Device-independent quantum random-number generation

Yang Liu1,2, Qi Zhao3, Ming-Han Li1,2, Jian-Yu Guan1,2, Yanbao Zhang5, Bing Bai1,2, Weijun Zhang3, Wen-Zhao Liu1,2, Cheng Wu1,2, Xiao Yuan1,2,3, Hao Li4, W. J. Munro5, Zhen Wang4, Lixing You4, Jun Zhang1,2, Xiongfeng Ma3,8, Jingyun Fan1,2, Qing Zhang1,2,8 & Jian-Wei Pan1,2,8

Randomness is important for many information processing applications, including numerical modelling and cryptography1,2. 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 science5–7. Previously reported experimental demonstrations of DIQRNG3,8 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 adversaries8–12. 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 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 × 1011 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 randomness7. 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 events12–20; 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 inequalities21–23 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 proved12,17–21, 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 recently12, based on the entropy accumulation theorem21. 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 DIQRNG22 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) game23. 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 protocol10,12,24 for our experimental implementation. In experimental trial 1, Alice and Bob, who are spatially separated, each receives a photon from an entangled pair. A classical
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 $\mathcal{J} \leq 0$. Therefore, $\mathcal{J} > 0$ 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:\cite{58}

$$H_{\varepsilon}^{\min}(AB|XYE) \geq n R_{\text{opt}}(\varepsilon, \varepsilon_{\text{EA}}, \omega_{\exp})$$

with smoothing parameter $\varepsilon_s$, expected CHSH game value $\omega_{\exp}$ and failure probability for the entropy accumulation protocol $\varepsilon_{\text{EA}}$, $X$ and $Y$ denote the input sequences for Alice and Bob, respectively, and $A$ and $B$ the corresponding output sequences. The lower bound of the generation rate, $R_{\text{opt}}(\varepsilon, \varepsilon_{\text{EA}}, \omega_{\exp})$, 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 $n \times [H_{\varepsilon}^{\min}(AB|XYE) - t_c]$, where $t_c$ 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 $H_{\text{EPR}}(AB;XY|E) \sim t_n$ random bits with genuine unpredictability from the raw data obtained in the $n$ experimental trials. The random bits are $\varepsilon + \varepsilon_{\text{EA}} + 2^{-5}$ close to a uniform distribution, where $2^{-5}$ is the failure probability in extraction, with $t_n = 100$.

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\textsuperscript{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\textsuperscript{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\textsuperscript{27}, we create a non-maximally polarization-entangled two-photon state, $\cos(22.05\degree)|HV\rangle + \sin(22.05\degree)|VH\rangle$ and choose the measurement settings to be $-83.5\degree$ (for $x = 0$) or $-194.4\degree$ (for $x = 1$) for Alice and $6.5\degree$ (for $y = 0$) or $-29.4\degree$ (for $y = 1$) 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 $n = 6.895 \times 10^8$ 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\textsuperscript{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 $P_{\text{LR}} = 10^{-204,792}$, indicating a strong rejection of local 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 $P_{\text{NS}} = 1$, 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 $J = 2.757 \times 10^{-4}$. By setting the expected CHSH game value to that measured in the experiment, $\omega_{\exp} = 2.757 \times 10^{-4}$, and assuming that $\varepsilon = \varepsilon_{\text{EA}} = \sqrt{1/n} = 3.8 \times 10^{-8}$ and that the width of the statistical confidence interval for the estimate of the Bell violation is $\varepsilon_{\text{raw}} = \sqrt{1/n} = 2.042 \times 10^{-8}$, we find a total failure probability of $\varepsilon + \varepsilon_{\text{EA}} + 2^{-5} < 1 \times 10^{-5}$. After developing a computing technique for fast Toeplitz-matrix multiplication (Supplementary Information section III.H) that allows us to apply an 137.90 Gb × 62.469 Mb Toeplitz-matrix hashing, we obtain 6.2469 × 10$^8$ 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 $n = 6.895 \times 10^8$, 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\textsuperscript{29}, the minimum assumption necessary for randomness generation, and fundamental problems relating to the understanding of non-locality, entanglement and randomness\textsuperscript{7}.
Online content

Fig. 3 | Randomness generation versus number of trials. The solid blue curve and dashed red curve show the theoretical rate of randomness generation $H^\text{th}$ versus the number of trials $n$ for a finite amount of data (up to $10^9$) 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 $\omega_{\text{exp}} = 2.757 \times 10^{-4}$, $\varepsilon_\text{f} = \varepsilon_\text{E} = 1/\sqrt{n}$ and $\varepsilon_\text{est} = \sqrt{10/n}$ for the finite data rate.

Acknowledgements We thank S.-R. Zhao, Y.-H. Li, L.-K. Chen and R. Jin for experimental assistance. Zhong and S.-L. 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.

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.-W.P.

Publisher’s note: Springer Nature remains neutral with regard to jurisdictional claims in published maps and institutional affiliations.
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\(^{28,30,31}\). 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 15250 nm wavelength operational at compact cryocooler temperature. **Sci. China Phys. Mech. Astron.** 60, 120314 (2017).