefinite Optimization (SDP) which can be used to bound the $H_{\min}(X|E)$ in the Source-DI scenario for an arbitrary set of POVM. Besides bounding the min-entropy, this numerical tool can also be useful to get a more precise understanding of Eve's optimal strategy, since it also returns the states $\hat{\rho}_a$ of the decomposition used by Eve. To start, we write Eq. (17) in the form of the primal SDP, where we introduce the states $\hat{\delta}_k = p_k \hat{\tau}_k$:

$$\begin{aligned} & \text{maximize}_{\hat{\delta}_k} \quad \sum_{k=1}^N \text{Tr}_A[\hat{F}_k \hat{\delta}_k] \\ & \text{subject to} \quad \hat{\delta}_k \geq 0 \forall k, \\ & \quad \text{Tr} \left[\sum_k \hat{\delta}_k \right] = 1, \\ & \quad |\text{Tr} \left[\hat{F}_i \sum_k \hat{\delta}_k \right] - P_i| \leq \zeta(\epsilon, n) \end{aligned} \quad (24)$$

where $\zeta(\epsilon, n)$ is a bound on the experimental probabilities p_j , such as the Chernoff-Hoeffding⁵¹ that is used to take into account finite-size effects.

We can rewrite the last constraint using slack variables s_i, t_i in order to have only the equality constraint except for the positive semidefinite condition.

$$\begin{aligned} & \text{maximize}_{\hat{\delta}_k} \quad \sum_x \text{Tr}_A[\hat{F}_k \delta_k] \\ & \text{subject to} \quad \hat{\delta}_k \geq 0 \forall k, \\ & \quad \text{Tr} \left[\sum_k \hat{\delta}_k \right] = 1, \\ & \quad \text{Tr} \left[\hat{F}_i \sum_k \hat{\delta}_k \right] - P_i + s_i = \zeta(\epsilon, n), \\ & \quad -\text{Tr} \left[\hat{F}_i \sum_k \hat{\delta}_k \right] + P_i + t_i = \zeta(\epsilon, n), \\ & \quad s_i \geq 0, \\ & \quad t_i \geq 0 \end{aligned} \quad (25)$$

This problem can be solved numerically directly using efficient SDP solvers such as refs. 52,53. After the optimization we obtain not only the maximum of the objective function p_{guess}^* but also the optimal states $\hat{\tau}_k = \hat{\delta}_k / \text{Tr}[\hat{\delta}_k]$ that Eve employs to maximize her p_{guess} . However, a solution to the primal problem provides a lower-bound on the guessing probability P_g , not an upper-bound. Thus, if the solver does not converge to the exact solution it will over-estimate the true amount of private randomness, compromising the security. To solve this problem, we can use the approach described in ref. 25 to derive the dual

form, which can be written as:

$$\begin{aligned} & \underset{b, e_i, f_i}{\text{minimize}} && -b + \sum_i P_i(e_i - f_i) + \zeta(\epsilon, n)(e_i + f_i) \\ & \text{subject to} && (\hat{F}_k + b\hat{1} + \sum_i (f_i - e_i)\hat{F}_i) \leq 0 \forall k, \\ & && e_i \geq 0 \forall i, \\ & && f_i \geq 0 \forall i \end{aligned} \quad (26)$$

The solution of this dual problem always provides an upper-bound to the guessing probability, resulting always in conservative bounds. Moreover, this dual formulation provides other advantages: the first advantage is related to the speed of the computation. With the primal, every time we obtain new data p_i , it is necessary to run the SDP again to obtain a bound on the guessing probability. With the dual, since the objective function is a linear function of the p_i , after an optimal solution has been found, a new (sub-optimal) upper-bound can be easily evaluated for different p_i , without running the optimization again. This aspect is particularly interesting for real-time applications, where the post-processing can be done efficiently using a Lookup table.

Data availability

The data that support the findings of this study are available from the corresponding author upon reasonable request.

Received: 24 November 2021; Accepted: 13 October 2022;

