Device-independent randomness expansion against quantum side information

Wen-Zhao Liu1,2,3, Ming-Han Li1,2,3, Sammy Ragy4, Si-Ran Zhao1,2,3, Bing Bai1,2,3, Yang Liu1,2,3, Peter J. Brown4, Jun Zhang1,2,3, Roger Colbeck4, Jingyun Fan1,2,3,5, Qiang Zhang1,2,3, and Jian-Wei Pan1,2,3

The ability to produce random numbers that are unknown to any outside party is crucial for many applications. Device-independent randomness generation does not require trusted devices and therefore provides strong guarantees of the security of the output, but it comes at the price of requiring the violation of a Bell inequality for implementation. A further challenge is to make the bounds in the security proofs tight enough to allow randomness expansion with contemporary technology. Although randomness has been generated in recent experiments, the amount of randomness consumed in doing so has been too high to certify expansion based on existing theory. Here we present an experiment that demonstrates device-independent randomness expansion. By developing a Bell test setup with a single-photon detection efficiency of around 84% and by using a spot-checking protocol, we achieve a net gain of $2.57 \times 10^9$ certified bits with a soundness error of $3.09 \times 10^{-12}$. The experiment ran for 19.2 h, which corresponds to an average rate of randomness generation of 13,527 bits per second. By developing the entropy accumulation theorem, we establish security against quantum adversaries. We anticipate that this work will lead to further improvements that push device-independence towards commercial viability.

According to quantum theory, measurement outcomes are in general unpredictable, even to observers who possess quantum devices. Quantum processes have therefore been studied extensively as a source of randomness. In a typical quantum random number generator, the user relies on the device working in a particular way, for instance, by detecting single photons after they pass through a 50:50 beam splitter. Deviations in the device behaviour affect the randomness of the outputs and are difficult to detect. Furthermore, any real device will be too complicated to model in its entirety, which leaves open the possibility that an adversary can exploit a feature of the device outside the model, as has been seen in quantum key distribution. To circumvent this, device-independent protocols have been introduced, which are proven to be secure without any assumptions about the devices used. This leads to a substantially higher level of security because any problems caused by unmodelled features are removed.

Experimental device-independent randomness generation (DIRNG) has been improving at a rapid pace. Some previous studies required additional assumptions, and even the most advanced to date consumed more randomness than they generated. Therefore, randomness expansion, which is a quantum feature without classical counterpart, remained elusive and technically challenging. For example, with our previous experimental setup, almost 118,000 experimental hours (at a repetition rate of 200 kHz) would be required to achieve randomness expansion with the protocol presented below, putting it out of reach in practice.

In this Letter, we report the experimental realization of device-independent randomness expansion (DIRNE) with high statistical confidence, the success of which is based on substantial improvements on both the theoretical and the experimental sides. We derive a tighter bound on entropy accumulation in the randomness generation process and construct a photonic entanglement platform to violate the Clauser–Horne–Shimony–Holt (CHSH) inequality as much as possible. The significance of this work is twofold in that it advances both our understanding of randomness and our experimental quantum optical capabilities. Such improvements bring us closer to being able to realize a number of other critical quantum information tasks such as device-independent quantum key distribution.

The entropy accumulation theorem (EAT) provides relatively tight bounds on the amount of randomness that can be extracted against an adversary that is limited only by quantum theory. Roughly speaking, the EAT shows that in an $n$-round protocol that achieves a CHSH game score of $\alpha$, the amount of output randomness is lower-bounded by

$$\text{rand}_{\text{out}} \geq n h(\alpha) - \sqrt{n} v,$$

where $h(\alpha)$ is the worst-case von Neumann entropy of an individual round of the protocol with expected score $\alpha$, and $v$ is a correction factor accounting for the finite statistics. The score on round $i$ is $\frac{1}{2} (1 + (-1)^{A_i B_i} E(X_i, Y_i))$, where $A_i$ and $B_i$ are measurement outcomes and $X_i$ and $Y_i$ are measurement setting choices at the two sites, with $A_i, B_i, X_i, Y_i \in \{0, 1\}$ (Fig. 1). By using ideas from the improved EAT, we derive a tighter lower bound on the accumulated entropy (Methods). This allows us to use a spot-checking protocol to experimentally realize randomness expansion with a state-of-art experimental quantum optical technique.

