Research Article | Vol. 32, No. 10 / 6 May 2024 / Optics Express 18237
Optics EXPRESS

Quantum randomness introduced through squeezing operations and random number generation

JIALIN CHENG,[1] SHAOCONG LIANG,[1] JILIANG QIN,[1,2] JIATONG LI,[1] BAIYUN ZENG,[1] YI SHI,[1] ZHIHUI YAN,[1,2,3] AND XIAOJUN JIA[1,2,4]

[1]State Key Laboratory of Quantum Optics and Quantum Optics Devices, Institute of Opto-Electronics, Shanxi University, 92 Wucheng Road, Taiyuan 030006, China
[2]Collaborative Innovation Center of Extreme Optics, Shanxi University, 92 Wucheng Road, Taiyuan 030006, China
[3]zhyan@sxu.edu.cn
[4]jiaxj@sxu.edu.cn

Abstract: Quantum random numbers play a crucial role in diverse applications, including cryptography, simulation, and artificial intelligence. In contrast to predictable algorithm-based pseudo-random numbers, quantum physics provides new avenues for generating theoretically true random numbers by exploiting the inherent uncertainty contained in quantum phenomena. Here, we propose and demonstrate a quantum random number generator (QRNG) using a prepared broadband squeezed state of light, where the randomness of the generated numbers entirely originates from the quantum noise introduced by squeezing operation rather than vacuum noise. The relationship between entropy rate and squeezing level is analyzed. Furthermore, we employ a source-independent quantum random number protocol to enhance the security of the random number generator.

1. Introduction

Random numbers have a wide range of applications in fields such as cryptography, modeling and simulation, statistical sampling, artificial intelligence, machine learning, network security, and hardware testing. The currently employed random numbers are algorithm-based pseudo-random numbers, which are characterized by predictability. Alternatively, random numbers can be generated through classical physical processes, including electronic noise and thermal noise. However, due to the deterministic nature of classical physics, these random numbers are theoretically predictable. On the other hand, exploiting the intrinsic uncertainty of quantum phenomena, quantum physics offers a unique avenue for generating true random numbers [1,2].

Extensive research has delved into numerous protocols and quantum systems to advance the field of quantum random number generators (QRNGs) [3–13]. These investigations involve device-independent QRNGs with extreme security [14–17] and those achieving ultra-high rates [18–20]. Quantum systems employed for generating random numbers include photon bits [21,22], continuous-variable (CV) quantum state of light [23–27], laser phase noise [20,28,29], spontaneous raman scattering [30], quantum tunneling diode [31,32] and others [33–35]. In these quantum systems, QRNGs based on the quadratures of the vacuum state and coherent state are extensively studied [24–26,36,37], primarily due to the high-speed measurement capability and economical devices. Intriguingly, there are QRNGs based on natural light [38–40], and some are specifically designed for integration into mobile phones [41]. These QRNGs can be classified into three types according to the security of the exploited protocol: trusted-device [12,18,19,24,37], semi-device-independent [42–51] and device-independent QRNGs [15–17,52]. The recent on-chip integrated QRNG has also achieved remarkable achievements [29,36,53]. These studies

#520041 https://doi.org/10.1364/OE.520041
Journal © 2024 Received 25 Jan 2024; revised 30 Mar 2024; accepted 22 Apr 2024; published 2 May 2024

Optics EXPRESS

on random number generation collectively constitute several major research directions and reach the forefront in terms of security, speed, and miniaturization in the field of current quantum random numbers.

In this work, we propose a QRNG whose randomness entirely originates from the quantum noise introduced by quantum squeezing operation. In fact, a squeezed state is more quantum compared to the vacuum state. Despite using the same measurement method for the vacuum and squeezed states, we establish the vacuum noise level as the threshold and solely regard pure quantum noise exceeding this level as the source of randomness for this quantum random number generator as depicted in Fig. 1. A broadband squeezed state of light, prepared through a short optical parametric amplifier (OPA), is the foundation for generating quantum random numbers. Based on a source-independent (SI) quantum random number protocol and balanced homodyne detection, we implement the QRNG system and achieve a generation rate of up to 92.8 Mbps, in which we assume the noise process is stationary and source emitting independent and identically distributed quantum states. The amount of the targeted randomness decreases when the decoherence effect of the squeezed state is enhanced, leading to a decrease in the rate of quantum random number generation.

