Device-independent randomness expansion against quantum side information

Wen-Zhao Liu[1,2], Ming-Han Li[1,2], Sammy Ragy[3], Si-Ran Zhao[1,2], Bing Bai[1,2], Yang Liu[1,2], Peter J. Brown[3], Jun Zhang[1,2], Roger Colbeck[3], Jingyun Fan[1,2,4], Qiang Zhang[1,2], Jian-Wei Pan[1,2]

[1]*Shanghai Branch, National Laboratory for Physical Sciences at Microscale and Department of Modern Physics, University of Science and Technology of China, Shanghai 201315, P. R. China.*

[2]*Shanghai Branch, CAS Center for Excellence and Synergetic Innovation Center in Quantum Information and Quantum Physics, University of Science and Technology of China, Shanghai 201315, P. R. China.*

[3]*Department of Mathematics, University of York, Heslington, York YO10 5DD, United Kingdom*

[4]*Shenzhen Institute for Quantum Science and Engineering and Department of Physics, Southern University of Science and Technology, Shenzhen, 518055, P. R. China*

The ability to produce random numbers that are unknown to any outside party is crucial for many applications. Device-independent randomness generation[1–4] does not require trusted devices, thus providing strong guarantees about the security of the output, but comes at the price of requiring the violation of a Bell inequality to implement. 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[5–9], 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[1–3,10–15]. By developing a Bell test setup with a single photon detection efficiency of around 84% and using a spot-checking protocol, we achieve a net gain of 2.57×10^8 certified bits with soundness error 3.09×10^{-12}. The experiment ran for 19.2 hours corresponding to an average rate of randomness generation of $13,527$ bits/s. By developing the Entropy Accumulation Theorem[4,16,17], 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 possessing quantum devices. Quantum processes have hence been extensively studied as a source of randomness[18,19]. In a typical quantum random number generator, the user relies on the device working in a particular way, for instance, by having single photons pass through a 50:50 beam splitter and being detected. Deviations in the device behaviour affect the randomness of the outputs, while being difficult to detect. Furthermore, any real device will be too complicated to model in its entirety, leaving open the possibility that an adversary can exploit a feature of the device outside the model, as has been seen in quantum key distribution[20]. To circumvent this, device-independent protocols were introduced, which are proven secure without any assumptions about the devices used. This leads to a significantly higher level of security by removing any problems caused by unmodelled features.

Recently we have witnessed significant advances in experimental device-independent randomness generation (DIRNG). Some previous works required additional assumptions[3,5–7], and

even the most advanced to date[8,9] consumed more randomness than they generated. Hence, randomness expansion, which is a quantum feature without classical counterpart, remained elusive and technically challenging. For example, with our previous experimental setup[8], almost $118,000$ experimental hours (at 200 kHz repetition rate) would be required to achieve randomness expansion with the protocol presented below, putting it out of reach in practice.

Here 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 experimental sides. We derive a tighter bound on entropy accumulation in the randomness generation process and construct a photonic entanglement platform to realise a record-high violation of the Clauser-Horne-Shimony-Holt (CHSH)[21] inequality. 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 realise a number of other critical quantum information tasks such as device-independent quantum key distribution[22].

The entropy accumulation theorem (EAT)[4,16,17] provides relatively tight bounds on the amount of randomness that can be extracted against an adversary limited only by quantum theory. Roughly speaking, the EAT shows that in an n-round protocol achieving a CHSH game score of ω, the amount of output randomness is lower bounded by

$$\mathrm{rand}_{\mathrm{out}} \geq nh(\omega) - \sqrt{n}v\,, \tag{1}$$

where $h(\omega)$ is the worst-case von Neumann entropy of an individual round of the protocol with

expected score ω. The score on round i is $\frac{1}{2}(1+(-1)^{A_i \oplus B_i \oplus (X_i \cdot Y_i)})$, 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 and $Y_i \in \{0, 1\}$ (see Fig. 1), and v is a correction factor accounting for the finite statistics. Using ideas from the improved EAT[17], we derive a tighter lower bound on the accumulated entropy (see the Methods). This allows us to use a spot-checking protocol to experimentally realise randomness expansion with a state-of-art experimental quantum optical technique.