We provide a conceptual drawing of our spot-checking device-independent protocol (Fig. 1) in which the assumptions are...
Fig. 1 | Conceptual sketch of the DIRNE protocol setup. The protocol (Box 1) takes place in a secure lab, which is shielded from direct communication to the outside. The lab contains two black-box devices that accept inputs and yield outputs from the binary alphabet (0, 1), and these can be shielded from communicating at will. In particular, we assume that the user can completely control the flow of classical communication in and out of these regions (indicated by the dashed lines). In our experiment, the secure lab contains two sites, Alice and Bob. They share a pair of entangled particles that may be distributed from a central station. (If we had good enough quantum storage, then all entanglement could be pre-shared.) Alice’s and Bob’s respective inputs are $X_i$ and $Y_i$, and their outputs are $A_i$ and $B_i$. The user also possesses a trusted classical computer (with which to process the classical data) and sources of initial randomness. In our experiment the initial randomness is shared using an extractor seed $R$ and three random number generators (RNGs) that determine the inputs to the devices. These RNGs output either 0 or 1, where the number in the box ($\gamma$ or 1/2) denotes the probability of 1. The central RNG determines the type of round ($T_i=1$ meaning test and $T_i=0$ meaning generate) and the peripheral RNGs determine the inputs if a test round is chosen. The final randomness output is denoted by $Z$.

The underlying idea is to check whether devices situated in a secure lab violate a Bell inequality; it is therefore important to ensure that the devices at both sites (labelled Alice and Bob) cannot signal to one another or to the outside of the lab. If a Bell inequality is violated while satisfying our assumptions, then the devices must be generating randomness, even relative to an adversary who may share entanglement with the devices. The generated randomness can be extracted by appropriate post-processing. In this protocol (Box 1), the initial randomness is required to decide whether a round is a test round, $T_i=1$ (with probability $\gamma$), or a generation round, $T_i=0$ (with probability $1-\gamma$). $T_i$ is then communicated to two separate sites (but not to the measurement devices). In a test round, an independent uniform random number generator at each site generates the input to each device to perform the CHSH game. A test round consumes 2 bits of randomness. In a generation round, the devices at the two sites are given the input ‘0’. Crucially, each measurement device learns only its own input and not whether a round was a test round or generation round.

We implement the protocol on a quantum optical platform (Fig. 2). Pairs of polarization-entangled photons with a wavelength of 1,560 nm are generated via spontaneous parametric down-conversion and are delivered through spatial optical paths to two sites where polarization-dependent measurements are conducted. Previously, and with space-like separation between Alice and Bob, this platform proved to be robust enough to realize loophole-free violation of a Bell inequality and DIRNG, in which the CHSH game scores $\omega$ violated the classical bound $\omega_{\text{class}}=3/4$ by 0.00027 (ref. 8). Under these conditions and with the same error parameters as elsewhere in this paper, it would take about $8.52 \times 10^{14}$ rounds of the experiment to witness randomness expansion according to our revised EAT theory (Extended Data Fig. 1a, open square). To go beyond this, in the present work we reduced the distance between Alice and Bob by replacing the fibre links with spatial optical paths to achieve single-photon detection efficiencies of $83.40\pm0.31\%$ for Alice and $84.80\pm0.31\%$ for Bob, which enables the detection loophole to be closed in the CHSH game. Following the spot-checking protocol, a biased quantum random number generator (QRNG) is used to decide whether to test or not. Its output $T_i$ is transmitted to Alice and Bob to determine whether to use the local unbiased QRNGs in each round. When $T_i=1$, the setting choices $A_i$ and $B_i$ are determined randomly, whereas when $T_i=0$, the local unbiased QRNGs are turned off and fixed measurements are made.

