Contents

A   Theoretical results

In this section, we derive the bound (3) presented in the main text. We follow a two-step approach. In Section A.1, we quantify the randomness of a pair of quantum systems characterized by a given Bell expectation I. In Section A.2, we apply these results to the experimental data produced by Bell-violating devices that are used n times in succession and which, in full generality, may not behave identically and independently at each trial.

A.1   Quantum randomness versus Bell violation

We establish here a relation between the randomness of the measurement outcomes of a quantum system and its expected Bell violation. In full generality, we consider a Bell scenario with m different measurements per system, each measurement having d possible results. The two quantum subsystems are characterized by the joint probabilities $P_{AB|XY} = \{P(ab|xy)\}$ to produce outcomes $a, b = 1, \ldots, d$, when measurements $x, y = 1, \ldots, m$ are made. A Bell expression associated to this scenario is a linear combination $I = \sum_{abxy} c_{abxy} P(ab|xy)$ of the probabilities specified by the $m^2 \times d^2$ coefficients $\{c_{abxy}\}$. Probabilities that admit a local description satisfy $I \leq I_0$, where I_0 is the local bound of the Bell inequality. The CHSH correlation function (1) is a particular example of such a Bell expression with $m = 2$ and $d = 2$.

We quantify the randomness of the output pairs conditioned on the input pairs by the min-entropy $H_\infty(AB|XY) = -\log_2 \max_{ab} P(ab|xy) = \min_{ab} [-\log_2 P(ab|xy)]$. For given Bell violation I, our aim is to obtain a lower bound on the min-entropy

$$H_\infty(AB|XY) \geq f(I) \tag{A.1}$$

satisfied by all quantum realizations of the Bell scenario. Let $P^*(ab|xy)$ denote the solution to the following optimization problem:

$$
\begin{aligned}
P^*(ab|xy) = \quad &\max \quad & P(ab|xy) \\
&\text{subject to} \quad & \sum_{abxy} c_{abxy} P(ab|xy) = I \\
& & P(ab|xy) = \mathrm{tr}\left(\rho M_x^a \otimes M_y^b\right)
\end{aligned}
\tag{A.2}
$$

where the optimization is carried over all states ρ and all measurement operators M_x^a and M_y^b, defined over Hilbert spaces of arbitrary dimension. The minimal value of the min-entropy compatible with the Bell violation I and quantum theory is then given by $H_\infty(AB|XY) = -\log_2 \max_{ab} P^*(ab|xy)$.

To obtain a lower-bound on the min-entropy as a function of the Bell violation I which does not depend on the input pair (x, y), it is thus sufficient to solve (A.2) for all output and input

pairs (a, b) and (x, y). This can be done by adapting in a straightforward way the technique introduced in [1, 2] and generalized in [3].

In [1, 2], an infinite hierarchy of conditions C_i ($i = 1, 2, \ldots$) necessarily satisfied by all probabilities of the form $P(ab|xy) = \text{tr}\left(\rho M_x^a \otimes M_y^b\right)$ are introduced. These conditions can be characterized by semidefinite programs (SDP) of finite size. Conditions higher in the hierarchy, that is corresponding to higher values of i, are more constraining, i.e., they better reflect the constraints $P(ab|xy) = \text{tr}\left(\rho M_x^a \otimes M_y^b\right)$, but they also correspond to SDP's of larger size. By replacing in (A.2) the conditions $P(ab|xy) = \text{tr}\left(\rho M_x^a \otimes M_y^b\right)$ by the semidefinite constraints C_i for $i = 1, 2, \ldots$, one obtains a sequence of relaxations $R_1, R_2, \ldots$ of the original problem that can be solved through semidefinite programming since the constraint $\sum_{abxy} c_{abxy} P(ab|xy) = I$ and the objective function in (A.2) are both linear in the probabilities $P(ab|xy)$. The solutions of these relaxations yield a sequence of upper-bounds on the optimum of (A.2), which in turn yields a sequence of lower bounds on the min-entropy: $f^{(1)}(I) \leq f^{(2)}(I) \leq \ldots \leq H_\infty(AB|XY)$. The exact form of these lower bounds depend on the Bell inequality specified by the coefficients $\{c_{abxy}\}$, but they are all convex functions that are equal to 0 at the classical point $I = I_0$.

Formulating the problem as an SDP is extremely useful, as numerical methods are guaranteed to find the global optimum of the SDP, i.e., will yield up to numerical precision the exact values of $f^{(1)}(I), f^{(2)}(I), \ldots$. We have solved the SDPs corresponding to the second relaxation step ($i = 2$) for the CHSH inequality using the matlab toolboxes SeDuMi [4] and YALMIP [5] (see Figure 2).

Upper bounds on the min-entropy can be obtained by searching numerically for solutions to (A.2) with fixed Hilbert space-dimension. Specifically, one can introduce a parameterization of the state and measurement operators and vary the parameters to maximize (A.2). We find that our upper and lower bounds coincide up to numerical precision (10^{-9}), that is, the relation between the min-entropy and the CHSH violation presented in Figure 2 is tight.

Using the same method, it is also possible to find a relation between the Bell violation I and the local min-entropy, defined by $H_\infty(A|X) = -\log_2 \max_{a,x} P(a|x)$, where $P(a|x) = \sum_b P(ab|xy)$ is the marginal probability distribution of Alice's system. Note that the local min-entropy gives a lower bound on the global min-entropy, since $H_\infty(AB|XY) \geq H_\infty(A|X)$.