Fig. 1 shows a conceptual drawing of our spot-checking device-independent protocol, where the assumptions are outlined. The underlying idea is to check that devices situated in a secure lab violate a Bell inequality, hence it is 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 γ), 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 only learns its own input and not whether a round was a test or generation round.

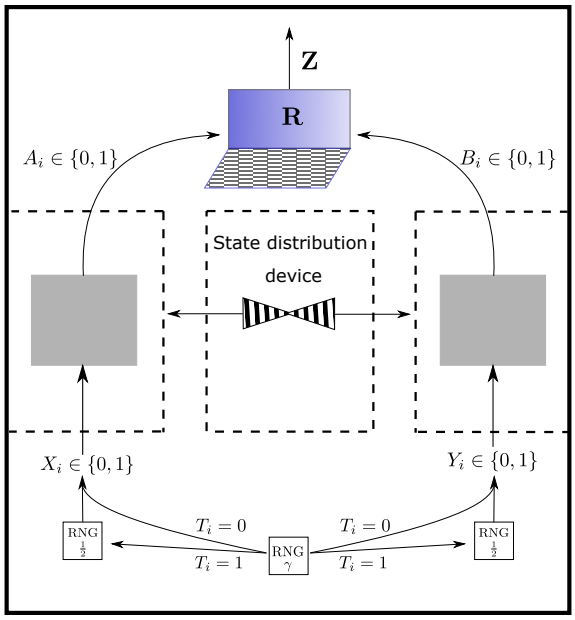

Figure 1: **Conceptual sketch of the DIRNE protocol setup (cf. Box 1).** The protocol takes place in a secure lab, which is shielded from direct communication to the outside. The lab contains two black-box devices which accept inputs and yield outputs from the binary alphabet $\{0, 1\}$ and these can be shielded from communicating at will. In particular, we assume 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 which may be distributed from a central station. (If we had good enough quantum storage, then all entanglement could be pre-shared.) Alice and Bob's respective inputs are X_i and Y_i and their outputs 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 depicted by an extractor seed $\mathbf{R}$ and three RNGs that determine the inputs to the devices. These output either 0 or 1, where the number in the box (γ or $1/2$) denotes the probability of 1. The central RNG determines the round-type ($T_i = 1$ meaning test and $T_i = 0$ meaning generate) and the peripheral ones determine the inputs if a test round is chosen. The final randomness output is denoted by $\mathbf{Z}$.

Box 1 : CHSH-based DIRNE Protocol

Arguments:

$n \in \mathbb{N}$ – number of rounds

$\gamma \in (0, 1]$ – test probability

ω_{exp} – expected CHSH score given a test round

$\delta \in (0, 1)$ – 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 $2 - 4$.
2. Set $U_i = \perp$. Choose $T_i \in \{0, 1\}$ such that $\Pr(T_i = 1) = \gamma$.
3. If $T_i = 0$ use the devices with inputs $(X_i, Y_i) = (0, 0)$, record A_i, replace B_i with 0 and set $U_i = \perp$.
4. If $T_i = 1$, choose the inputs X_i and Y_i uniformly at random from $\{0, 1\}$ and record A_i and B_i and set $U_i = \frac{1}{2}(1 + (-1)^{A_i \oplus B_i \oplus (X_i \cdot Y_i)})$.
5. If $|\{U_i : U_i = 0\}| > n\gamma(1 - (\omega_{\text{exp}} - \delta))$, then abort the protocol.
6. Apply a strong quantum-proof randomness extractor to get output randomness $\mathbf{M} = \text{Ext}(\mathbf{AB}, \mathbf{R})$. (Because we use a strong extractor $\mathbf{M}$ can be concatenated with $\mathbf{R}$ to give $\mathbf{Z} = (\mathbf{M}, \mathbf{R})$.)

