

Supplementary Information
**Experimental device-independent certified randomness generation with an
instrumental causal structure**

Iris Agresti, Davide Poderini, Leonardo Guerini, Michele Mancusi, Gonzalo
Carvacho, Leandro Aolita, Daniel Cavalcanti, Rafael Chaves, and Fabio Sciarrino

Supplementary Note 1. NPA METHOD APPLIED TO THE INSTRUMENTAL SCENARIO

In order to estimate the randomness generated in our experiment, we will adopt a similar strategy to that used in the Bell scenario (see [1]). We assume that there exists an external observer, called Eve, that wants to predict the measurement outcomes (a, b) of the instrumental test. The system used in the protocol is assumed to be quantumly correlated to a system held by Eve. In this scenario, the randomness in the outcomes (a, b) is given by the min entropy of Eve's guessing probability (the probability that Eve correctly predicts the outcomes).

In order to make this idea rigorous, let us first define the correlations that can be observed in the quantum instrumental scenario. Without loss of generality [2, 3], these can be expressed by the Born rule:

$$P_Q^{\text{Inst}}(a, b|x) = \text{Tr}(M_{a|x} \otimes N_{b|y=a} \rho_{AB}), \quad (1)$$

where $M_{a|x}$ and $N_{b|y}$ define proper quantum measurements ($M_{a|x} \geq 0$, $\sum_a M_{a|x} = \mathbb{1}$, $N_{b|y} \geq 0$, $\sum_b N_{b|y} = \mathbb{1}$) and ρ_{AB} a bipartite quantum state ($\rho_{AB} \geq 0$ and $\text{Tr} \rho_{AB} = 1$). Indeed, the observed correlations, of the form $p(a, b|x, y = a)$, are given by local projective measurements on a bipartite state. In the randomness analysis, we assume that additionally to systems AB there exists a third party, Eve, that is trying to guess the outcomes a and b . The full picture is described by a tripartite state $|\Psi_{ABE}\rangle$, onto which local measurements are performed (notice that the state can be assumed to be pure since the dimension of the systems are considered arbitrary). The statistics obtained is then evaluated on an instrumental functional $\mathcal{I}$ (e.g. the left-hand-side of inequality 1 of the main text), which allows us to calculate Eve's maximum guessing probability. Eve is assumed to know $|\Psi_{ABE}\rangle$ and the measurement implemented at AB .

In this case, the maximum probability that Eve guesses correctly (a, b) for a fixed setting $x = j$, and given that $\mathcal{I} = \beta$, can be written as follows:

$$\begin{aligned} \max_{a, b} \quad & \langle \Psi_{ABE} | \Pi_{a|x=j} \otimes \Pi_{b|y=a} \otimes \Pi_{e=(a,b)} | \Psi_{ABE} \rangle \\ \text{s.t.} \quad & P(a, b|x) = \langle \Psi_{ABE} | \Pi_{a|x} \otimes \Pi_{b|y=a} \otimes \mathbb{I}_E | \Psi_{ABE} \rangle, \\ & \forall a, b, x \quad \mathcal{I}(\{P(a, b|x)\}) = \beta, \end{aligned}$$

where the maximization is taken over all possible tripartite states Ψ_{ABE} and local measurements $\{\Pi_{a|x}\}, \{\Pi_{b|y}\}, \{\Pi_e\}$. In other words, we want the maximum probability that Eve's outcome e equals (a, b) , among all tripartite quantum correlations satisfying $\mathcal{I} = \beta$. The amount of randomness (in bits) is given by $H_\infty(A, B|E, x = j) = -\log_2(P_{\text{guess}}(x = j))$, where $P_{\text{guess}}(x = j)$ denotes the solution of the previous optimization problem.

This optimization problem is computationally intractable, as it considers quantum systems of arbitrary dimension. A way out is to upper-bound its value by using the Navascués- Pironio-Acín (NPA) hierarchy [4]. The NPA hierarchy is a numerical tool used to generate a sequence of sets of correlations $\mathcal{Q}_1 \supset \mathcal{Q}_2 \supset \dots \mathcal{Q}_n$ that converges to the set of quantum correlations of any bipartite system in the Bell scenario, defined as those that can be written as

$$P_Q^{\text{Bell}}(a, b|x, y) = \text{Tr}(M_{a|x} \otimes N_{b|y} \rho_{AB}), \quad (2)$$

where, as previously mentioned, $M_{a|x}$ and $N_{b|y}$ define proper quantum measurements ρ_{AB} a bipartite quantum state. Notice that, by definition, $P_Q^{\text{Inst}}(a, b|x) = P_Q^{\text{Bell}}(a, b|x, y = a)$. We can now use the NPA hierarchy to define the following optimization problem that upper bounds the guessing probability of Eve in an instrumental scenario:

$$\begin{aligned} P_{\text{guess}}^k(x = j) = \max_{P(a, b, e|x, y)} \quad & \sum_{a, b} P(a, b, e = (a, b)|x = j, y = a) \\ \text{s.t.} \quad & \{P(a, b|x, y, e = e_0)\} \in \mathcal{Q}_k, \forall e_0 \\ & \mathcal{I}(\{\sum_e P(a, b, e|x, y = a)\}) = \beta. \end{aligned} \quad (3)$$

This problem maximises the probability that Eve's outcome e equals (a, b) , among all of the possible correlations achieving the observed instrumental violation value β and for which the conditional correlations within the systems AB , conditioned to Eve's outcomes, belong to $\mathcal{Q}_k$. Note that no constraints are imposed on the untested terms $p(a, b|x, y \neq a)$. This implies that the optimization will be carried out on a larger set than the one corresponding to a scenario where all the combinations were tested. Hence, in general, the resulting min-entropy will be lower, accounting for any eventual advantage that an eavesdropper could get, by exploiting the fact that some probability terms are not well defined. On the contrary, on the tested terms, we imposed the same constraints that would be used in a Bell-like scenario, i.e. normalization, $\sum_{a, b} p(a, b|x, y = a) = 1$, no-signalling, $p(b|x, y) = p(b|x', y)$, and commutation

between Alice's and Bob's operators. Furthermore, since for every k the set of correlations over which we perform our optimization is bigger than the quantum one, $P_{\text{guess}}^k(x = j) \geq P_{\text{guess}}(x = j)$, the solution of (3) provides a lower bound to the randomness obtained. In our implementation, we used $\mathcal{I}$ as the left-hand-side of inequality (1) of the main text, and $k = 2$.