Published online: 05 November 2022

References

- Hensen, B. et al. Loophole-free Bell inequality violation using electron spins separated by 1.3 kilometres. *Nature* **526**, 682–686 (2015).
- Giustina, M. et al. Significant-loophole-free test of Bell's theorem with entangled photons. *Phys. Rev. Lett.* **115**, 250401 (2015).
- Shalm, L. K. et al. Strong loophole-free test of local realism. *Phys. Rev. Lett.* **115**, 250402 (2015).
- Acín, A. & Masanes, L. Certified randomness in quantum physics. *Nature* **540**, 213–219 (2016).
- Bierhorst, P. et al. Experimentally generated randomness certified by the impossibility of superluminal signals. *Nature* **556**, 223–226 (2018).
- Liu, Y. et al. High-speed device-independent quantum random number generation without a detection loophole. *Phys. Rev. Lett.* **120**, 010503 (2018).
- Liu, W.-Z. et al. Device-independent randomness expansion against quantum side information. *Nat. Phys.* **17**, 448–451 (2021).
- Zhang, Y. et al. Experimental low-latency device-independent quantum randomness. *Phys. Rev. Lett.* **124**, 010505 (2020).
- Shalm, L. K. et al. Device-independent randomness expansion with entangled photons. *Nat. Phys.* **17**, 452–456 (2021).
- Herrero-Collantes, M. & García-Escartín, J. C. Quantum random number generators. *Rev. Mod. Phys.* **89**, 15004 (2017).
- Ma, X., Yuan, X., Cao, Z., Qi, B. & Zhang, Z. Quantum random number generation. *npj Quantum Inform.* **2**, 16021 (2016).
- Lunghi, T. et al. Self-testing quantum random number generator. *Phys. Rev. Lett.* **114**, 150501 (2015).
- Vallone, G., Marangon, D. G., Tomasin, M. & Villoresi, P. Quantum randomness certified by the uncertainty principle. *Phys. Rev. A Atomic, Mol. Optical Phys.* **90**, 052327 (2014).
- Marangon, D. G., Vallone, G. & Villoresi, P. Source-device-independent ultrafast quantum random number generation. *Phys. Rev. Lett.* **118**, 060503 (2017).
- Avesani, M., Marangon, D. G., Vallone, G. & Villoresi, P. Source-device-independent heterodyne-based quantum random number generator at 17 Gbps. *Nat. Commun.* **9**, 5365 (2018).
- Drahi, D. et al. Certified quantum random numbers from untrusted light. *Phys. Rev. X* **10**, 041048 (2020).
- Smith, P. R., Marangon, D. G., Lucamarini, M., Yuan, Z. L. & Shields, A. J. Simple source device-independent continuous-variable quantum random number generator. *Phys. Rev. A* **99**, 062326 (2019).
- Nie, Y.-Q. et al. Experimental measurement-device-independent quantum random-number generation. *Phys. Rev. A* **94**, 060301 (2016).
- Bischof, F., Kampermann, H. & Bruß, D. Measurement-device-independent randomness generation with arbitrary quantum states. *Phys. Rev. A* **95**, 062305 (2017).
- Brask, J. B. et al. Megahertz-rate semi-device-independent quantum random number generators based on unambiguous state discrimination. *Phys. Rev. Appl.* **7**, 054018 (2017).
- Tebyanian, H. et al. Semi-device independent randomness generation based on quantum state's indistinguishability. *Quantum Sci. Technol.* **6**, 045026 (2021).
- Rusca, D. et al. Self-testing quantum random-number generator based on an energy bound. *Phys. Rev. A* **100**, 062338 (2019).
- Himbeek, T. V. et al. Semi-device-independent framework based on natural physical assumptions. *Quantum* **1**, 33 (2017).
- Van Himbeek, T. & Pironio, S. Correlations and randomness generation based on energy constraints. <http://arxiv.org/abs/1905.09117> (2019).
- Avesani, M., Tebyanian, H., Villoresi, P. & Vallone, G. Semi-device-independent heterodyne-based quantum random-number generator. *Phys. Rev. Appl.* **15**, 034034 (2021).
- Rusca, D., Tebyanian, H., Martin, A. & Zbinden, H. Fast self-testing quantum random number generator based on homodyne detection. *Appl. Phys. Lett.* **116**, 264004 (2020).
- Tebyanian, H., Avesani, M., Vallone, G. & Villoresi, P. Semi-device-independent randomness from d -outcome continuous-variable detection. *Phys. Rev. A* **104**, 062424 (2021).
- Zhang, Y. et al. A simple low-latency real-time certifiable quantum random number generator. *Nat. Commun.* **12** <https://doi.org/10.1038/s41467-021-21069-8> (2021).
- Acín, A., Pironio, S., Vértesi, T. & Wittek, P. Optimal randomness certification from one entangled bit. *Phys. Rev. A* **93**, 040102 (2016).
- Andersson, O., Badziag, P., Dumitru, I. & Cabello, A. Device-independent certification of two bits of randomness from one entangled bit and gisin's elegant bell inequality. *Phys. Rev. A* **97**, 012314 (2018).
- Gómez, S. et al. Experimental nonlocality-based randomness generation with nonprojective measurements. *Phys. Rev. A* **97**, 040102 (2018).
- Curchod, F. J. et al. Unbounded randomness certification using sequences of measurements. *Phys. Rev. A* **95**, 020102 (2017).
- Foletto, G. et al. Experimental test of sequential weak measurements for certified quantum randomness extraction. *Phys. Rev. A* **103**, 062206 (2021).
- Tomamichel, M., Schaffner, C., Smith, A. & Renner, R. Leftover hashing against quantum side information. *IEEE Trans. Inform. Theory* **57**, 5524–5535 (2011).
- Florentino, M., Santori, C., Spillane, S. M., Beausoleil, R. G. & Munro, W. J. Secure self-calibrating quantum random-bit generator. *Phys. Rev. A* **75**, 032334 (2007).
- König, R., Renner, R. & Schaffner, C. The operational meaning of min- and max-entropy. *IEEE Trans. Inform. Theory* **55**, 4337–4347 (2009).
- Faist, P. & Renner, R. Practical and reliable error bars in quantum tomography. *Phys. Rev. Lett.* **117**, 010404 (2016).
- Ślomczyński, W. & Szymusiak, A. Highly symmetric POVMs and their informational power. *Quantum Inform. Process.* **15**, 565–606 (2016).
- Cao, Z., Zhou, H., Yuan, X. & Ma, X. Source-independent quantum random number generation. *Phys. Rev. X* **6**, 011020 (2016).
- Michel, T. et al. Real-time source-independent quantum random-number generator with squeezed states. *Phys. Rev. Appl.* **12**, 034017 (2019).
- Clarke, R. B. M. et al. Experimental realization of optimal detection strategies for overcomplete states. *Phys. Rev. A* **64**, 012303 (2001).
- Schiavon, M., Vallone, G. & Villoresi, P. Experimental realization of equiangular three-state quantum key distribution. *Sci. Rep.* **6**, 30089 (2016).
- D'Ariano, G. M., Paris, M. G. & Sacchi, M. F. Quantum tomography. *Adv. Imag. Electron Phys.* **128**, 206–309 (2003).
- James, D. F., Kwiat, P. G., Munro, W. J. & White, A. G. Measurement of qubits. *Phys. Rev. A - Atom. Mol. Optical Phys.* **64**, 15 (2001).
- Luis, A. & Sánchez-Soto, L. L. Complete characterization of arbitrary quantum measurement processes. *Phys. Rev. Lett.* **83**, 3573–3576 (1999).
- Dupuis, F., Fawzi, O. & Renner, R. Entropy accumulation. *Commun. Math. Phys.* **379**, 867–913 (2020).
- Zhang, Y., Fu, H. & Knill, E. Efficient randomness certification by quantum probability estimation. *Phys. Rev. Res.* **2**, 013016 (2020).
- Brown, P. J., Ragy, S. & Colbeck, R. A framework for quantum-secure device-independent randomness expansion. *IEEE Trans. Inform. Theory* **66**, 2964–2987 (2020).
- Dai, H., Chen, B., Zhang, X. & Ma, X. Intrinsic randomness under general quantum measurements. *arXiv preprint arXiv:2203.08624* (2022).
- Tomamichel, M., Renner, R., Schaffner, C. & Smith, A. Leftover Hashing against quantum side information. In *Proc. IEEE International Symposium on Information Theory*, 2703–2707 (IEEE, 2010). <http://ieeexplore.ieee.org/lpdocs/epic03/wrapper.htm?arnumber=5513652>.
- Hoeffding, W. Probability inequalities for sums of bounded random variables. *J. Am. Stat. Assoc.* **58**, 13–30 (1963).
- ApS, M. The MOSEK optimization toolbox for MATLAB manual. Version 9.0. <http://docs.mosek.com/9.0/toolbox/index.html> (2019).
- Yamashita, M., Fujisawa, K., Fukuda, M., Nakata, K. & Nakata, M. A High-performance Software Package for Semidefinite Programs: Sdpa 7. 2010. Department of Mathematical and Computing Science, Tokyo Institute of Technology, Tokyo, Japan (2010).

