PHOTONICS Research

Mutually testing source-device-independent quantum random number generator

JIALIN CHENG,[1,†] JILIANG QIN,[1,2,†] SHAOCONG LIANG,[1] JIATONG LI,[1] ZHIHUI YAN,[1,2,3] XIAOJUN JIA,[1,2,4] AND KUNCHI PENG[1,2]

[1]State Key Laboratory of Quantum Optics and Quantum Optics Devices, Institute of Opto-Electronics, Shanxi University, Taiyuan 030006, China
[2]Collaborative Innovation Center of Extreme Optics, Shanxi University, Taiyuan 030006, China
[3]e-mail: zhyan@sxu.edu.cn
[4]e-mail: jiaxj@sxu.edu.cn

Received 4 October 2021; revised 8 December 2021; accepted 26 December 2021; posted 4 January 2022 (Doc. ID 444853); published 17 February 2022

Quantum random numbers have an incomparable advantage over pseudo-random numbers since randomness originates from intrinsic property of quantum mechanics. The generation rate and the security of quantum random numbers are two significant indicators of a quantum random number generator (QRNG) for practical applications. Here we propose a mutually testing source-device-independent QRNG by simultaneously measuring a pair of conjugate quadratures from two separate parts of an untrusted continuous-variable quantum state. The amounts of randomness of the quadratures can be mutually estimated by each other via entropic uncertainty principle. Instead of randomly toggling between the conjugate quadratures of one state for collecting different types of data, two quadratures can generate check data and raw bits simultaneously and continuously in this mutually testing manner, which enhances the equivalent generation rate of private random bits to around 6 Gbit/s with a 7.5 mW laser beam. Moreover, the overall security is also improved by adjusting the conditional min-entropy in real time according to the continually monitored fluctuations of the local oscillator and the randomly measured electronic noise of homodyne detectors.

https://doi.org/10.1364/PRJ.444853

1. INTRODUCTION

Simulation, computation, and number theory may have a demanding requirement for the generation rate of the exploited random numbers following the right statistics, while other applications, such as the classical communications based on the RSA cryptosystem, the current quantum key distribution [1,2], signature schemes [3,4], and quantum secret sharing [5], place greater demand on the security or privacy of random numbers. It has been reported that thousands of servers are attacked by inferior hackers for the lousy randomness of pseudo-random numbers every year [6]. It can be argued that the private randomness is a potential necessary condition of any secure and secret communications. Even in daily life, the security and the non-repeatability of random numbers can also be crucially significant. Defective products can pass the quality inspection exploiting random sampling just because the illegitimate manufacturer gets the random numbers for sampling and changes the order of products beforehand. An illegal gambler may get a bigger bang for the buck by receiving partial random numbers and adopting the best guessing strategy. A lottery draw may be rigged by an unlawful manager, who obtains the side information of the random number generator during routine maintenance.

Leaning toward the mainstream viewpoint, random numbers generated by classical systems are all pseudo-random numbers, while only quantum theory can offer true randomness [7,8]. The earliest quantum random number generator (QRNG) is based on radioactive decay [9], which generates true random numbers with a low bit rate taking demanding safety measures. Moreover, the source generating quantum random numbers (i.e., entropy source) can be quantum tunneling [10,11], Majorana fermions [12], quantum fluctuations of the collective spin of an alkali-metal vapor [13], phase noise of a single-mode laser [14], etc. However, there have been demonstrations of random numbers generated on a mobile phone [15], in which the random numbers are generated from resolving photon-number distribution of a camera. Most QRNGs are currently based on quantum optics since different quantum states with inherent randomness offer a rich choice of implementations and complete analytical methods [7,8,16–25]. The polarization of single photons [26], temporal [27, 28] or spatial mode [29,30] of photons can generate random bits; photon counting [31], amplified spontaneous emission [32,33], and stimulated Raman scattering [34] can also be the entropy source. In recent years, there have been reports of a quantum random number generator with a photonic integrated chip [21] and even a quantum random number cloud platform [35]. Among all quantum resources, measurement of the vacuum noise via homodyne detection is one of the most efficient and economical methods with high-speed and secure bits generation [36–38]. For a general entropy source, it is far from trivial to estimate the min-entropy. Consequently, there have been many QRNG protocols [7,8]. In practical terms the measurement device can be characterized easily by the user at close range, while the entropy source and local oscillator (LO) can be distributed remotely for the convenience of users. Therefore, the entropy source and LO are more vulnerable to attack. Based on this consideration, the QRNG protocol with an untrusted source and indeterminate LO is needed, i.e., the source-device-independent (SDI) QRNG. In the SDI QRNG, the secure randomness needs to be estimated and quantified in the presence of the eavesdropper attacking the source. Finally, the private random bits can be extracted by the Toeplitz-matrix hashing algorithm from the raw random numbers.

The entropic uncertainty principle (EUP) [39,40] gives a lower bound on the conditional min-entropy that estimates the amount of secure randomness in the presence of the eavesdropper and is used to calibrate the randomness extractor in the SDI QRNG where the entropy source is completely untrusted [41–43]. A pair of non-commutative operators $\hat{P}$ and $\hat{Q}$ are normally seen as the data quadrature and check quadrature, respectively. Estimating the conditional min-entropy of data quadrature is achieved by randomly switching conjugate quadratures of one state for measuring. Up to now, QRNGs based on the EUP have been realized in discrete-variable system [44,45] and continuous-variable system [41]. Then an SDI QRNG based on generic positive operator valued measurements with heterodyne measurements has been proposed [42]. Very recently, the squeezed state has been applied in the SDI QRNG [43].