In the case of the CHSH inequality, we are able to obtain the following tight analytical lower bound (see Figure 2):

$$H_\infty(A|X) \geq 1 - \log_2\left(1 + \sqrt{2 - \frac{I^2}{4}}\right). \tag{A.3}$$

To derive the above bound we use the fact that the in the case of the CHSH inequality (two in-

puts with binary outcomes), it is sufficient to consider measurements on a two-qubit system [6] of the form $|\Psi_\theta\rangle = \cos\theta|00\rangle + \sin\theta|11\rangle$. For a given state $|\Psi_\theta\rangle$, one can then easily compute both $P_\theta^* = \max_{a,x} P_\theta(a|x) \leq \cos 2\theta$, and using the Horodecki criterion [7], the maximal CHSH violation $I_\theta \leq 2\sqrt{1 + \sin^2\theta}$. The region that is accessible to quantum theory, is then given by the convex hull of the above set of points when we let $0 \leq \theta \leq \pi/4$. This corresponds to the region characterized by the inequality $P(a|x) \leq \frac{1}{2}\left(1 + \sqrt{2 - I^2/4}\right)$, which implies Eq. (A.3). The above bound is tight because it is possible to achieve simultaneously $P_\theta^* = \cos 2\theta$ and $I_\theta = 2\sqrt{1 + \sin^2\theta}$ with the same set of measurements on the state $|\Psi_\theta\rangle$.

A.2   Randomness produced by Bell devices used n times in succession

To apply the results of the previous section to the experimental data produced by devices that violate a Bell inequality, one has first to estimate the Bell violation. This requires to use the devices a large number n of times in succession. In full generality, one cannot assume, however, that the devices behave identically and independently at each use. For instance, they may have an internal memory, so that what happens at the ith use of the devices depends on what happened during the $i - 1$ previous uses. The results derived in the previous section must therefore be combined with a statistical approach that takes into account such memory effects. We carry out this analysis below and show how the randomness produced by the devices can be quantified and determined experimentally without making any particular assumptions about their internal behaviour.

We thus suppose that we have devices that violate a Bell inequality. The devices are used n times in succession. We denote by $x_i, y_i \in \{1, \ldots, m\}$ the measurement inputs and by $a_i, b_i \in \{1, \ldots, d\}$ the measurements outputs at round i. We denote by $a^k = (a_1, a_2, \ldots, a_k)$ the string of the first k outputs a_i, and we define similarly b^k, x^k, and y^k. We suppose that the input pairs (x_i, y_i) at round i are independent and identical random variables with distribution $P(x_i = x, y_i = y) = P(x, y)$. Note that in general $P(x, y)$ may not be a product distribution $P(x, y) = P(x)P(y)$.

Let $P_{R|S} = \{P(a^n b^n | x^n y^n)\}$ be the probability distribution of the final output string $r = (a^n, b^n)$ given the fact that the sequence of inputs $s = (x^n, y^n)$ has been inserted in the devices. Similarly to the single-copy case, the randomness of the output string conditioned on the inputs can be characterized by the min-entropy $H_\infty(R|S) = -\log_2 \max_r P(r|s) = \min_{a^n b^n} (-\log_2 P(a^n b^n | x^n y^n))$. We derive here a lower bound on $-\log_2 P(a^n b^n | x^n y^n)$ valid for all $(a^n b^n)$ and (x^n, y^n). This implies a lower bound on $H_\infty(R|S)$, as $H_\infty(R|S) \geq -\log_2 P(a^n b^n | x^n y'$

We start with the identities

$$
\begin{aligned}
-\log_2 P(a^n b^n | x^n y^n) &= -\log_2 \prod_{i=1}^{n} P(a_i b_i | a^{i-1} b^{i-1} x^i y^i) \\
&= -\log_2 \prod_{i=1}^{n} P(a_i b_i | x_i y_i W^i) \qquad \text{(A.4)} \\
&= \sum_{i=1}^{n} -\log_2 P(a_i b_i | x_i y_i W^i)
\end{aligned}
$$

The first equality follows from Bayes rule together with the fact that the response of the system at round i does not depend on future inputs (x_j, y_j) with $j > i$. In the second equality, we introduced the variable $W^i = (a^{i-1} b^{i-1} x^{i-1} y^{i-1})$ to denote all events in the past of round i. The behaviour of the devices at round i conditioned on the past is characterized by a response function $P(a_i b_i | x_i y_i W^i)$ and a Bell violation $I(W^i)$. Whatever be the precise form of the quantum state and measurements implementing this behaviour, they are bound to satisfy the constraint $-\log_2 P(a_i b_i | x_i y_i W^i) \geq f(I(W^i))$, as required by (A.1). Inserting this relation into Eq. (A.4), we obtain

$$
\begin{aligned}
-\log_2 P(a^n b^n | x^n y^n) &\geq \sum_{i=1}^{n} f\left(I(W^i)\right) \\
&\geq n f\left(\frac{1}{n} \sum_{i=1}^{n} I(W^i)\right) \qquad \text{(A.5)}
\end{aligned}
$$

where we used the convexity of the function f to deduce the second inequality. We now show that the quantity $\frac{1}{n} \sum_{i=1}^{n} I(W^i)$ can be estimated with precision using only the information coming from the input and output strings observed in the experiment.

Let $\chi(e)$ be the indicator function for the event e, i.e. $\chi(e) = 1$ if the event e is observed, $\chi(e) = 0$ otherwise. Consider the random variable

$$
\hat{I}_i = \sum_{abxy} c_{abxy} \frac{\chi(a_i = a, b_i = b, x_i = x, y_i = y)}{P(x, y)}, \qquad \text{(A.6)}
$$

which is chosen so that its expectation conditioned on the past W^i is equal to $E(\hat{I}_i | W^i) = I(W^i)$. We define $\hat{I} = \frac{1}{n} \sum_{i=1}^{n} \hat{I}_i$ as our estimator of the Bell violation. In the case of the CHSH inequality, it is readily verified that (A.6) correspond to the expression (2) given in the main text. Let $q = \min_{xy}\{P(x, y)\}$ and let us assume that $q > 0$ (that is, we assume that each possible pair of inputs (x, y) has a non-zero probability to be chosen). Let us introduce the random variables $Z^k = \sum_{i=1}^{k} (I_i - I(W^i))$. It can be verified that (i) $E(|Z^k|) < \infty$, and that (ii) $E(Z^k | W^1, \ldots, W^j) = E(Z^k | W^j) = Z^j$ for $j \leq k$. Thus the sequence $\{Z^k : k \geq 1\}$ is a

martingale[1] [10] with respect to the sequence $\{W^k : k \geq 2\}$.