Before the start of the main experiment, a systematic experimental calibration is implemented and some calculations are performed to predetermine several parameters that are mentioned in the protocol. The calibration yielded a CHSH game score of 0.752487, and we compute that for $\gamma_{\exp}=3.393 \times 10^{-4}$, which corresponds to an average input entropy rate of $0.0049 \text{ bits per round}$, randomness expansion with a soundness error (Methods) of $3.09 \times 10^{-12}$ can be witnessed after at least $8.951 \times 10^{10}$ rounds (Extended Data Fig. 1a, cross), that is, the randomness produced in the experiment surpasses the consumed entropy after this number of rounds (Supplementary Section III.A).

In the main experiment, we set $\omega_{\exp}=0.752487$, $\delta=3.52 \times 10^{-4}$ and $\gamma=3.264 \times 10^{-4}$, and conservatively set the number of rounds to $n=1.3824 \times 10^{11}$, which is slightly larger than the $8.951 \times 10^{10}$ rounds required (see Supplementary Section III.A for computation of the latter). We complete all the rounds of the experiment in 19.2 h at a repetition rate of 2 MHz, which is much shorter than 118,000 h (which would have been required by the previous experiment). The resulting CHSH game score is $\omega_{\text{CHSH}}=0.752484$, which is consistent with the value we expect (and the protocol did not abort).

### Box 1 | CHSH-based DIRNE protocol

**Arguments.**
- $n \in \mathbb{N}$—number of rounds
- $\gamma \in (0,1)$—test probability
- $\omega_{\exp}$—expected CHSH score given a test round
- $\delta > 0$—width of the statistical confidence interval for the CHSH score
- $R$—random seed for the extractor

**Protocol.**
1. For every round $i \in \{1, \ldots, n\}$, do steps 2–4.
2. Set $U_i=\perp$. Choose $T_i \in \{0,1\}$ such that $\text{Pr}(T_i=1)=\gamma$.
3. If $T_i=0$, use the devices with inputs $(X_i,Y_i)=(0,0)$, record $A_i$ and $B_i$, and if $U_i=\perp$, repeat the test.
4. If $T_i=1$, choose the inputs $X_i$ and $Y_i$ uniformly at random from $\{0,1\}$, record $A_i$ and $B_i$, and set $U_i=\frac{1}{2}(1-(-1)^{A_i\oplus B_i \oplus X_i \oplus Y_i})$.
5. If $|\{U_i : U_i=0\}| > n\gamma(1-(\omega_{\exp}-\delta))$, then abort the protocol.
6. Apply a strong quantum-proof randomness extractor to get output randomness $M=\text{Ext}(AB,R)$. (Because we use a strong extractor, $M$ can be concatenated with $R$ to give $Z=(M,R)$.)
Overall, we achieve DIRNE, gaining 2.57 because of the possibility of some subtle attacks (see section 4.2 of the test rounds and the inputs on the test rounds) to be reusable the other randomness required in the protocol (that is, for choosing above (Supplementary Section I.C)). Note that we do not consider a net rate of 1.86 quantum-certified bits of randomness, which exceeds the amount 450 multiplication (0.935 Gb and Supplementary Section III.A). We use a personal computer to perform a Toeplitz matrix (0.935 Gb × 0.138 Tb) multiplication to extract the quantum-certified random bits from the raw output. The soundness error of the final output is 3.09 × 10−12.

Because a quantum-proof strong extractor is applied, the seed required for the extraction remains random after its use and is therefore not consumed11. (Technically, the seed degrades by a very small amount, which is accounted for in the soundness error given above (Supplementary Section I.C).) Note that we do not consider the other randomness required in the protocol (that is, for choosing the test rounds and the inputs on the test rounds) to be reusable because of the possibility of some subtle attacks (see section 4.2 of ref. 3). Overall, we achieve DIRNE, gaining 2.57 × 109 net bits with a net rate of 1.86 × 10−12 bits per round against an eavesdropper that is limited by quantum theory (Extended Data Fig. 1b, red cross).