The optimal value of the above problem is used to define $f_{x=j}(\mathcal{I}) = -\log_2(P_{\text{guess}}^k(x = j))$ in the lower bound $H_\infty(A, B|E, x = j) \geq f_{x=j}(\mathcal{I})$ mentioned in the main text.

Supplementary Note 2. ENTROPY ACCUMULATION THEOREM IN THE INSTRUMENTAL SCENARIO

In order to make our protocol secure against general quantum adversaries, we adapt the techniques developed by [5] to our scenario. This method, as mentioned in the main text, resorts to the ‘‘Entropy Accumulation Theorem’’ (EAT), in order to deal with processes not necessarily made of independent and identically distributed (iid) runs. This tool ensures that our protocol is secure, even if an adversary has access to the devices and introduces a (quantum) memory inside, making each run possibly depend on the previous ones. In this paragraph, we briefly recall the EAT and then explain in further details how we applied it to our case.

The EAT provides a lower bound on the smooth min-entropy of any process that can be described as a sequential application of n ‘‘EAT channels’’. Hence, it will hold also in our case, if we show that our protocol consists in the sequence of such channels. This bound is polynomial in the number of runs n and, when the number of runs grows, it tends to that obtaining assuming iid. The i -th EAT channel ($\mathcal{M}_i$) can be described as follows: it outputs two registers O_i , which are given to the honest parties Alice and Bob and that represent the information that should be kept secret, another system S_i constituting some side-information leaked by the channel, and a memory R_i , which is passed as input to the next map ($\mathcal{M}_{i+1}$). Also a system E is considered in the model, representing any additional side information correlated to the initial state. Hence the systems O are the ones in which the entropy is accumulated, conditioned on S and E . We also consider, for each round, a classical value C_i which is evaluated from O_i and S_i . Hence, $\mathcal{M}_i : R_{i-1} \rightarrow R_i O_i S_i C_i$ for $i \in [n]$. A subset $c_1^n \in C^n$, where C^n is the space of all possible n -bit sequences, defines an event Ω and we indicate with $\hat{\Omega}$ the empirical statistics of c_1^n , i.e. $\hat{\Omega} = \{\text{freq}(c_1^n) | c_1^n \in \Omega\}$.

The conditions that a EAT channel must fulfil are the following (for a formal definition, see the Methods section of [5]):

- C_i are classical systems of finite-dimension (random variables), while O_i , R_i , and S_i are quantum registers. d_{O_i} is the maximum dimension of O_i ;
- for any input state $\sigma_{R_{i-1}R'}$, where R' is isomorphic to R_{i-1} , the output state $\sigma_{R_i O_i S_i C_i R'} = (\mathcal{M}_i \otimes \mathbb{I}_{R'}) \sigma_{R_{i-1}R'}$ has the property that C_i can be evaluated from $\sigma_{O_i S_i}$ without changing the state;
- (Markov chain condition) for any initial state $\rho_{R_0 E}^0$, the final state $\rho_{O_1^n S_1^n C_1^n E} = \text{Tr}_{R^n}(\mathcal{M}_n \otimes \mathcal{M}_{n-1} \dots \mathcal{M}_1 \otimes \mathbb{I}_E) \rho_{R_0 E}^0$ fulfils the Markov chain condition $O_1^{i-1} \leftrightarrow S_1^{i-1} E \leftrightarrow S_i$ for each $i \in [n]$. In other words, $I(O_1^{i-1} : S_i | S_1^{i-1} E) = 0$, so the previous outcomes O_1^{i-1} are independent of future side information S_i^i , given all the past side information $S_1^{i-1} E$.

Now, we state the EAT, as in [5]:

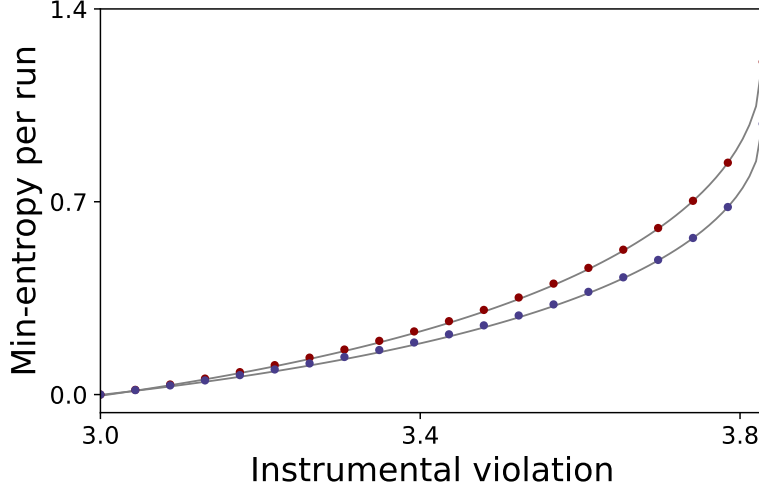
Entropy Accumulation Theorem (EAT). Let $\mathcal{M}_i : R_{i-1} \rightarrow R_i O_i S_i C_i$ be the for $i \in [n]$ be EAT channels, ρ be the final state, Ω an event defined over C^n , p_Ω the probability of Ω in ρ , and $\rho_{|\Omega}$ the final state conditioned on Ω and let $\epsilon \in (0, 1)$. For $f_{\min}$ a tradeoff function for $\{\mathcal{M}_i\}$, $\hat{\Omega} = \{\text{freq}(c_1^n) | c_1^n \in \Omega\}$ convex and any $t \in \mathbb{R}$, such that $f_{\min}(\text{freq}(c_1^n)) \geq t$ for any $c_1^n \in C_1^n$ for which $P(c_1^n)_{\rho_{|\Omega}} \geq 0$,

$$\mathcal{H}_{\min}^\epsilon(O^n | S^n E^n) > nt - \nu \sqrt{n} \quad (4)$$

where $t(\mathcal{I})|_{\mathcal{I}_{\text{exp}}}$ represents the Von-Neumann entropy, which depends on the extent of the violation that would be obtained from an honest implementation of the protocol, i.e. with no adversary, $\mathcal{I}_{\text{exp}}$. On the other hand, ν depends on $\|\nabla f_{\min}\|_\infty$, on the smoothing parameter ϵ and on ϵ_{EA} , which can be interpreted as the error probability of the entropy accumulation protocol.

