npj | Quantum Information www.nature.com/npjqi

ARTICLE OPEN

Quantum random number generation with uncharacterized laser and sunlight

Yu-Huai Li[1,2], Xuan Han[1,2], Yuan Cao[1,2*], Xiao Yuan[1,2,3], Zheng-Ping Li[1,2], Jian-Yu Guan[1,2], Juan Yin[1,2], Qiang Zhang[1,2], Xiongfeng Ma[3*], Cheng-Zhi Peng[1,2*] and Jian-Wei Pan[1,2]

The entropy or randomness source is an essential ingredient in random number generation. Quantum random number generators generally require well modeled and calibrated light sources, such as a laser, to generate randomness. With uncharacterized light sources, such as sunlight or an uncharacterized laser, genuine randomness is practically hard to be quantified or extracted owing to its unknown or complicated structure. By exploiting a recently proposed source-independent randomness generation protocol, we theoretically modify it by considering practical issues and experimentally realize the modified scheme with an uncharacterized laser and a sunlight source. The extracted randomness is guaranteed to be secure independent of its source and the randomness generation speed reaches 1 Mbps, three orders of magnitude higher than the original realization. Our result signifies the power of quantum technology in randomness generation and paves the way to high-speed semi-self-testing quantum random number generators with practical light sources.

npj Quantum Information (2019)5:97 ; https://doi.org/10.1038/s41534-019-0208-1

INTRODUCTION

Random numbers play a vital role in various tasks, such as cryptography,[1] numerical simulation,[2] and lottery. For example, in the well-known quantum key distribution (QKD) protocol proposed by Bennett and Brassard,[3] the security is guaranteed by random choices of the encoding and measurement bases. Distinct from deterministic evolution of classical processes, quantum mechanics endows the capability of generating genuine randomness by collapsing the coherence in the measurement basis.[4,5]

According to the generation speed and the randomness reliability, quantum random number generators (QRNGs) can be categorized into following three types. Practical QRNGs, which assume well characterized devices, normally have a fast generation speed.[6–8] Fully self-testing QRNGs, which adopt no assumptions on device implementations, generally have a low randomness generation speed owing to the stringent requirements.[9–13] Semi-self-testing QRNGs lies somewhere in between, which have certain assumptions of device implementations while have high randomness generation speed in the meantime.[14–21] We refer to ref. [22] for a detailed review of the developments of different types of QRNGs. For these three types, a tradeoff between the randomness generation speed and the randomness reliability exists in practice. In many tasks such as QKD, both the randomness generation speed and the reliability are required in order to ensure the key generation rate and the security. For those tasks, semi-self-testing QRNGs serve as promising candidates that fulfill both requirements.

Recently, several semi-self-testing QRNG schemes have been proposed.[14–21] By assuming the underlying dimension and the independence of the source and the measurement, a QRNG scheme[14] has been proposed such that the output randomness can be self-tested. While, as the randomness is certified by the input and output statistics, the random number generation rate is only about 23 bps. The generation rate was further improved to the order of MHz with input and output statistics and weaker assumptions.[18,19] Later, with trusted measurement but uncharacterized randomness source, a source-independent (SI) QRNG scheme is proposed,[15] where the randomness generation speed is analyzed to be comparable to practical QRNGs that has characterized devices. Conventionally, QRNGs make use of special light sources, such as lasers, and specific physical model to characterize the randomness source. With more common light sources, such as sunlight, and no assumptions of the randomness origin, the SI-QRNG scheme can still faithfully generate random numbers.

In this work, we explore randomness generation with general light sources, laser and sunlight without assuming the physical structures. By exploiting the SI-QRNG scheme[15] and considering practical issues of measurement device imperfections, we experimentally demonstrate the possibility of fast and reliable randomness generation.

RESULTS

Scheme

As shown in Fig. 1, a conventional QRNG is composed of the randomness source and the detection device.[22] In the source part, it consists of a light source and a state preparation device. Generally, practical QRNGs[6–8] make use of specific models to describe the structure of the randomness source. While the SI-QRNG scheme[15] supplies the possibility of randomness generation without assuming neither the light source nor the state preparation devices.