When playing the CHSH game, we close the detection loophole. Given the assumption that the devices are well shielded, it is not necessary to close the locality loophole (Supplementary Section I.B). Considering the demanding experimental requirements to close both loopholes24–28, the use of shielding assumptions instead of space-like separation improves efficiency and brings DIRNE closer to commercialization. We also remark that the randomness we generate is secure according to a composable security definition (Methods) and therefore can be used in any application that requires random numbers. Strictly, because of an issue with the composability of device-independent protocols29, without further assumption, ongoing security of the output randomness relies on the devices not being reused.

We also upgraded our previous platform1 where we closed the locality loophole to use higher-efficiency detectors, resulting in overall efficiencies of 80.41 ± 0.34% for Alice and 82.24 ± 0.32% for Bob (slightly lower than those of the main experiment). As a comparison, we analyse the performance of that setup by using the EAT framework with the same error parameters as our main experiment (Table 1). Because of the need for additional rounds, we increased the repetition rate to 4 MHz for this experiment. A comparison of the results (Table 1) shows that overall, we obtained 6.496 × 109 random bits within 3.168 × 1012 experimental rounds, exceeding the amount of entropy (6.233 × 109 bits) consumed during the protocol (Methods and Supplementary Section III.A) and gaining 2.63 × 109 net bits with a net rate of 8.32 × 10−5 bits per round against an eavesdropper that is limited by quantum theory (Extended Data Fig. 1b, blue open circle). The outputs of both experiments are available online (https://tinyurl.com/qssxxaq).

Beyond the work here, we would like protocols to have an improved rate. Robust protocols that achieve up to 2 bits of randomness per entangled qubit pair are known11. However, using such protocols to gain an experimental advantage requires improvement in the detection efficiency, which is challenging with a photonic setup. On the theory side, better rates could be achieved by developing improved protocols to gain an experimental advantage requires improvement in the detection efficiency, which is challenging with a photonic setup.
Table 1 | Comparison between the two experiments

|                               | Main experiment | Space-like experiment |
|-------------------------------|----------------|----------------------|
| Expected CHSH score ($\chi_{\text{exp}}$) | 0.752487       | 0.750809             |
| $\chi_{\text{exp}}$           | 3.393 $\times$ 10^{-4} | 9.851 $\times$ 10^{-3} |
| $n_{\text{min}}$             | 8.951 $\times$ 10^{12} | 2.888 $\times$ 10^{12} |
| Repetition rate               | 2 MHz           | 4 MHz                |
| Time taken                    | 19.2 h          | 220 h               |
| Observed CHSH score ($\chi_{\text{obs}}$) | 0.752848       | 0.750805             |
| Test probability ($\gamma$)   | 3.264 $\times$ 10^{-4} | 1.194 $\times$ 10^{-3} |
| Number of rounds ($n$)       | 1.3824 $\times$ 10^{11} | 3.168 $\times$ 10^{10} |
| Confidence width ($\delta$)  | 3.52 $\times$ 10^{-4} | 1.22 $\times$ 10^{-4} |
| Soundness error ($\epsilon_\delta$) | 3.09 $\times$ 10^{-12} | 3.09 $\times$ 10^{-12} |
| Completeness error ($\epsilon_C$) | 10^{-6}       | 10^{-6}             |
| Entropy in output            | 9.350 $\times$ 10^{8} bits | 6.496 $\times$ 10^{7} bits |
| Randomness generation rate   | 13,527 bits s^{-1} | 8,202 bits s^{-1} |
| Entropy in input             | 6,778 $\times$ 10^{6} bits | 6,233 $\times$ 10^{6} bits |
| Net gain                     | 2.57 $\times$ 10^{7} bits | 2.63 $\times$ 10^{7} bits |

Here, $\gamma$ is the optimal test probability to witness expansion in the minimum number of rounds $n_{\text{min}}$ with the error parameters chosen.

