

ARTICLE

https://doi.org/10.1038/s42005-020-0375-6

OPEN

Check for updates

# Experimental device-independent certified randomness generation with an instrumental causal structure

Iris Agresti<sup>1</sup>, Davide Poderini<sup>1</sup>, Leonardo Guerini<sup>©</sup><sup>2</sup>, Michele Mancusi<sup>®</sup><sup>1</sup>, Gonzalo Carvacho<sup>1</sup>, Leandro Aolita<sup>3</sup>, Daniel Cavalcanti<sup>4</sup>, Rafael Chaves<sup>5,6</sup> & Fabio Sciarrino<sup>®</sup><sup>1⊠</sup>

The intrinsic random nature of quantum physics offers novel tools for the generation of random numbers, a central challenge for a plethora of fields. Bell non-local correlations obtained by measurements on entangled states allow for the generation of bit strings whose randomness is guaranteed in a device-independent manner, i.e. without assumptions on the measurement and state-generation devices. Here, we generate this strong form of certified randomness on a new platform: the so-called instrumental scenario, which is central to the field of causal inference. First, we theoretically show that certified random bits, private against general quantum adversaries, can be extracted exploiting device-independent quantum instrumental-inequality violations. Then, we experimentally implement the corresponding randomness-generation protocol using entangled photons and active feed-forward of information. Moreover, we show that, for low levels of noise, our protocol offers an advantage over the simplest Bell-nonlocality protocol based on the Clauser-Horn-Shimony-Holt inequality.

<sup>&</sup>lt;sup>1</sup> Dipartimento di Fisica, Sapienza Università di Roma, Piazzale Aldo Moro 5, I-00185 Roma, Italy. <sup>2</sup> International Center of Theoretical Physics - South American Institute for Fundamental Research, Instituto de Física Teórica - UNESP, R. Dr. Bento T. Ferraz 271, 01140-070 São Paulo, Brazil. <sup>3</sup> Instituto de Física, Universidade Federal do Rio de Janeiro, Caixa Postal 68528, Rio de Janeiro, RJ 21941-972, Brazil. <sup>4</sup> ICFO - Institut de Ciencies Fotoniques, The Barcelona Institute of Science and Technology, E-08860 Castelldefels, Barcelona, Spain. <sup>5</sup> International Institute of Physics, Federal University of Rio Grande do Norte, 59078-970P. O. Box 1613, Natal, Brazil. <sup>6</sup> School of Science and Technology, Federal University of Rio Grande do Norte, 59078-970 Natal, Brazil. <sup>6</sup> email: fabio.sciarrino@uniroma1.it

he generation of random numbers has applications in a wide range of fields, from scientific research—e.g. to simulate physical systems—to military scopes—e.g. for effective cryptographic protocols—and every-day concerns—like ensuring privacy and gambling. From a classical point of view, the concept of randomness is tightly bound to the incomplete knowledge of a system; indeed, classical randomness has a subjective and epistemological nature and is erased when the system is completely known<sup>1</sup>. Hence, classical algorithms can only generate pseudo-random numbers<sup>2</sup>, whose unpredictability relies on the complexity of the device generating them. Besides, the certification of randomness is an elusive task, since the available tests can only verify the absence of specific patterns, while others may go undetected but still be known to an adversary<sup>3</sup>.

On the other hand, randomness is intrinsic to quantum systems, which do not possess definite properties until these are measured. In real experiments, however, this intrinsic quantum randomness comes embedded with noise and lack of complete control over the device, compromising the security of a quantum random-number generator. A solution to that is to devise quantum protocols whose correctness can be certified in a deviceindependent (DI) manner. In such a framework, properties of the considered system can be inferred under some causal assumptions, not requiring a precise knowledge of the devices adopted in the implementation. For instance, from the violation of a Bell inequality<sup>4,5</sup>, under the assumption of measurement independence and locality, one can ensure that the statistics of certain quantum experiments cannot be described in the classical terms of local deterministic models, hence being impossible to be deterministically predicted by any local observer. Moreover, the extent of such a violation can provide a lower bound on the certified randomness characterizing the measurement outputs of the two parties performing the Bell test, as introduced and developed in refs. 6-8. Several other seminal works based on Bell inequalities have been developed9-22, advancing the topics of randomness amplification (the generation of near-perfect randomness from a weaker source), randomness expansion (the expansion of a short initial random seed), and quantum key distribution (sharing a common secret string through communication over public channels). In particular, loophole-free Bell tests based on randomness generation protocol have been implemented<sup>7,20,23</sup> and more advanced techniques have been developed to provide security against general adversarial attacks<sup>19,21,24,25</sup>

From a causal perspective, the non-classical behavior revealed by a Bell test lies in the incompatibility of quantum predictions with our intuitive notion of cause and effect<sup>26-28</sup>. Given that the causal structure underlying a Bell-like scenario involves five variables (the measurement choices and outcomes for each of the two observers and a fifth variable representing the common cause of their correlations), it is natural to wonder whether a different, and simpler, causal structure could give rise to an analogous discrepancy between quantum and classical causal predictions<sup>29,30</sup>. The instrumental causal structure<sup>31,32</sup>, where the two parties (A and B) are linked by a classical channel of communication, is the simplest model (in terms of the number of involved nodes) achieving this result<sup>33</sup>. This scenario has fundamental importance in causal inference, since it allows the estimation of causal influences even in the presence of unknown latent factors<sup>31</sup>.