First, we review the concept of SI-QRNG based on the scheme of ref. [15] The SI randomness generation procedure is summarized by

[1]Hefei National Laboratory for Physical Sciences at Microscale and Department of Modern Physics, University of Science and Technology of China, Hefei, Anhui 230026, China. [2]CAS Center for Excellence and Synergetic Innovation Center in Quantum Information and Quantum Physics, University of Science and Technology of China, Shanghai 201315, China. [3]Center for Quantum Information, Institute for Interdisciplinary Information Sciences, Tsinghua University, Beijing 100084, China. *email: yuancao@ustc.edu.cn ; xma@tsinghua.edu.cn; pcz@ustc.edu.cn

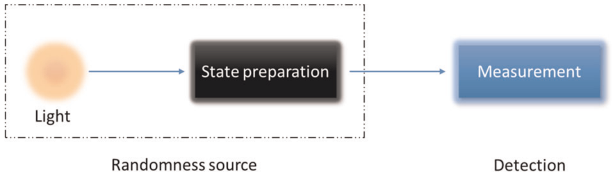

Fig. 1 Source-independent randomness generation with uncharacterized light source and state preparation

source, squashing, random sampling, parameter estimation, and randomness extraction, as follows.

- The state preparation device is expected to prepare the light in the polarization state of $|+\rangle = (|H\rangle + |V\rangle)/\sqrt{2}$, where $Z = \{|H\rangle, |V\rangle\}$ is the computational basis. While no assumption is made on the photon source, it is untrusted and could be controlled by Eve. Thus, the actual prepared quantum state may have an arbitrary and unknown dimension. Randomness can still be quantified and extracted with the following steps.
- The squashing process maps arbitrary quantum states into qubits and vacuum states. The vacuum components are regarded as loss. In practice, the squashing process can be realized by adding a series of spectrum, spatial and temporal filters to post-select the expected optical modes.
- In the measurement, we randomly choose the $X = \{|\pm\rangle = (|H\rangle \pm |V\rangle)/\sqrt{2}\}$ and Z basis to measure according to a random seed. The random seed needed is exponentially smaller than the number of extracted random bits.[15] Suppose that the number of runs in total is N, including N_X in the X basis and N_Z in the Z basis. Due to the loss, the output of detection could be null. In this case, the number of qubits measured in total is n, including n_X in the X basis and n_Z in the Z basis. It is worth noting that this protocol is loss tolerance. In the ideal case, the measurement device chooses the measurement basis after confirming the received state is not a vacuum state. In practice, the measurement basis is chosen before the confirmation of loss, which is usually done by observing whether detectors click or not. However, the detection device does not anticipate the position of losses. Thus the effect of loss only decreases n_X and n_Z, but the positions of the effective X and Z measurements are still uniformly random.
- When measuring in the X basis, the result of $|-\rangle$ is defined to be an error, and a double click is considered as a half error. Then, we can evaluate the phase error e_{pZ} in the Z basis according to the bit error rate e_{bX} in the X basis and its statistical deviation θ[23] according to

$$\varepsilon_\theta = \mathrm{Prob}\left(\mathrm{e_{pZ}} > \mathrm{e_{bX}} + \theta\right) \le \frac{1}{\sqrt{\mathrm{q_X(1-q_X)e_{bX}(1-e_{bX})n}}} 2^{-\mathrm{n}\xi(\theta)}, \tag{1}$$

  where $\xi(\theta) = H(e_{bX}+\theta-q_X\theta) - q_X H(e_{bX}) - (1-q_X)H(e_{bX}+\theta)$. Here $q_X = n_X/n$ is the ratio of the X basis measurement. $H(x) = -x\log_2(x) - (1-x)\log_2(1-x)$ is the binary Shannon entropy function. Since the dimension of the source is unlimited, it may emit multiphoton states. When using threshold detectors, multiphoton states may cause double clicks, which directly contribute to the error rate e_{bX} and decrease the number of extracted random bits.
- By utilizing the Toeplitz-matrix hashing method,[24] the phase error can be corrected by consuming $n_Z H(e_{bX}+\theta)$ number of bits with a failing probability of 2^{-t_e}.[25] Thus, we can finally extract

$$R_0 = n_Z - n_Z H(e_{bX}+\theta) - t_e \tag{2}$$

  number of random bits and the final failure probability (in trace-distance measure) is given by $\varepsilon = \sqrt{(\varepsilon_\theta + 2^{-t_e})(2 - \varepsilon_\theta - 2^{-t_e})}$.