We implement the protocol on a quantum optical platform (see Fig. 2). Pairs of polarization-entangled photons with wavelength 1560 nm are generated via spontaneous parametric downcon-

version and are delivered to two sites through spatial optical paths, where polarization-dependent measurements are conducted. Previously and with space-like separation between Alice and Bob, this platform proved to be robust enough to realise loophole free violation of a Bell inequality and DIRNG, in which the CHSH game scores ω violated the classical bound $\omega_{\text{class}} = 3/4$ by 0.00027[8]. Under these conditions and using the same error parameters as elsewhere in this paper, it would take about 8.52×10^{13} rounds of the experiment to witness randomness expansion according to our revised EAT theory (open square in Extended Data Fig. 1a). 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 record-high single-photon detection efficiencies of $83.40 \pm 0.32\%$ for Alice and $84.80 \pm 0.31\%$ for Bob, enabling 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 randomly determined, while 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 performed to predetermine several parameters mentioned in the protocol. The calibration yielded a CHSH game score of 0.752487, and we compute that for $\gamma_{\text{opt}} = 3.393 \times 10^{-4}$ corresponding to an average input entropy rate of 0.0049 bits per round, randomness expansion with a soundness error (see the Methods) of 3.09×10^{-12} can be witnessed after at least 8.951×10^{10} rounds (cross in Extended Data Fig. 1a), i.e., the randomness produced in the

experiment surpasses the consumed entropy after this number of rounds (see the Supplementary Information, Section III.A).

In the main experiment, we set $\omega_{\mathrm{exp}} = 0.752487$, $\delta = 3.52 \times 10^{-4}$, $\gamma = 3.264 \times 10^{-4}$, and conservatively set the number of rounds to $n = 1.3824 \times 10^{11}$, which is slightly larger than the 8.951×10^{10} rounds required (see Section III.A of the Supplementary Information for computation of the latter). We complete all the rounds of the experiment in 19.2 hours at a repetition rate of 2 MHz, which is much smaller than $118,000$ hours[8]. The resulting CHSH game score is $\omega_{\mathrm{CHSH}} = 0.752484$, which is consistent with the value we expect (and the protocol did not abort), $|\omega_{\mathrm{CHSH}} - \omega_{\mathrm{exp}}| < \delta$. The raw experimental output has size 0.138Tb. According to the development of the EAT presented in the Supplementary Information, it contains at least 9.350×10^8 quantum-certified bits of randomness, exceeding the amount of entropy (6.778×10^8 bits) required for its generation (see the Supplementary Information, Section III.A and the Methods). We use a personal computer to perform a Toeplitz matrix (0.935Gb $\times$ 0.138Tb) 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 hence is not consumed[23]. (Technically, the seed degrades by a very small amount, which is accounted for in the soundness error given above; see the Supplementary Information, Section I.C). Note that we do not consider the other randomness required in the protocol (i.e., 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. 2). Overall we achieve DIRNE,

gaining 2.57×10^8 net bits with a net rate of 1.86×10^{-3} bits per round against an eavesdropper limited by quantum theory (shown by the red cross in Extended Data Fig. 1b).

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 (see the Supplementary Information, Section I.B). Considering the demanding experimental requirements to close both loopholes[24–28], using 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 (see the Methods) and hence can be used in any application requiring random numbers. Strictly, because of an issue with the composability of device independent protocols[29], without further assumption, ongoing security of the output randomness relies on the devices not being reused.

