LETTER

https://doi.org/10.1038/s41586-018-0559-3

Device-independent quantum random-number generation

Yang Liu[1,2], Qi Zhao[3], Ming-Han Li[1,2], Jian-Yu Guan[1,2], Yanbao Zhang[5], Bing Bai[1,2], Weijun Zhang[4], Wen-Zhao Liu[1,2], Cheng Wu[1,2], Xiao Yuan[1,2,3], Hao Li[4], W. J. Munro[5], Zhen Wang[4], Lixing You[4], Jun Zhang[1,2], Xiongfeng Ma[3]*, Jingyun Fan[1,2]*, Qiang Zhang[1,2]* & Jian-Wei Pan[1,2]*

Randomness is important for many information processing applications, including numerical modelling and cryptography[1,2]. Device-independent quantum random-number generation (DIQRNG)[3,4] based on the loophole-free violation of a Bell inequality produces genuine, unpredictable randomness without requiring any assumptions about the inner workings of the devices, and is therefore an ultimate goal in the field of quantum information science[5–7]. Previously reported experimental demonstrations of DIQRNG[8,9] were not provably secure against the most general adversaries or did not close the 'locality' loophole of the Bell test. Here we present DIQRNG that is secure against quantum and classical adversaries[10–12]. We use state-of-the-art quantum optical technology to create, modulate and detect entangled photon pairs, achieving an efficiency of more than 78 per cent from creation to detection at a distance of about 200 metres that greatly exceeds the threshold for closing the 'detection' loophole of the Bell test. By independently and randomly choosing the base settings for measuring the entangled photon pairs and by ensuring space-like separation between the measurement events, we also satisfy the no-signalling condition and close the 'locality' loophole of the Bell test, thus enabling the realization of the loophole-free violation of a Bell inequality. This, along with a high-voltage, high-repetition-rate Pockels cell modulation set-up, allows us to accumulate sufficient data in the experimental time to extract genuine quantum randomness that is secure against the most general adversaries. By applying a large (137.90 gigabits × 62.469 megabits) Toeplitz-matrix hashing technique, we obtain 6.2469 × 10^7 quantum-certified random bits in 96 hours with a total failure probability (of producing a random number that is not guaranteed to be perfectly secure) of less than 10^{-5}. Our demonstration is a crucial step towards transforming DIQRNG from a concept to a key aspect of practical applications that require high levels of security and thus genuine randomness[7]. Our work may also help to improve our understanding of the origin of randomness from a fundamental perspective.

The security, or unpredictability, of randomness generated by a device-independent quantum random-number generator can be assessed via the observation of the loophole-free violation of a Bell inequality. A Bell test involves two entangled particles, with each party choosing the measurement settings according to a random input and outputting a classical bit. To create a device-independent quantum random-number generator based on the violation of a Bell inequality, two sets of conditions must be fulfilled rigorously and simultaneously.

First, it is necessary in the experimental implementations of DIQRNG to detect entangled particles with high efficiency in order to close the detection loophole and to ensure the no-signalling condition—which requires that there is no information exchange between the preparation of input randomness and the preparation of entangled particles, or between the measurement setting at one detector and measurement outcome at the other—by space-like separating relevant events. Alternatively, proper shielding could be applied to prohibit communications between relevant events[7,8]; however, in practice, it is impossible to shield all of the known and unknown types of communication. Although recent progress in loophole-free tests of Bell inequalities[13–16] provides a way of realizing DIQRNG based on the violation of Bell inequalities, the implementation demands unprecedented detection efficiency and system stability. Therefore, DIQRNG remains a formidable challenge.