Here, R_0 is the number of extracted random bits without considering the imperfections of the measurement devices. In practice, the measurement bases may not be exactly complementary to each other, and the detection efficiencies of the two detectors might be different. With a slight modification to Eq. (2), the number of extracted random bits with imperfect measurement devices R_{final} can still be quantified when these imperfections are characterized. On the other hand, dark counts of the detectors may also increase the phase error rate and decrease the number of extracted random bits. Since the dark counts are independent with respect to the measurement basis, the effect of dark counts can be regarded as noise of the photon source which has already been considered in the analysis.

In the original theoretical proposal, the X and Z basis measurements are assumed perfect. In our work, we also take measurement imperfections into account. Specifically, we consider the case that the actual measurement bases X' and Z' are not complementary to each other. In this case, we can make use of the general uncertainty relation for two general bases,[26]

$$H(Z') \ge -\log_2 \max_{x',z'} |\langle x'|z'\rangle|^2 - H(X'), \tag{3}$$

where $\{|x'\rangle\}$ and $\{|z'\rangle\}$ are, respectively, the eigenstates of X' and Z', and $H(Z')$ and $H(X')$ are, respectively, the entropy of the measurement outcome of X' and Z'. In quantum random number generation, we can regard $-\log_2 \max_{x',z'} |\langle x'|z'\rangle|^2$ as the randomness that we can obtained by measuring an eigenstate of the X' basis, and regard $H(X')$ as the amount of states that are required to distill the eigenstate.[5,27] That is, given N copies of the quantum state ρ, one can effectively first perform a dephasing operation in the X' basis to collapse them into one of its eigenstates. Then we aim to distill the dephased state into a specific eigenstate, which costs $NH(X')$ copies of states. For each eigenstate, it generates $-\log_2 \max_{x',z'} |\langle x'|z'\rangle|^2$ randomness. Therefore, the total randomness obtained is $-N\log_2 \max_{x',z'} |\langle x'|z'\rangle|^2 - NH(X')$ and each state generates $-\log_2 \max_{x',z'} |\langle x'|z'\rangle|^2 - H(X')$ randomness on average. In practice, the dephasing and distillation process can be equivalently achieved with the recently proposed coherence distillation protocols, which can be further reduced to a randomness extraction procedure. Therefore, the final randomness output for two general imperfect bases is

$$R_1 = -2n_Z \log_2 \max_{x',z'} |\langle x'|z'\rangle| - n_Z H(e_{bX}+\theta) - t_e. \tag{4}$$

Note that the randomness output only depends on the term $\max_{x',z'} |\langle x'|z'\rangle|$ instead of a full description of the X' and Z' bases.

In addition, we also consider the case that the measurement efficiencies in the two eigenstates are different. Suppose the efficiencies of projecting onto $|0\rangle$ and $|1\rangle$ are given by η_0 and η_1, respectively. Then according to the standard analysis in QKD,[28] the randomness output will be further modified to

$$R_{\mathrm{final}} = \frac{2\min(\eta_0, \eta_1)}{\eta_0 + \eta_1} \left[-2n_Z \log_2 \max_{x',z'} |\langle x'|z'\rangle| - n_Z H(e_{bX}+\theta) - t_e\right], \tag{5}$$

That is, the total randomness is rescaled with a factor $\frac{2\min(\eta_0,\eta_1)}{\eta_0+\eta_1} \le 1$. The maximum value of 1 can be achieved when $\eta_0 = \eta_1$. Here, we assume that the adversary has no information of the detection efficiency mismatch, otherwise there may exist attacks in analogy to the time-shift attack from QKD.[29] With such an assumption, the factor can be understood as a simple strategy that we randomly discard the measurement outcome of the higher efficiency detector such that the effective efficiencies of the two detectors are the same.