Acknowledgements

This work was supported by: "Fondazione Cassa di Risparmio di Padova e Rovigo" with the project QUASAR, and by the call "Ricerca Scientifica di Eccellenza 2018"; MIUR (Italian Minister for Education) under the initiative "Departments of Excellence" (Law 232/2016); EU-H2020 program under the Marie Skłodowska Curie action, project QCALL (Grant No. GA 675662).

Author contributions

M.A. and G.V. conceived the work. M.A. and H.T. realized the experiment. M.A. and H.T. analyzed the data. M.A. and G.V. developed the security proof. G.V. and P.V. supervised the experiment. All authors discussed the results and contributed to the final manuscript.

Competing interests

The authors declare that there are no competing interests.

Additional information

Supplementary information The online version contains supplementary material available at <https://doi.org/10.1038/s42005-022-01038-3>.

Correspondence and requests for materials should be addressed to Marco Avesani.

Peer review information *Communications Physics* thanks Hong Hao Fu and the other, anonymous, reviewer(s) for their contribution to the peer review of this work.

Reprints and permission information is available at <http://www.nature.com/reprints>

Publisher's note Springer Nature remains neutral with regard to jurisdictional claims in published maps and institutional affiliations.



Open Access This article is licensed under a Creative Commons Attribution 4.0 International License, which permits use, sharing, adaptation, distribution and reproduction in any medium or format, as long as you give appropriate credit to the original author(s) and the source, provide a link to the Creative Commons license, and indicate if changes were made. The images or other third party material in this article are included in the article's Creative Commons license, unless indicated otherwise in a credit line to the material. If material is not included in the article's Creative Commons license and your intended use is not permitted by statutory regulation or exceeds the permitted use, you will need to obtain permission directly from the copyright holder. To view a copy of this license, visit <http://creativecommons.org/licenses/by/4.0/>.

© The Author(s) 2022