Second, an independent and identical distribution (i.i.d.) must not be assumed for the behaviour of the adversary, the most general quantum adversary should be considered in the security analysis and the production of random bits must occur at a non-vanishing rate and be noise-tolerant. In the i.i.d. scenario, assuming that the adversarial strategy follows a predetermined probability distribution, the security analysis is greatly simplified, even without considering any internal memory or time-dependent behaviour; however, the i.i.d. assumption in these theories fails in practice because, for example, the adversary may attack the system using the previous results in an adaptive, non-i.i.d. way. Although security against the most general quantum adversaries and without the i.i.d. assumption has been rigorously proved[12,17–21], a method for security analysis that is efficient for a non-infinite amount of data (and can therefore be tested experimentally) was demonstrated only very recently. A method for DIQRNG that does not use the i.i.d. assumption and that considers a general quantum adversary was proposed recently[12], based on the entropy accumulation theorem[21]. With this method, the rate of randomness generation approaches the value for the i.i.d. case in the limit of a large amount of data. We have previously presented an experimental demonstration of DIQRNG[22] that closed the detection loophole but did not consider space-like-separated events. Here we report fully functional DIQRNG, evidenced by rigorously satisfying the two sets of conditions discussed above in our experimental set-up and by accounting for general quantum adversaries in the security analysis. The device-independent quantum random-number generator that we demonstrate outputs genuinely, quantum-certified random bits at a rate of 181 bits s^{-1}—an important step towards practical applications.

Our realization of DIQRNG is based on a sequence of Bell-test experiments in the format of the Clauser–Horne–Shimony–Holt (CHSH) game[23]. We assume neither modelling of the physical apparatus nor any relation between different experimental trials. Time-dependent or memory-like effects may be present across experimental trials. We adopt the spot-checking protocol[10,12,24] for our experimental implementation. In experimental trial *i*, Alice and Bob, who are spatially separated, each receives a photon from an entangled pair. A classical

[1]National Laboratory for Physical Sciences at Microscale and Department of Modern Physics, University of Science and Technology of China, Hefei, 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, China. [3]Center for Quantum Information, Institute for Interdisciplinary Information Sciences, Tsinghua University, Beijing, China. [4]State Key Laboratory of Functional Materials for Informatics, Shanghai Institute of Microsystem and Information Technology, Chinese Academy of Sciences, Shanghai, China. [5]NTT Basic Research Laboratories and NTT Research Center for Theoretical Quantum Physics, NTT Corporation, Atsugi, Japan. *e-mail: xma@tsinghua.edu.cn; fanjy@ustc.edu.cn; qiangzh@ustc.edu.cn; pan@ustc.edu.cn