In fact, the check quadrature $\hat{Q}$ that estimates the randomness of the data quadrature $\hat{P}$ also contains the secure randomness estimated by the data quadrature $\hat{P}$. In contrast, the mutually testing QRNG does not require random switching and can further increase the generation rate of private bits. A comparison between mutual testing and random switching can be found in Appendix A.

The implementation of our protocol is shown in Fig. 1. An untrusted coherent state (CS) is divided into two identical parts (CS1 and CS2 with equal power and fluctuation) in which quadrature $\hat{Q}$ and quadrature $\hat{P}$ are severally measured. The entropy source has not been characterized while the equipartition process must be completely trusted. The eavesdropper may replace the untrusted coherent state by other states (for instance, a submode of a two-mode squeezed state) for side information, which results in an inevitable increase of insecure quantum noise on the probably impure CS1 and CS2. The attack on the source can be eliminated via the EUP with a trusted division process. The quadratures are measured using balanced homodyne detectors (BHDs) and all data are collected by an oscilloscope (OSC). The details about the measurement of quadratures can be found in Appendix B. The data of quadrature $\hat{Q}$ measured on CS1 are used as the check data to estimate the data of quadrature $\hat{P}$ measured on CS2, and the quadrature $\hat{P}$ measured on CS2 in turn is used to estimate quadrature $\hat{Q}$ measured on CS1. The data of both quadrature $\hat{Q}$ measured on CS1 and $\hat{P}$ measured on CS2 are used to generate the raw random bits. Eventually the secure random bits are obtained by applying randomness extractors to the raw data, where the extractors are constructed with two Toeplitz matrices calibrated by the quantum conditional min-entropy. It should be noted that the quadrature $\hat{Q}$ of one quantum state generally cannot be used to estimate the quadrature $\hat{P}$ of the others. It is not in accordance with the EUP. However, for a pair of continuous-variable quantum states with equal power and fluctuation, the distributions of corresponding quadratures should be the same, which can be achieved by setting a trusted equipartition process to the unknown source. Therefore, the quadrature of one state can be used to test the conjugate quadrature of the other state and the relation is mutual. All the data of the

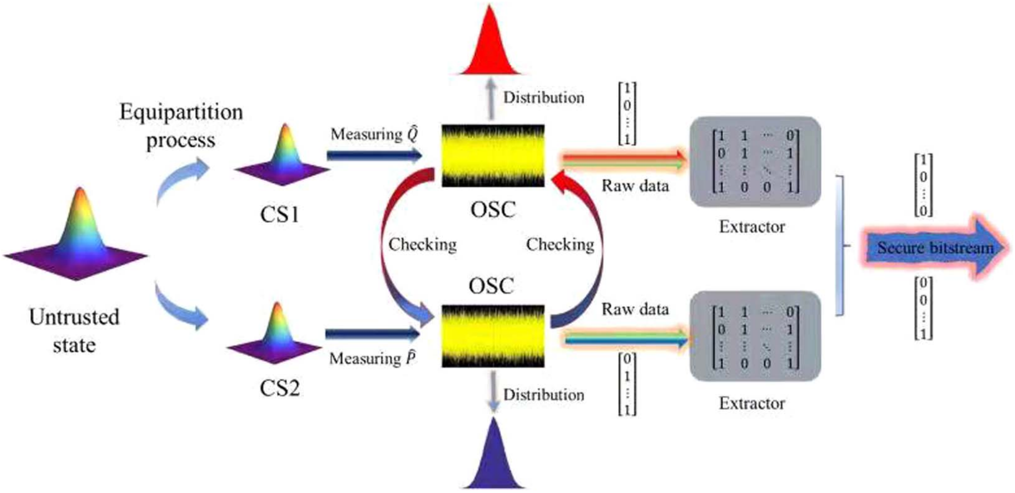
Equipartition process
Untrusted state
CS1
CS2
Measuring $\hat{Q}$
Measuring $\hat{P}$
OSC
OSC
Distribution
Distribution
Checking
Checking
Raw data
Raw data
Extractor
Extractor
Secure bitstream
$\begin{bmatrix}1\\0\\\vdots\\1\end{bmatrix}$
$\begin{bmatrix}0\\1\\\vdots\\1\end{bmatrix}$
$\begin{bmatrix}1 & 1 & \cdots & 0\\0 & 1 & \cdots & 1\\\vdots & \vdots & \ddots & \vdots\\1 & 0 & 0 & 1\end{bmatrix}$
$\begin{bmatrix}1\\0\\\vdots\\0\end{bmatrix}$
$\begin{bmatrix}0\\0\\\vdots\\1\end{bmatrix}$

Fig. 1. Flow diagram of the experimental structure. An untrusted coherent state (CS) is divided into two identical and probably impure parts, CS1 for measuring quadrature $\hat{Q}$ and CS2 for quadrature $\hat{P}$. The collected data of one quadrature are chosen as the check quadrature to estimate the conditional min-entropy of the conjugate quadrature of the other state since the dividing process is completely trusted and the distributions of two parts are identical. After two randomness extractors, the secure random bits are obtained. CS, coherent state; OSC, oscilloscope.

pair of quadratures can generate random numbers with mutual testing and estimating in real time.