In this letter, we provide a proof-of principle demonstration of the implementation of a DI random number generator based on instrumental correlations, secure against general quantum attacks<sup>19</sup>.

Our protocol is DI, since it does not require any assumption about the measurements and states used in the protocol, not even their dimension. Furthermore, in our case, the causal assumption consists in the requirement that A's measurement choice does not have a direct influence over B. In practical applications, this premise can be enforced, by shielding A's measurement station, in order to allow only for the communication of its outcome bit to B and prevent any other unwanted communication. To implement the protocol in all of its parts, we have set up a classical extractor following the theoretical design by Trevisan<sup>34</sup>. Moreover, we prove that DI randomness generation protocols implemented in this scenario, for high state visibilities, can bring an advantage in the gain of random bits when compared to those based on the simplest two-input-two-output Bell scenario, the Clauser-Horn-Shimony-Holt (CHSH)<sup>35</sup>. Therefore, this work paves the way to further applications of the instrumental scenario in the field of DI protocols, which, until now, have relied primarily on Bell-like tests.

# Results

**Randomness certification via instrumental violations**. Let us first briefly review some previous results obtained in the context of Bell inequalities<sup>4</sup>. In a CHSH scenario<sup>35</sup>, two parties, *A* and *B*, share a bipartite system and, without communicating to each other, perform local measurements on their subsystems. If *A* and *B* choose between two given operators each, i.e.  $(A_1, A_2)$  and  $(B_1, B_2)$  respectively, and then combine their data, the mean value of the operator  $S = |\langle A_1, B_1 \rangle - \langle A_1, B_2 \rangle + \langle A_2, B_1 \rangle + \langle A_2, B_2 \rangle|$  should be upper-bounded by 2, for any deterministic model respecting a natural notion of locality. However, as proved in ref. <sup>35</sup>, if *A* and *B* share an entangled state, they can get a value exceeding this bound, whose explanation requires the presence of non-classical correlations between the two parties. Hence, Bell inequalities have been adopted in ref. <sup>7</sup> to guarantee the intrinsic random nature of *A*'s and *B*'s measurements' outcomes, within a DI randomness generation and certification protocol.

In the instrumental causal model, which is depicted in Fig. 1a, the two parties (Alice and Bob) still share a bipartite state. Alice can choose among l possible d-outcome measurements ( $O_A^1$ , ...,  $O_A^l$ ), according to the instrument variable x, which is independent of the shared correlations between Alice and Bob ( $\Lambda$ ) and can assume l different values. On the other hand, Bob's choice y is among d observables  $(O_B^1, ..., O_B^d)$  and depends on Alice's outcome a, specifically y = a. In other words, as opposed to the spatiallyseparated correlations in a Bell-like scenario, the instrumental process constitutes a temporal scenario, with one-way communication of Alice's outcomes to select Bob's measurement. This implies, first, that Alice and Bob are not space-like separated, to ensure that the causal structure's constraints are fulfilled, unlike in Bell-like scenarios. Secondly, due to the communication of Alice's outcome a to Bob, Bob's outcome b is not independent of *x*; however, the instrumental network specifies this influence to be indirect, formalized by the constraint  $p(b|x, a, \lambda) = p(b|a, \lambda)$  and justifying the absence of an arrow from X to B in Fig. 1a. This is the aforementioned causal assumption within our protocol.

Similarly to Bell-like scenarios, the causal structure underlying an instrumental process imposes some constraints on the classical joint probabilities  $\{p(a, b|x)\}_{a,b,x}$  that are compatible with it<sup>31,32</sup> (the so-called instrumental inequalities). In the particular case where the instrument *x* can assume three different values (1,2,3), while *a* and *b* are dichotomic, the following inequality holds<sup>32</sup>:

$$\mathcal{I} = \langle A \rangle_1 - \langle B \rangle_1 + 2 \langle B \rangle_2 - \langle AB \rangle_1 + 2 \langle AB \rangle_3 \le 3 \tag{1}$$

where  $\langle AB \rangle_x = \sum_{a,b=0,1} (-1)^{a+b} p(a,b|x)$ . Remarkably, this inequality can be violated with the correlations produced by quantum instrumental causal models<sup>33</sup>, up to the maximal value



Fig. 1 Randomness generation and certification protocol. a Instrumental causal structure represented as a directed acyclic graph<sup>26</sup> (DAG), where each node represents a variable and the arrows link variables between which there is causal influence. In this case, X, A, and B are observable, while  $\Lambda$  is a latent variable. **b** The plot shows the smooth min-entropy bound for the CHSH (Clauser-Horn-Shimony-Holt) inequality and the instrumental scenario (respectively dashed and continuous curve), in terms of the state visibility v, i.e. considering the extent of violation that would be given by the following state:  $\rho = v |\psi^-\rangle \langle \psi^-| + (1-v) \frac{\mathbb{I}}{4}$ . The bounds were obtained through the analysis of ref. <sup>19</sup>, secure against general quantum adversaries, which was adapted to our case. The choice of parameters was the following:  $n = 10^{12}$ ,  $\epsilon = \epsilon_{EA} = 10^{-6}$ ,  $\delta' = 10^{-4}$  and  $\gamma = 1$ . In detail, n is the number of runs,  $\epsilon$  is the smoothing parameter characterizing the minentropy  $\mathcal{H}_{\min}^{e}, \, \epsilon_{\mathsf{EA}}$  is the desired error probability of the entropy accumulation protocol,  $\delta'$  is the experimental uncertainty on the evaluation of the violation  $\mathcal{I}$  and  $\gamma$  is the parameter of the Bernoulli distribution according to which we select "test" and "accumulation" runs throughout the protocol. c Simplified scheme of the proposed randomness generation and certification protocol (in the case  $\gamma = 1$ ): (i) initial seed generation (defining, at each run, Alice's choice among the operators), (ii) instrumental process implementation, (iii) classical randomness extractor. The initial seed is obtained from the random bits provided by the NIST Randomness Beacon<sup>42</sup>. In the second stage, Alice's and Bob's outputs are collected and the corresponding value of the instrumental violation  $\mathcal{I}^*$  is computed. If it is higher than a threshold set by the user, the smooth minentropy is bounded by inequality (2), otherwise the protocol aborts. The value of the min-entropy indicates the maximum number of certified random bits that can be extracted. At the end, if the protocol does not abort, the output strings are injected in a classical randomness extractor (Trevisan's extractor<sup>34</sup>) and the final string of certified random bits is obtained. The extractor's seed is as well provided by the NIST Randomness Beacon.