In experiment, the term $\max_{x',z'} |\langle x'|z'\rangle|$ and the efficiency η_0, η_1 can be first measured during a calibration procedure on the measurement device. Then, the SI-QRNG scheme can be applied to produce randomness according to the randomness rate formulae in Eq. (5).

Experimental realization

As shown in Fig. 2, the experiment setup can be accordingly divided into two parts, the randomness source part and the detection part. While the detection part should be elaborately designed and carefully calibrated, the randomness source part can be uncharacterized or even untrusted.

In the detection part, filters in several dimensions are employed to rule out unexpected optical modes. Spectral filters, including two 100 GHz DWDMs and several interference filters, are used to guarantee that only photons with expected wavelength can enter, and the isolation on unwanted wavelength is over 60 dB. The coupling of single mode fiber excluded unwanted spatial modes. Finally, photons arrived at wrong time will be inspected and eliminated by a time-digital converter (TDC). The selection of measurement basis is realized by a Sagnac type interferometer and a phase modulator (PM) to obtain high visibility and stability, as shown in Fig. 2. For an input pulse with arbitrary polarization state of $\alpha|H\rangle + \beta|V\rangle$, where $\alpha^2 + \beta^2 = 1$, it is split by a fiber polarized beam splitter (FPBS2) when entering the Sagnac interferometer. The length of fiber from PM to one port of FPBS2 is 25.2 m shorter than to the other port. Thus, the time for the clockwise ($|H\rangle$) and anti-clockwise ($|V\rangle$) parts of the split pulses reach the PM are separated by around 126 ns, and finally back to FPBS2 at the same time. By carefully control the PM, the two parts of pulse can be applied by different phase, named φ_c and φ_a. After combined again in FPBS2, the state of output pulse is $\alpha e^{i\varphi_c}|H\rangle + \beta e^{i\varphi_a}|V\rangle$, correspond to a unitary operation of U_F. A fiber polarization controller is employed to perform an additional unitary operation of U_C. Here,

$$U_F = \begin{pmatrix} e^{i\varphi_c} & 0 \\ 0 & e^{i\varphi_a} \end{pmatrix}, \quad U_C = \frac{1}{2}\begin{pmatrix} 1+i & 1-i \\ 1-i & 1+i \end{pmatrix}. \tag{6}$$

Finally, after appropriate attenuation, the pulse is separated by FPBS3 and detected by two up-conversion single photon detectors with efficiency of 10%, dark count of 200 cps and dead time of 5 ns.[30] In this way, we can choose to perform Z (X) basis measurement by setting φ_c to be 0 ($-\pi/4$) and φ_a to be 0 ($\pi/4$). The probability of measuring in the Z (X) basis is selected as 99.6% (0.4%) in our experiment and the average photon number per pulse is selected around 13.9 before detection to maximize the generation rate of random number. Generally, higher photon number per pulse brings higher error rate in the X basis and higher double clicks probability in the Z basis that need to be discarded, while lower photon number per pulse leads to lower n_z. Thus, there is a tradeoff for choosing a proper average photon number. The details of optimizing the probability of measuring in the Z (X) basis and the average photon number per pulse is discussed in Methods.

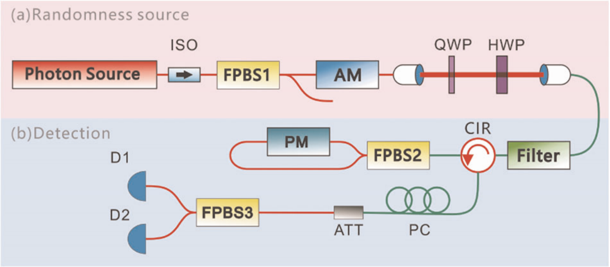

Fig. 2 The setup of the experiment can be divided into the photon source and detection parts. In the detection part, a Sagnac type interferometer with a phase modulator (PM) is used to select the measurement basis by applying a controllable unitary operator. After proper attenuation, the photons are detected by two up-conversion single photon detectors. In the randomness source part, a photon source is modulated by an amplitude modulator (AM) and transmit through a polarized beam splitter (PBS), a half-wave plate (HWP) and a quarter-wave plate (QWP) to prepare the desired state. The photon source used here is a cw laser and the sunlight, and can be replaced by any other light if necessary. ISO optical isolator, CIR optical circulator, FPBS fiber polarized beam splitter, ATT attenuator, PC polarization controller