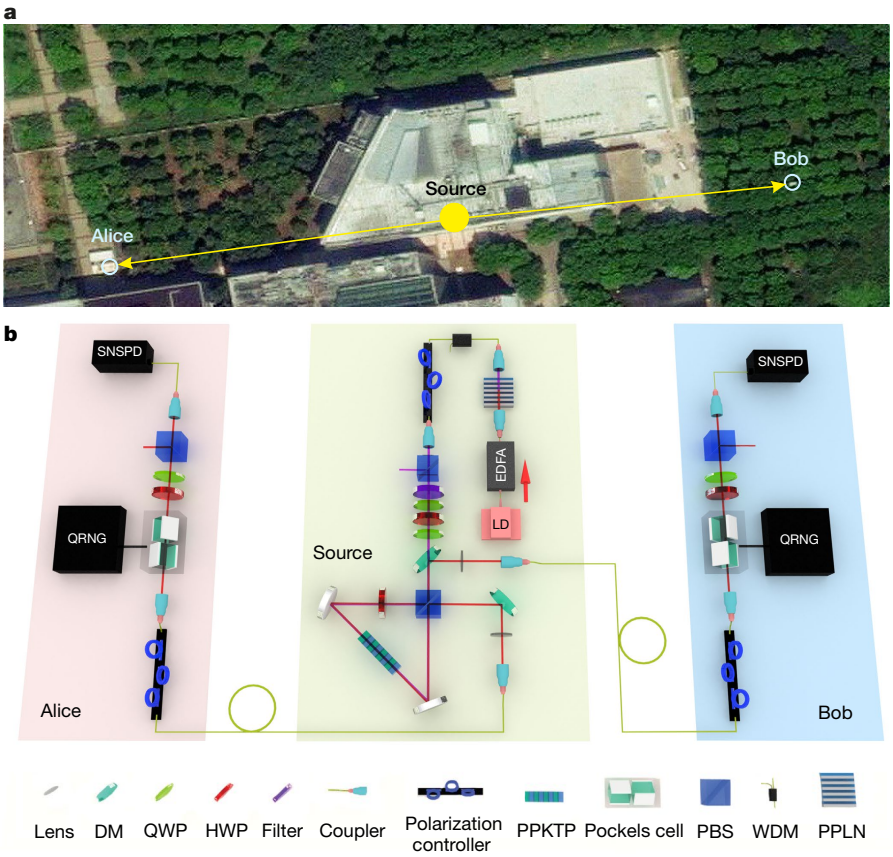

Fig. 1 | Schematics of the experiment. a, Top view of the experimental layout. Alice's and Bob's measurement stations are on the opposite sides of the source of entangled photon pairs, at distances of 93 ± 1 m and 90 ± 1 m, respectively, where the errors quoted are system errors. (We measure the distance by holding whiteboards and measuring the distance with a laser ranger; the error measured this way is estimated to be less than 1 m.) **b**, Middle, creation of pairs of entangled photons. Light pulses of 10-ns duration and 200-kHz frequency from a 1,560-nm laser diode (LD) are amplified by an erbium-doped fibre amplifier (EDFA) and frequency-doubled in an in-line periodically poled lithium niobate crystal (PPLN); the red arrow indicates the direction of the light. The resultant 780-nm light pulses are focused into a periodically poled potassium titanyl phosphate crystal (PPKTP) in a Sagnac loop to generate polarization-entangled photon pairs. A half-wave plate (HWP) and two quarter-wave plates (QWPs) are used to control the relative amplitude and phase in the polarization-entangled two-photon state that is created. Left and right, measuring the polarization of single photons. The single photons exit the fibre, experience the polarization-state measurement in free space and are collected into single-mode optical fibres to be detected by superconducting nanowire single-photon detectors (SNSPDs). The apparatus that is used to perform the measurement consists of a Pockels cell, a quarter-wave plate, a half-wave plate and a polarizing beam splitter (PBS). Quantum random-number generators (QRNGs) output random bits, triggering the Pockels cell to switch between two polarization orientations. DM, dichroic mirror; WDM, wavelength-division multiplexer. Underlying map in **a** from Google, DigitalGlobe.

bit $t_i = 0$ or $t_i = 1$ is generated with probability $1 - q$ or q, respectively. If $t_i = 0$, then the trial is a 'generation' trial, with fixed inputs for Alice and Bob, $x_i = 0$ and $y_i = 0$, respectively. If $t_i = 1$, then the trial is a 'test' trial to test against adversaries. In our experiment, we set all trials to be test trials by choosing $q = 0$. In each test trial, Alice and Bob each receives a bit from a quantum random-number generator, $x_i, y_i \in \{0, 1\}$, as an input that determines their measurement setting. Alice's (Bob's) measurement setting is not affected by Bob's (Alice's) measurement setting or measurement outcome, and is independent of the entanglement creation at the source. Hence, the experiment satisfies the no-signalling condition. We assume that the two random inputs, x_i and y_i, are created independently of the rest of the experiment, and that their creation is i.i.d. for all of the n trials. The corresponding measurement outcomes are $a_i, b_i \in \{0, 1\}$. We assign a CHSH game value of $J_i = 1$ if $a_i \oplus b_i = x_i y_i$ and of $J_i = 0$ otherwise.

Considering uniform inputs for all n experimental trials (so that the probability of selecting any $x_i, y_i \in \{0, 1\}$ is 1/4), the CHSH game value $\bar{J}$ over all n experimental trials is

$$\bar{J} = \frac{1}{n}\sum_{i=1}^{n} J_i - 3/4$$

The experiment is subject to various possible loss mechanisms. We require that the photon loss is low enough to close the detection loophole. Any adversarial strategies based on local hidden-variable models yield $\bar{J} \leq 0$. Therefore, $\bar{J} > 0$ indicates that the measurement outcomes cannot be pre-determined and therefore represent genuine, unpredictable quantum randomness.

The amount of unpredictable randomness that can be extracted in the presence of the quantum adversary system E is quantified by the smooth min-entropy[12]:

$$H_{\min}^{\varepsilon_s}(\mathbf{AB}|\mathbf{XY}E) \geq nR_{\text{opt}}(\varepsilon_s, \varepsilon_{\text{EA}}, \omega_{\text{exp}})$$