The range of the martingales increment are bounded by $|I_i - I(W^i)| \leq \frac{1}{q} + I_q$, where I_q is the highest possible violation of the inequality I allowed by quantum theory. We can therefore apply the Azuma-Hoeffding inequality [10–13] $P(Z^n \geq \epsilon') \leq \exp\left(-\frac{\epsilon'^2}{2n(1/q+I_q)^2}\right)$, which implies that (with $\epsilon' = n\epsilon$)

$$P\left(\frac{1}{n}\sum_{i=1}^{n} I(W^i) \leq \frac{1}{n}\sum_{i=1}^{n} I_i - \epsilon\right) \leq \delta, \qquad (A.7)$$

where

$$\delta = \exp\left(-\frac{n\epsilon^2}{2(1/q + I_q)^2}\right). \qquad (A.8)$$

Thus the sum of the Bell expressions $\frac{1}{n}\sum_{i=1}^{n} I(W^i)$ can be lower than the observed value $\hat{I} = \frac{1}{n}\sum_{i=1}^{n} I_i$ up to some ϵ only with some small probability δ. Combining this last result with Eq. (A.5), we conclude that

$$H_\infty(R|S) \geq -\log_2 P(a^n b^n | x^n y^n) \geq nf\left(\hat{I} - \epsilon\right) \qquad (A.9)$$

with probability at least $1 - \delta$.

A.3   Bounds using no-signalling only

As mentioned in the main text, it is also possible to prove lower bounds on the min-entropy of the form Eq. (A.1), but where we impose rather than the full quantum formalism only the no-signalling conditions. That is, we impose that the measurement outcomes produced by the devices cannot be used for arbitrary fast communication, even at a hidden level. We are thus led to a new optimisation problem, which replaces the optimisation problem Eq. (A.2) we studied

---

[1]A martingale is a stochastic process (i.e., a sequence of random variables) such that the conditional expected value of an observation at some time k, given all the observations up to some earlier time j, is equal to the observation at that earlier time j. This causality constraint — expressed formally by condition (ii) above — is very strong, and it implies that in some respects martingales behave like sums of independent variables. In particular, if the martingale increments (from time k to the time $k + 1$) are bounded, they obey a large deviation theorem, the Azuma-Hoeffding inequality, which we use to derive Eq. (A.7). Martingales were introduced in quantum information in the context of Bell tests in order to show that having an internal memory of past events is only of marginal help to local models [8, 9]. Here we use the theory of martingales in the context of randomness generation to show that the same device can be used n times in succession without significantly changing the rate of randomness generation with respect to the mathematically simpler but impractical case where n independent devices are used in parallel.

previously:

$$P^*(ab|xy) = \max \quad P(ab|xy)$$
$$\text{subject to} \quad \sum_{abxy} c_{abxy} P(ab|xy) = I$$
$$P(ab|xy) \geq 0,$$
$$\sum_{ab} P(ab|xy) = 1, \quad \text{(A.10)}$$
$$\sum_{a} P(ab|xy) = P(a|x),$$
$$\sum_{b} P(ab|xy) = P(b|y),$$

where the last two equalities are the no-signalling conditions. Solving (A.10) (which can be done using linear programming), one deduces a bound of the form $P^*(ab|xy) \leq \alpha I + \beta$, where in full generality α and β may depend on a, b, x, y. This follows from the fact that the constraints in eq. (A.10) define a polytope.

In analogy to Eq. (A.3), one could also consider the maximum of $P(a|x)$ subject to the conditions enumerated in Eq. (A.10), which we denote $P^*(a|x)$. In this case also the maximum is bounded by a finite set of linear inequalities.

In the case of the CHSH expression, the relevant inequalities are:

$$P^*(a|x) = P^*(ab|xy) \leq \frac{3}{2} - \frac{I}{4} \quad \text{(A.11)}$$

This follows easily by recalling that the extremal points of the no-signalling polytope when $a, b, x, y \in \{0, 1\}$ fall into two classes, the deterministic points for which $P(ab|xy) \leq 1$ and $I = \pm 2$, and the Popescu-Rohrlich boxes for which $P(ab|xy) \leq 1/2$ and $I = \pm 4$. This in turn immediately implies a bound of the form eq. (A.3):

$$H_\infty(AB|XY) \geq -\log_2\left(\frac{3}{2} - \frac{I}{4}\right) . \quad \text{(A.12)}$$

Using this bound, one can now apply directly all the results presented in section A.2 to obtain a bound on the min-entropy when the devices are used n times in succession. The only modification is that in Eq. (A.8), the maximal possible violation I_q of the Bell inequality allowed by quantum theory, must be replaced by the maximal possible violation I_{ns} allowed by no-signalling.

B Quantum randomness expanders

We now discuss how the results that we have just derived can be used in the context of randomness expansion. Relations between randomness and Bell inequality violations have been discussed in different contexts in several works, see for instance [14–16]. In his PhD thesis [17], Colbeck proposed to exploit this connection for the task of private randomness generation and formalized this idea concretely. Moreover, he introduced a protocol for randomness

expansion based on Greenberger-Horne-Zeilinger (GHZ) multipartite pure-state correlations. Following [17], we define quantum private randomness expansion (QPRE) as a single-party task where a user, Alice, expands a small random initial seed[2] into a larger string which is close to uniformly random, even when conditioned on the information of a potential quantum adversary. In detail QPRE is realised as follows:

1. The setting: Alice has a pair of devices, each of which has m inputs and can produce d outputs. We assume that Alice starts the protocol with an initial private random seed $t = (t_1, t_2)$ divided in two strings t_1 and t_2. At the beginning of the protocol, Alice also chooses a security parameter δ that bounds the probability with which an adversary can cheat.

2. Use of the devices: Alice uses the string t_1 to generate pairs of inputs $s = (x_1, y_1; \ldots; x_n, y_n)$. Every pair is generated independently with a probability distribution $P(x, y)$. Alice then introduces the inputs (x_i, y_i) in her devices and obtains the outputs (a_i, b_i); she repeat this last step n times for $i = 1, \ldots, n$.