As aforementioned, the detection may have imperfections. Therefore, the detection part is first calibrated by an auxiliary cw laser diode with expected wavelength of 1550.12 nm. Considering the imperfect measurement basis of X' and Z', an additional process is performed to estimate $\max_{x',z'}|\langle x'|z'\rangle|$ in (5). Firstly, the input state is prepared as the eigenstate of $Z^{'}$ basis, that is, the ratio of photon counting between detector 1 and detector 2 is above 30 dB under $Z^{'}$ basis measurement. Then, in the $X^{'}$ basis measurement, the ratio of photon counting between detector 1 and detector 2 is measured and the bound of $-2\,\mathrm{log}\max_{x',z'}|\langle x'|z'\rangle|$ is calculated to be 0.952.

Although the randomness source part can be untrusted, to demonstrate the high generation rate of the setup, a carefully calibrated randomness source is realized. An amplitude modulator (AM) is used to modulate the input photons to pulses with frequency of 4 MHz and the full width at half maximum (FWHM) of 100 ns. Another fiber polarized beam splitter (FPBS1), a half-wave plate (HWP) and a quarter-wave plate (QWP), is used to prepare the desired polarization state for the detection part.

As the photon source can be any light that does not need to be trustable, the choice of photon source is flexible. Here, we also demonstrate the use of the most common light in the nature—the sunlight, as the photon source to generate random numbers. A collimator mounted on an equatorial mount is placed on the rooftop to collect sunlight into a single mode fiber. The sun can be approximately considered as an area light source with divergence angle around 0.5°.[31] Thus, a common collimator with focus length of 11 mm is enough to collect sufficient photon intensities. About 49 nW of light can be collected into single mode fiber under a good weather after filtered by a 1550 ± 1.5 nm bandpass filter.

The optimal input state for the detection part is the eigenstate of X basis. However, input state with other polarization state does not affect the reliability of randomness. Although the error rate in the X basis will increase and the random number generation rate will reduce. By rotating the HWP in randomness source part to different angles, the relationship between the input state and the error rate of X basis measurement is shown in Fig. 3. Under the

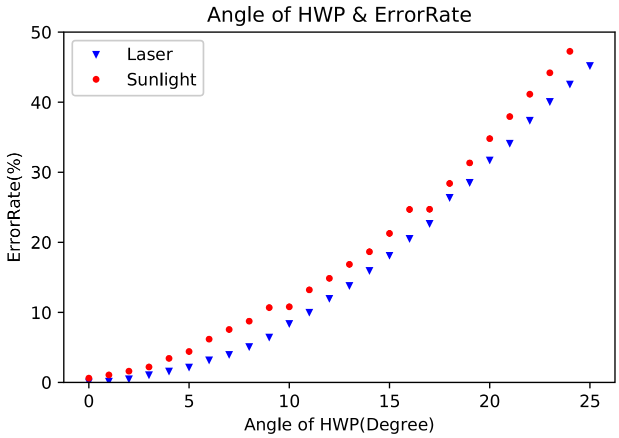

Fig. 3 For our experiment, when the input state is $|+\rangle$, the bit error rate close to zero. Rotating the HWP change the input state while the bit error rate. This figure shows the relationship between the angle of HWP and the error rate

near optimal condition with the input state of $|+\rangle$, we performed the experiment for both laser and sunlight. The error rate in the X basis measurement is 0.33% for laser and 0.21% for sunlight. The quantum random number generation rate is 1.81 Mbps for laser and 1.72 Mbps for sunlight. The detailed results is shown as Table 1. The extracted random bits can pass NIST randomness test as shown in Fig. 4.