with smoothing parameter ε_s, expected CHSH game value ω_{exp} and failure probability for the entropy accumulation protocol ε_{EA}. $\mathbf{X}$ and $\mathbf{Y}$ denote the input sequences for Alice and Bob, respectively, and $\mathbf{A}$ and $\mathbf{B}$ the corresponding output sequences. The lower bound of the generation rate, $R_{\text{opt}}(\varepsilon_s, \varepsilon_{\text{EA}}, \omega_{\text{exp}})$, is used as the theoretical amount of randomness on average for each trial. See Supplementary Information section I.B for details. By using a Toeplitz-matrix hashing extractor with a size of $n \times [H_{\min}^{\varepsilon_s}(\mathbf{AB}|\mathbf{XY}E) - t_e]$, where t_e is the number of bits sacrificed to minimize the information that an adversary may acquire (a parameter that is relevant to the failure probability of the extractor),

we extract $H_{\min}^{\varepsilon_s}(\mathbf{AB}|\mathbf{XY}E) - t_e$ random bits with genuine unpredictability from the raw data obtained in the n experimental trials. The random bits are $\varepsilon_s + \varepsilon_{EA} + 2^{-t_e}$ close to a uniform distribution, where 2^{-t_e} is the failure probability in extraction, with $t_e = 100$.

Although we do not assume the inner workings of the devices, we still require a few assumptions in our experimental implementation: (1) that the devices and adversaries behave according to the laws of either classical or quantum mechanics; (2) that Alice's and Bob's devices are located in one secure laboratory so that the adversaries cannot access their measurement outcomes; (3) that Alice and Bob each receives a sequence of uniform random bits to determine their measurement setting from an independent, trusted source; and (4) that Alice and Bob each has a trusted classical post-processing unit to extract the final random bits. In general, device-independent protocols (in particular for quantum key distribution) assume that Alice's and Bob's devices are located in two secure laboratories and in between them there is a classical authentication channel. In these cases, the publicly announced information may be leaked to the adversaries. The security is then compromised by reusing the devices. Any attack based on this premise is known as a memory attack[25]. With the above assumptions and by ensuring no information leakage, our implementation is secure against memory attacks. In our experiment, quantum random numbers are required as inputs to switch the measurement basis in the Bell inequality. In this sense, our experiment can be seen as a type of randomness expansion, which generates more randomness from a random seed. An interesting future direction of research would be to create nearly perfect random numbers from weak randomness, which may require more than one set of Bell-test equipment.

Our experimental implementation is depicted in Fig. 1. We create entangled photon pairs at a wavelength of 1,560 nm using spontaneous parametric downconversion in a Sagnac interferometer (see Methods). We then distribute the two photons of a pair in opposite directions to Alice's and Bob's measurement stations, which are at distances of 93 m and 90 m from the source, respectively. A detailed space–time analysis (Fig. 2) shows that the relevant events in the experiment are space-like-separated (Supplementary Information section II.E). We obtain an overall efficiency from the creation to the detection of the entangled photons of 78.8% ± 1.9% for Alice and 78.5% ± 1.5% for Bob[26] (where the errors quoted are one standard deviation), surpassing the threshold to close the detection loophole (Supplementary Information section II.C).

To achieve the maximum violation of the Bell inequality[27], we create a non-maximally polarization-entangled two-photon state, $\cos(22.05^\circ)|HV\rangle + \sin(22.05^\circ)|VH\rangle$ and choose the measurement settings to be -83.5° (for $x_i = 0$) or -119.4° (for $x_i = 1$) for Alice and 6.5° (for $y_i = 0$) or -29.4° (for $y_i = 1$) for Bob when measuring the polarization state of the entangled photons. The measurement settings are selected randomly by the quantum random-number generators in each experimental trial. The two quantum random-number generators are based on vacuum noise fluctuation (Supplementary Information section II.A).

Our system is now robust against noise, which allows us to complete $n = 6.895 \times 10^{10}$ experimental trials in 95.77 experimental hours, operating continuously. To quantify the significance of our experimental results, we perform a hypothesis test of local realism. The null hypothesis is that the experimental results are explainable by local realism under the assumption that the input distribution at each trial is uniform. The evidence against local realism, under the above assumption, is quantified by a statistical P value computed using a test statistic. The P value is the maximum probability according to local realism that the statistic takes a value as extreme as the observed one. Hence, small P values imply strong evidence against local realism. We apply the prediction-based ratio (PBR) method of analysis[28] to design the test statistic and compute an upper bound for the P value. The PBR analysis provides valid upper bounds for P values without assuming the i.i.d. condition. The upper bound that is returned after the whole experiment is $p_{LR} = 10^{-204,792}$, indicating a strong rejection of local