of  $\mathcal{I} = 1 + 2\sqrt{2}$ . Recently, the relationship of the instrumental processes with the Bell scenario has been studied in ref. <sup>36</sup>.

In this context, we rely on the fact that if a given set of statistics  $\{p(a, b|x)\}_{a,b,x}$  violates inequality (1), then the system shared by the two parties exhibits non-classical correlations that impose non-trivial constraints on the information a potential eavesdropper could obtain, represented in the probability distributions  $\{p(a, b, e|x)\}_{a,b,e,x}$  where *e* is the eventual side information of the eavesdropper. Consequently, this restricts the values of the conditional min-entropy, a randomness quantifier defined as  $\mathcal{H}_{\min} = -\log_2[\sum_e P(e)\max_{a,b} P(a, b|e, x)]^{37}$ . Indeed, it is possible

to obtain a lower-bound on the min-entropy, for each x, as a function  $f_x$  of  $\mathcal{I}: \mathcal{H}_{\min} \ge f_x(\mathcal{I})$  (or, equivalently, of the visibility, see Fig. 1b). For each x and  $\mathcal{I}$ , the lower bound  $f_x(\mathcal{I})$  can be computed via semidefinite programming (SDP), by maximizing P(a, b|e, x), under the constraint that the observable terms of the probability distribution are compatible to the laws of quantum mechanics and that the corresponding violation is  $\mathcal{I}$ . The first

constraint is imposed by exploiting the NPA hierarchy<sup>38</sup>. Indeed, such a general method can be applied to any casual model involving a shared bipartite system, on whose subsystems local measurements are performed. Note that, when adopting the NPA method for an instrumental process, no constraints are applied to the untested terms of the form  $p(a, b|e, x, y \neq a)$  and that the solution of such an optimization will, in general, provide a lower amount of certifiable randomness, with respect to a scenario where all the combinations were tested (for further details, see Supplementary Information note 1). The functions  $f_r$  are convex and grow monotonically with  $\mathcal{I}$ ; so, the higher the violation of inequality (1) is, the higher the min-entropy lower bound will be. Nevertheless, in real experimental conditions, in order to evaluate the quantum violation extent  $\mathcal{I}^*$  (or, analogously, the probability distribution  $p^*(a, b|x)$  to compute  $f_x$ , several experimental runs are necessary. Therefore, unless one makes the "iid assumption" (i.e. all the experimental runs are assumed to be identically and independently distributed, "iid", so both the state source, as well as Alice's and Bob's measurement devices, are supposed not to exhibit time-dependent behaviors), this bound  $f_{*}(\mathcal{I}^{*})$  will not hold in the presence of an adversary that could include a (quantum) memory in the devices, introducing interdependences among the runs. Several DI protocols have been proposed so far addressing the most general non-iid case<sup>13,16,39</sup>, but at the cost of a low feasibility. Only very recently feasible solutions have been proposed<sup>19,24,25,40</sup>. In particular, we will consider the technique developed in ref. 19, resorting to the "Entropy Accumulation Theorem" (EAT), in order to deal with processes not necessarily made of independent and identically distributed runs. Such a method has been recently applied to the CHSH scenario<sup>21</sup>.

Here we adapt the technique developed in ref. <sup>19</sup> to the instrumental scenario, making our randomness certification, whose scheme is depicted in Fig. 1*c*, secure against general quantum attacks. According to the EAT, for a category of processes that comprehends also an implemented instrumental process composed of several runs, the following bound on the smooth min-entropy holds:

$$\mathcal{H}_{\min}^{\epsilon}(O^n|S^nE^n) > nt - \nu\sqrt{n}, \tag{2}$$

where *O* are the quantum systems given to the honest parties Alice and Bob, at each run, *S* constitutes the leaked sideinformation, while *E* represents any additional side information correlated to the initial state. Then, *t* is a convex function which depends on the extent of the violation, expected by an honest, although noisy, implementation of the protocol, i.e. in a scenario with no eavesdropper ( $I_{exp}$ ). On the other hand, *v* depends also on the smoothing parameter  $\epsilon$ , which characterizes the smooth min-entropy  $\mathcal{H}_{min}^{\epsilon}$ , and  $\epsilon_{EA}$ , i.e. the desired error probability of the entropy accumulation protocol; in other words, either the protocol aborts with probability higher than  $1 - \epsilon_{EA}$  or bound (2) holds (for further detail, see Supplementary Information note 2).