When an untrusted state is used as the entropy source, the amount of private random bits based on the EUP is given by [40,41,46–51]

$$H_{\min}(P_{\delta p}|E) \geq -\log_2 c(\delta q, \delta p) - H_{\max}(Q_{\delta q}) = H_{\rm low}(P_{\delta p}|E), \tag{1}$$

$$c(\delta q, \delta p) = \frac{1}{2\pi}\delta q \delta p S_0^{(1)}\left(1, \frac{\delta q \delta p}{4}\right)^2, \tag{2}$$

where $H_{\min}(P_{\delta p}|E)$ is the quantum conditional min-entropy of quadrature $\hat{P}$. The term $c(\delta q, \delta p)$ denotes "incompatibility" of quadratures $\hat{P}$ and $\hat{Q}$, and $H_{\max}(Q_{\delta q})$ is the max-entropy expressing the user's lack of knowledge about quadrature $\hat{Q}$. $H_{\rm low}(P_{\delta p}|E)$ is the lower bound on the conditional min-entropy, which bounds the amount of secure and private random numbers. Both the δp and δq mean the measurement accuracy of quadratures $\hat{P}$ and $\hat{Q}$, and $S_0^{(1)}(1, \frac{\delta q \delta p}{4})^2$ is the 0th radial prolate spheroidal wave function of the first kind [40,41,52]. Similarly, quadrature $\hat{Q}$ can be estimated by quadrature $\hat{P}$.

In fact, the coherent state before division is an uncharacterized state in our mutually testing QRNG protocol. Therefore, the total amount of extractable randomness of two separated impure states (CS1 and CS2, in Fig. 1) can be represented as

$$\begin{aligned} H_{\min}^{(T)}(Q_{\delta q}^{(1)} \cup P_{\delta p}^{(2)}|E) &= H_{\min}^{(1)}(Q_{\delta q}^{(1)}|E) + H_{\min}^{(2)}(P_{\delta p}^{(2)}|E) \\ &\geq -2\log_2 c(\delta q, \delta p) \\ &\quad - H_{\max}^{(1)}(P_{\delta p}^{(1)}) - H_{\max}^{(2)}(Q_{\delta q}^{(2)}), \end{aligned} \tag{3}$$

where $H_{\min}^{(T)}(Q_{\delta q}^{(1)} \cup P_{\delta p}^{(2)}|E)$ is the total amount of extractable randomness, and $H_{\min}^{(i)}(K_{\delta k}^{(i)}|E)$ and $H_{\max}^{(i)}(K_{\delta k}^{(i)})$ are the conditional min-entropy and max-entropy of quadrature $\hat{K}$ $(\hat{K} = \hat{P}, \hat{Q})$ of the ith $(i = 1, 2)$ coherent state, respectively.

Taking into account the finite-size effects and the security of the extractor during the randomness extraction, the bound on the conditional min-entropy should be further lowered as

$$\begin{aligned} H_{\min}^{\epsilon}(P_{\delta p}|E) &\geq H_{\rm low}(P_{\delta p}|E) \\ &- \frac{4}{\sqrt{n_p}}\sqrt{\log_2\left(\frac{2}{\epsilon^2}\right)}\log_2\left[2^{1+\frac{H_{\max}(Q_{\delta q})}{2}} + 1\right], \end{aligned} \tag{4}$$

where $H_{\min}^{\epsilon}(P_{\delta p}|E)$ is the smooth quantum conditional min-entropy, n_p is the number of measurements for the quadrature $\hat{P}$, and ϵ is the security parameter.

It is a remarkable fact that the electronic noise may be controlled by the eavesdropper, so it needs to be measured at random times. Moreover, the fluctuations of the LO need to be monitored since the fluctuations can add insecure noise to the measured noise of the quadratures via an imperfect homodyne detector from the eavesdropper [53]. The collected data consist of the vacuum noise, extra noise introduced by LO fluctuations, and electronic noise of the detection system:

$$\sigma_T^2 = \sigma_V^2 + \sigma_{\rm LO}^2 + \sigma_E^2, \tag{5}$$

where σ_T^2 is the total noise contained in the measured data. The electronic noise σ_E^2 can be measured by randomly blocking all the light paths of the detectors according to the random seed. The extra noise $\sigma_{\rm LO}^2$ can be estimated by analyzing the LO fluctuations in real time. The extra noise and electronic noise are eventually regarded as impurity of the vacuum noise.

2. PRINCIPLE AND EXPERIMENTAL SETUP

The schematic of the experimental setup of the mutually testing SDI QRNG is illustrated in Fig. 2. A laser beam at the wavelength of 1342 nm from the Nd:YVO$_4$ laser (Yuguang Company) passes through a mode-cleaner with a finesse of 300 for spatiotemporal filtering and intensity stability. The output beam is divided into the signal beam and LO via a beam splitter (BS) with reflectivity of about 98%. The intensity of the signal beam is decreased further, and about 2% of the LO is used to monitor the power and fluctuations to resist the attacks from the eavesdropper. The signal beam and LO then are split into two identical parts respectively for data collection via a pair of identical BHDs. The BHD1 (BHD2) was used to measure quadrature $\hat{Q}$ $(\hat{P})$ with the relative phase 0 $(\pi/2)$ between the coherent state and the LO. The interference signals are detected by the broadband BHDs (PDB480C-AC, Thorlabs) with two photodiodes FD150 (Fermionics Opto-Technology). The LO power and measurement bandwidth for each of the two BHDs are set as 7.5 mW and 1 GHz (from 3 MHz to about 1 GHz), respectively, since the signal-to-noise ratio of the homodyne detector should be maximized and the response is close to uniform in a bandwidth of at least 1 GHz. Then the signals are filtered, amplified, and collected by two 1.9 MHz low-pass filters, two broadband amplifiers, and an OSC. After the min-entropy of the quadrature $\hat{Q}$ $(\hat{P})$ of one coherent state is mutually estimated by the quadrature $\hat{P}$ $(\hat{Q})$ of the other coherent state, the two sets of data are put into the extractor for terminal uniform-distribution random bits. Finally, few random bits are injected into the chopper to measure the electronic noise of the measurement device randomly.