DISCUSSION

In this work, we theoretically modified the SI-QRNG scheme by considering practical issues of measurement devices and experimentally demonstrated the applicability of the scheme in generating reliable and fast random numbers. Compared to the proof-of-principle demonstration in the theoretical work[15] whose randomness generation rate is about 10^{-3} Mbps, our implementation improved the generation speed over three orders. Therefore, our SI-QRNG scheme can be applied in many scenarios where both the randomness generation speed and reliability are required. The randomness generation rate here is mainly limited by the detection rate of the single photon detector. Improving the detection rate of the single photon detector can thus further increase the randomness generation rate.

Our result highlighted the power of the state-of-the-art quantum technology. In previous works, it was shown that randomness can be obtained by measuring the intensity of an LED light with a mobile phone[32] or by measuring the arrival time of photons from cosmic sources.[33,34] However, such QRNG schemes are based on physical models of the LED light or the cosmic source. In our work, we showed that such assumptions are not necessary. Even with a common light in the nature—sunlight, we can still generate randomness both reliably and fast. Since no assumption is made on the photon source, the coherence or photon number statistics of the photon source does not affect the randomness of the extracted bits. In future works, by exploiting the SI-QRNG scheme, it is also interesting to modify (in theory) and realize (in experiment) those QRNG schemes such that the assumption of the source is removed.

Table 1. Experiment result

Photon source	Laser	Sunlight
APD1 click at Z basis (count)	1733623848	1638255301
APD2 click at Z basis (count)	1843484418	1725825404
Bit error rate at X basis (%)	0.33	0.21
Time (s)	1800	1800
θ	0.001	0.001
Extracted raw number (bit)	3.26×10^9	3.10×10^9
Generation rate (bps)	1.81×10^6	1.72×10^6

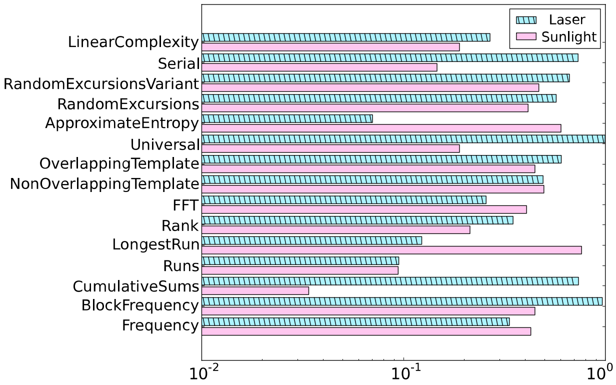

Fig. 4 The *P* value of NIST tests. Blue represents laser and red represents sunlight

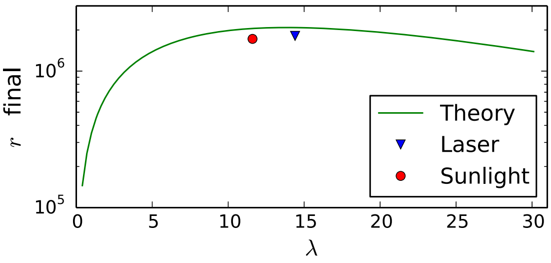

Fig. 5 Relationship between the average photon number λ per pulse and final random number generation rate. r have the maximal value for $\lambda = 13.9$. In this experiment, λ is 14.4 for laser and is 11.6 for sunlight. The circle and the triangle denote the actual key generation rate for the two photon sources, respectively. These two values are slightly deviated from the theoretical curve owing to the imperfections

METHODS

Optimizing the generation rate

To optimize the final quantum random number generation rate, some proper parameters should be chosen or measured in Eq. (5). The first term $\frac{2\min(\eta_0,\eta_1)}{\eta_0+\eta_1}$ depends on the efficiencies of the two detectors, and has a maximal value of 1 when the two efficiencies are equal. Thus, η_0 and η_1 are configured to be approximatively uniform ($\eta = 10\%$) in our experiment. The second term $-2\log_2\max_{x',z'}|\langle x'|z'\rangle|$ depends on the accuracy of controlling the PC and the PM. Due to the imperfection of the actual measurement basis, this term is calculated to be 0.952. t_e is chosen as 100.[35] Other terms are related to the average photon number λ per pulse before detection. A low average photon number lowers n_z, while a high average photon number brings higher e_{pz} and higher double click probability in the Z basis. We can rewrite the final random number generation rate as follows:

$$r_{\text{final}} = G\cdot p_{z(\text{single-click})}(0.952 - H(e_{bX}+\theta)) - 100. \tag{7}$$