Our protocol is implemented as follows (see Fig. 2): for each run, a random binary variable T is drawn according to a Bernoulli distribution of parameter  $\gamma$  (set by the user); if T = 0, the run is an "accumulation" run, so x is deterministically set to 2 (which guarantees a higher  $f(\mathcal{I})$ , see Supplementary Information note 2); on the other hand, if T = 1, the run is a "test" run, so x is randomly chosen among 1, 2 and 3. After m test runs (with m chosen by the user), the quantum instrumental violation is evaluated from the bits collected throughout the test runs and, if lower than  $I_{exp} - \delta'$  ( $\delta'$  being the experimental uncertainty on  $\mathcal{I}$ ), the protocol aborts; otherwise the certified smooth min-entropy is bounded by inequality (2). This lower bound on the certified min entropy represents the maximum certified amount of bits that we



**Fig. 2 Implementation of the device-independent randomness certification protocol.** The implementation of our proposed protocol involves three steps. First of all, an instrumental process is implemented on a photonic platform. Then, for each round of the experiment, a binary random variable *T* is evaluated. Specifically, *T* can get value 1 with probability  $\gamma$ , previously chosen by the user (in our implementation,  $\gamma = 1$ ). If *T* = 0, the run is an "accumulation" one, and *x* is deterministically equal to 2. If *T* = 1, the run is a "test" run and *x* is randomly chosen among 1, 2, and 3. Note that, in our case, we only have "test" runs. Secondly, after *n* runs, through the bits collected in the test runs, we evaluate the corresponding instrumental violation and see whether it is higher than the expected violation for an honest implementation of the protocol, i.e. in a scenario with no eavesdroppers. In our case, we set the threshold to 3.5. If it is lower, the protocol aborts, otherwise, the protocol reaches the third stage, where we employ the Trevisan extractor, to extract the final certified random bit string. The extractor takes, as input, the raw data (weak randomness source), a random seed (given by the NIST Randomness Beacon<sup>42</sup>) and the minentropy of the input string. In the end, according to the classical extractor statistical error ( $\epsilon_{ext}$ ) set by the user (in our case 10<sup>-6</sup>), the algorithm extracts *m* truly random bits, with *m* < *n*.

can extract from our collected data. Hence, feeding the raw bit string and the  $\mathcal{H}_{\min}^{e}$  to the classical extractor<sup>34</sup>, the algorithm will output at most  $\mathcal{H}_{\min}^{e}(O^{n}|S^{n}E^{n})$  certified random bits, the exact value depending on its internal error parameter  $\epsilon_{\text{ext}}$ . Specifically, we resorted to the classical extractor devised by Trevisan<sup>34</sup>. This algorithm takes as inputs a "weak randomness source", in our case the 2n raw bits long string, and a seed, which is polylogarithmic in the input size (our code for the classical extractor can be found at<sup>41</sup> and, for a detailed description of the classical randomness extractor, see Supplementary Information note 3).

**Experimental implementation of the protocol**. The DI random numbers generator, in our proposal, is made up of three main parts, which are seen as black boxes to the user: the state generation and Alice's and Bob's measurement stations. The causal correlations among these three stages are those of an instrumental scenario (see Fig. 1a,c) and are implemented through the photonic platform depicted in Fig. 3.

Within this experimental apparatus, the qubits are encoded in the photon's polarization: horizontal (H) and vertical (V) polarizations represent, respectively, qubits 0 and 1, eigenstates of the Pauli matrix  $\sigma_z$ . A spontaneous parametric down-conversion (SPDC) process generates the two-photon maximally entangled state  $|\Psi^-\rangle = \frac{|HV\rangle - |VH\rangle}{\sqrt{2}}$ . One photon is sent to path 1, towards Alice's station, where an observable among  $O_A^1$ ,  $O_A^2$  and  $O_A^3$  is measured, applying the proper voltage to a liquid crystal device (LCD). The voltage must be chosen according to a random

seed, made of a string of trits (indeed, in our case, we take  $\gamma = 1$ , so x is chosen among (1,2,3) at every run). This seed is obtained from the NIST Randomness Beacon<sup>42</sup>, which provides 512 random bits per minute. After Alice has performed her measurement, whenever she gets output 1 (i.e.  $D_A^0$  registers an event), the detector's signal is split to reach the coincidence counter and, at the same time, trigger the Pockels cell on path 2. Bob's station is made of a half waveplate (HWP) followed by this fast electro-optical device. When no voltage is applied to the Pockels cell, Bob's operator is  $O_B^1$  and, when it is turned on, there is a swift change to  $O_B^2$  (the cell's time response is of the order of nanoseconds). In order to have the time to register Alice's output and select Bob's operator accordingly, the photon on path 2 is delayed, through a 125 m long single-mode fiber.