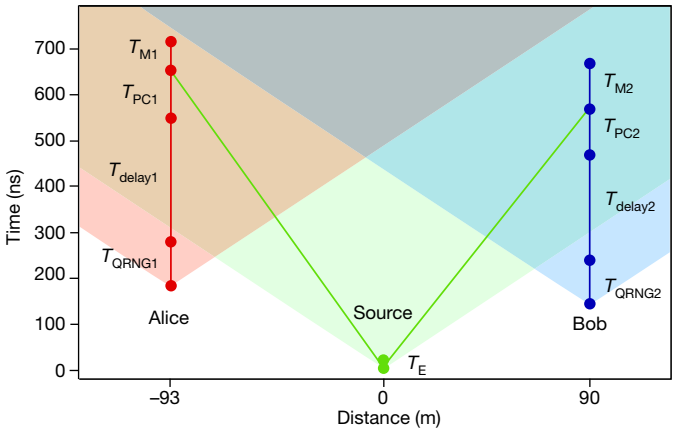

Fig. 2 | Space–time diagram for the experimental design. $T_E = 10$ ns is the time taken to generate a pair of entangled photons. $T_{QRNG1,2}$ are the times required to generate random bits to switch the Pockels cells. $T_{delay1,2}$ are the lengths of time between the random bits being generated and delivered to the Pockels cells. $T_{PC1,2}$ are the waiting times for the Pockels cells to be ready to perform state measurements after receiving the random bits. $T_{M1,2}$ are the times taken by the superconducting nanowire single-photon detectors to output electronic signals. For $T_{QRNG1} = T_{QRNG2} = 96$ ns, $T_{delay1} = 270$ ns, $T_{delay2} = 230$ ns, $T_{PC1} = 112$ ns, $T_{PC2} = 100$ ns, $T_{M1} = 50$ ns and $T_{M2} = 100$ ns, we place Alice's and Bob's measurement stations on opposite sides of the source at distances of 93 m and 90 m, respectively. The effective optical length between Alice's (Bob's) station and the source is 132 m (119 m). This arrangement ensures no signalling between relevant events in the experiment. The shaded areas are the future light cones for the source, Alice and Bob.

hidden-variable models (see Supplementary Information III.C). With the PBR method, we also test the null hypothesis that the experimental results satisfy the no-signalling condition under the assumption that the input distribution at each trial is uniform. In this case, we obtain an upper bound of $p_{NS} = 1$, indicating no evidence of anomalous signalling in the experiment (see Supplementary Information section III.B).

We compute the CHSH game value J over n experimental trials to be $\bar{J} = 2.757 \times 10^{-4}$. By setting the expected CHSH game value to that measured in the experiment, $\omega_{exp} = 2.757 \times 10^{-4}$, and assuming that $\varepsilon_s = \varepsilon_{EA} = \sqrt{1/n} = 3.8 \times 10^{-6}$ and that the width of the statistical confidence interval for the estimate of the Bell violation is $\delta_{est} = \sqrt{10/n} = 1.2042 \times 10^{-5}$, we find a total failure probability of $\varepsilon_s + \varepsilon_{EA} + 2^{-t_e} < 1 \times 10^{-5}$. After developing a computing technique for fast Toeplitz-matrix multiplication (Supplementary Information section II.H) that allows us to apply an 137.90 Gb × 62.469 Mb Toeplitz-matrix hashing, we obtain 6.2469×10^7 genuinely, quantum-certified random bits, corresponding to a rate of 181.2 bits s^{-1}, with a total failure probability of 10^{-5}. The stream of random bits passes the National Institute of Standards and Technology (NIST) statistic test suite (Supplementary Information section III.A). As shown in Fig. 3, the amount of randomness generated with our experimental set-up is 56.9% of the optimal value in the i.i.d. case for $n = 6.895 \times 10^{10}$, and asymptotically approaches the optimal value with an increasing number of experimental trials. In the inset of Fig. 3 we plot the randomness production as a function of time, demonstrating the robustness of the system.