Online content
Any methods, additional references, Nature Research reporting summaries, source data, extended data, supplementary information, acknowledgements, peer review information; details of author contributions and competing interests; and statements of data and code availability are available at https://doi.org/10.1038/s41567-020-01147-2.

Received: 20 December 2019; Accepted: 10 December 2020; Published online: 11 February 2021

References

1. Colbeck, R. Quantum and Relativistic Protocols for Secure Multi-Party Computation. PhD thesis, Univ. Cambridge (2007); https://arxiv.org/abs/0911.3814
2. Colbeck, R. & Kent, A. Private randomness expansion with untrusted devices. J. Phys. A 44, 095305 (2011).
3. Pironio, S. et al. Random numbers certified by Bell’s theorem. Nature 464, 1021–1024 (2010).
4. Arnon-Friedman, R., Dupuis, F., Fawzi, O., Renner, R. & Vidick, T. Practical device-independent quantum cryptography via entropy accumulation. Nat. Commun. 9, 459 (2018).
5. Liu, Y. et al. High-speed device-independent quantum random number generation without a detection loophole. Phys. Rev. Lett. 120, 010503 (2018).
6. Shen, L. et al. Randomness extraction from Bell violation with continuous parametric down-conversion. Phys. Rev. Lett. 121, 150402 (2018).
7. Bierhorst, P. et al. Experimentally generated randomness certified by the impossibility of superluminal signals. Nature 556, 223–226 (2018).
8. Liu, Y. et al. Device-independent quantum random-number generation. Nature 562, 548–551 (2018).
9. Zhang, Y. et al. Experimental low-latency device-independent quantum randomness. Phys. Rev. Lett. 124, 010505 (2020).
10. Fehr, S., Gelles, R. & Schaffner, C. Security and compositability of randomness expansion from Bell inequalities. Phys. Rev. A 87, 012335 (2013).
11. Coudron, M. & Yuen, H. Infinite randomness expansion with a constant number of devices. In Proc. 46th Annual ACM Symposium on Theory of Computing 427–436 (Association for Computing Machinery, 2014).
12. Miller, C. A. & Shi, Y. Robust protocols for securely expanding randomness and distributing keys using untrusted quantum devices. In Proc. 46th Annual ACM Symposium on Theory of Computing 417–426 (Association for Computing Machinery, 2014).
13. Miller, C. A. & Shi, Y. Universal security for randomness expansion from the spot-checking protocol. SIAM J. Comput. 46, 1304–1335 (2017).
14. Vazirani, U. & Vidick, T. Certifiable quantum dice: or, true random number generation secure against quantum adversaries. In Proc. 44th Annual ACM Symposium on Theory of Computing 61–76 (Association for Computing Machinery, 2012).
15. Brown, P. J., Ragy, S. & Colbeck, R. A framework for quantum-secure device-independent randomness expansion. IEEE Trans. Inf. Theory 66, 2964–2987 (2020).
16. Dupuis, F., Fawzi, O. & Renner, R. Entropy accumulation. Commun. Math. Phys. 379, 867–913 (2020).
17. Dupuis, F. & Fawzi, O. Entropy accumulation with improved second-order term. IEEE Trans. Inf. Theory 65, 7596–7612 (2019).
18. Acin, A. & Masanes, L. Certified randomness in quantum physics. Nature 540, 213–219 (2016).
19. Herrero-Collantes, M. & Garcia-Escartin, J. C. Quantum random number generators. Rev. Mod. Phys. 89, 015004 (2017).
20. Gerhardt, I. et al. Full-field implementation of a perfect eavesdropper on a quantum cryptography system. Nat. Commun. 2, 349 (2011).
21. 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).
22. Murta, G., van Dam, S. B., Ribeiro, J., Hanson, R. & Wehner, S. Towards a realization of device-independent quantum key distribution. Quantum Sci. Technol. 4, 035001 (2019).
23. Konig, R. & Renner, R. Sampling of min-entropy relative to quantum knowledge. IEEE Trans. Inf. Theory 57, 4760–4787 (2011).
24. Hensen, B. et al. Loophole-free Bell inequality violation using electron spins separated by 1.3 kilometres. Nature 526, 682–686 (2015).
25. Shalm, L. K. et al. Strong loophole-free test of local realism. Phys. Rev. Lett. 115, 250401 (2015).
26. Giustina, M. et al. Significant-loophole-free test of Bell’s theorem with entangled photons. Phys. Rev. Lett. 115, 250401 (2015).
27. Rosenfeld, W. et al. Event-ready Bell test using entangled atoms simultaneously closing detection and locality loopholes. Phys. Rev. Lett. 119, 010402 (2017).
28. Li, M.-H. et al. Test of local realism into the past without detection and locality loopholes. Phys. Rev. Lett. 121, 080404 (2018).
29. Barrett, J., Colbeck, R. & Kent, A. Memory attacks on device-independent quantum cryptography. Phys. Rev. Lett. 110, 010503 (2013).
30. Colbeck, R. & Renner, R. Free randomness can be amplified. Nat. Phys. 8, 450–453 (2012).