The four detectors are synchronized in order to distinguish the coincidence counts generated by the entangled photons' pairs from the accidental counts. Let us note that our proof of principle is not loophole free, since it requires the fair sampling assumption, due to our overall low detection efficiency. However, such a limitation belongs to this specific implementation and not to the proposed method. The measurement operators achieving maximal violation of  $\mathcal{I} = 1 + 2\sqrt{2}$ , when applied to the state  $|\psi^-\rangle$ , are the following:  $O_A^1 = -(\sigma_z - \sigma_x)/\sqrt{2}$ ,  $O_A^2 = -\sigma_x$ ,  $O_A^3 = \sigma_z$  and  $O_B^1 = (\sigma_x - \sigma_z)/\sqrt{2}$ ,  $O_B^2 = -(\sigma_x + \sigma_z)/\sqrt{2}$ . Once the instrumental process is implemented, the threshold

Once the instrumental process is implemented, the threshold  $I_{exp}$  is set, corresponding to the violation that is expected by an honest implementation of the protocol. In our case, given that our



**Fig. 3 Experimental apparatus.** A polarization-entangled photon pair is generated via spontaneous parametric down-conversion (SPDC) process in a nonlinear crystal. Photon 1 is sent to Alice's station, where one of three observables  $(O_A^1, O_A^2, \text{ and } O_A^3)$  is measured through a liquid crystal followed by a polarizing beam splitter (PBS). The choice of the observable relies on the random bits generated by the NIST Randomness Beacon<sup>42</sup>. Detector  $D_A^0$  acts as trigger for the application of a 1280 V voltage on the Pockels cell, whenever the measurement output 0 is registered. The photon 2 is delayed 600 ns before arriving to Bob's station by employing a single-mode fiber 125 m long. After leaving the fiber, the photon passes through the Pockels cell, followed by a fixed half waveplate (HWP) at 56.25° and a PBS. If the Pockels cell has been triggered (in case of A measurement outcome is 0), its action combined to the fixed HWP in Bob's station allows us to perform  $O_B^1$ . Otherwise (if A measurement outcome is 1), the Pockels cell acts as the identity and we implement  $O_B^2$ .



Fig. 4 Comparison between Clauser-Horn-Shimony-Holt (CHSH) and Instrumental random bits gain. The plot shows the ratio between the random bits gained throughout all the runs of the proposed protocol (given by  $\mathcal{H}^{\epsilon}_{min}$ ), involving the instrumental scenario, over those gained in its regular CHSH-based counterpart<sup>19,21</sup>, when fixing the amount of random bits feeding both the protocols. Under these circumstances, given that for each test run the instrumental test requires log<sub>2</sub>(3) input bits, instead of the 2 of the regular CHSH, the final amounts of random bits in the two cases will differ, due to the different amounts of performed runs, besides their different min-entropies per run. Note that the amount of performed runs depends on the value of  $\gamma$ , i.e. the probability of a test run, which was optimized separately for the two scenarios. In particular, the curves represent different amounts of initially invested random bits, in particular  $n = 10^8$  (blue, lowest curve),  $n = 10^9$  (golden, middle curve) and  $n = 10^{10}$ (red, highest curve), in terms of the state visibility v, i.e. corresponding to the extent of violation that would correspond to the following state:  $\rho = \mathbf{v} |\psi^{-}\rangle \langle \psi^{-}| + (1 - \mathbf{v}) \frac{\mathbb{I}}{4}.$ 

expected visibility amounts to 0.915,  $I_{exp} = 3.5$ . Then, the desired level of security is imposed by tuning the internal parameters, detailed in the SI, contributing to v. As next step, according to Eq. (2), one can either fix the number of the desired output random bits and perform the required number of runs or, viceversa, fix the amount of initial randomness to feed the protocol, and hence the number of feasible runs. In the end, the classical randomness extractor is applied to the raw bit strings. Specifically, in our case, we adopted the one devised by Trevisan<sup>34</sup>. The complete procedure is summarized in Fig. 2.

Theoretical results. The DI random number generation protocol we propose for the instrumental scenario was developed adapting the pre-existing techniques for the Bell scenario<sup>19,21</sup>, and is secure against general quantum adversaries. The most striking aspect of our protocol, shown in Fig. 4, is that, under given circumstances, our protocol proves to be more convenient than its CHSH-based counterpart. This becomes visible if we compare the amount of truly random bits within Alice's and Bob's output strings throughout all the experimental runs (given by  $\mathcal{H}_{\min}^{e}$ ) for our protocol and its CHSH-based counterpart, in the case of a fixed amount of invested bits, for the parties' inputs and for T. This will result in a different number of feasible runs for the two cases. Such a difference, in the regime of high state visibilities  $v (\sim 0.98)$ , considering a violation extent compatible to the following state  $\rho = \nu |\psi^{-}\rangle \langle \psi^{-}| + (1-\nu) \frac{1}{4}$ , and large amounts of invested random bits, brings the ratio of the two gains  $(\mathcal{H}_{min}^{e\,Instr}/\mathcal{H}_{min}^{e\,CHSH})$ , as shown in Fig. 4, to be higher than 1.

Experimental results. We implemented the instrumental scenario on a photonic platform and provided a proof of principle of the proposed quantum adversary-proof protocol in our experimental conditions. In particular, for our expected visibility, of 0.915, we put our threshold to  $I_{\rm exp}=$  3.5, with  $\bar{\delta}'=$  0.011. Furthermore, we set  $\epsilon_{\rm EA} = \epsilon = 10^{-1}$  and fixed the amount of initial randomness to 172,095 experimental runs. Since the registered violation was of 3.516 ± 0.011, compatible to a state  $\rho = \nu |\psi^-\rangle \langle \psi^-| + (1-\nu) \frac{1}{4}$ with  $v = 0.9186 \pm 0.030$ , our certified smooth min-entropy bound, according to inequality (2), was 0.031125, which allowed us to gain, through the classical extractor, an overall number of 5270 random bits, with an error on the classical extractor of  $\epsilon_{\text{ext}} = 10^{-6}$ . Note that each experimental run lasted ~1s and the bottleneck of our implementation is the time response of the liquid crystal, ~700 ms, that implements Alice's operator. Hence, in principle, significantly higher rates can be reached on the same platform, adopting a fast electro-optical device also for Alice's station, with a response time of ~100 ns.