3. Evaluation of the min-entropy: from the final input and output strings $s = (x_1, y_1; \ldots; x_n, y_n)$ and $r = (a_1, b_1; \ldots a_n, b_n)$ Alice computes $\hat{I}$ (see (A.6)), and from the chosen value for the security parameter δ, Alice computes ϵ (see (A.8)). From these values Alice then computes the bound (A.9) on the min-entropy $H_\infty(R|SE)$ of the raw output string r.

4. Randomness extraction: Alice uses a randomness extractor[3] and the string t_2 to convert the raw string r into a slightly smaller string $\bar{r}$ of size $O(nf(\hat{I} - \epsilon))$ which is close to uniform and uncorrelated to the adversary's information.

The final random string $(t, \bar{r})$ of Alice is clearly longer than the initial string t provided that the bound on the entropy $H_\infty(R|SE)$ is strictly positive. However, when the number n of uses of the devices is sufficiently large, it is possible to start from an initial seed of length $O(\sqrt{n} \log_2 \sqrt{n})$ to produce a much longer final string of length $O(n)$. Indeed, if Alice selects one of the d^2 possible input pairs (x, y) with probability $1 - (d^2 - 1)q$ and the remaining $d^2 - 1$

---

[2]Any device-independent random number generation protocol must necessarily use an initial random seed. Indeed, if Alice follows a deterministic procedure, then there exists a predetermined set of measurement outcomes that will pass all the tests performed by Alice, and the adversary can simply provide devices that generate these classical outputs. Thus the fact that we need an initial random seed is not a weakness of our scheme but a necessity inherent to the concept of device-independent RNG itself.

[3]Randomness extractors are classical functions that take as input a small uniform random string t_2 and a much longer string whose min-entropy is lower bounded by H_∞, and produce as output a string of length H_∞ which is nearly uniform.

ones with probability q, with q small, the randomness required to generate the inputs is then equal to $nO(-q\log_2 q)$. Taking $q = O(1/\sqrt{n})$, the initial random seed t_1 must thus be of length $O(\sqrt{n}\log_2\sqrt{n})$. The randomness of the raw string r, on the other hand, is given by (A.9) where ϵ is of order $O(1)$. For fixed Bell violation $\hat{I}$, the output entropy is thus linear in n. The raw string r can then be transformed into the fully secure random string $\bar{r}$ using a randomness extractor with the help of a small random seed t_2, say of length $O(\text{poly}\log n)$ [18]. This shows that it is possible to construct device-independent QPRE producing $O(n)$ random bits from an initial seed of total length $O(\sqrt{n}\log_2\sqrt{n})$.

The security of this protocol only holds for the moment against quantum adversaries that measure their quantum side-information before the randomness extraction step. That our analysis holds in this situation follows from the fact that when the adversary performs a measurement on his system, the outcome that he obtains amounts to the preparation of Alice's devices in some particular state. But the bound (A.9) is independent of the way in which the devices have been prepared and thus also holds when conditioned on the outcome of the adversary's measurement.

Our protocol is thus not yet proven to be universally-composable against a full quantum adversary, that is, secure against an adversary that stores his side-information in a quantum memory which can be measured at a later stage. A universally-composable proof would cover the situation in which the adversary tries to estimate the random numbers after getting partial information about them. To obtain a full universally-composable proof of security of our QPRE protocol, a bound on the entropy of the raw string conditioned on the quantum information of an adversary must be derived. Such a bound could then be used in a randomness extraction procedure secure against a fully quantum adversary [19].

Proving universally-composable security of our protocol might also open the possibility of more elaborated protocols where Bell violating devices are used in a concatenated way: the random string produced by a first device is used as seed for a second device, whose input is in turn used as seed for the first and so on. Such more complex solutions could lead to much more efficient QPRE devices. Related to this efficiency question, we note that the results of [20] and [21] imply that exponential randomness expansion, i.e., the generation of an output random string of size $O(n)$ starting from a seed of size $O(\text{poly}\log n)$, is possible in the situation where the devices have no classical or quantum memory. Note, however, that the fact that our bound (3) holds for devices that have an internal memory is the crucial feature that makes our protocol practical. It would be interesting to show that exponential randomness expansion is also possible in this situation.

Finally, we mention that although we focused here our theoretical analysis on a bipartite protocol (which is easier to implement in practice), our theoretical approach can also probably be generalized to compute a bound on the randomness produced by the randomness expansion protocol based on GHZ multipartite correlations introduced in [17].

C   Requirements on the devices

In this section, we discuss the requirements that are necessary to generate random numbers certified by a Bell inequality violation and clarify the concept of device-independence. We also discuss these requirements in the context of the security of the QPRE task and in the context of our experimental demonstration.

We recall that the QPRE system is composed of two devices, referred to in the follows as device A and device B. The derivation of the min-entropy bound (3) rests on the following assumptions.

1. *Quantum-theory: The two devices behave according to quantum theory.*
   That is when an input x (y) is introduced in a device, an output a (b) is produced according to some quantum process.

2. *Input randomness: The inputs x_i, y_i at round i are generated by random processes that are independent and uncorrelated from the devices and their values is revealed to the devices only at round i.*
   This guarantees that the behaviour of the devices at round i does not depend on the values of the inputs used in later rounds, i.e., that the following condition is satisfied

$$P(a_i b_i | x_i y_i \ldots x_n y_n W^i) = P(a_i b_i | x_i y_i W^i) \, , \qquad \text{(C.1)}$$

   where W^i denotes, as in Section A.2, all events in the past of round i. This condition is used in the first line of Eq. (A.4).

3. *Locality: From the moment that the inputs are introduced until the outputs are produced, the two devices are separated and no signal (quantum or classical) can travel from one device to the other. Moreover, the input x is introduced only in device A and the input y only in device B.*
   This assumption ensures that the Hilbert space describing the two devices factorizes as a tensor product and that the measurement operators act on each factor in a way that depends only on the corresponding local input. That is, that the probabilities characterizing

a single-run of the experiment are of the form

$$P(ab|xy) = \text{tr}\left(\rho M_x^a \otimes M_y^b\right) . \tag{C.2}$$

This mathematical condition is used in the optimization problem (A.2) in Section A.1.