We also upgraded our previous platform where we closed the locality loophole to use higher efficiency detectors[8]. The efficiencies there are sightly reduced giving $80.41 \pm 0.34\%$ for Alice and $82.24 \pm 0.32\%$ for Bob. As a comparison, we analyse the performance of that setup using the EAT framework with the same error parameters as our main experiment. Because of the need for additional rounds, we increased the repetition rate to 4 MHz for this. The parameters used and a comparison of the results are listed in Tab. 1. Overall, we obtained 6.496×10^9 random bits within 3.168×10^{12} experimental rounds, exceeding the amount of entropy (6.233×10^9 bits) required for its generation (see the Supplementary Information, Section III.A and the Methods), gaining 2.63×10^8 net bits with a net rate of 8.32×10^{-5} bits per round against an eavesdropper limited

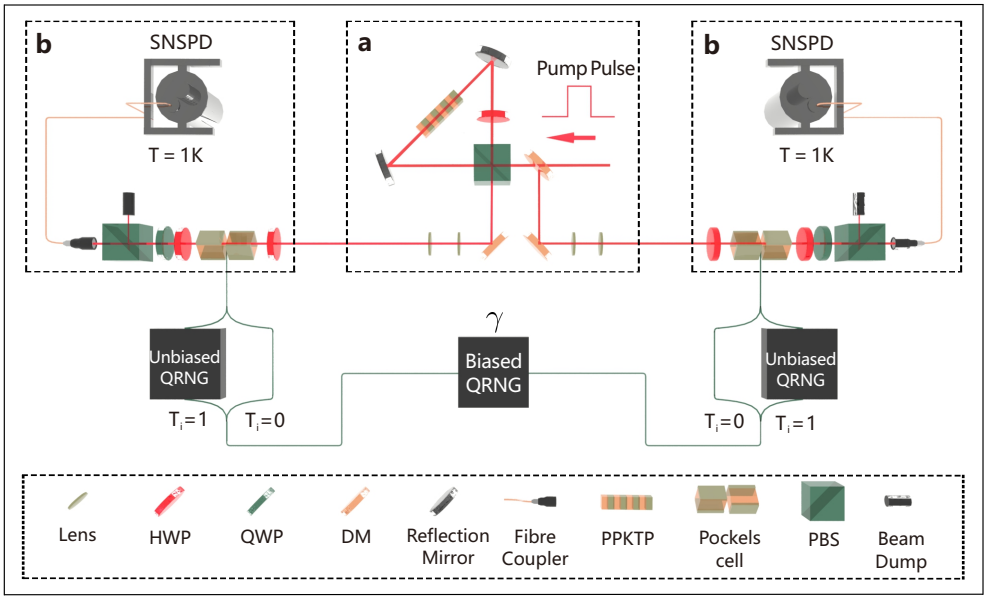

Figure 2: **Schematic of the experiment.** **a** Entanglement Source, Creation of pairs of entangled photons: Light pulses of 10 ns are injected at a repetition rate of 2 MHz into a periodically poled potassium titanyl phosphate (PPKTP) crystal in a Sagnac loop to generate polarization-entangled photon pairs[8]. The two photons of an entangled pair at 1560 nm travel in opposite directions to two sites Alice and Bob, where they are subject to polarization projection measurements. **b** Alice and Bob, Single photon polarization measurement: In the measurement sites, Alice (Bob) uses a Pockels cell to project the single photon into one of two pre-determined measurement bases, and then detects single photons with a superconducting nanowire single-photon detector (SNSPD). In each round, a biased QRNG in the lab creates a random bit T_i with probability distribution $(\gamma, 1-\gamma)$ to determine in advance whether this round will be a test or generation round. In test rounds Alice and Bob each receive a random bit "0" or "1" from a local quantum random number generator (QRNG) to set Pockels cell to zero and half-wave voltage accordingly (in generation rounds they always use zero). HWP – half-wave plate; QWP – quarter-wave plate; DM – dichroic mirror; PBS – polarizing beam splitter.