In order to adapt the protocol of [5] to our case, we first of all need to build a $f_{\min}(p(a, b|x))$ function for the instrumental process and evaluate the smooth min-entropy bound according to inequality (4). In order to perform the required derivatives, we fit the data computed via SDP (see previous section), as shown in Supplementary Figure 1. The obtained fits $f_x(\mathcal{I})$, for $x = 1, 2, 3$, are the following:

$$f_1 = u_1 - w_1 \mathcal{I} - z_1 \sqrt{1 + 2\sqrt{2} - \mathcal{I}} \quad (5)$$



Supplementary Figure 1: **Lower bounds of $f_x(\mathcal{I})$.** In this plot, we present the $f_x(\mathcal{I})$ min-entropy lower bounds obtained fitting the numerical data given by the techniques of [1, 4]. The red dots correspond to $x = 2, 3$, while the blue ones to $x = 1$. The grey curves represent the lowered best fit functions $f'_1 = u'_1 - w_1\mathcal{I} - z_1\sqrt{1 + 2\sqrt{2} - \mathcal{I}}$ (lowest curve) and $f'_2 = f'_3 = u'_{2,3} - w_{2,3}\mathcal{I} - z_{2,3}\sqrt{1 + 2\sqrt{2} - \mathcal{I}}$ (highest curve). We have $(u'_1, w_1, z_1) = (3.062, 0.542, 1.579)$ and $(u'_{2,3}, w_{2,3}, z_{2,3}) = (3.735, 0.657, 1.942)$.

and

$$f_2 = f_3 = u_{2,3} - w_{2,3}\mathcal{I} - z_{2,3}\sqrt{1 + 2\sqrt{2} - \mathcal{I}} \quad (6)$$

where $(u_1, w_1, z_1) = (3.067, 0.542, 1.579)$ and $(u_{2,3}, w_{2,3}, z_{2,3}) = (3.740, 0.657, 1.942)$. To ensure that we will not overestimate the min-entropy, we lower these curves along the y-axis, in order to give a lower bound on the numerically evaluated min-entropies (see Supplementary Figure 1). Hence, the parameters u'_1 and $u'_{2,3}$ that we will use in our calculations will be respectively $u'_1 = 3.062$ and $u'_{2,3} = 3.735$.

Then, we can implement the protocol, as follows: we group our experimental runs in k blocks, with no fixed length; at each run, a binary variable T is evaluated, in particular, it is 1 with an arbitrary probability γ . Each block ends either when $T = 1$, or when $T = 0$ for $s_{\max}$ times in a row (this parameter is set by the user). So, after n runs, we will have k blocks, each one containing at most 1 test run. Each of these blocks corresponds to a EAT channel $\mathcal{M}_i$ and we consider that $O_i \rightarrow \mathbf{A}_i\mathbf{B}_i$ and $S_i \rightarrow \mathbf{X}_i\mathbf{T}_i$, where $\mathbf{A}_i$ and $\mathbf{B}_i$ are classical registers containing the string that Alice and Bob get throughout the i -th block; on the other hand, $\mathbf{X}_i$ and $\mathbf{T}_i$ are the strings of Alice's inputs and of the T values for the same block. In the end, C_i is the tuple (a_i, b_i, x_i) , obtained still in the i -th block, for $T = 1$, i.e. in the test run.

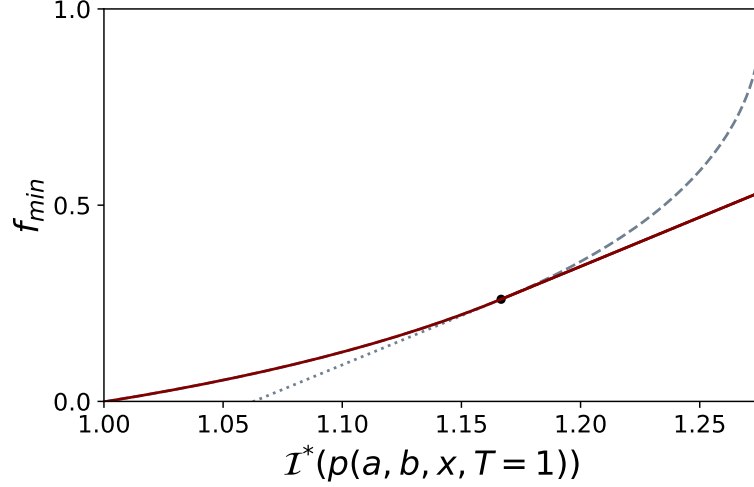
The length of the blocks (as well as that of $\mathbf{A}_i$, $\mathbf{B}_i$, $\mathbf{X}_i$ and $\mathbf{T}_i$) is not fixed, but the expected value is the following: $s' = \frac{1-(1-\gamma)^{s_{\max}}}{\gamma}$. Now, let us check whether the aforementioned channel $\mathcal{M}_i : R_{i-1} \rightarrow R_i\mathbf{A}_i\mathbf{B}_i\mathbf{X}_i\mathbf{T}_iC_i$, is indeed an EAT channel.