In conclusion, we report here the realization of DIQRNG that is secure against the most general quantum adversaries and outputs 181 quantum-certified random bits per second. A next step will be to improve the violation of the Bell inequality and the stability of the system to achieve higher production rates of quantum-certified random bits for practical applications that require high levels of security. We anticipate that our work will be helpful in topics such as randomness amplification[29], the minimum assumption necessary for randomness generation, and fundamental problems relating to the understanding of non-locality, entanglement and randomness[7].

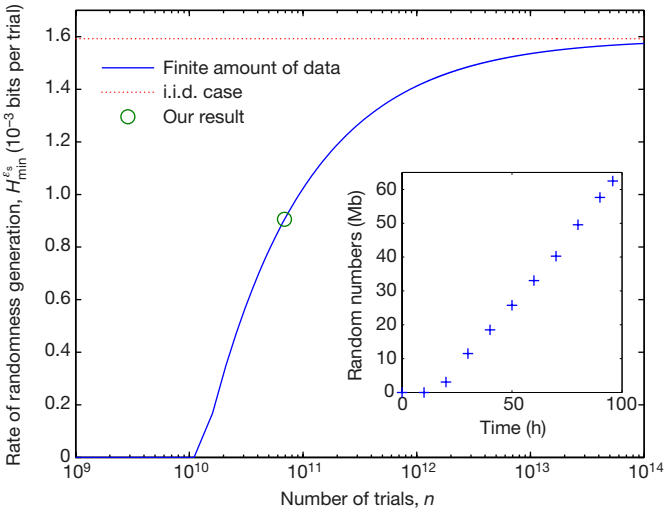

Fig. 3 | Randomness generation versus number of trials. The solid blue curve and dashed red curve show the theoretical rate of randomness generation $H_{\min}^{\varepsilon_s}$ versus the number of trials n for a finite amount of data (up to 10^{14}) and the i.i.d. case, respectively. The green circle denotes our experimental result. The inset shows the number of random numbers generated versus time in our experiment. We set $\omega_{\exp} = 2.757 \times 10^{-4}$, $\varepsilon_s = \varepsilon_{EA} = 1/\sqrt{n}$ and $\delta_{est} = \sqrt{10/n}$ for the finite data rate.

Online content

Any methods, additional references, Nature Research reporting summaries, source data, statements of data availability and associated accession codes are available at https://doi.org/10.1038/s41586-018-0559-3.

Received: 7 February 2018; Accepted: 23 August 2018;
Published online 19 September 2018.