When the above three conditions are satisfied, the min-entropy bound (3) derived in Section A follows without additional assumptions on the quantum states, the measurements, the dimension of the Hilbert space, or any other aspects concerning the internal working of the quantum devices. This is what we refer to as *device-independence* — the fact that the min-entropy bound or the security proof does not depend on a model of the devices.

The conditions listed above represent minimal requirements to apply the device-independence proof in practice: if one of them is not satisfied then it is no longer possible to guarantee the presence of randomness through the violation of a Bell inequality [4]. Whether these conditions are verified in an implementation is therefore an important question. However, it is not a question that has a unique and well-defined answer. Depending on the application, the adversarial scenario under consideration, and our level of "trust" in the devices, there may be different ways to enforce these conditions or verify that they are satisfied. As an illustration, we discuss below three possible ways to ensure that condition 3 is satisfied: i) by imposing space-like separation between the measurement devices; ii) by shielding the devices; iii) by proper design of the setup.

i) Strict space-like separation. Condition 3 states that the devices should be separated and non-interacting during the measurement process. Obviously strict space-like separation between the devices could be used to enforce this separability condition. This space-like separation is required to close the locality loophole in standard Bell tests, where the objective is to disprove alternative theoretical models of Nature that can overcome the laws of physics as they are currently known. Here, however, we assume from the beginning the validity of quantum theory and we use Bell inequalities not as a test of hidden variable models but as a tool to quantify the randomness of quantum theory. Once we assume quantum theory, they are many ways to ensure that the two systems are not interacting other than placing them in space-like intervals, e.g. by shielding the devices as discussed below in point ii).

---

[4]Note that although these three conditions are necessary and that we cannot go completely without them, they can probably be weakened at the expense of the randomness generation rate. This is clear for the first assumption, as we have seen in Section A.3 that the validity of quantum theory can be replaced by the no-signalling principle. But it might also be possible to weaken the two other assumptions and show that Bell-violating devices can generate randomness even if they have a limited amount of prior information about the future inputs or if they can exchange some limited communication.

The view that there is no satisfying way to prevent information from being exchanged between two systems except by strict space-like separation is very conservative. The main problem with this level of paranoia is that it makes cryptography impossible. Indeed, a basic assumption behind all cryptography (classical or quantum) is that users must be confident that information cannot leak out of their location, devices, computers, etc. If the only constraints on the flow of information are those which follows from special relativity, cryptography becomes impossible: any secret bit or key inevitably leaks out to the adversary at the speed of light as soon as produced.

The space-like separation approach may be relevant for non-cryptographic applications of random numbers, where privacy is not an issue, such as Monte Carlo algorithms. Its main advantage is that the condition (C.2) follows immediately. A secondary point to take into account in this approach, however, is that the inputs x and y must be generated locally and immediately before being introduced into the devices, so that they are prevented from knowing the other device's input[5].

Note that space-like separation is essential to test more fundamental implications of our results, such as the compatibility between determinism and no-signalling mentioned at the end of the paper.

ii) Shielding of the devices. Here, condition 3 is enforced by separating and shielding the devices and the relevant part of the laboratory. This view is consistent with the known forces in physics which are either extremely weak (gravity), short range (weak and strong force), or can be screened by conductors (electro-magnetic force). Note that the shields must have doors with allow the boxes to interact with the external world (dotted lines in Figure 1). The doors must allow both classical and quantum information through, to let the devices establish shared entanglement, receive the inputs x, y, and produce the outputs a, b.

The assumption that laboratories and devices can be adequately shielded against unwanted leakage of information is implicit in all of cryptography. From the basic cryptographic requirement that the two devices can be adequately shielded so that they do not send information to the adversary, it is only a small extra step to require that they can also be adequately shielded so that they cannot signal to each other. It would be very artificial to assume that the devices

---

[5]This implies that the inputs must be generated with a product probability distribution $P(x, y) = P(x)P(y)$. In particular, the joint input distribution cannot be of the form $P(00) = 1 - 3q, P(01) = P(10) = P(11) = q$ which leads to the quadratic catalysis effect discussed in the previous Section and illustrated in Figure 3. A weaker catalysis effect is nonetheless possible if each individual input is chosen with probabilities $P(0) = 1 - q, P(1) = q$, resulting in the joint probability $P(00) = (1 - q)^2, P(01) = P(10) = q(1 - q), P(11) = q^2$. Taking $q^2 = O(n^{1/4})$, we find that ϵ in Eq. (A.9) is of order $O(1)$, and thus that the output randomness is of order $O(n)$. The randomness consumed at the inputs, on the other hand, is $nO(-q \log_2 q) = O(n^{3/4} \log_2 n^{1/4})$.

are not able to communicate to the adversary, an essential requirement for any cryptographic application, but can communicate between each other.

The main disadvantage of this approach is that we are making a technological assumption. One can never completely rule out that the shielding is sufficient. Particular attention would have to be paid to this point if it is an adversary that has provided the devices.

iii) Proper design of the experiment. We may have a good confidence that condition 3 is satisfied simply based on a proper design and superficial description of the devices. For instance in the experiment reported here we are using two atoms that are confined in two independent vacuum chambers separated by about 1 meter. At this distance, direct interaction between the atoms is negligible and classical microwave and optical fields used to perform measurements on one atom have no influence on the other atom. Based on this superficial description of the setup, we can safely assume that we are dealing with two independent quantum systems and that the general formalism used to derive our bound applies[6].