3. RESULTS

In our experiment, the electronic noise is basically maintained because there is no interference in the surroundings of the detectors from the eavesdropper. The measured shot noises of two BHDs severally contain $(5.8 \pm 0.1)\%$ and $(5.9 \pm 0.1)\%$ of electronic noise and less than $10^{-4}\%$ of the extra noise caused by the power fluctuations of the LO. The measuring time of electronic noise needs to be randomly chosen; the average duration we set is equal to 1/20 total measuring time. The nominal resolution of the OSC is 10 bits. Taking into account the high-speed dual-channel sampling, we use a conservative bit depth of 6 bits. In a round of our experimental process, we measure the data of $\hat{P}$ and $\hat{Q}$ quadratures, each with 1 million samples obtained. The smooth conditional min-entropies of quadratures are both estimated as 3.13 ± 0.05 bits; more details can be found in Appendix C. The randomness extractor is applied to extract terminal random bits from the raw data. Eventually, the equivalent generation rate of private random bits is around 6 Gbit/s.

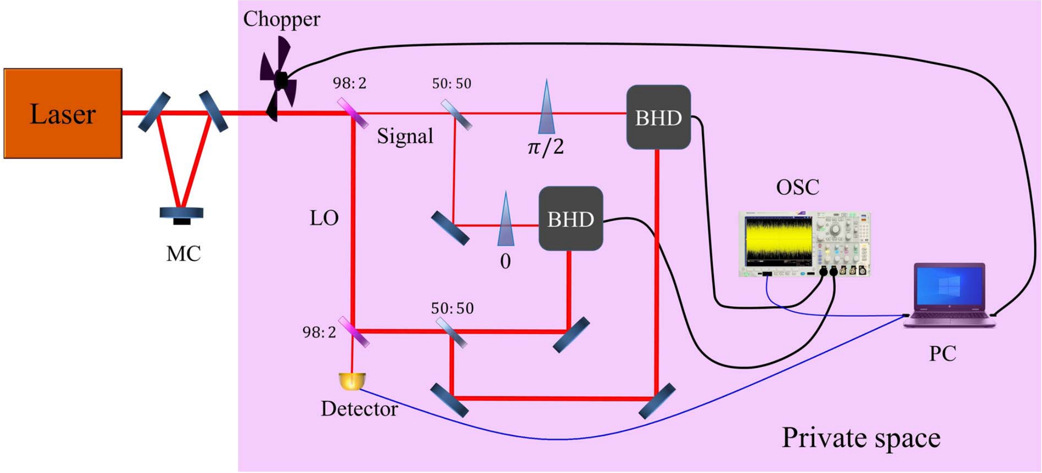

Fig. 2. Experimental schematic configuration for mutually testing SDI QRNG. The pink area is a private space that no eavesdropper has access to. The black and blue curves represent the electric and data cables, respectively. The coherent state is generated via a laser and MC. The laser beam is divided into the signal beam and LO via a 98:2 BS. Both the signal beam and the LO are split in half via two 50:50 BSs. Two BHDs are used to measure the quadrature $\hat{P}$ and $\hat{Q}$ of the two coherent states with the phase differences (0 and $\pi/2$) between the signal beam and LO, respectively. All data are recorded by an OSC, and the post-processing is achieved via a PC. Laser, Nd:YVO$_4$; MC, mode-cleaner; 98:2, 98:2 beam splitter; 50:50, 50:50 beam splitter; LO, local oscillator; BHD, balanced homodyne detector; HR, mirror with high reflectivity; OSC, oscilloscope; PC, personal computer.

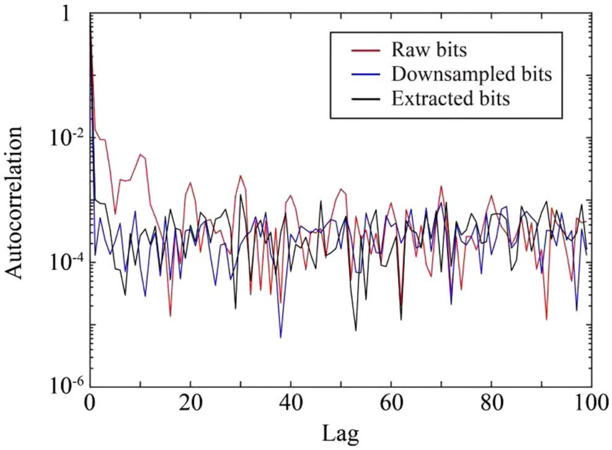

Fig. 3. Red, blue, and black curves show the autocorrelations calculated from the raw bits, the downsampled bits, and the extracted bits, respectively. The three data streams have the same length of 5×10^7.

We perform autocorrelation analysis on raw bits, the downsampled bits, and the extracted bits from the same raw dataset, as shown in Fig. 3. The raw random bits show a stronger autocorrelation than the extracted bits between multiples of about 10 lags, due to the continuous high-speed sampling via the OSC. The effective bit depth of 6 bits is exploited and we perform a downsampling on the raw data, and the autocorrelation is removed. After applying a Toeplitz-hashing extractor, there is no obvious autocorrelation in the extracted bits. To test the statistical randomness of the terminal random bits, we test them with the NIST suite [54]. The results of the randomly selected run of the NIST test are reported in Table 1. In the case of multiple tests in a category, the smallest has been reported. Eventually, the private bits pass all the NIST statistical tests.

Table 1. Results of NIST Test Suite on the Extracted Random Bits[a]

Test	P-Value	Result
Block frequency	0.133214	Pass
Cumulative sums	0.449712	Pass
Runs	0.698439	Pass
Longest run	0.015302	Pass
Rank	0.988609	Pass
DFT	0.762020	Pass
Non-overlapping template	0.065286	Pass
Overlapping template	0.854193	Pass
Universal	0.728325	Pass
Approximate entropy	0.029844	Pass
Random excursions	0.218360	Pass
Random excursions variant	0.045362	Pass
Serial	0.869390	Pass
Linear complexity	0.562328	Pass

[a] In the case of multiple tests in a category, the smallest have been reported.