1. Shannon, C. E. Communication theory of secrecy systems. *Bell Labs Tech. J.* **28**, 656–715 (1949).
2. Metropolis, N. & Ulam, S. The Monte Carlo method. *J. Am. Stat. Assoc.* **44**, 335–341 (1949).
3. Colbeck, R. *Quantum and Relativistic Protocols for Secure Multi-party Computation*. PhD thesis, Cambridge Univ. (2009).
4. Mayers, D. & Yao, A. Quantum cryptography with imperfect apparatus. In *Proc. 39th Annual Symposium on Foundations of Computer Science* (ed. Motwani, R.) 503–509 (IEEE, 1998).
5. Ma, X., Yuan, X., Cao, Z., Qi, B. & Zhang, Z. Quantum random number generation. *npj Quantum Inf.* **2**, 16021 (2016).
6. Herrero-Collantes, M. & Garcia-Escartin, J. C. Quantum random number generators. *Rev. Mod. Phys.* **89**, 015004 (2017).
7. Acín, A. & Masanes, L. Certified randomness in quantum physics. *Nature* **540**, 213–219 (2016).
8. Pironio, S. et al. Random numbers certified by Bell's theorem. *Nature* **464**, 1021–1024 (2010).
9. Bierhorst, P. et al. Experimentally generated randomness certified by the impossibility of superluminal signals. *Nature* **556**, 223–226 (2018).
10. Miller, C. A. & Shi, Y. Universal security for randomness expansion from the spot-checking protocol. *SIAM J. Comput.* **46**, 1304–1335 (2017).
11. Vazirani, U. V. & Vidick, T. Certifiable quantum dice - or, testable exponential randomness expansion. Preprint at https://arxiv.org/abs/1111.6054 (2011).
12. Arnon-Friedman, R., Renner, R. & Vidick, T. Simple and tight device-independent security proofs. Preprint at https://arxiv.org/abs/1607.01797 (2016).
13. Hensen, B. et al. Loophole-free Bell inequality violation using electron spins separated by 1.3 kilometres. *Nature* **526**, 682–686 (2015).
14. Shalm, L. K. et al. Strong loophole-free test of local realism. *Phys. Rev. Lett.* **115**, 250402 (2015).
15. Giustina, M. et al. Significant-loophole-free test of Bell's theorem with entangled photons. *Phys. Rev. Lett.* **115**, 250401 (2015).
16. Rosenfeld, W. et al. Event-ready Bell test using entangled atoms simultaneously closing detection and locality loopholes. *Phys. Rev. Lett.* **119**, 010402 (2017).
17. Vazirani, U. & Vidick, T. Fully device-independent quantum key distribution. *Phys. Rev. Lett.* **113**, 140501 (2014).
18. Miller, C. A. & Shi, Y. Robust protocols for securely expanding randomness and distributing keys using untrusted quantum devices. *J. ACM* **63**, 33 (2016).
19. Chung, K.-M., Shi, Y. & Wu, X. Physical randomness extractors: generating random numbers with minimal assumptions. Preprint at https://arxiv.org/abs/1402.4797 (2014).
20. Coudron, M. & Yuen, H. Infinite randomness expansion with a constant number of devices. In *Proc. 46th Annual ACM Symposium on Theory of Computing* (ed. Shmoys, D.) 427–436 (ACM, 2014).
21. Dupuis, F., Fawzi, O. & Renner, R. Entropy accumulation. Preprint at https://arxiv.org/abs/1607.01796 (2016).
22. Liu, Y. et al. High-speed device-independent quantum random number generation without a detection loophole. *Phys. Rev. Lett.* **120**, 010503 (2018).
23. 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).
24. Coudron, M., Vidick, T. & Yuen, H. Robust randomness amplifiers: upper and lower bounds. In *Proc. APPROX 2013: Approximation, Randomization, and Combinatorial Optimization. Algorithms and Techniques* (eds Raghavendra, P. et al.) 468–483 (Springer, 2013).
25. Barrett, J., Colbeck, R. & Kent, A. Memory attacks on device-independent quantum cryptography. *Phys. Rev. Lett.* **110**, 010503 (2013).
26. Pereira, M. D. C. et al. Demonstrating highly symmetric single-mode, single-photon heralding efficiency in spontaneous parametric downconversion. *Opt. Lett.* **38**, 1609–1611 (2013).
27. Eberhard, P. H. Background level and counter efficiencies required for a loophole-free Einstein-Podolsky-Rosen experiment. *Phys. Rev. A* **47**, R747–R750 (1993).
28. Zhang, Y., Glancy, S. & Knill, E. Asymptotically optimal data analysis for rejecting local realism. *Phys. Rev. A* **84**, 062118 (2011).
29. Kessler, M. & Arnon-Friedman, R. Device-independent randomness amplification and privatization. Preprint at https://arxiv.org/abs/1705.04148 (2017).

Acknowledgements We thank S.-R. Zhao, Y.-H. Li, L.-K. Chen and R. Jin for experimental assistance, J. Zhong and S.-C. Shi for low-temperature system maintenance, and T. Peng, Y. Cao, C.-Z. Peng and Y.-A. Chen for discussions. This work was supported by the National Key R&D Program of China (2017YFA0303900, 2017YFA0304000), the National Natural Science Foundation of China, the Chinese Academy of Sciences and the Anhui Initiative in Quantum Information Technologies.

Reviewer information *Nature* thanks R. Colbeck and the other anonymous reviewer(s) for their contribution to the peer review of this work.

Author contributions X.M., J.F., Q.Z. and J.-W.P. conceived the research. Y.L., X.M., J. F., Q.Z. and J.-W.P. designed the experiment. Y.L., M.-H.L. and C.W. designed and implemented the source of entangled photon pairs. W.-Z.L. and J.-Y.G. designed the data acquisition software. W.Z., H.L., Z.W. and L.Y. fabricated and characterized the superconducting nanowire single-photon detector. B.B. and J.Z. designed the quantum random-number generators for the measurement setting choices. Q. Zhao, X.Y. and X.M. performed the protocol analysis, numerical modelling and randomness extraction. Y.Z. and W.J.M. performed the hypothesis tests. All authors contributed to the experimental realization, data analysis and manuscript preparation. J.-W.P. supervised the project.