- $C_i \in \{\{0, 1, -\}, \{0, 1, -\}, \{0, 1, 2, -\}\}$ for any $i \in [1, k]$, where $\{-, -, -\}$ is the case in which the i -th block ends with no test run, and $d_{O_i} \leq 6^{s_{\max}}$.
- C_i is evaluated by the classical registers $\mathbf{A}_i$, $\mathbf{B}_i$, $\mathbf{X}_i$ and $\mathbf{T}_i$, so it does not modify the marginals on those registers.
- the Markov chain condition holds, provided that the inputs are chosen independently at each round. In this case, the condition $\mathbf{A}_{1,\dots,i-1}\mathbf{B}_{1,\dots,i-1} \leftrightarrow \mathbf{X}_{1,\dots,i-1}\mathbf{T}_{1,\dots,i-1}E \leftrightarrow \mathbf{X}_i\mathbf{T}_i$ trivially holds.

Hence, the min-entropy in the i -th block will be bounded as follows:

$$H(\mathbf{A}_i, \mathbf{B}_i | \mathbf{X}_i, \mathbf{T}_i, E) > (s' - 1) \cdot f'_{2,3}(\mathcal{I}) + f'_1(\mathcal{I}) \quad (7)$$

Note that, since our protocol consists in the sequential application of EAT channels, the demonstration of Eq. (7) is analogous to the one in the Methods section of [5]). In the inequality (7), we are considering that, for $x = 2, 3$ and



Supplementary Figure 2: **Tradeoff function** $f_{\min}$. In this plot, we show the construction of the min-tradeoff function $f_{\min}(I_t^*(p(a, b, x, T=1)))$. To ensure that its derivative does not explode, we cut the function in an arbitrary point and glue it to a linear function.

$x = 1$, the bounds are different. Hence, in the accumulation rounds, we consider $f_{2,3}$, while, for the test round, we take f_1 , i.e. the lowest bound. The relation (7) holds when the min-entropy is evaluated on a state conditioned on the event Ω that, in our case, consists in obtaining an instrumental violation value higher than the threshold I_{exp} , throughout the test runs. In other words, given the input x_i of the i -th test run, the outputs (a_i and b_i) follow the joint probability distribution $P(a, b|x, T=1) = \frac{3p(a, b, x, T=1)}{1-(1-\gamma)^{s_{\max}}}$, with corresponding violation $\mathcal{I}(\frac{3p(a, b, x, T=1)}{1-(1-\gamma)^{s_{\max}}}) = \frac{3I^*(p(a, b, x, T=1))}{1-(1-\gamma)^{s_{\max}}} = I_{\text{exp}}$. Let us note that $\sum_{a, b, x} p(a, b, x, T=1) = 1 - (1-\gamma)^{s_{\max}}$.

At this point, we define

$$g(\mathcal{I}^*) = (s' - 1) \cdot f_{2,3}(\mathcal{I}) + f_1(\mathcal{I}) \quad (8)$$

and, substituting (5) and (6) in (8), we obtain:

$$g(\mathcal{I}^*) = (u'_1 + (s' - 1)u'_{2,3}) - 3(w_1 + (s' - 1)w_{2,3}) \frac{\mathcal{I}^*}{1 - (1 - \gamma)^{s_{\max}}} - (z_1 + (s' - 1)z_{2,3}) \sqrt{1 + 2\sqrt{2} - 3 \frac{\mathcal{I}^*}{1 - (1 - \gamma)^{s_{\max}}}} \quad (9)$$

The $f_{\min}$ convex tradeoff function will be defined as: $f_{\min}(\mathcal{I}^*(a, b, x, T=1), \mathcal{I}_t^*) = g(\mathcal{I}^*)$, for $\mathcal{I}^*(p(a, b, x, T=1)) \frac{3}{1-(1-\gamma)^{s_{\max}}} \in (0, \mathcal{I}_t)$

and $g(\mathcal{I}^*) \frac{3}{1-(1-\gamma)^{s_{\max}}} \in (\mathcal{I}_t, 1+2\sqrt{2})$. Concatenating the function $g(\mathcal{I}^*)$ to a linear function in a given point $\mathcal{I}_t = \frac{3\mathcal{I}_t^*}{1-(1-\gamma)^{s_{\max}}}$, as shown in Supplementary Figure 2, ensures that the derivative of $f_{\min}$, which contributes to the right term of inequality (4), does not explode.

In the end, for a given $\mathcal{I}_{\text{exp}}$, as proven in [5], the protocol either aborts with probability higher than $1 - \epsilon_{\text{EA}}$, or it gives at least the following smooth min-entropy:

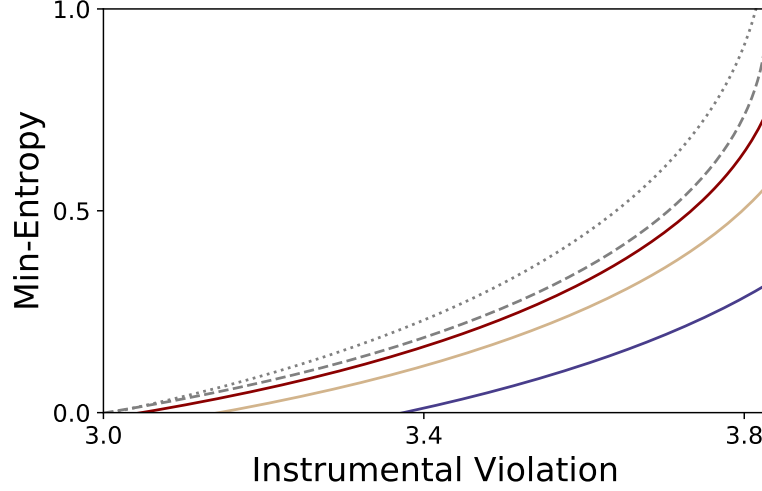
$$\frac{n}{s'} \eta_{\text{opt}}(\epsilon, \epsilon_{\text{EA}}) \quad (10)$$

where $\eta(I^*, I_t^*, \epsilon, \epsilon_{\text{EA}}) = f_{\min}(I^*, I_t^*) - \sqrt{s/n 2(\log(1 + 2 \times 6^{s_{\max}}) + 4) \left\| \frac{dg(I^*)}{dI^*} \right\|_{I_t^*} \sqrt{1 - 2\log(\epsilon \epsilon_{\text{EA}})}}}$ and $\eta_{\text{opt}}(\epsilon, \epsilon_{\text{EA}}) = \max_{(I_t^*)} \eta(I(1 - (1 - \gamma^{s_{\max}}))/3 - 4\delta', I_t^*, \epsilon, \epsilon_{\text{EA}}))$.