4. CONCLUSION

In summary, we experimentally demonstrate a mutually testing SDI QRNG based on an untrusted source and a trusted equipartition process. The lower bounds on the amount of secure randomness of a pair of conjugate quadratures of two identical states are mutually estimated with the simultaneously measured data of the two quadratures; thus, it is convenient for users to avoid switching the measurement types of quadrature components. An SDI QRNG protocol based on the EUP is exploited to make the terminal random bits secure from the eavesdropper's attacks on the entropy source. Moreover, the electronic noise of the homodyne detection system and the fluctuations of the LO are monitored to eliminate the interference around the detectors and resist the attacks on the LO to improve the total security. A coherent state is divided into two identical parts in which the quadrature $\hat{P}$ on one part and the quadrature $\hat{Q}$ on the other part can be measured simultaneously. It is noteworthy that the EUP cannot be applied to two quadratures from two different states in principle [40,41]. However, taking into account a trusted equipartition process operated on an untrusted state, for instance, by exploiting a completely trusted beam splitter, two identical impure coherent states are split from the untrusted state, then the distributions of corresponding quadratures of different states should be the same. Consequently, the max-entropy of a quadrature of one state is equal to that of the same quadrature of the other one. Accordingly, the conjugate quadratures from two states can be mutual check quadratures for each other. Eventually, measuring a pair of quadratures of a coherent state (two separate coherent states, actually) simultaneously can double the generation rate of the SDI QRNG based on the vacuum. It allows us to construct a certified SDI QRNG with a generation rate greater than 7.5 Tbit/s via a 20 W laser beam and 1250 integrated boxes containing all stuff in the private space in Fig. 2 with an external data-collecting and data-processing system.

APPENDIX A: BETWEEN MUTUAL TESTING AND RANDOM TOGGLING

As mentioned above, the mutually testing SDI QRNG can generate private random numbers with a higher bit rate than randomly toggling QRNG. This point can be seen intuitively from the data acquisition and appropriate time sequences. The data acquisitions and appropriate time sequences for the mutually testing and randomly toggling QRNGs are shown schematically in Fig. 4, in which the time of measuring electronic noise and check quadrature accounts for 5% of the total measurement time, respectively. For the mutually testing QRNG, both quadratures $\hat{P}$ and $\hat{Q}$ can generate random bits, as shown in Figs. 4(a) and 4(b). However, in a randomly toggling manner, only one quadrature $\hat{Q}$ is used to generate random bits and the switching time for the check quadrature $\hat{P}$ needs to be deducted, as shown in Fig. 4(c). The time sequences for mutually testing and randomly toggling QRNGs are shown in Fig. 4(d). The high levels in the time sequences are determined by private random seed. Therefore, the mutually testing manner enhances the generation rate of the SDI QRNG with an untrusted entropy source.

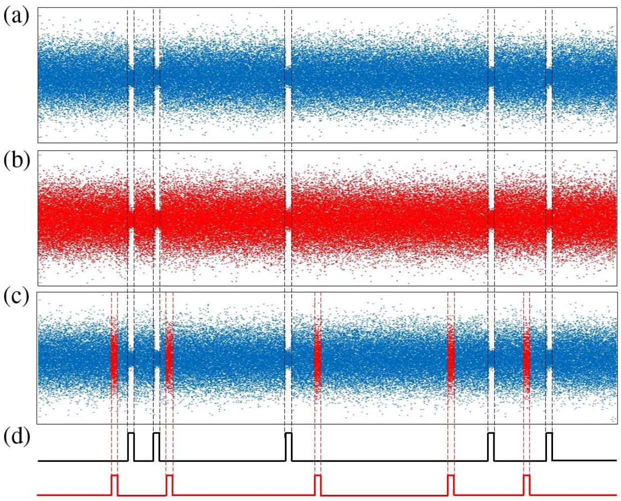

Fig. 4. Comparison of the data acquisitions and appropriate time sequences of mutually testing and randomly toggling manners. The red and blue points represent the measured data of quadratures $\hat{P}$ and $\hat{Q}$, respectively. (a), (b) The data acquisitions on the conjugate quadratures $\hat{P}$ and $\hat{Q}$ in mutually testing manner. (c) The data acquisitions for raw random numbers on the quadratures $\hat{Q}$ in randomly toggling manner. The data of quadratures $\hat{P}$ are used to estimate the randomness of quadratures $\hat{Q}$ and never generate random numbers. (d) Time sequences. Black and red curves represent the time sequences for randomly measuring electronic noise and check quadrature, respectively.

APPENDIX B: MEASUREMENT OF QUADRATURES WITH HOMODYNE DETECTION

A schematic of the balanced homodyne detection is shown in Fig. 5. Mode s is the signal field and L is the strong classical LO that can be taken as a coherent state of amplitude L. Mode s and L are combined on a 50:50 beam splitter with a relative phase ϕ, and then two output fields ($\hat{a}$, $\hat{b}$) and input field are related according to

$$\hat{a} = \frac{1}{\sqrt{2}}(\hat{s} + e^{i\phi}\hat{L}), \tag{B1}$$

$$\hat{b} = \frac{1}{\sqrt{2}}(\hat{s} - e^{i\phi}\hat{L}). \tag{B2}$$

The output current of the detector is proportional to the number of detected photons. The currents can be expressed by

$$i_a = \hat{a}^\dagger\hat{a} = \frac{1}{2}(\hat{s}^\dagger\hat{s} + e^{i\phi}\hat{s}^\dagger\hat{L} + e^{-i\phi}\hat{L}^\dagger\hat{s} + \hat{L}^\dagger\hat{L}), \tag{B3}$$