Obviously, this approach is insecure in the adversarial scenario where the devices are untrusted and assumed to be prepared by an adversary, in which case it is necessary to take active measures to control the flow of information in and out of the devices, as in point ii) above. The application of the concept of device-independence, however, is not restricted to this strong adversarial scenario with untrusted devices. It may be perfectly legitimate to assume that the devices have been built in good faith and that they do not contain any sneaky component sending unwanted signals (we must anyway trust the classical computers, devices, etc., used to analyze the data). The problem, however, is that it is very difficult, even for honest parties, to construct reliable random number generators. The theoretical modeling of the physical process at the origin of the randomness source is often incomplete and relies on assumptions which may be very difficult to confirm. This makes an accurate estimation of the entropy produced by the devices difficult. Most RNGs break silently, often producing decreasingly random numbers as they degrade. Failure modes in such devices are plentiful and are complicated, slow, and hard to detect. Imperfections can introduce patterns undetected by statistical tests but known to an adversary. The generation of randomness in a device-independent way (that is without detailed modeling of the devices) solves all these shortcomings of traditional random number generators: the violation of a Bell inequality provides a bound on the randomness produced by

---

[6]At first sight a better way to implement our proposal experimentally would be to use two ions in the same trap, as in [22], as data rates orders of magnitude higher can be achieved. But in this case we cannot assume that the two ions are separate and non interacting without modeling the details of the experiment. Indeed the ions are at all times strongly coupled through the vibrational modes of the cavity, and furthermore the measurements cannot be assumed to act on each ion separately as they are separated by a few microns, comparable to the wavelength of light used for readout.

the devices, independently of any noise, imperfections, lack of knowledge, or limited control of the apparatuses.

Considerations similar to the above ones can be made for the second condition in our list of assumptions, i.e., the requirement that the inputs should be chosen in a way that appears "random" to the devices. In our experiment, the value of the chosen measurement bases (x_i, y_i), obtained by combining the outputs of several (public) random number generators, is unlikely to be correlated to the state of the atoms before the measurement microwave pulses are applied, and we can safely assume that Eq. (C.1) is satisfied. Of course in a strong adversarial scenario where the devices are untrusted, the adversary could exploit a prior knowledge of the inputs in the design of the devices. In this case, it is thus important to generate the inputs with a private random source.

Finally, it is tacit, but obvious, that the implementation should conform to the theoretical description detailed in Section B. For instance, in the case of the CHSH inequality, we consider devices that produce binary outcomes $a, b \in \{0, 1\}$ and use all the raw data produced over the n runs of the experiment in our analysis. In photonic Bell tests, detectors have low efficiencies, and device often produce a no-event outcome $\perp$ corresponding to the absence of a click, i.e., $a, b \in \{0, 1, \perp\}$. This leads to the famous detection loophole which is circumvented by applying a post-selection to the observed data. This represents a departure from our description and our results can therefore no longer be applied in this case. In our experiment, this problem is not an issue, as every event is recorded.

More generally, it is straightforward that a Bell violation without closing the detection loophole (or other loopholes arising from post selection, such as the coincidence time loophole [23]) cannot be used to certify randomness generation. In a scenario where the devices are trusted, one could address this requirement by means of the fair sampling assumption, which states that the detected events represent a fair sample of all the events (including the undetected ones). However, making the fair sampling assumption requires a detailed knowledge of the devices, and could fail without one being aware of it (see also attacks based on the detection loophole in traditional QKD [24, 25].).

D Experiment

D.1 Experimental system

Individual $^{171}\text{Yb}^+$ atomic ions are stored in two rf Paul traps located in two independent vacuum chambers separated by about 1 meter and placed in the magnetic field of 3.4 G that defines the quantization axis. We encode qubits in the $F = 1, m_F = 0$ and $F = 0, m_F = 0$ hyperfine levels

of the $S_{1/2}$ ground state of each atom, denoted by $|1\rangle$ and $|0\rangle$, respectively. Each experimental sequence begins with a 1 μs optical pumping pulse and 10 μs microwave pulse that prepares each atom in the $|0\rangle+|1\rangle$ state. Next, a fast laser pulse linearly polarized along the direction of magnetic field excites both ions to the $P_{1/2}$ state with a probability close to unity. If the atoms each return to the ground state by emission of a π-polarized photon, the frequency of the emitted photons are entangled with the atomic qubit states. With a small probability, both photons are collected from each atom and interfered on a 50:50 beamsplitter, with polarizing filters selecting only π-polarized light. Detection of coincident photons behind the beamsplitter heralds the preparation of the entangled state of the two atoms: $|0\rangle|1\rangle - e^{i\chi}|1\rangle|0\rangle$ [26, 27]. The experiment is repeated at 95 kHz, but due to finite collection and detection efficiency of the photons, we observe on average only 1 entanglement event every 8 minutes. Given a successful entanglement event, we finally detect each qubit in measurement bases determined by the input variables x and y [28]. Before measurement, microwave pulses with a controlled phase and duration resonant with the $|0\rangle \rightarrow |1\rangle$ transition rotate each atomic qubit through a polar angle of $\pi/2$ on the Bloch sphere. The phase difference $\varphi_x - \varphi_y$ between the rotations on the two atoms is adjusted with respect to the phase χ of the entangled state so that the qubits are appropriately rotated for a Bell inequality violation [29]. Finally, each atom is illuminated with laser light resonant with the $S_{1/2}$ $F = 1 \rightarrow P_{1/2}$ $F = 0$ transition, and the $|1\rangle$ state fluoresces strongly while the $|0\rangle$ state is nearly dark, resulting in a detection of each qubit state with 98.5% accuracy [28].

D.2 Generation of measurement settings

The measurement settings were chosen by combining several online random number generators that use: radioactive decay as a source of randomness [30]; atmospheric noise as a source of randomness [31]; and randomness derived from remote computer and network activity [32]. We requested 128 bytes (corresponding to 32 integer numbers) from each of these generators and combined them using XOR function. This procedure should produce measurement settings that are independent and uniform. Indeed the measurement settings were tested to ascertain that they did not contain any obvious bias (see Appendix D.4).

Before every entanglement event the two least significant bits of one of the above integer numbers was transmitted to the FPGA board that controls our experimental time sequence. After a two photon coincidence event the board applies microwave pulses to both ions with a phase that depends on the measurement setting it obtains from the computer, counts the number of photons during ions state detection, transmits the state detection results and the measurement settings it used back to the computer, and receives new measurement settings

for the next entanglement event. When the number of available random numbers in the buffer approaches 0, a new block of random numbers is requested from the random number generators and added to the buffer.