The length of the seed required by the classical extractor, as mentioned, is poly-logarithmic in the input size and its length also depends on the chosen error parameter  $\epsilon_{ext}$  (which is the tolerated distance between the uniform distribution and the one of the final string) and on the particular algorithm adopted. In our case, we used the same implementation of refs. 41,43, which was proven to be a strong quantum proof extractor by De et al. 44. With respect to other implementations of the Trevisan extractor<sup>45</sup>, ours requires a longer seed, but allows to extract a higher amount of random bits. Let us note that, since the length of the seed grows as  $log(2n)^3$ , where n is the number of experimental runs, the randomness gain is not modified if we take also into account the bits invested in the classical extractor's seed. Indeed, the number of extracted bits grows polynomially in n. Hence, if  $H_{\min^{\text{Instr}}}^{e} > H_{\min^{\text{CHSH}}}^{e}$ , then  $m_{\text{Instr}} - d_{\text{Instr}} > m_{\text{CHSH}} - d_{\text{CHSH}}$ , where m is the length of the final string (after the classical extraction) and d the length of the required extractor's seed. For more details

about the internal functioning of the classical randomness extractor and its specific parameter settings, see Supplementary Information note 3.

# Discussion

In this work we implemented a DI random number generator based on the instrumental scenario. This shows that instrumental processes constitute an alternative venue with respect to Bell-like scenarios. Moreover, we also showed that, in regimes of high visibilities and high amounts of performed runs, the efficiency of the randomness generated by the violation of the instrumental inequality (1) can surpass that of efficiency of the CHSH inequality, as shown in Fig. 4. Indeed, for high visibilities, as it can be seen in Fig. 1b, the min-entropy per run guaranteed in the two scenarios has a similar value and, when the number of runs raises, the advantage brought by the instrumental test, by needing only  $log_2(3)$  input bits, instead of 2, prevails.

Through the proposed protocol, we could extract an overall number of 5270 random bits, considering a threshold for the instrumental violation of  $I_{exp} = 3.5$  and  $10^{-1}$ , both as error probability of the entropy accumulation protocol ( $\epsilon_{EA}$ ), as well as smoothing parameter ( $\epsilon$ ). The conversion rate, from public to private randomness, as well as the security parameters, could be improved on the same platform, by raising the number of invested initial random bits, or, analogously, the number of runs. To access the regime in which the instrumental scenario is more convenient than the CHSH one, we should invest a number of random bits over  $10^9$  and obtain a visibility of ~0.98 (note that, the more the amount of invested bits grows, the more the threshold for the visibility lowers down).

This proof of principle opens the path for further investigations of the instrumental scenario as a possible venue for other information processing tasks usually associated to Bell scenarios, such as self-testing<sup>46–55</sup> and communication complexity problems<sup>56–58</sup>.

## Methods

**Experimental details.** Photon pairs were generated in a parametric downconversion source, composed by a nonlinear crystal beta barium borate (BBO) of 2mm thick injected by a pulsed pump field with  $\lambda = 392.5$  nm. After spectral filtering and walk-off compensation, photons of  $\lambda = 785$  nm are sent to the two measurement stations A and B. The crystal used to implement active feed-forward is a LiNbO<sub>3</sub> high-voltage micro Pockels Cell—made by Shangai Institute of Ceramics with < 1 ns risetime and a fast electronic circuit transforming each Siavalanche photodetection signal into a calibrated fast pulse in the kV range needed to activate the Pockels Cell—is fully described in ref. <sup>59</sup>. To achieve the active feedforward of information, the photon sent to Bob's station needs to be delayed, thus allowing the measurement on the first qubit to be performed. The amount of delay was evaluated considering the velocity of the signal transmission through a singlemode fiber and the activation time of the Pockels cell. We have used a fiber 125 m long, coupled at the end into a single-mode fiber that allows a delay of 600 ns of the second photon with respect to the first.

## **Data availability**

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

### Code availability

All the custom code developed for this study is available from the corresponding author upon request. Furthermore, the code developed for the classical extractor is available at https://github.com/michelemancusi/libtrevisan.

Received: 10 February 2020; Accepted: 6 May 2020; Published online: 18 June 2020

#### References

 Grangier, P. & Auffèves, A. What is quantum in quantum randomness? *Philos. Trans. Roy. Soc. A* 376, 20170322 (2018).