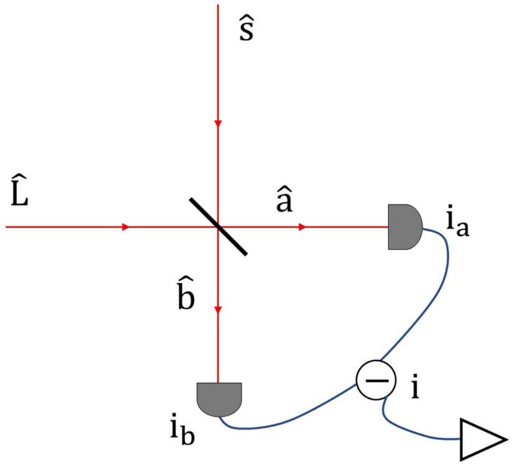

Fig. 5. Schematic of the balanced homodyne detection. The difference current is converted into an amplified voltage signal by a transimpedance amplifier.

$$i_b = \hat{b}^\dagger \hat{b} = \frac{1}{2}(\hat{s}^\dagger \hat{s} - e^{i\phi}\hat{s}^\dagger \hat{L} - e^{-i\phi}\hat{L}^\dagger \hat{s} + \hat{L}^\dagger \hat{L}). \tag{B4}$$

The difference current is

$$i = i_a - i_b = e^{i\phi}\hat{s}^\dagger \hat{L} + e^{-i\phi}\hat{L}^\dagger \hat{s}. \tag{B5}$$

Assuming the LO to be strong enough and in the coherent state, the LO can be regarded as a classical field with a mean value L. Finally,

$$\langle i \rangle = |L| \langle e^{i\phi}\hat{s}^\dagger + e^{-i\phi}\hat{s} \rangle, \tag{B6}$$

where we set $\hat{K}(\phi) = (e^{i\phi}\hat{s}^\dagger + e^{-i\phi}\hat{s})/2$. The phase difference of the signal beam and LO is locked to 0 and $\pi/2$. The quadratures $\hat{Q} = (\hat{s}^\dagger + \hat{s})/2$ and $\hat{P} = i(\hat{s}^\dagger - \hat{s})/2$ can be measured respectively.

APPENDIX C: SUPPLEMENT TO ENTROPIC UNCERTAINTY PRINCIPLE AND ESTIMATION OF GENERATION RATE

For the measured noise of quadratures $\hat{Q}$, assume its distribution is Gaussian with variance σ^2. Exploiting frequentist estimator, the measurement results are assigned to 2^n separated bins $\{q_k\}$, in which n is the resolution of the OSC. The probability that one measured result falls on a certain bin q_k is

$$p(q_k) \simeq \frac{\delta q e^{-\frac{(\delta q k)^2}{\sigma^2}}}{\sigma\sqrt{\pi}}. \tag{C1}$$

Then the lower bound on the conditional min-entropy is given by

$$H_{\text{low}}(P_{\delta p}|E) = -\log_2 c(\delta q, \delta p) - 2\log_2 \sqrt{\frac{\delta q}{\sigma\sqrt{\pi}} \vartheta_3\left(0, e^{-\frac{(\delta p)^2}{2\sigma^2}}\right)}, \tag{C2}$$

where $\vartheta_3(z, q)$ is the Jacobi theta function. The $H_{\text{low}}(Q_{\delta q}|E)$ can be estimated in the same manner. Let σ_V^2 [σ_T^2 in Eq. (5)] be the pure (impure) vacuum noise, and then the loss of security bits introduced by electronic noise and LO fluctuations can be calculated from Eq. (C2).

In addition, the measurement accuracies δp and δq in phase space need to be determined in the experiment. First, the measurement accuracy of voltage signals can be estimated readily from the measured signals once the voltage range of the OSC is set. Then the vacuum noise of 1/2 in phase space corresponds to the calculated variance from the measured vacuum signal. Based on this, the accuracy in phase space can be estimated.

The effective sampling rate of raw data is 1 GS/s, and the security parameter is set as 10^{-12}. According to Eqs. (4), (5), and (C2), the smooth conditional min-entropies of quadratures can be estimated.

Funding. National Natural Science Foundation of China (61925503, 62122044, 11904218, 12147215, 11834010); Program for the Innovative Talents of Higher Education Institutions of Shanxi; Program for the Outstanding Innovative Teams of Higher Learning Institutions of Shanxi; Program for Sanjin Scholars of Shanxi Province; Fund for Shanxi "1331 Project" Key Subjects Construction.

Disclosures. The authors declare no conflicts of interest.

Data Availability. Data underlying the results presented in this paper are not publicly available at this time but may be obtained from the authors upon reasonable request.

†These authors contributed equally to this work.