D.3   Comparison with local causality

The usual interpretation of the experimental violation of a Bell inequality is that the observed correlations cannot be reproduced by a local model [33]. This should be properly expressed as a statistical statement. Here we follow the approach of [8, 9] (see also Section A.2) to derive the relevant statement.

We consider the quantity I_i defined in Eq. (A.6), and focus on the CHSH inequality with uniform choice of settings ($P(xy) = 1/4$). We denote by the superscript l the predictions of local theories.

Let us consider the predictions of local theories. In this case we have $-2 \leq E(I_i^l(W^i) = I^l(W^i)) \leq 2$. The random variables $Z^k = \sum_{i=1}^{k} \left(\hat{I}_i - I^l(W^i) \right)$ are a martingale with respect to the sequence $\{W^k : k \geq 2\}$. The range of the martingales increments are bounded by $\left| \hat{I}_i - I^l(W^i) \right| \leq 4 + 2 = 6$, where the 4 comes from the possible range of $\hat{I}_i$ and the 2 comes from the range of $I^l(W^i)$. Applying the Azuma-Hoeffding inequality then implies that the probability that a local deterministic theory will yield a violation greater or equal than the observed violation $\hat{I} = \frac{1}{n} \sum_{i=1}^{n} I_i$ is bounded by:

$$P(\frac{1}{n} \sum_{i=1}^{n} I^l(W^i) \geq \hat{I}) \leq \exp\left(-\frac{n\left(\hat{I} - 2\right)^2}{72} \right). \tag{D.1}$$

This inequality holds for all local models (even if they can exploit an internal memory that remembers past measurement settings and past outputs) which attempt to violate the CHSH inequality (with the measurement settings uniformly distributed). Inserting the data from our experiment (Table 1) shows that the probability that the measurement results could have been produced by a local model is less than 0.000767.

D.4   Statistical tests

As a check of consistency and of the quality of our experiment, we verified that the bit strings $(x_1, y_1; \ldots; x_n, y_n)$ used as measurement settings and the bit strings $a_1, b_1; \ldots; a_n, b_n$ produced as outputs did not reveal any obvious non-random pattern using a standard battery of statistical tests [34–36]. However, those batteries were originally designed for sequences containing millions of bits. As the strings we consider contain several thousands of bits, only the tests statisti-

cally relevant for such small strings were performed. Specifically the tests called "Frequency", "Block frequency", "Runs", "DFT", "Serial" and "Approximate Entropy" were reprogrammed from [35] (sections 2.1, 2.2, 2.3, 2.6, 2.11, 2.12) and the tests called "Two-bit" and "Poker" were reprogrammed from [36] (section 5.4.4.).

The result of these statistical tests are described by a p-value, which is the probability that a perfect random number generator would have produced a sequence less random than the sequence that was tested, given the kind of non-randomness assessed by the test. A p-value of 1 therefore means that the sequence tested appears to have been generated by a perfectly random process, while a p-value of 0 implies that the sequence appear to be completely non-random [35]. Together with computing the p-value, a significance level α should be chosen for the tests. If the p-value $\geq \alpha$, then the hypothesis that the sequence appears to be random is accepted. If the p-value $< \alpha$, then this hypothesis is rejected, i.e., the sequence appears to be non-random. Typical values for α are in the range [0.0001, 0.01] and we choose α =0.001. An α of 0.001 indicates that one would expect one sequence in 1000 sequences to be rejected by the test if the sequence was generated by a perfect random number generator. For a p-value $\geq$ 0.001, a sequence would be considered to be random with a confidence of 99.9%. For a p-value < 0.001, a sequence would be considered to be non-random with a confidence of 99.9% [35].

The results of these statistical tests (given by the p-value) evaluated on our data are given in Table 2. As in Section A.2, we use the notation $x^n = (x_1, ..., x_n)$, $a^n = (a_1, ..., a_n)$ for the settings and outputs for the first ion; and $y^n = (y_1, ..., y_n)$, $b^n = (b_1, ..., b_n)$ for the settings and outputs for the second ion. Each of these strings contains $n = 3016$ bits and the combination $(a_1, b_1, ..., a_n, b_n)$ contains therefore 6032 bits.

As we see from the data in Table 2, the input string $x^n y^n$ passes all the tests since the p-values are larger than the chosen significance level α =0.001. This is expected as the random number generators we used have already been extensively tested. The outputs strings a^n and b^n taken separately also pass all the tests. This confirms that the experiment performed well and did not have any important internal bias. Finally, as expected, if all the outputs are grouped into the combination $(a_1, b_1, ..., a_n, b_n)$, then the results do not pass the tests because the measurement outputs on the two atoms are correlated and thus are not independent random variables.

Note that the general theory described in this paper guarantee that the measurement outputs contain at the 99% confidence level 42 new random bits, independently of any hypothesis on how the experiment was realised. This is a much stronger statement than passing or not passing the statistical tests mentioned above, which merely indicate that no obvious non-random patterns are present in the measurement outputs.

Statistical test	$x^n y^n$	a^n	b^n	$(a_1, b_1, ..., a_n, b_n)$
Frequency	0.9795	0.7988	0.0743	0.1493
Block Frequency	0.2668	0.5540	0.0592	0.1360
Runs	0.6616	0.2904	0.4312	0.0000
DFT	0.8542	0.3096	0.8686	0.3081
Serial	0.1681	0.1300	0.0119	0.0000
Approximate Entropy	0.2445	0.5568	0.0130	0.0000
Two Bit	0.9024	0.5699	0.1579	0.0000
Poker	0.0189	0.1933	0.0353	0.0000

Table 2: Results of the statistical tests given by the p-values evaluated on the measurement settings, the outputs of one atom and the other taken separately, and the outputs of the two atoms taken together.