The η_{opt} bound is plotted in terms of the expected violation of the instrumental inequality, for different parameter settings in Supplementary Figure 3.

The protocol described above is a (ϵ_c, ϵ_s) -secure protocol, where ϵ_c and ϵ_s indicate, respectively, the “completeness” and the “soundness” of the protocol, which are defined as follows [5–7]:

- **Soundness:** in its implementation the protocol either aborts or returns an m -bit string $Z \in \{0, 1\}^m$, which is characterized by $(1 - P(\text{abort})) \|\rho_{ZRE} - \rho_{U_m} \otimes \rho_{U_R} \otimes \rho_E\| \leq \epsilon_s$ where R is the input randomness register, E is the adversary system, and ρ_{U_R} and ρ_{U_m} are completely mixed states on the appropriate registers.



Supplementary Figure 3: **Smooth min-entropy lower bound given by EAT.** In this plot, we show the lower bound, guaranteed by the EAT, on the smooth min-entropy, in terms of the expected instrumental violation I_{exp} for the different $(\epsilon, \epsilon_{\text{EA}}, \delta', n)$ parameters' choices. The red curve is obtained with $(10^{-6}, 10^{-6}, 10^{-3}, 10^8)$, the golden curve is obtained with $(10^{-6}, 10^{-6}, 10^{-3}, 10^7)$ and the blue curve is obtained with $(10^{-5}, 10^{-5}, 10^{-3}, 10^6)$. The dotted curve represents the iid bound for $x = 2, 3$, while the dashed one is for $x = 1$.

- **Completeness:** there exists an honest implementation which aborts with probability less than ϵ_c

In our case, ϵ_c and ϵ_s are quantified as follows. ϵ_s is made of several contributions [5–7], in particular we have to take into account 3 terms: (i) the ϵ_{ext} , which is the internal error of the classical extractor, described in Par. “Randomness Extractor” of this supplemental material, (ii) the parameter ϵ characterizing the smooth min-entropy $\mathcal{H}_{\text{min}}^\epsilon$ and (iii) the probability of the protocol not aborting (ϵ_{EA}). Hence $\epsilon_s = \epsilon_{\text{EA}} + m\epsilon_{\text{ext}} + \frac{\epsilon}{2}$. In our experimental condition, the resulting soundness amounts to $\epsilon_s \sim 10^{-1}$. On the other hand, the completeness can be evaluated by the Hoeffding’s inequality [8] (since it refers a iid honest implementation), as $P(\text{abort}) \leq e^{-2n\delta'^2} = \epsilon_c$, so it depends on the experimental uncertainty on the violation. In our case, $\epsilon_c \sim 10^{-37}$.

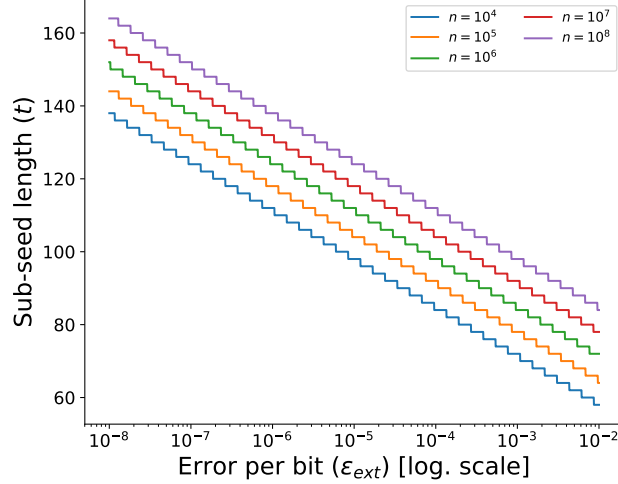
Note that, if $\gamma \neq 1$, both the soundness and completeness get an extra-contribution, given by the maximum statistical distance between the distribution of the drawn $\{T_1, \dots, T_n\}$ from the ideal one, i.e. that of n iid random variables drawn according to the Bernoulli distribution, with parameter γ , if the “interval algorithm” [9] is adopted.

Supplementary Note 3. RANDOMNESS EXTRACTOR

Quantum correlations can be exploited to generate random numbers, whose randomness can be device-independently certified. However, in real experimental conditions, quantum correlations are inevitably mixed with classical noise, which could be controlled and used by an adversary (Eve) to gain partial information about the output random bits. This is the reason why there is the need to apply a post-processing procedure to filter the true randomness out of the raw bits generated by a Quantum Random Numbers Generator (QRNG). This procedure is called “randomness extraction” and it involves the use of classical algorithms known as “randomness extractors” [10, 11]. The aim of these algorithms is to obtain a bit sequence, following an almost uniform distribution, up to an error parameter ϵ_{ext} , which can be made arbitrarily small. The inputs of a randomness extractors are the following: a weak random source, constituted by the raw bits and characterized by a min-entropy of at least k , and a seed of length d , not necessarily uniform [12]. The accuracy of the extractor can be increased, for a given min-entropy k , by reducing the number of extracted bits and by injecting a longer seed.

A deterministic function which takes as inputs the source and the seed and achieves these goals is called $(k, \epsilon_{\text{ext}})$ -*extractor*. The optimum situation, therefore, would be to have m , the number of extracted bits, as close to k as possible, meaning that all the available min-entropy has been extracted (indeed $k - m$ is the “entropy loss”), and the seed, of length d , as small as possible, to minimise the amount of additional randomness.