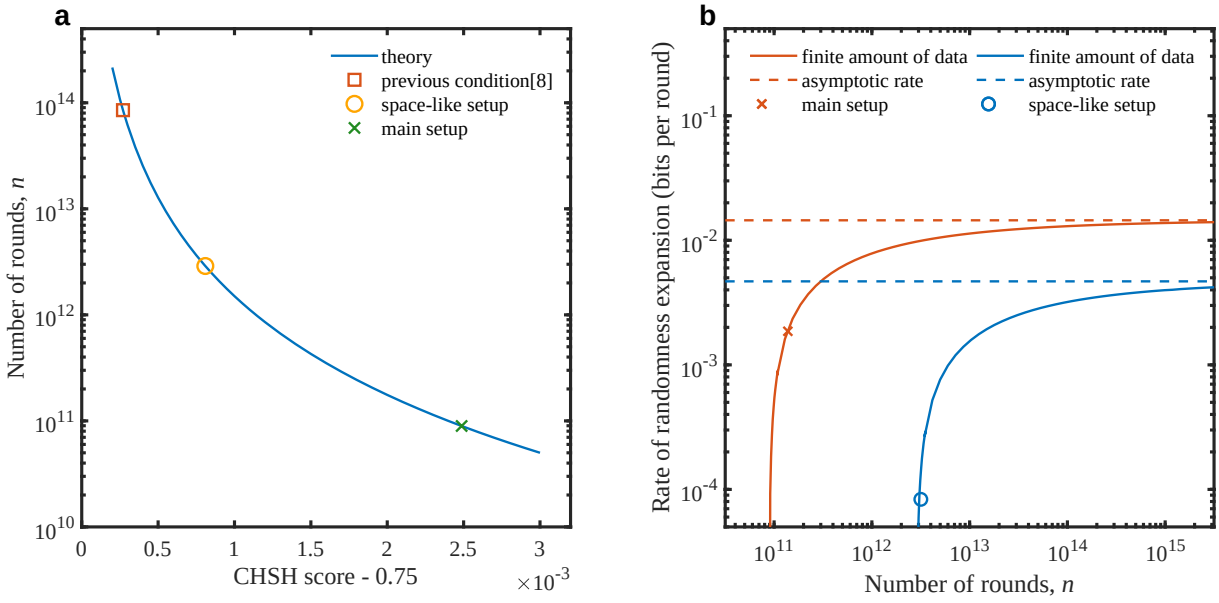

Figure 3: **Rounds needed and expansion rate depending on rounds for the main and space-like experiments.** **a**: We estimate the minimum number of experimental runs with our revised EAT theory to witness randomness expansion as a function of CHSH violation (smooth curve) with soundness error 3.09×10^{-12}. The red square, yellow circle and green cross indicate the previous[8], 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 soundness error 3.09×10^{-12}. The cross and circle indicate the experimental parameters used, red indicates the main experiment and blue indicates the space-like experiment.

by quantum theory (shown by the blue open circle in Extended Data Fig. 1b). The outputs of both experiments are available online at https://tinyurl.com/qssxxaq.

Going beyond the work here we would like protocols that have an improved rate. Robust protocols that achieve up to two bits of randomness per entangled qubit pair are known[15]. However, to experimentally use such protocols to gain an advantage requires a significant improvement in the detection efficiency, which is challenging with a photonic setup. On the theory side, better rates could be achieved by developing tighter bounds on the output randomness. It would also be interesting to put into practice a protocol for randomness amplification[30], hence reducing the assumption on the input randomness.

1. Colbeck, R. *Quantum and relativistic protocols for secure multi-party computation*. Ph.D. thesis, University of Cambridge (2007). Also available as arXiv:0911.3814.

2. Colbeck, R. & Kent, A. Private randomness expansion with untrusted devices. *Journal of Physics A: Mathematical and Theoretical* **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. *Nature Communications* **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 composability 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 *Proceedings of the Forty-Sixth Annual ACM Symposium on Theory of Computing*, 427–436 (2014).