Here, G stands for the repetition rate of squash speed and equal to 4 MHz in our experiment. $p_{z(\text{single-click})}$ is the probability that one and only one detector clicks for a pulse. As Poisson distribution for laser and multi-mode sunlight,

$$p_{z(\text{single-click})} = 2e^{-\frac{\lambda'}{2}}(1 - e^{-\frac{\lambda'}{2}}), \tag{8}$$

where $\lambda^{'} = \lambda\cdot\eta$. For large n_X, e_{pZ} and e_{bX} can be regarded as the same. The relationship between λ and the final raw rate is shown in Fig. 5. The optimal λ is about 14.4. For sunlight, the actual λ of 11.6 is slightly deviated from the optimal value, due to the intensity fluctuate of sunlight. However, for a wide range of λ the random number generation rate is not obviously dropped.

DATA AVAILABILITY

Data available on request from authors.

Received: 17 January 2019; Accepted: 2 October 2019;
Published online: 14 November 2019

REFERENCES

1. Shannon, C. E. Communication theory of secrecy systems. *Bell Syst. Tech. J.* **28**, 656 (1949).
2. Metropolis, N. & Ulam, S. The monte carlo method. *J. Am. Stat. Assoc.* **44**, 335 (1949).
3. Bennett, C. H. & Brassard, G. Quantum cryptography: public key distribution and coin tossing. In *Proc. IEEE International Conference on Computers, Systems and Signal Processing* 175 (IEEE Press, New York, 1984).