Recently, an important and promising randomness extractor, Trevisan’s extractor [13], has aroused considerable theoretical interest, since it has been proven to be secure against quantum adversaries [12]. This algorithm requires a



Supplementary Figure 4: **Length of the sub-seeds produced by the weak design depending on the error per bit.** This plot shows how the sub-seed’s length produced by the weak design, i.e. the small sets into which the weak design algorithm divides the seed, changes in terms of the error per bit ϵ_{ext} . It can be noted that in semi-log scale, the sub-seed’s length t is a step function and decreases linearly as the error per bit ϵ_{ext} increases. Furthermore, the greater the input n , the greater the length of the single sub-seed created by the weak design. This plot refers both to the Standard weak design [17] as well as the Block weak [16] design (which we adopt in our paper) algorithms.

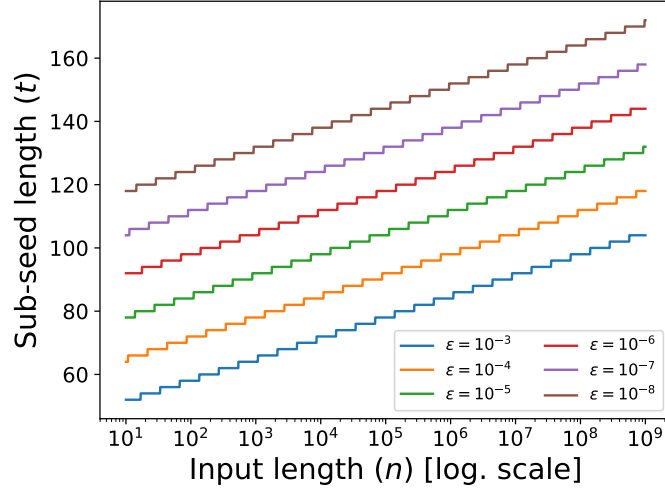
seed that scales polylogarithmically in the input size, giving an advantage over extractors adopting (almost) universal hashing, whose seed grows polynomially with the length of the input. Furthermore, Trevisan’s extractor is also proven to be a strong extractor [14], i.e. the seed can be concatenated to the extracted string and used as a part of the result, being nearly independent from the output string. Two implementations of this extractor were made by Ma et al. [15] and Maurer et al. [16].

Trevisan’s construction, in a few words, is a recipe to build a randomness extractor combining two elements: (i) the “weak design”, that divides the initial seed into smaller blocks of random bits of length t (“sub-seeds”) and (ii) the “one bit extractor”, which extracts a single random bit from the random source for each block. In the “weak design”, the blocks $\{S_1, \dots, S_j\}$ into which the seed is divided should be nearly independent to ensure that the maximum amount of entropy is extracted. Hence, a family of sets $S_1, \dots, S_m \subset [d]$ is a weak (m, t, r, d) -design if

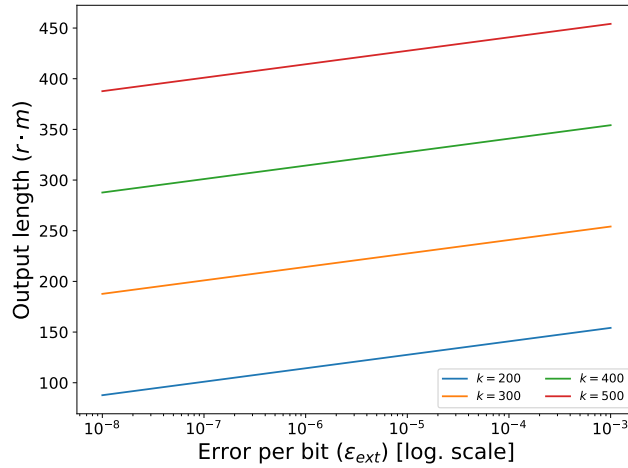
1. For all i , $|S_i| = t$
2. For all i , $\sum_{j=1}^{i-1} 2^{|S_j \cap S_i|} \leq rm$, where the parameter r is the so-called “overlap” of the weak design.

Each of the S_j is fed into a one bit extractor and they are all in the end concatenated into a final random string.

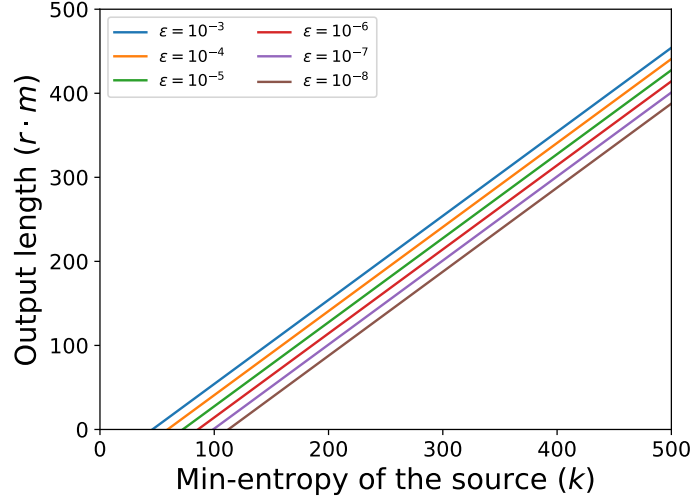
In our work, we adopt the so-called “Block weak design”, which is a variation of another algorithm, which we will refer to as the “Standard weak design”. The latter is a refined version of Nisan and Wigderson [17], whose effectiveness was proved by Hartman and Raz [18], under the parameters choice given by $r = 2e$ and $d = t^2$ with $t = 2\lceil \log n + 2\log 2/\epsilon_{\text{ext}} \rceil$, where n is the number of runs. The “Block weak design”, on the other hand, was developed by Ma and Ta [19] modified by Maurer et al. [16] with $r = 1$ and $d = (l+1)t^2$, where $l := \max\{1, \lceil \frac{\log(m-r') - \log(t-r')}{\log(r') - \log(r'-1)} \rceil\}$ and $r' = 2e$. In comparison, the “Block weak design” requires a seed’s length exceeding that of the input weak random source’s string, but it allows to extract more bits from the source, due to a smaller r , with respect to the “Standard weak design”. The one-bit extractor is realized by an error correcting code, which is constructed by concatenating a Reed-Solomon code with an Hadamard code. Hence, as a preliminary step, we fix the following three parameters: (i) $2n$ (input length), (ii) α (min-entropy per bit, certified by the experimental instrumental violation) and (iii) ϵ_{ext} (error per bit). After that, we derive the seed length, the total min-entropy $k = \mathcal{H}_{\text{min}}^\epsilon$ and $m = (k - 4\log \frac{1}{\epsilon_{\text{ext}}} - 6)/r$. As we can see, fixing the length m of the output string and the error per bit ϵ_{ext} , the required min-entropy increases with the overlap of the sets $\{S_i\}$. In Supplementary Figures 4-11, we show the behaviour of our extractor’s parameters.