To verify that the atoms did not influence each other during the measurement in an obvious way, we also performed statistical tests to check that the data reported in Table 1 in the main text are compatible with the no-signalling conditions given in Eq. (A.10). There are 4 no-signalling conditions to check. In each case we performed a two-sided Fisher's test. We found p-values of 0.7610; 0.7933; 0.7933; 0.2867 which show that the data are compatible with the no-signalling hypothesis.

References

[1] Navascues, M., Pironio, S. & Acin, A. A convergent hierarchy of semidefinite programs characterizing the set of quantum correlations. *New Journal of Physics* **10**, 073013 (2008).

[2] Navascues, M., Pironio, S. & Acin, A. Bounding the set of quantum correlations. *Physical Review Letters* **98**, 010401 (2007).

[3] S. Pironio, M. Navascues, A, Acin, Convergent relaxations of polynomial optimization problems with non-commuting variables, arXiv:0903.4368 (2009).

[4] Sturm, J. SeDuMi, a MATLAB toolbox for optimization over symmetric cones. http://sedumi.mcmaster.ca.

[5] Löfberg, J. Yalmip : A toolbox for modeling and optimization in MATLAB. http://control.ee.ethz.ch/ joloef/yalmip.php.

[6] Pironio, S. *et al.* Device-independent quantum key distribution secure against collective attacks. *New Journal of Physics* **11**, 045021 (2009).

[7] Horodecki, R., Horodecki, P. & Horodecki, M. Violating Bell inequality by mixed spin-1/2 states: necessary and sufficient condition. *Physics Letters A* **200**, 340 (1995).

[8] Gill, R. D. In Mathematical Statistics and Applications: Festschrift for Constance van Eeden, Lecture Notes-Monograph series, M. Moore, C. Leger, and S. Froda (Eds.), Hayward, Ca. Institute of Mathematical Statistics (2003).

[9] Gill, R. D. In Proc. of Foundations of Probability and Physics - 2, Ser. Math. Modelling in Phys., Engin., and Cogn. Sc., vol. 5, pp. 179-206 Vxj Univ. Press (2003).

[10] G. Grimmett and D. Stirzaker, Probability and Random Processes (Oxford University Press, Oxford, 2001).

[11] Hoeffding, W. Probability inequalities for sums of bounded random variables. *Journal of the American Statistical Association* **58**, 13 (1963).

[12] Azuma, K. Weighted sums of certain dependent random variables. *Tohoku Mathematical Journal* **19**, 357 (1967).

[13] N. Alon and J. Spencer, The Probabilistic Method. Series in Discrete Mathematics and Optimization. Wiley-Interscience, 2nd edition, 2000.

[14] Valentini, A. Signal-locality in hidden-variables theories. *Phys. Lett. A* **297**, 273 (2002).

[15] Conway, J. & Kochen, S. The free will theorem. *Found. of Physics* **36**, 1441 (2006).

[16] Barrett, J., Hardy, L. & Kent, A. No signaling and quantum key distribution. *Phys. Rev. Lett.* **95**, 010503 (2005).

[17] Colbeck, R. Quantum and Relativistic Protocols for Secure Multi-Party Computation. PhD Dissertation, University of Cambridge (2007).

[18] Nisan, N. & Ta-Shma, A. *Journal of Computer and System Sciences* **58**, 148 (1999).

[19] De, A., Portmann, C., Vidick, T. & Renner, R. Trevisan's extractor in the presence of quantum side information. ArXiv:0912.5514.

[20] Masanes, L. Universally composable privacy amplification from causality constraints. *Physical Review Letters* **102**, 140501 (2009).

[21] Hanggi, E., Renner, R. & Wolf, S. Quantum cryptography based solely on Bell's theorem. ArXiv:0911.4171.

[22] Rowe, M. A. *et al.* Experimental violation of a Bell's inequality with efficient detection. *Nature* **409**, 791–794 (2001).

[23] Larsson, J.-A. & Gill, R. Bell's inequality and the coincidence-time loophole. *Europhysics Letters* **67**, 707 (2004).

[24] Zhao, Y., Fred Fung, C.-H., Qi, B., Chen, C. & Lo, H.-K. Experimental demonstration of time-shift attack against practical quantum key distribution systems. *Physical Review A* **78**, 042333 (2008).

[25] Fred Fung, C.-H., Tamaki, K., Qi, B., Lo, H.-K. & Ma, X. Security proof of quantum key distribution with detection efficiency mismatch. *Quantum Information and Computation* **9**, 0131 (2009).

[26] Maunz, P. *et al.* Heralded quantum gate between remote quantum memories. *Physical Review Letters* **102**, 250502 (2009).

[27] Olmschenk, S. *et al.* Quantum teleportation between distant matter qubits. *Science* **323**, 486 (2009).

[28] Olmschenk, S. *et al.* Manipulation and detection of a trapped yb+ hyperfine qubit. *Physical Review A* **76**, 052314 (2007).

[29] Matsukevich, D. N., Maunz, P., Moehring, D. L., Olmschenk, S. & Monroe, C. Bell inequality violation with two remote atomic qubits. *Physical Review Letters* **100**, 150404 (2008).

[30] HotBits: Genuine random numbers, generated by radioactive decay. Available at: http://www.fourmilab.ch/hotbits.

[31] Random.org. Available at http://www.random.org.

[32] EntropyPool and Entropy Filter Home Page. Available at http://random.hd.org/index.html.

[33] Bell, J. S. *Speakable and Unspeakable in Quantum Mechanics: Collected Papers on Quantum Philosophy* (Cambridge University Press, 2004).

[34] The Marsaglia Random Number CDROM including the Diehard Battery of Tests of Randomness. Available at http://www.stat.fsu.edu/pub/diehard/ (2008).

[35] Rukhin, A. et al. A Statistical Test Suite for Random and Pseudorandom Number Generators for Cryptographic Applications. National Institute of Standards and Technology, Special Publication 800-22 Revision 1. Available at http://csrc.nist.gov/publications/PubsSPs.html (2008).

[36] A. Menezes, P. van Oorschot, S. Vanstone, Handbook of Applied Cryptography. CRC Press, 1996.