- Matsumoto, M. & Nishimura, T. 623-dimensionally equidis- tributed uniform pseudo-random number generator. ACM Trans. Modeling Comput. Simul. 8, 3–30 (1998).
- Rukhin, A., Soto, J., Nechvatal, J., Smid, M. & Barker, E. A Statistical Test Suite for Random and Pseudo-random Numbers Generators for Cryptographic Applications Technical Report (Booz-Allen and Hamilton Inc. McLean VA, 2001).
- 4. Bell, J. S. On the Einstein-Podolsky-Rosen paradox. Physics 1, 195 (1964).
- Brunner, N., Cavalcanti, D., Pironio, S., Scarani, V. & Wehner, S. Bell nonlocality. *Rev. Mod. Phys.* 86, 419–478 (2014).
- Colbeck, R. Quantum and Relativistic Protocols for Secure Multi-Party Computation. Ph.D. thesis, University of Cambridge (2007).
- 7. Pironio, S. et al. Random numbers certified by bellas theorem. *Nature* 464, 1021-1024 (2010).
- Colbeck, R. & Kent, A. Private randomness expansion with untrusted devices. J. Phys. A: Math. Theor. 44, 095305 (2011).
- Colbeck, R. & Renner, R. Free randomness can be amplified. Nat. Phys. 8, 450–453 (2012).
- 10. Gallego, R. et al. Full randomness from arbitrarily deterministic events. *Nat. Commun.* **4**, 2654 (2013).
- 11. Brandão, F. G. S. L. et al. Realistic noise-tolerant randomness amplification using finite number of devices. *Nat. Commun.* 7, 11345 (2016).
- Ramanathan, R. et al. Randomness amplification under minimal fundamental assumptions on the devices. *Phys. Rev. Lett.* **117**, 230501 (2016).
- Miller, C. A. & Shi, Y. Robust protocols for securely expanding randomness and distributing keys using untrusted quantum devices. J. ACM 63, 33:1–33:63 (2016).
- Vazirani, U. V. & Vidick, T. Certifiable quantum dice: or, true random number generation secure against quantum adversaries. In *Proc. of the Forty-Fourth Annual ACM Symposiumon Theory of Computing*, STOC '12, 61–76 (Association for Computing Machinery, New York, NY, USA, 2012). https:// doi.org/10.1145/2213977.2213984.
- Liu, Y. et al. High-speed device-independent quantum random number generation without a detection loophole. *Phys. Rev. Lett.* **120**, 010503 (2018).
- Vazirani, U. & Vidick, T. Fully device-independent quantum key distribution. *Phys. Rev. Lett.* **113**, 140501 (2014).
- Chung, K. M., Shi, Y., & Wu, X. Physical randomness extractors: generating random numbers with minimal assumptions. Preprint at https://arxiv.org/abs/ 1402.4797 (2014).
- Dupuis, F., Fawzi, O. & Renner, R. Entropy accumulation. Preprint at https://arxiv.org/abs/1607.01796 (2016).
- Arnon-Friedman, R., Dupuis, F., Fawzi, O., Renner, R. & Vidick, T. Practical device-independent quantum cryptography via entropy accumulation. *Nat. Commun.* 9, 459 (2018).
- Christensen, B. G. et al. Detection-loophole-free test of quantum nonlocality, and applications. *Phys. Rev. Lett.* 111, 130406 (2013).
- 21. Shen, L. et al. Randomness extraction from bell violation with continuous parametric down-conversion. *Phys. Rev. Lett.* **121**, 150402 (2018).
- 22. Bancal, J.-D., Sheridan, L. & Scarani, V. More randomness from the same data. N. J. Phys. 16, 033011 (2014).
- 23. Bierhorst, P. et al. Experimentally generated randomness certified by the impossibility of superluminal signals. *Nature* **556**, 223–226 (2018).
- Kessler, M. & Arnon-Friedman, R. Device-independent randomness amplification and privatization. Preprint at https://arxiv.org/abs/1705.04148 (2017).
- Knill, E., Zhang, Y. & Fu, H. Quantum probability estimation for randomness with quantum side information. Preprint at https://arxiv.org/abs/ 1806.04553 (2018).
- 26. Pearl, J. Causality (Cambridge University Press, 2009).
- Wood, C. J. & Spekkens, R. W. The lesson of causal discovery algorithms for quantum correlations: causal explanations of Bell-inequality violations require fine-tuning. N. J. Phys. 17, 033002 (2015).
- Chaves, R., Kueng, R., Brask, J. B. & Gross, D. Unifying framework for relaxations of the causal assumptions in Bell's theorem. *Phys. Rev. Lett.* 114, 140403 (2015).
- 29. Henson, J., Lal, R. & Pusey, M. F. Theory-independent limits on correlations from generalized bayesian networks. *N. J. Phys.* **16**, 113043 (2014).
- Carvacho, G., Chaves, R. & Sciarrino, F. Perspective on experimental quantum causality. *EPL (Europhys. Lett.)* 125, 30001 (2019).
- Pearl, J. On the testability of causal models with latent and instrumental variables. In Proc. 11th Conference on Uncertainty in Artificial Intelligence 435–443 (Morgan Kaufmann Publishers Inc., 1995).
- Bonet, B. Instrumentality tests revisited. In Proc. 17th Conference on Uncertainty in Artificial Intelligence 48–55 (Morgan Kaufmann Publishers Inc., 2001).
- Chaves, R. et al. Quantum violation of an instrumental test. Nat. Phys. 14, 291–296 (2018).