12. Miller, C. A. & Shi, Y. Robust protocols for securely expanding randomness and distributing keys using untrusted quantum devices. In *Proceedings of the Forty-Sixth Annual ACM Symposium on Theory of Computing*, 417–426 (2014).

13. Miller, C. A. & Shi, Y. Universal security for randomness expansion from the spot-checking protocol. *SIAM Journal on Computing* **46**, 1304–1335 (2017).

14. Vazirani, U. & Vidick, T. Certifiable quantum dice: Or, true random number generation secure against quantum adversaries. In *Proceedings of the Forty-Fourth Annual ACM Symposium on Theory of Computing*, 61–76 (2012).

15. Brown, P. J., Ragy, S. & Colbeck, R. A framework for quantum-secure device-independent randomness expansion. *IEEE Transactions on Information Theory* **66**, 2964–2987 (2020).

16. Dupuis, F., Fawzi, O. & Renner, R. Entropy accumulation. *Communications in Mathematical Physics* **379**, 867–913 (2020).

17. Dupuis, F. & Fawzi, O. Entropy accumulation with improved second-order term. *IEEE Transactions on Information Theory* **65**, 7596–7612 (2019).

18. Acín, 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. *Nature Communications* **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 Science and Technology* **4**, 035011 (2019).

23. Konig, R. & Renner, R. Sampling of min-entropy relative to quantum knowledge. *IEEE Transactions on Information 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**, 250402 (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. *Nature Physics* **8**, 450–453 (2012).

Methods

Security definition. In this work we use a composable security definition[31–33].

Definition 1 (security)**.** A protocol with an output $\mathbf{Z}$ is called $(\epsilon_{\mathcal{S}}, \epsilon_{\mathcal{C}})$-secure if it satisfies

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

$$\frac{1}{2} p_{\Omega} \| \rho_{\mathbf{Z}E|\Omega} - \tau_m \otimes \rho_{E|\Omega} \|_1 \leq \epsilon_{\mathcal{S}} \,, \tag{2}$$

   where τ_m represents a completely mixed state on m qubits, E represents all systems that could be held by an adversary (Eve), Ω the event that the protocol does not abort, p_{Ω} the probability of this occurring. $\| \cdot \|_1$ is the trace norm.

2. (Completeness) There exists an honest implementation such that $p_{\Omega} \geq 1 - \epsilon_{\mathcal{C}}$.

The soundness error bounds the distance between the output of the protocol and that of an idealized protocol where 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 distinguishable from uniform. However, by applying an appropriate randomness extractor, which is a classical function taking 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 conditioned on the side information held by Eve[34,35].

Definition 2 (Smooth min-entropy)**.** For any classical-quantum density matrix $\rho_{AE} = \sum_a p(a) \left|a\right\rangle\!\left\langle a\right| \otimes \rho_E^a$ acting on the joint Hilbert space $\mathcal{H}_{AE}$, the ϵ_h-smooth min-entropy is defined by

$$H_{\min}^{\epsilon_h}(A|E)_{\rho_{AE}} = \max_{\tilde{\rho}_{AE}} \left(-\log \max_{\{\Pi_a\}} \sum_a \tilde{p}(a) \mathrm{Tr}(\Pi^a \tilde{\rho}_E^a) \right), \tag{3}$$