REFERENCES

1. H.-K. Lo and H. F. Chau, "Unconditional security of quantum key distribution over arbitrarily long distances," Science **283**, 2050–2056 (1999).
2. S.-K. Liao, W.-K. Cai, W.-Y. Liu, L. Zhang, Y. Li, J.-G. Ren, J. Yin, Q. Shen, Y. Cao, Z.-P. Li, F.-Z. Li, X.-W. Chen, L.-H. Sun, J.-J. Jia, J.-C. Wu, X.-J. Jiang, J.-F. Wang, Y.-M. Huang, Q. Wang, Y.-L. Zhou, L. Deng, T. Xi, L. Ma, T. Hu, Q. Zhang, Y.-A. Chen, N.-L. Liu, X.-B. Wang, Z.-C. Zhu, C.-Y. Lu, R. Shu, C.-Z. Peng, J.-Y. Wang, and J.-W. Pan, "Satellite-to-ground quantum key distribution," Nature **549**, 43–47 (2017).
3. P. J. Clarke, R. J. Collins, V. Dunjko, E. Andersson, J. Jeffers, and G. S. Buller, "Experimental demonstration of quantum digital signatures using phase-encoded coherent states of light," Nat. Commun. **3**, 1174 (2012).
4. R. J. Collins, R. J. Donaldson, V. Dunjko, P. Wallden, P. J. Clarke, E. Andersson, J. Jeffers, and G. S. Buller, "Realization of quantum digital signatures without the requirement of quantum memory," Phys. Rev. Lett. **113**, 040502 (2014).
5. Y. Zhou, J. Yu, Z. Yan, X. Jia, J. Zhang, C. Xie, and K. Peng, "Quantum secret sharing among four players using multipartite bound entanglement of an optical field," Phys. Rev. Lett. **121**, 150502 (2018).
6. N. Heninger, Z. Durumeric, E. Wustrow, and J. A. Halderman, "Mining your Ps and Qs: detection of widespread weak keys in network devices," in *Proceeding of the 21st USENIX Security Symposium* (2012), pp. 205–220.
7. X. Ma, X. Yuan, Z. Cao, B. Qi, and Z. Zhang, "Quantum random number generation," npj Quantum Inf. **2**, 16021 (2016).
8. M. Herrero-Collantes and J. C. Garcia-Escartin, "Quantum random number generators," Rev. Mod. Phys. **89**, 015004 (2017).
9. M. Isida and H. Ikeda, "Random number generator," Ann. Inst. Stat. Math. **8**, 119–126 (1956).
10. D. Vartsky, D. Bar, P. Gilad, and A. Schon, "High-speed, true random-number generator," U.S. patent 7,930,333B2 (19 April 2011).
11. K. Aungskunsiri, R. Amarit, and K. Wongpanya, "Random number generation from a quantum tunneling diode," Appl. Phys. Lett. **119**, 074002 (2021).
12. D.-L. Deng and L.-M. Duan, "Fault-tolerant quantum random-number generator certified by Majorana fermions," Phys. Rev. A **88**, 012323 (2013).
13. G. E. Katsoprinakis, M. Polis, A. Tavernarakis, A. T. Dellis, and I. K. Kominis, "Quantum random number generator based on spin noise," Phys. Rev. A **77**, 054101 (2008).
14. B. Qi, Y.-M. Chi, H.-K. Lo, and L. Qian, "High-speed quantum random number generation by measuring phase noise of a single-mode laser," Opt. Lett. **35**, 312–314 (2010).
15. B. Sanguinetti, A. Martin, H. Zbinden, and N. Gisin, "Quantum random number generation on a mobile phone," Phys. Rev. X **4**, 031056 (2014).
16. J. Yang, J. Liu, Q. Su, Z. Li, F. Fan, B. Xu, and H. Guo, "5.4 Gbps real time quantum random number generator with simple implementation," Opt. Express **24**, 27475–27481 (2016).
17. Y.-H. Li, X. Han, Y. Cao, X. Yuan, Z.-P. Li, J.-Y. Guan, J. Yin, Q. Zhang, X. Ma, C.-Z. Peng, and J.-W. Pan, "Quantum random number generation with uncharacterized laser and sunlight," njp Quantum Inf. **5**, 97 (2019).
18. Y.-Q. Nie, L. Huang, Y. Liu, F. Payne, J. Zhang, and J.-W. Pan, "68 Gbps quantum random number generation by measuring laser phase fluctuations," Rev. Sci. Instrum. **86**, 063105 (2015).