- 34. Trevisan, L. Extractors and pseudorandom generators. J. ACM (JACM) 48, 860–879 (2001).
- Clauser, J. F., Horne, M. A., Shimony, A. & Holt, R. A. Proposed experiment to test local hidden-variable theories. *Phys. Rev. Lett.* 23, 880–884 (1969).
- 36. Van Himbeeck, T. et al. Quantum violations in the Instrumental scenario and their relations to the Bell scenario. *Quantum* **3**, 186 (2019).
- Pironio, S. & Massar, S. Security of practical private randomness generation. *Phys. Rev. A* 87, 012336 (2013).
- Navascués, M., Pironio, S. & Acín, A. Bounding the Set of Quantum Correlations. *Phys. Rev. Lett.* 98, 010401 (2007).
- Reichardt, B. W., Unger, F. & Umesh, V. Classical command of quantum systems. *Nature* https://doi.org/10.1038/nature12035 (2013).
- Dupuis, F. & Fawzi, O. Entropy accumulation with improvedsecond-order term. *IEEE Transactions on Information Theory* 65, 7596–7612 (2019).
- 41. GitHub. https://github.com/michelemancusi/libtrevisan (2019).
- Fischer., M. J., Iorga., M. & Peralta., R. A public randomness service. In Proc. of the International Conference on Security and Cryptography 1, 434–438 (SciTe Press, 2011).
- Mauerer, W., Portmann, C. & Scholz, V. B. A modular framework for randomness extraction based on trevisan's construction. Preprint at https:// arxiv.org/abs/1212.0520 (2012).
- De, A., Portmann, C., Vidick, T. & Renner, R. Trevisan's extractor in the presence of quantum side information. *SIAM J. Comput.* 41, 915–940 (2012).
- Gross, R. & Aaronson, S. Bounding the seed length of miller and shi's unbounded randomness expansion protocol. Preprint at https://arxiv.org/abs/ 1410.8019(2014).
- Mayers, D. & Yao, A. Self testing quantum apparatus. Quantum. Inf. Comput. 4, 273 (2004).
- Yang, T. H. & Navascués, M. Robust self-testing of unknown quantum systems into any entangled two-qubit states. *Phys. Rev. A* 87, 050102 (2013).
- McKague, M., Yang, T. H. & Scarani, V. Robust self-testing of the singlet. J. Phys. A: Math. Theor. 45, 455304 (2012).
- Bamps, C. & Pironio, S. Sum-of-squares decompositions for a family of clauser-horne-shimony-holt-like inequalities and their application to selftesting. *Phys. Rev. A* **91**, 052111 (2015).
- Wu, X., Bancal, J.-D., McKague, M. & Scarani, V. Device-independent parallel self-testing of two singlets. *Phys. Rev. A* 93, 062121 (2016).
- Šupić, I., Augusiak, R., Salavrakos, A. & Acín, A. Self-testing protocols based on the chained bell inequalities. *N. J. Phys.* 18, 035013 (2016).
- Coladangelo, A., Goh, K. T. & Scarani, V. All pure bipartite entangled states can be self-tested. *Nat. Commun.* 8, 15485 (2017).
- 53. McKague, M. Self-testing in parallel with chsh. Quantum 1, 1 (2017).
- Šupić, I., Coladangelo, A., Augusiak, R. & Acín, A. Self-testing multipartite entangled states through projections onto two systems. *N. J. Phys.* 20, 083041 (2018).
- Bowles, J., Šupić, I., Cavalcanti, D. & Acín, A. Self-testing of pauli observables for device-independent entanglement certification. *Phys. Rev. A* 98, 042336 (2018).
- Brukner, Č., Żukowski, M., Pan, J.-W. & Zeilinger, A. Bell's inequalities and quantum communication complexity. *Phys. Rev. Lett.* 92, 127901 (2004).
- 57. Buhrman, H., Cleve, R., Massar, S. & De Wolf, R. Nonlocality and communication complexity. *Rev. Mod. Phys.* **82**, 665 (2010).
- Buhrman, H. et al. Quantum communication complexity advantage implies violation of a bell inequality. *Proc. Natl Acad. Sci.* 113, 3191–3196 (2016).

59. Giacomini, S., Sciarrino, F., Lombardi, E. & De Martini, F. Active teleportation of a quantum bit. *Phys. Rev. A* **66**, 030302 (2002).

# Acknowledgements

The authors aknowledge Gláucia Murta for stimulating discussion. We acknowledge support from John Templeton Foundation via the grant Q-CAUSAL No. 61084 (the opinions expressed in this publication are those of the authors and do not necessarily reflect the views of the John Templeton Foundation). I.A., D.P., M.M., G.C., and F.S. aknowledge project Lazio Innova SINFONIA. D.C. acknoledges a Ramon y Cajal fellowship, Spanish MINECO (Severo Ochoa SEV-2015-0522), Fundació Privada Cellex and Generalitat de Catalunya (CERCA Program). L.G. and L.A. acknowledge financial support from the São Paulo Research Foundation (FAPESP) under grants 2016/01343-7 and 2018/04208-9. RC acknowledges the Brazilian ministries MCTIC, MEC and the CNPq (grants No. 307172/2017-1 and 406574/2018-9 and INCT-IQ) and the Serrapilheira Institute (grant number Serra-1708-15763). G.C. aknowledges Conicyt and Becas Chile. L.A. acknowledges financial support also from the Brazilian agencies CNPq (PQ grant No. 305420/2018-6 and INCT-IQ), FAPERJ (JCNE E-26/202.701/2018), CAPES (PROCAD2013 project), and the Brazilian Serrapilheira Institute (grant number Serra-1708).

# Author contributions

I.A., D.P., L.G., G.C., F.S., R.C., L.A., D.C. developed the theory; I.A., D.P., G.C., F.S., L.G., L.A., D.C., R.C. designed the experiment; I.A., D.P., M.M., G.C., F.S. performed the experiment; all the authors participated in the discussions and contributed to writing the manuscript.

## **Competing interests**

The authors declare no competing interest.

# Additional information

Supplementary information is available for this paper at https://doi.org/10.1038/s42005-020-0375-6.

Correspondence and requests for materials should be addressed to F.S.

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) 2020