2. Theory and protocol

Squeezed states of light are produced in nonlinear processes, in which pairs of correlated photons of the same frequency can be generated. The squeezing operator describing the time evolution of the light field in the process is $\hat{S}(\xi) = e^{\frac{\xi}{2}\hat{a}^{\dagger 2} - \frac{\xi^*}{2}\hat{a}^2}$, and the squeezed state $|\xi\rangle$ can be represented as [54]

$$\hat{S}|0\rangle = \frac{1}{\sqrt{\cosh r}} \sum_{n=0}^{\infty} \frac{\sqrt{(2n)!}}{2^n n!} \tanh r^n |2n\rangle, \tag{1}$$

where $\xi = |\xi| e^{i\theta}$, $r \in \mathbb{R}$ is called the squeezing parameter and θ is the squeezing angle. In comparison to the vacuum and coherent states, the squeezed vacuum state is a superposition of only even Fock states, endowing it with stronger non-classical properties. For the proposed QRNG, the targeted randomness solely stems from quantum noise introduced by quantum squeezing operations. Consequently, we do not consider the randomness inherent in vacuum noise within this context.

In general QRNGs based on balanced homodyne detection, the measurement results of quadrature amplitude $\hat{Q}$ and quadrature phase $\hat{P}$ are typically discretized with an oscilloscope or analog-to-digital converter (ADC) during data collection. The effect of measurement discretization needs to be considered. A coarse-grained version of the operator $\hat{P}$ is obtained by introducing a partition $\mathcal{P}_{\delta p} = \{I^k_{\delta p}\}_{k=-\infty}^{+\infty}$ for the positive operator value measure (POVM) $\left\{\hat{P}^k_{\delta p}\right\}$ with elements $\hat{P}^k_{\delta p} = \int_{k\delta p}^{(k+1)\delta p} dp|p\rangle\langle p|$, where the elements $I^k_{\delta p}$ consist of half-open intervals defined as $I^k_{\delta p} = (k\delta p, (k+1)\,\delta p]$, and δp represents the measurement precision and $k \in \mathbb{N}$. The same applies to the discretized measurement of quadrature $\hat{Q}$. The discretization process distributes the measurement outcomes among individual result bins. By encoding these bins, the measured results can be transformed into raw quantum random bits.

To enhance the security of the QRNG, we employ the SI quantum random number protocol and the obtained squeezing level to estimate the amount of secure quantum randomness within the anti-squeezed quantum noise [55]. Derived from the well-known Heisenberg uncertainty principle

$$\triangle P \cdot \triangle Q \geq \frac{1}{2} \left|\langle [P, Q] \rangle\right|, \tag{2}$$

the entropic uncertainty principle [56]

$$H(P) + H(Q) \geq \log_2 c_0 \tag{3}$$

Optics EXPRESS

stands as the foundational theory of this SI quantum random number protocol, where $H(\cdot)$ represents von Neumann entropy and the term c_0 quantifies the complementarity of the observables. Consider a system with a partition state ω_{ABC}. Under the conditions of discretization measurement mentioned above, the uncertainty relationship described by the conditional max-entropy and conditional min-entropy is given by [57]

$$H_{\min}(P_{\delta p}|C) + H_{\max}(Q_{\delta q}|B) \geq -\log_2 c(\delta q, \delta p), \tag{4}$$

where $H_{\min}(P_{\delta p}|C)$ and $H_{\max}(Q_{\delta q}|B)$ are the conditional quantum min- and max-entropy, respectively. The complementarity $c(\delta q, \delta p)$ can be expressed in terms of the 0th radial prolate spheroidal wave function of the first kind $S_0^{(1)}$ as

$$c(\delta q, \delta p) = \frac{1}{2\pi}\delta q \delta p S_0^{(1)}(1, \frac{\delta q \delta p}{4})^2, \tag{5}$$

taking into account the POVMs $\left\{\hat{P}_{\delta p}^k\right\}$ and $\left\{\hat{Q}_{\delta q}^k\right\}$. Here δp and δq represent the measurement precision of quadratures $\hat{P}$ and $\hat{Q}$ in phase space using an actual digital device. Typically, δp and δq are set as equal, denoted by δ.

For the partition state ω_{ABC}, we assume that system C is held by Eve, and the system B coincides with A in the quantum random number scheme. Equation (4) is further represented as

$$\begin{aligned} H_{\min}(P_{\delta p}|E) &\geq -\log_2 c(\delta q, \delta p) - H_{\max}(Q_{\delta q}) \\ &\equiv H_{\text{low}}(P_{\delta p}|E) \end{aligned} \tag{6}$$

Here, $H_{\text{low}}(P_{\delta p}|E)$ represents the lower bound on the conditional min-entropy, i.e., the maximum amount of secure extractable randomness. $H_{\max}(Q_{\delta q})$ is the max-entropy that reflects Alice's lack of knowledge about outcomes when measuring the quadrature $\hat{Q}$. Here $\hat{P}$, $\hat{Q}$ are defined as the data quadrature and check quadrature, respectively. Assuming the injected squeezed state follows a Gaussian distribution, it is easy to estimate the rate of random number generation using $H_{\max}(Q_{\delta q}) = 2\log_2 \sum_k \sqrt{\mathfrak{p}(q_k)}$, where $\mathfrak{p}(q_k)$ is the probability of the measurement result falling into the kth bin.