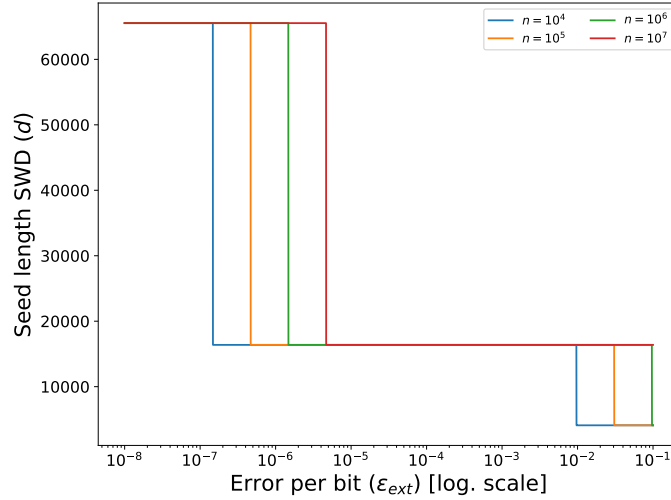
Supplementary Figure 5: **Length of the sub-seeds produced by the weak design depending on the input length of the source.** In this figure is represented how the sub-seed length t , i.e. the small sets into which the weak design algorithm divides the seed, varies as a function of the input length n , plotted for different error per bit ϵ_{ext} parameters. We can see that in semi-log scale the sub-seed length is a step function and increases linearly with the input. Furthermore, the greater the error per bit, the smaller will be the length of the single sub-seed created by the weak design. This plot refers both to the Standard weak design [17] as well as the Block weak [16] design (which we adopt in our paper) algorithms.



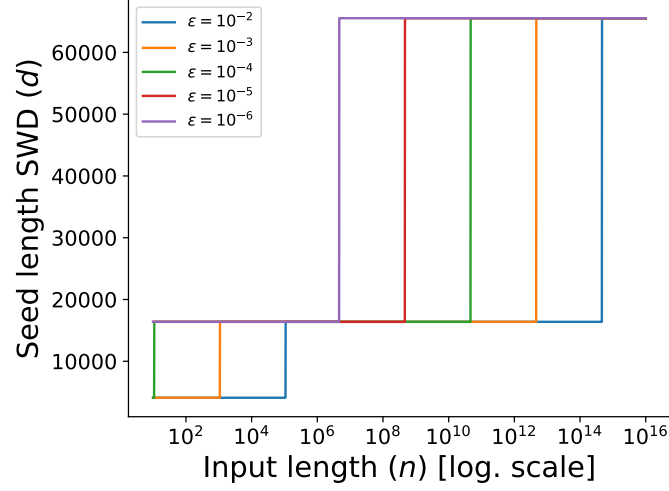
Supplementary Figure 6: **Ratio between the output length of the extractor and the error per bit parameter.** This figure shows linear dependence in semi-log scale of the output length m (multiplied by a constant factor r) as a function of the error per bit ϵ_{ext} . Output length increases with the error and the greater the min-entropy k , the greater the output length. This plot refers both to the Standard weak design [17] as well as the Block weak [16] design (which we adopt in our paper) algorithms.



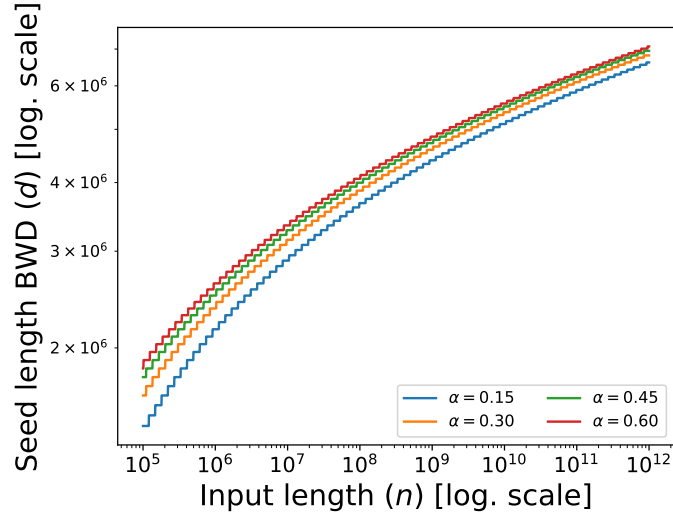
Supplementary Figure 7: **Final random string length in terms of the min-entropy of the source.** It can be noted that the output length m (multiplied by a constant factor r) is a linear growing monotone function of the min-entropy of the source $k = \mathcal{H}_{\min}^{\epsilon}$ and it also increases with the error per bit ϵ_{ext} . This plot refers both to the Standard weak design [17] as well as the Block weak [16] design (which we adopt in our paper) algorithms.