4. Yuan, X., Zhou, H., Cao, Z. & Ma, X. Intrinsic randomness as a measure of quantum coherence. *Phys. Rev. A* **92**, 022124 (2015).
5. Yuan, X., Zhao, Q., Girolami, D. & Ma, X. Interplay between local quantum randomness and non-local information access. http://arXiv.org/abs/1605.07818 (2016).
6. Yuan, Z. L. et al. Robust random number generation using steady-state emission of gain-switched laser diodes. *Appl. Phys. Lett.* **104**, 261112 (2014).
7. Abellán, C. et al. Ultra-fast quantum randomness generation by accelerated phase diffusion in a pulsed laser diode. *Opt. Express* **22**, 1645 (2014).
8. Nie, Y.-Q. et al. The generation of 68 Gbps quantum random number by measuring laser phase fluctuations. *Rev. Sci. Instrum.* **86**, 063105 (2015).
9. Pironio, S. et al. Random numbers certified by Bellas theorem. *Nature* **464**, 1021 (2010).
10. Giustina, M. et al. Bell violation using entangled photons without the fair-sampling assumption. *Nature* **497**, 227 (2013).
11. Liu, Y. et al. Device-independent quantum random-number generation. *Nature* **562**, 548 (2018).
12. Bierhorst, P. et al. Experimentally generated randomness certified by the impossibility of superluminal signals. *Nature* **556**, 223 (2018).
13. Liu, Y. et al. High-speed device-independent quantum random number generation without a detection loophole. *Phys. Rev. Lett.* **120**, 010503 (2018).
14. Lunghi, T. et al. Self-testing quantum random number generator. *Phys. Rev. Lett.* **114**, 150501 (2015).
15. Cao, Z., Zhou, H., Yuan, X. & Ma, X. Source-independent quantum random number generation. *Phys. Rev. X* **6**, 011020 (2016).
16. Marangon, D. G., Vallone, G. & Villoresi, P. Source-device-independent ultrafast quantum random number generation. *Phys. Rev. Lett.* **118**, 060503 (2017).
17. Avesani, M., Marangon, D. G., Vallone, G. & Villoresi, P. Source-device-independent heterodyne-based quantum random number generator at 17 Gbps. *Nat. Commun.* **9**, 5365 (2018).
18. Brask, J. B. et al. Megahertz-rate semi-device-independent quantum random number generators based on unambiguous state discrimination. *Phys. Rev. Appl.* **7**, 054018 (2017).
19. Rusca, D. et al. Practical self-testing quantum random number generator based on an energy bound. http://arXiv.org/abs/1904.04819 (2019).
20. Xu, B. et al. High speed continuous variable source-independent quantum random number generation. *Quantum Sci. Technol.* **4**, 025013 (2019).
21. Gehring, T. et al. 8 GBit/s real-time quantum random number generator with non-iid samples. http://arXiv.org/abs/1812.05377 (2018)
22. Ma, X., Yuan, X., Cao, Z., Qi, B. & Zhang, Z. Quantum random number generation. *npj Quantum Inf.* **2**, 16021 (2016).
23. Fung, C.-H. F., Ma, X. & Chau, H. F. Practical issues in quantum-key-distribution postprocessing. *Phys. Rev. A* **81**, 012318 (2010).
24. Mansour, Y., Nisan, N. & Tiwari, P. The computational complexity of universal hashing. *Theor. Comput. Sci.* **107**, 121 (1993).
25. Ma, X., Fung, C.-H. F., Boileau, J.-C. & Chau, H. F. Universally composable and customizable post-processing for practical quantum key distribution. *Comput. Security* **30**, 172 (2011).
26. Coles, P. J., Berta, M., Tomamichel, M. & Wehner, S. Entropic uncertainty relations and their applications. *Rev. Mod. Phys.* **89**, 015002 (2017).
27. Winter, A. & Yang, D. Operational resource theory of coherence. *Phys. Rev. Lett.* **116**, 120404 (2016).
28. Fung, C.-H. F., Tamaki, K., Qi, B., Lo, H.-K. & Ma, X. Security proof of quantum key distribution with detection efficiency mismatch. *Quantum Inf. Comput.* **9**, 0131 (2009).
29. Qi, B., Fung, C.-H. F., Lo, H.-K. & Ma, X. Time-shift attack in practical quantum cryptosystems. *Quantum Inf. Comput.* **7**, 073 (2007).
30. Shentu, G.-L. et al. Ultralow noise up-conversion detector and spectrometer for the telecom band. *Opt. Express* **21**, 13986 (2013).
31. Fontani, D. et al. Solar divergence collimators for optical characterisation of solar components. *Int. J. Photoenergy* **2013**, 610173 (2013).
32. Sanguinetti, B., Martin, A., Zbinden, H. & Gisin, N. Quantum random number generation on a mobile phone. *Phys. Rev. X* **4**, 031056 (2014).
33. Handsteiner, J. et al. Cosmic bell test: measurement settings from milky way stars. *Phys. Rev. Lett.* **118**, 060401 (2017).
34. Wu, C. et al. Random number generation with cosmic photons. *Phys. Rev. Lett.* **118**, 140402 (2017).
35. Ma, X. et al. Postprocessing for quantum random-number generators: entropy evaluation and randomness extraction. *Phys. Rev. A* **87**, 062327 (2013).

ACKNOWLEDGEMENTS

This work was supported by the National Natural Science Foundation of China (under Grant No. 11654005, U1738201, U1738142), the National Key Research and Development Program of China (under Grant No. 2017YFA0303901), the Shanghai Sailing Program, and the Chinese Academy of Sciences (CAS). Yuan Cao was supported by the Youth Innovation Promotion Association of CAS (under Grant No. 2018492).

AUTHOR CONTRIBUTIONS

Y.-H.L., X.H., Y.C. and J.Y. designed the experiment; Y.-H.L., X.H., Z.-P.L. J.-Y.G. and Q.Z. performed research; Y.-H.L., X.H. and X.Y. analyzed data; X.Y. and X.M. provided the theoretical support; Y.C., X.M., C.-Z.P., and J.-W.P. supervised the project. All authors contributed to the research and the preparation of the manuscript.

COMPETING INTERESTS

The authors declare no competing interests.

ADDITIONAL INFORMATION

Correspondence and requests for materials should be addressed to Y.C., X.M. or C.-Z.P.

Reprints and permission information is available at http://www.nature.com/reprints

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