In this scheme, we exploit quantum noise introduced by squeezing operation instead of vacuum noise to generate quantum random numbers. Therefore, the amount of extractable quantum randomness for this scheme can be expressed as

$$H_{\text{SQ}}\left(P_{\delta p}|E\right) = H_{\text{S}}(P_{\delta p}|E) - H_{\text{V}}(P_{\delta p}|E) \tag{7}$$

where $H_{\text{S}}(P_{\delta p}|E)$ and $H_{\text{V}}(P_{\delta p}|E)$ represent the amount of extractable randomness of the anti-squeezed quadrature of the squeezed vacuum state and the vacuum before squeezing respectively, as shown in Eq. (6). It can be seen that we remove the randomness contained in the anti-squeezed noise that is not caused by nonlinear effects.

In addition, the smooth min-entropy is taken into account in the practical random number protocol, which is related to the randomness extraction. Based on this, the amount of extractable quantum randomness can be further expressed as [55,58,59]

$$H_{\text{SQ}}^{\epsilon}\left(P_{\delta p}|E\right) = H_{\text{SQ}}\left(P_{\delta p}|E\right) - \frac{4}{\sqrt{n_p}}\sqrt{\log_2(\frac{2}{\epsilon^2})}\log_2(2^{1+\frac{H_{\max}(Q_{\delta q})}{2}} + 1), \tag{8}$$

where $H_{\text{SQ}}^{\epsilon}\left(P_{\delta p}|E\right)$ is the smooth min-entropy, representing the secure quantum randomness accounting for finite-size effects. n_p is the number of measurements for quadrature $\hat{P}$ and ϵ is the security parameter. The protocol is called ϵ-secure, which means that it is ϵ-indistinguishable

Optics EXPRESS

from an ideal protocol that is perfectly secure. The term $H_{\max}(Q_{\delta q})$ is the max-entropy of the vacuum quadrature, considering the most conservative scenario.

It is important to note that we assume the source emit independent and identically distributed quantum states. Furthermore, we handle vacuum noise and other classical noise differently in this scheme. Under the requirements of the SI protocols, vacuum noise within the measured noise is considered pure and eliminated using Eq. (7). On the other hand, classical noise, assumed as stationary and Gaussian, including electronic noise and additional noises from local oscillator (LO) fluctuations, phase drift, temperature variations, external electromagnetic field interference, and others, is treated as impurities in the input pure state and therefore untrusted. An observed increase in classical noise reduces the amount of secure randomness, following the entropic uncertainty principle, as represented by Eq. (6).

3. Experimental setup

The experimental setup is illustrated in Fig. 2. The Nd: YVO_4/LBO dual-wavelength laser emits beams with wavelengths of 1342 nm and 671 nm. The two beams are separated by a dichroic beam splitter (DBS) and then pass through two mode-cleaners (MCs) respectively, reaching two coherent states at least 3 MHz, where the quadrature noise is equal to the vacuum noise. Differing from the previously used OPA [60–63], we design a short half-monolithic optical cavity to serve as the OPA for the preparation of a broadband squeezed state [64]. The lengths of the periodically polarized $KTiOPO_4$ (PPKTP) crystal in OPA and whole cavity are approximately 10 mm and 6 mm respectively. The front surface of the crystal is coated with reflectivity R>99.9% at 1342 nm and transmission T = 85.3% at 671 nm, while the piezo-actuated concave mirror is coated with reflectivity R = 88.2% at 1342 nm and reflectivity R = 99.9% at 671 nm. The 671 nm laser is used as the pump beam for OPA, while the 1342 nm laser is used as the seed beam for OPA and LO for balanced homodyne detection. The PPKTP crystal's temperature is controlled at around 53 °C to achieve simultaneous resonance for both the seed beam (8 mW injection power) and pump beam (80 mW injection power). When the relative phase between the seed and pump beam is locked in $n\pi$ (n is an odd integer), a bright broadband squeezed state of light is prepared, characterized by a squeezed quadrature amplitude and an anti-squeezed quadrature phase. We employ the quadratures of the sideband of bright squeezed light to evaluate the secure randomness and generate the raw random numbers.