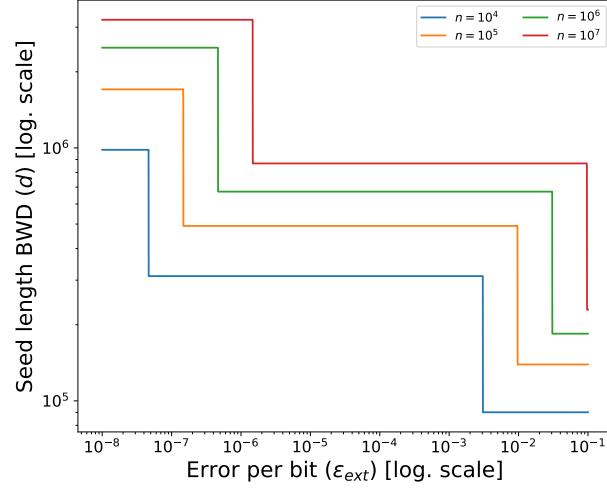
Supplementary Figure 8: **Dependency of seed length for the Standard weak design from the error per bit.** Here different graphs of the seed length d as a function of the error per bit ϵ_{ext} are plotted, for different input source length in semi-log scale. These functions are step functions and, with the same error, the seed increases with the size of the input n . This plot refers to the Standard weak design algorithm [17].



Supplementary Figure 9: **Comparison between seed length and the input length of the source.** In this figure is represented the seed length d vs the input length n in semi-log scale, plotted for different error per bit ϵ_{ext} parameters. The seed is a step function of the input length, it increases with n and, with the same input length, the seed length is greater for lower errors. This plot refers to the Standard weak design algorithm [17].



Supplementary Figure 10: **Relation between the seed length of Block weak design and the input length of the source.** The seed length d as a function of the input length n is plotted for different values of min-entropy per bit α and the error per bit ϵ_{ext} parameter is fixed at $\epsilon_{\text{ext}} = 10^{-7}$. d is a monotone increasing function of n and it increases also with α . Both the axes are in logarithmic scale. This plot refers to the Block weak design algorithm, which was used in our paper, [16].



Supplementary Figure 11: **Seed length of Block weak design depending on the error per bit.** For different input length of the source, the seed length d as function of the error per bit ϵ_{ext} is plotted. d is a descending step function of ϵ_{ext} , but it increases with n . The min-entropy is fixed at $\alpha = 0.4$ and both the axes are in logarithmic scale. This plot refers to the Block weak design algorithm, which was used in our paper, [16].

SUPPLEMENTARY REFERENCES

- [1] Pironio, S. *et al.* Random numbers certified by bell's theorem. *Nature* **464**, 1021–1024 (2010). URL <http://dx.doi.org/10.1038/nature09008>.
- [2] Van Himbeeck, T. *et al.* Quantum violations in the Instrumental scenario and their relations to the Bell scenario. *Quantum* **3**, 186 (2019).
- [3] Henson, J., Lal, R. & Pusey, M. F. Theory-independent limits on correlations from generalized bayesian networks. *New J. of Phys.* **16**, 113043 (2014).
- [4] Navascués, M., Pironio, S. & Acín, A. Bounding the Set of Quantum Correlations. *Physical Review Letters* **98**, 010401 (2007). [quant-ph/0607119](https://arxiv.org/abs/quant-ph/0607119).
- [5] Arnon-Friedman, R., Dupuis, F., Fawzi, O., Renner, R. & Vidick, T. Practical device-independent quantum cryptography via entropy accumulation. *Nature Communications* **9**, 459 (2018). URL <https://doi.org/10.1038/s41467-017-02307-4>.
- [6] Shen, L. *et al.* Randomness extraction from bell violation with continuous parametric down-conversion. *Physical Review Letters* **121**, 150402– (2018). URL <https://link.aps.org/doi/10.1103/PhysRevLett.121.150402>.
- [7] Kessler, M. & Arnon-Friedman, R. Device-independent randomness amplification and privatization. *arXiv preprint: arXiv:1705.04148* (2017).
- [8] Hoeffding, W. Probability inequalities for sums of bounded random variables. *Journal of the American Statistical Association* **58**, 13–30 (1963). URL <https://amstat.tandfonline.com/doi/abs/10.1080/01621459.1963.10500830>. <https://amstat.tandfonline.com/doi/pdf/10.1080/01621459.1963.10500830>.
- [9] Hao, H. M., T. S. Interval algorithm for random number generation. *IEEE Transactions on Information Theory* **43** (1997).
- [10] Nisan, N. & Ta-Shma, A. Extracting randomness: A survey and new constructions. *Journal of Computer and System Sciences* **58**, 148 – 173 (1999). URL <http://www.sciencedirect.com/science/article/pii/S0022000097915464>.
- [11] Shaltiel, R. An introduction to randomness extractors. In Aceto, L., Henzinger, M. & Sgall, J. (eds.) *Automata, Languages and Programming*, 21–41 (Springer Berlin Heidelberg, Berlin, Heidelberg, 2011).
- [12] De, A., Portmann, C., Vidick, T. & Renner, R. Trevisan's extractor in the presence of quantum side information. *SIAM Journal on Computing* **41**, 915–940 (2012). URL <https://doi.org/10.1137/100813683>. <https://doi.org/10.1137/100813683>.
- [13] Trevisan, L. Extractors and pseudorandom generators. *Journal of the ACM (JACM)* **48**, 860–879 (2001).
- [14] Raz, R., Reingold, O. & Vadhan, S. Extracting all the randomness and reducing the error in trevisan's extractors. *Journal of Computer and System Sciences* **65**, 97 – 128 (2002). URL <http://www.sciencedirect.com/science/article/pii/S0022000002918246>.
- [15] Ma, X. *et al.* Postprocessing for quantum random-number generators: Entropy evaluation and randomness extraction. *Physical Review A* **87**, 062327 (2013). URL <https://link.aps.org/doi/10.1103/PhysRevA.87.062327>.
- [16] Maurer, W., Portmann, C. & Scholz, V. B. A modular framework for randomness extraction based on trevisan's construction. *arXiv preprint arXiv:1212.0520* (2012).
- [17] Nisan, N. & Wigderson, A. Hardness vs randomness. *Journal of computer and System Sciences* **49**, 149–167 (1994).
- [18] Hartman, T. & Raz, R. On the distribution of the number of roots of polynomials and explicit weak designs. *Random Structures & Algorithms* **23**, 235–263 (2003).
- [19] Ma, X., Zhang, Z. & Tan, X. Explicit combinatorial design. *arXiv preprint arXiv:1109.6147* (2011).