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

© The Author(s), under exclusive licence to Springer Nature Limited 2021
Methods

Security definition. In this work, we use a composable security definition\(^{1-13}\).

Definition 1. (Security) A protocol with an output \(Z\) is called \((\varepsilon, \epsilon)\)-secure if it satisfies the following:

(1) (Soundness) For an implementation of the protocol that produces \(m\) bits of output, we have

\[
\frac{1}{2} \max_{\rho_0} \mathbb{P}[Z|\hat{E} = 0] - \varepsilon_m \leq \epsilon_S;
\]

where \(\varepsilon_m\) represents a completely mixed state on \(m\) qubits, \(E\) represents all systems that could be held by an adversary (Eve), and \(\epsilon_S\) is the event that the protocol does not abort, and \(\rho_0\) is the probability of this occurrence. If \(\epsilon_S\), it is the trace norm.

(2) (Completeness) There exists an honest implementation such that \(\rho_0 \geq 1 - \epsilon_c\).

The soundness error bounds the distance between the output of the protocol and that of an idealized protocol in which Eve's marginal is the same as in the real protocol but the output is perfectly uniform and independent of Eve.

In general, the raw output of a protocol can have a lot of randomness while being easily distinguished from uniform. However, with the application of an appropriate randomness extractor, which is a classical function that takes a random seed and the raw output, an almost uniform output can be recovered. The length of this output can be taken to be roughly equal to the smooth min-entropy of the raw string that is conditioned on the side information held by Eve\(^{14,15}\).

Definition 2. (Smooth min-entropy) For any classical–quantum density matrix \(\rho_{\mathcal{AE}} = \sum_{a|\mathcal{E}} \hat{p}(a)\rho_{a|\mathcal{E}} \otimes \hat{p}_E\) acting on the joint Hilbert space \(\mathcal{H}_{\mathcal{AE}}\), the smooth min-entropy is defined by

\[
H_{\text{min}}^{\epsilon}(A|E)_{\rho_{\mathcal{AE}}} = \max_{\rho_{\mathcal{A}}} \left( -\log \max_{\{i\}} \sum_{a|\mathcal{E}} \hat{p}(a) \text{Tr}(\rho_{a|\mathcal{E}}^{i}\hat{p}_E) \right),
\]

where the outer maximization is over the set \(\mathcal{E}^n(\rho_{\mathcal{AE}})\) of all sub-normalized states \(\rho_{\mathcal{AE}} = \sum_{a|\mathcal{E}} \hat{p}(a)\rho_{a|\mathcal{E}} \otimes \hat{p}_E\) within puriﬁed distance\(^\epsilon\) of \(\rho_{\mathcal{AE}}\). Note that \(\max_{\{i\}} \sum_{a|\mathcal{E}} \hat{p}(a) \text{Tr}(\rho_{a|\mathcal{E}}^{i}\hat{p}_E)\) can be interpreted as the maximum probability of guessing \(A\) given access to the system \(E\).