where the outer maximisation is over the set $\mathcal{B}^{\epsilon_h}(\rho_{AE})$ of all sub-normalized states $\tilde{\rho}_{AE} = \sum_a \tilde{p}(a) \left|a\right\rangle\!\left\langle a\right| \otimes \tilde{\rho}_E^a$ within purified distance[36] ϵ_h of ρ_{AE}. Note that $\max_{\{\Pi_a\}} \sum_a \tilde{p}(a) \mathrm{Tr}(\Pi^a \tilde{\rho}_E^a)$ 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 which 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 inputs denoted by $X, Y \in \{0, 1\}$, and each produces an output, denoted $A, B \in \{0, 1\}$ respectively. The CHSH game is scored according to the function $\frac{1}{2}(1 + (-1)^{A \oplus B \oplus (X \cdot Y)})$. In other words, the game is won (with a score of 1) if $A \oplus B = X \cdot Y$ 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 $n\gamma(1 - (\omega_{\text{exp}} - \delta))$. The challenge in a randomness expansion protocol is to go from this to the amount of extractable randomness. For this we use the EAT, which we state informally here (note that the version we use is a development of Ref. 17; for more details, see the

Supplementary Information).

Theorem 1 (Entropy accumulation, informal)**.** *Suppose the protocol of Box 1 is performed and that devices are such that p_Ω is the probability that the protocol does not abort. Let $\alpha \in (1,2)$, $\epsilon_h \in (0,1)$ and $f(s)$ be an affine lower bound on the single-round von Neumann entropy for any strategy achieving an expected score of s. If the protocol does not abort, we can assume*

$$\begin{aligned} H_{\min}^{\epsilon_h}(\mathbf{AB}|E) \geq\ & nf(\omega) + n\Delta(f,\omega) - n(\alpha-1)V(f,\gamma,\omega) \\ & - \frac{\alpha}{\alpha-1}\log\left(\frac{1}{p_\Omega(1-\sqrt{1-\epsilon_h^2})}\right) \\ & + n(\alpha-1)^2 K_\alpha(f,\gamma), \end{aligned} \tag{4}$$

where $\omega = \omega_{\text{exp}} - \delta$ and the explicit forms of the functions Δ, V and K_α can be found in the Supplementary Information.

By setting $\alpha - 1 \propto \frac{1}{\sqrt{n}}$, the subtracted terms scale as $\sqrt{n}$ whereas the leading rate term scales with n, leading to the relation in Eqn. (1) when $f(\omega)$ is a good approximation to $h(\omega)$, the worst-case von Neumann entropy for the observed score.

In order to produce the output string $\mathbf{M}$, we apply a strong quantum-proof randomness extractor. The reason we use a strong extractor is that the random seed, $\mathbf{R}$, required for the extractor remains random even conditioned on the extractor's output and is hence not consumed. This means that $\mathbf{M}$ can be concatenated with the extractor seed $\mathbf{R}$ to give output $\mathbf{Z} = (\mathbf{M}, \mathbf{R})$. We discuss the extraction in more detail in the Supplementary Information. Importantly, the length of the output (excluding the recycled seed), will be roughly $\text{rand}_{\text{out}} \approx H_{\min}^{\epsilon_h}(\mathbf{AB}|E)$. We need this to be greater than the randomness consumed.

Remark 1 (Input randomness)**.** The expected input randomness, $\mathrm{rand}_{\mathrm{in}}$ of the protocol in Box 1 is

$$\mathrm{rand}_{\mathrm{in}} = n(H_{\mathrm{bin}}(\gamma) + 2\gamma) + 2\,, \tag{5}$$

where H_{bin} denotes the binary Shannon entropy. The contribution $H_{\mathrm{bin}}(\gamma)$ comes from the selection of the test rounds and 2γ from the selection of the input bits for the CHSH game. The interval algorithm[37] can be used to turn uniform random bits to biased ones at the claimed rate.

We do not include the randomness 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 ω_{exp}. To demonstrate randomness expansion, i.e., $\mathrm{rand}_{\mathrm{out}} - \mathrm{rand}_{\mathrm{in}} > 0$, at this performance we have to choose the parameters n and γ appropriately. Increasing n leads to an improvement in the rate, but takes longer and increases the experimental difficulty. The tradeoff with γ appears in the $\mathrm{rand}_{\mathrm{out}}$ and $\mathrm{rand}_{\mathrm{in}}$ terms. The input randomness evidently decreases as γ shrinks, which is favourable since this term is subtracted. However, the min-entropy also decreases because the error term scales roughly as $\frac{1}{\sqrt{\gamma}}$[17]. Moreover, the statistical confidence decreases with less frequent testing and as such the threshold score for successful parameter estimation must be lowered (i.e., δ increased) in order to obtain a small completeness error. This also has a negative impact on the randomness produced. We outline how to calculate the completeness error in the Supplementary Information.