19. S.-H. Sun and F. Xu, "Experimental study of a quantum random-number generator based on two independent lasers," Phys. Rev. A **96**, 062314 (2017).
20. Q. Zhang, D. Kong, Y. Wang, H. Zou, and H. Chang, "Dual-entropy-source quantum random number generation based on spontaneous emission," Opt. Lett. **45**, 304–307 (2020).
21. B. Bai, J. Huang, G.-R. Qiao, Y.-Q. Nie, W. Tang, T. Chu, J. Zhang, and J.-W. Pan, "18.8 Gbps real-time quantum random number generator with a photonic integrated chip," Appl. Phys. Lett. **118**, 264001 (2021).
22. M. Ren, E. Wu, and Y. Liang, "Quantum random-number generator based on a photon-number-resolving detector," Phys. Rev. A **83**, 023820 (2011).
23. Z. L. Yuan, M. Lucamarini, J. F. Dynes, B. Frohlich, A. Plews, and A. J. Shields, "Robust random number generation using steady-state emission of gain-switched laser diodes," Appl. Phys. Lett. **104**, 261112 (2014).
24. C. Abellan, W. Amaya, D. Domenech, P. Munoz, J. Capmany, S. Longhi, M. W. Mitchell, and V. Pruneri, "Quantum entropy source on an InP photonic integrated circuit for random number generation," Optica **3**, 989–994 (2016).
25. Q. Zhou, R. Valivarthi, C. John, and W. Tittel, "Practical quantum random-number generation based on sampling vacuum fluctuations," Quantum Eng. **1**, e8 (2019).
26. P. X. Wang, G. Longo, and Y. S. Li, "Scheme for a quantum random number generator," J. Appl. Phys. **100**, 056107 (2006).
27. Y.-Q. Nie, H.-F. Zhang, Z. Zhang, J. Wang, X. Ma, J. Zhang, and J.-W. Pan, "Practical and fast quantum random number generation based on photon arrival time relative to external reference," App. Phys. Lett. **104**, 051110 (2014).
28. H.-Q. Ma, Y. Xie, and L.-A. Wu, "Random number generation based on the time of arrival of single photons," Appl. Opt. **44**, 7760–7763 (2005).
29. Q. Luo, Z. Cheng, J. Fan, L. Tan, H. Song, G. Deng, Y. Wang, and Q. Zhou, "Quantum random number generator based on single-photon emitter in gallium nitride," Opt. Lett. **45**, 4224–4227 (2020).
30. Q. Yan, B. Zhao, Q. Liao, and N. Zhou, "Multi-bit quantum random number generation by measuring positions of arrival photons," Rev. Sci. Instrum. **85**, 103116 (2014).
31. E. de Jesus Lopes Soares, F. A. Mendonça, and R. V. Ramos, "Quantum random number generator using only one single photon detector," IEEE Photonics Technol. Lett. **26**, 851–853 (2014).
32. L. Li, A. Wang, P. Li, H. Xu, L. Wang, and Y. Wang, "Random bit generator using delayed self-difference of filtered amplified spontaneous emission," IEEE Photonics J. **6**, 7500109 (2014).
33. C. R. S. Williams, J. C. Salevan, X. Li, R. Roy, and T. Murphy, "Fast physical random number generator using amplified spontaneous emission," Opt. Express **18**, 23584–23597 (2010).
34. P. J. Bustard, D. G. England, J. Nunn, D. Moffatt, M. Spanner, R. Lausten, and B. J. Sussman, "Quantum random bit generation using energy fluctuations in stimulated Raman scattering," Opt. Express **21**, 29350–29357 (2013).
35. L. Huang, H. Zhou, K. Feng, and C. Xie, "Quantum random number cloud platform," npj Quantum Inf. **7**, 107 (2021).
36. J. Ma, A. Hakande, X. Yuan, and X. Ma, "Coherence as a resource for source-independent quantum random-number generation," Phys. Rev. A **99**, 022328 (2019).
37. Z. Zheng, Y. Zhang, W. Huang, S. Yu, and H. Guo, "6 Gbps real-time optical quantum random number generator based on vacuum fluctuation," Rev. Sci. Instrum. **90**, 043105 (2019).
38. M. Huang, Z. Chen, Y. Zhang, and H. Guo, "A Gaussian-distributed quantum random number generator using vacuum shot noise," Entropy **22**, 618 (2020).
39. C.-F. Li, J.-S. Xu, X.-Y. Xu, K. Li, and G.-C. Guo, "Experimental investigation of the entanglement-assisted entropic uncertainty principle," Nat. Phys. **7**, 752–756 (2011).
40. F. Furrer, M. Berta, M. Tomamichel, V. B. Scholz, and M. Christandl, "Position-momentum uncertainty relations in the presence of quantum memory," J. Math. Phys. **55**, 122205 (2014).
41. D. G. Marangon, G. Vallone, and P. Villoresi, "Source-device-independent ultra-fast quantum random number generation," Phys. Rev. Lett. **118**, 060503 (2017).
42. M. Avesani, D. G. Marangon, G. Vallone, and P. Villoresi, "Source-device-independent heterodyne-based quantum random number generator at 17 Gbps," Nat. Commun. **9**, 5365 (2018).
43. T. Michel, J. Y. Haw, D. G. Marangon, O. Thearle, G. Vallone, P. Villoresi, P. K. Lam, and S. M. Assad, "Real-time source independent quantum random number generator with squeezed states," Phys. Rev. Appl. **12**, 034017 (2019).
44. Z. Cao, H. Zhou, X. Yuan, and X. Ma, "Source-independent quantum random number generation," Phys. Rev. X **6**, 011020 (2016).
45. G. Vallone, D. G. Marangon, M. Tomasin, and P. Villoresi, "Quantum randomness certified by the uncertainty principle," Phys. Rev. A **90**, 052327 (2014).
46. W. Beckner, "Inequalities in Fourier analysis," Ann. Math. **102**, 159–182 (1975).
47. I. Bialynicki-Birula and J. Mycielski, "Uncertainty relations for information entropy in wave mechanics," Comm. Math. Phys. **44**, 129–132 (1975).
48. R. Konig, R. Renner, and C. Schaffner, "The operational meaning of min- and max-entropy," IEEE Trans. Inf. Theory **55**, 4337–4347 (2009).
49. L. Rudnicki, S. P. Walborn, and F. Toscano, "Optimal uncertainty relations for extremely coarse-grained measurements," Phys. Rev. A **85**, 042115 (2012).
50. F. Furrer, J. Aberg, and R. Renner, "Min- and max-entropy in infinite dimensions," Math. Phys. **306**, 165–186 (2011).
51. T. Eberle, V. Handchen, J. Duhme, T. Franz, F. Furrer, R. Schnabel, and R. F. Werner, "Gaussian entanglement for quantum key distribution from a single-mode squeezing source," New J. Phys. **15**, 053049 (2013).
52. H. J. Landau and H. O. Pollak, "Prolate spheroidal wave functions, Fourier analysis and uncertainty – ii," Bell Syst. Tech. J. **40**, 65–84 (1961).
53. W. Huang, Y.-C. Zhang, Z. Zheng, Y. Li, B. Xu, and S. Yu, "Practical security analysis of a continuous-variable quantum random-number generator with a noisy local oscillator," Phys. Rev. A **102**, 012422 (2020).
54. L. E. Bassham, A. L. Rukhin, J. Soto, J. R. Nechvatal, M. E. Smid, S. D. Leigh, M. Levenson, M. Vangel, N. A. Heckert, and D. L. Banks, "A statistical test suite for random and pseudorandom number generators for cryptographic applications," https://www.nist.gov/publications/statistical-test-suite-random-and-pseudorandom-number-generators-cryptographic (2010).