Competing interests The authors declare no competing interests.

Additional information
Supplementary information is available for this paper at https://doi.org/10.1038/s41586-018-0559-3.
Reprints and permissions information is available at http://www.nature.com/reprints.
Correspondence and requests for materials should be addressed to X.M. or J.F. or Q.Z. or J.-W.P.
Publisher's note: Springer Nature remains neutral with regard to jurisdictional claims in published maps and institutional affiliations.

METHODS

No statistical methods were used to predetermine sample size.

Entanglement creation, distribution, and detection at low loss. The experimental layout is depicted in Fig. 1. A 1,560-nm laser outputs 10-ns laser pulses periodically at a repetition rate of 200 kHz. The pulses are amplified by an erbium-doped fibre amplifier and frequency-doubled in an in-line periodically poled lithium niobate crystal. After removing the residual 1,560-nm light with a wavelength-division multiplexer and spectral filters, the 780-nm light pulses that are generated are focused into a periodically poled potassium titanyl phosphate (PPKTP) crystal with a poling period of 46.5 μm in a Sagnac loop to generate polarization-entangled photon pairs via a type-II spontaneous parametric downconversion process.

We optimize the efficiency to couple the entangled photons that are created into a single-mode optical fibre by setting their beam waists to the theoretical optimized size with respect to that of the pump beam[26,30,31]. For the pump light exiting a 780HP single-mode fibre, which has a mode field diameter of 5 μm, we focus it with a focal length of $f = 8$ mm aspherical lens to the centre of the crystal at a distance of 70 cm, with a measured beam waist of 180 μm and a beam quality factor of $M^2 = 1.05$. The entangled photons are collected into a SMF28e single-mode optical fibre, which has a mode field diameter of 10.4 μm. With a $f = 11$ mm aspherical lens and a $f = 175$ mm spherical lens, we set the beam waist to be 85 μm at the centre of the PPKTP crystal. The spherical lens is at a distance of 19 cm from the aspherical lens and 45 cm from the PPKTP crystal.

A half-wave plate and two quarter-wave plates in the beam path of the pump light are used to control the relative amplitude and phase in the polarization-entangled two-photon state. The residual 780-nm pump light is removed by dichroic mirrors. The entanglement source is placed on a 1 m × 1 m breadboard, with the ambient temperature stabilized to be within ±1 °C to improve the stability of the system.

The entangled photons are sent in opposite directions to two remote measurement stations that are 93 ± 1 m and 90 ± 1 m away, ensuring space-like separation between the event of entanglement creation in the source and the event of choosing the measurement settings at the measurement stations, and between the event of choosing the measurement setting at one station and the events of choosing the measurement setting and outputting the outcomes at the other station (Supplementary Information section II.E).

At the measurement station, the single photons exit the fibre, pass the Pockels cell, a quarter-wave plate and a half-wave plate, and a polarizing beam splitter, and are coupled into the single-mode optical fibre to be detected by the superconducting nanowire single-photon detectors[32]. The Pockels cell is switched to set the base for the measurement of the single-photon polarization upon receiving a bit from a quantum random-number generator. A time–digital converter is used to time-tag the events for random-number generation, single-photon detection and synchronization signal.

We measure the overall efficiency from the creation to the detection of single photons to be 78.8% ± 1.9% for Alice and 78.5% ± 1.5% for Bob, surpassing the threshold to close the detection loophole. The loss is mainly due to the limited efficiency: 94% in collecting the photon pairs that are created into single-mode optical fibre, and 92% for the superconducting nanowire single-photon detectors (Supplementary Information section II.C).

Data availability

The data that support the findings of this study are available from the corresponding authors on reasonable request. Source Data for Fig. 3 is provided with the online version of the paper.

30. Bennink, R. Optimal collinear Gaussian beams for spontaneous parametric down-conversion. *Phys. Rev. A* **81**, 053805 (2010).
31. Dixon, P. B. et al. Heralding efficiency and correlated-mode coupling of near-IR fiber-coupled photon pairs. *Phys. Rev. A* **90**, 043804 (2014).
32. Zhang, W. et al. NbN superconducting nanowire single photon detector with efficiency over 90% at 1550 nm wavelength operational at compact cryocooler temperature. *Sci. China Phys. Mechan. Astron.* **60**, 120314 (2017).