Data availability Source data are available for this paper. All other data that support the plots within this paper and other findings of this study are available from the corresponding author upon reasonable request.

Code availability All relevant codes or algorithms are available from the corresponding author upon reasonable request.

References

31. Canetti, R. Security and composition of multiparty cryptographic protocols. *Journal of Cryptology* **13**, 143–202 (2000).

32. Ben-Or, M. & Mayers, D. General security definition and composability for quantum & classical protocols. e-print quant-ph/0409062 (2004).

33. Portmann, C. & Renner, R. Cryptographic security of quantum key distribution. e-print arXiv:1409.3525 (2014).

34. Renner, R. *Security of Quantum Key Distribution*. Ph.D. thesis, Swiss Federal Institute of Technology, Zurich (2005). Also available as quant-ph/0512258.

35. Konig, R., Renner, R. & Schaffner, C. The operational meaning of min- and max-entropy. *IEEE Transactions on Information Theory* **55**, 4337–4347 (2009).

36. Tomamichel, M., Colbeck, R. & Renner, R. Duality between smooth min- and max-entropies. *IEEE Transactions on Information Theory* **56**, 4674–4681 (2010).

37. Te Sun Hao & Hoshi, M. Interval algorithm for random number generation. *IEEE Transactions on Information Theory* **43**, 599–611 (1997).

Acknowledgements The authors would like to 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 numbers, 2017YFA0303900, 2017YFA0304000), the National Natural Science Foundation of China, the Chinese Academy of Sciences, the Shanghai Municipal Science and Technology Major Project (grant number 2019SHZDZX01), the Anhui Initiative in Quantum Information Technologies, the Guangdong Innovative and Entrepreneurial Research Team Program (grant number 2019ZT08X324), the Key-Area Research and Development Program of Guangdong Province (grant number 2020B0303010001), the EPSRC's Quantum Communications Hub (grant numbers EP/M013472/1 and EP/T001011/1) and an EPSRC First Grant (grant number 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.-W.P. conceived the research. Y.L., J.F., Q.Z. and J.-W.P. 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 significantly to the experimental realization, data analysis, and manuscript preparation.

Competing interests The authors declare that they have no competing financial interests.

Table 1: **Comparison between the two experiments.** Here γ_{opt} is the optimal test probability to witness expansion in the minimum number of rounds $n_{\min}$ with the error parameters chosen.

	main expt.	space-like expt.
expected CHSH score (ω_{exp})	0.752487	0.750809
γ_{opt}	3.393×10^{-4}	9.851×10^{-5}
$n_{\min}$	8.951×10^{10}	2.888×10^{12}
test probability (γ)	3.264×10^{-4}	1.194×10^{-4}
number of rounds (n)	1.3824×10^{11}	3.168×10^{12}
confidence width (δ)	3.52×10^{-4}	1.22×10^{-4}
soundness error ($\epsilon_{\mathcal{S}}$)	3.09×10^{-12}	3.09×10^{-12}
completeness error ($\epsilon_{\mathcal{C}}$)	1×10^{-6}	1×10^{-6}
observed CHSH score (ω_{CHSH})	0.752484	0.750805
repetition rate	2 MHz	4 MHz
time taken	19.2 hours	220 hours
entropy in output	9.350×10^8 bits	6.496×10^9 bits
entropy in input	6.778×10^8 bits	6.233×10^9 bits
net gain	2.57×10^8 bits	2.63×10^8 bits