The interpretation in terms of guessing probability makes clear that this quantity is a measure of unpredictability. Bounding the smooth min-entropy for a device-independent protocol is challenging. We do this by means of the entropy accumulation theorem and state an informal version that is applicable to the CHSH game below.

Theoretical details about the protocol. In the protocol, the user has two devices that are prevented from communicating with one another and with which the CHSH game can be played. To do so, each device is supplied with a uniformly chosen input denoted by \(X, Y \in \{0, 1\}\), and each produces an output, denoted by \(A, B \in \{0, 1\}\), respectively. The CHSH game is scored according to the function \(\frac{1}{2}(1 + (-1)^{X \cdot Y}AB)\). In other words, the game is won (with a score of 1) if \(AB = X \cdot Y\) and is lost (with a score of 0) otherwise.

At the end of the protocol, the number of rounds in which the CHSH game was lost is counted and compared to \(\pi\sigma(1 - (\alpha_{}\text{opt} - \delta))\). The challenge in a randomness expansion protocol is to go from this to the amount of extractable randomness. For that we use the EAT, which we state informally here (note that the version we use is (0, 1) and (0, 1)) (see Supplementary Information for a detailed discussion of the extraction).

\[
H_{\text{min}}^{\epsilon}(A|E)_{\rho_{\mathcal{AE}}} = \max_{\rho_{\mathcal{A}}} \left( -\log \max_{\{i\}} \sum_{a|\mathcal{E}} \hat{p}(a) \text{Tr}(\rho_{a|\mathcal{E}}^{i}\hat{p}_E) \right),
\]

Excluding the recollected seed will be roughly \(H_{\text{min}}(A|E)\) to be greater than the randomness consumed.

Remark 1. (Input randomness) The expected input randomness, \(\text{rand}_i\) of the protocol in Box 1 is

\[
\text{rand}_i = n(H_{\text{min}}(\gamma) + 2\gamma) + 2\delta,
\]

where \(H_{\text{min}}\) denotes the binary Shannon entropy. The contribution \(\text{rand}_i\) comes from the selection of the test rounds and \(\gamma\) from the selection of the input bits for the CHSH game. The interval algorithm\(^1\) can be used to turn uniform random bits to biased ones at the claimed rate.

We do not include the randomness that is necessary for seeding the extractor in the above because it is not consumed, although it is needed to run the protocol.

Suppose that a protocol has some fixed expected score \(\text{expected}\). To demonstrate randomness expansion, that is, \(\text{rand}_i - \text{rand}_o > 0\), at this performance we have to choose the parameters \(\alpha\) and \(\delta\) appropriately. Increasing \(\alpha\) leads to an improvement in the rate, but takes longer and increases the experimental difficulty. The trade-off with \(\delta\) appears in the \(\text{rand}_i\) and \(\text{rand}_o\) terms. The input randomness evidently decreases as \(\gamma\) shrinks, which is favourable because the input randomness is substituted to calculate the randomness gained. However, the min-entropy also decreases because the error term scales roughly as \(\delta\) (ref. \(\delta\)). Moreover, the statistical confidence decreases with less frequent testing, and as such the threshold score for successful parameter estimation must be lowered (that is, \(\delta\) increased) to obtain a small completeness error (see Supplementary Information for how to calculate this error). This also has a negative impact on the randomness produced.

Data availability

Source data are provided with this paper. All other data that support the plots within this paper and other findings of this study are available from the corresponding authors upon reasonable request.

Code availability

All relevant codes or algorithms are available from the corresponding authors upon reasonable request.

References

31. Canetti, R. Security and composition of multiparty cryptographic protocols. J. Cryptol. 13, 143–202 (2000).
32. Ben-Or, M. & Myers, D. General security definition and computability for quantum & classical protocols. Preprint at https://arxiv.org/abs/quant-ph/0409062 (2004).
33. Portmann, C. & Renner, R. Cryptographic security of quantum key distribution. Preprint at https://arxiv.org/abs/1409.3525 (2014).
34. Renner, R. Security of Quantum Key Distribution. PhD thesis, Swiss Federal Institute of Technology (2005); https://arxiv.org/pdf/quant-ph/0512248.pdf.
35. Konig, R., Renner, R. & Schaffner, C. The operational meaning of min- and max-entropy. IEEE Trans. Inf. Theory 55, 4337–4347 (2009).
36. Tomamichel, M., Colbeck, R. & Renner, R. Duality between smooth min- and max-entropies. IEEE Trans. Inf. Theory 56, 4674–4681 (2010).
37. Hao, T. S. & Hoshi, M. Interval algorithm for random number generation. IEEE Trans. Inf. Theory 43, 599–611 (1997).

Acknowledgements

We thank C.-L. Li for experimental assistance and J.-D. Bancal and E. Tan for comments on an earlier draft. This work was supported by the National Key R&D Program of China (grant nos. 2017YFA0303900 and 2017YFA0304000), the National Natural Science Foundation of China, the Chinese Academy of Sciences, the Shanghai Municipal Science and Technology Major Project (grant no. 201913Z15DZX01), the Anhui Initiative in Quantum Information Technologies, the Guangdong Innovative and Entrepreneurial Research Team Program (grant no. 2019ZXT083324), the Key Area R&D Program of Guangdong Province (grant no. 2020B0803010001), the Quantum Communications Hub of the Engineering and Physical Sciences Research Council (EPSRC) (grant nos. EP/M013472/1 and EP/T001011/1) and an EPSRC First Grant (grant no. EP/P016588/1). We are grateful for computational support from the University of York High Performance Computing Service, Viking, which was used for the randomness extraction.

Author contributions

R.C., J.F., Q.Z. and J.-P.W. conceived the research. Y.L., J.F., Q.Z. and J.-P.W. designed the experiment. W.-Z.L., M.-H.L., S.-R.Z. and Y.L. designed and implemented the entangled photon pair source. W.-Z.L. designed the data acquisition software. B.B. and J.Z. designed the biased and unbiased quantum random number generators for measurement setting choices. S.R., P.J.B. and R.C. developed the theory. S.R., P.J.B., W.-Z.L. and R.C. performed the protocol analysis, numerical modelling and randomness extraction. All authors contributed to the experimental realization, data analysis and manuscript preparation.

Competing interests

The authors declare no competing interests.
Additional information
Extended data is available for this paper at https://doi.org/10.1038/s41567-020-01147-2.
Supplementary information is available for this paper at https://doi.org/10.1038/s41567-020-01147-2.

Correspondence and requests for materials should be addressed to R.C., J.F., Q.Z. or J.-W.P.

Peer review information Nature Physics thanks Thomas Vidick and the other, anonymous, reviewer(s) for their contribution to the peer review of this work.

Reprints and permissions information is available at www.nature.com/reprints.
Extended Data Fig. 1 | Rounds needed and expansion rate for the main and space-like experiments. a, We estimate the minimum number of experimental runs with our revised EAT theory to witness randomness expansion as a function of CHSH violation (smooth curve) with a soundness error $3.09 \times 10^{-12}$. The red square, yellow circle and green cross indicate the previous, space-like and main experimental conditions, respectively. b, We estimate the randomness expansion rate based on our revised EAT theory as a function of number of rounds (smooth line) and the asymptotic rate (dashed line) with a soundness error $3.09 \times 10^{-12}$. The cross and circle indicate the experimental parameters used, red indicates the main experiment and blue indicates the space-like experiment.