The squeezed state is detected using a LO and a balanced homodyne detector. The obtained alternating current component is amplified using a broadband amplifier. We employ a 103 MHz signal and a 100 MHz low-pass filter for mixing and filtering the amplified signal. Subsequently, the signal is collected using an oscilloscope for data acquisition, enabling discrete measurement of the anti-squeezed quadrature and the evaluation of targeted quantum randomness. The choice of quadrature measurements is governed by a random seed that alternates between data quadrature and check quadrature measurements. The detected squeezing level of the check quadrature is exploited to estimate the amount of secure randomness and raw random numbers are generated based on the quadrature measurements. To ensure the uniformity of the random switching, we segment the total measurement time into a large number of 20-μs intervals, selecting only 1 μs randomly within each interval for measuring the check quadrature. Consequently, we input 5 random bits every 20 μs to facilitate the selection and switching of quadrature measurements. During the generation of raw random numbers, the oscilloscope assigns each measurement result to a different bin and converts it into an n-bit raw random number. These raw random numbers are processed offline using a computer, with the check quadrature used for evaluating the conditional min-entropy. Exploiting the randomness extractor, we obtain the ultimate secure quantum random bits. A small portion of these random numbers is recycled into the phase modulator, enabling randomly switching measurements of quadrature components. The LO

Optics EXPRESS

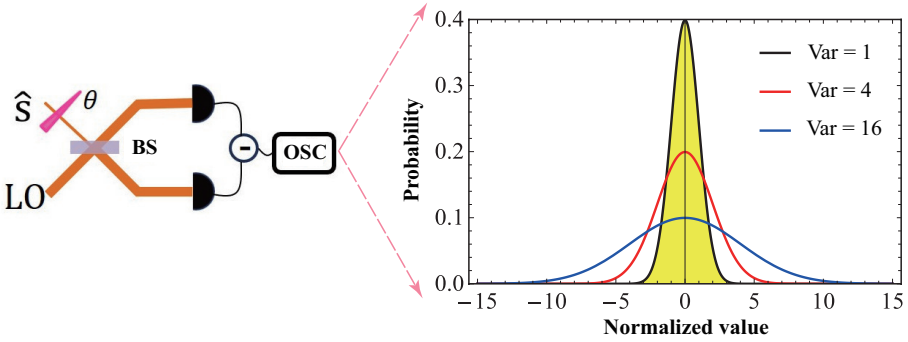

Fig. 1. Schematic diagram for generating random numbers with the signal field $\hat{s}$. The left side is a balanced homodyne detection used to measure the quadrature components of the signal field. The right side depicts the distribution of the measured data, i.e., the measured anti-squeezed quadratures of squeezed states with variances of 1, 4, and 16, corresponding to the black, red, and blue curves respectively. The yellow area enclosed by the black curve represents the distribution of measurement results with the vacuum and coherent states. The distribution of measurement results becomes flatter and more uniform with the enhancement of the anti-squeezing, indicating an increase in targeted entropy. LO: local oscillator, BS: 50:50 beam splitter, OSC: oscilloscope.

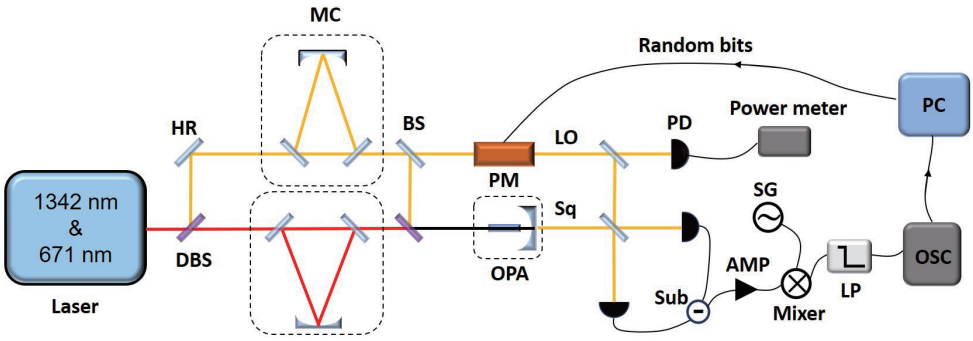

Fig. 2. Schematics of the setup for the quantum random number generation. HR: mirror with high reflectivity, DBS: dichroic beam splitter, MC: mode cleaner, BS: 50:50 beam splitter, PM: phase modulator, OPA: optical parametric amplifier, LO: local oscillator, Sq: squeezed state, PD: photoelectric detector, Sub: subtractor, SG: signal source, AMP: broadband amplifier, LP: low-pass filter, PC: computer, OSC: oscilloscope.

power is continuously monitored in real-time using a detector and a power meter, ensuring the reliability of the measurement results.

Before initiating random number generation, it is necessary to characterize the relevant devices. Firstly, the electronic noise level of the homodyne detector is recorded. Subsequently, the LO is measured via the balanced homodyne detector to record the vacuum noise level. Continuous monitoring of the LO power level is essential throughout the random number generation process. Maintaining a constant LO power ensures that the measured vacuum noise level remains unchanged. Additionally, random switching to the check quadrature (i.e., the squeezed quadrature) is necessary to assess the anti-squeezing level and the amount of the targeted quantum randomness. The switching time is set to 5% of the total measurement time, and the starting point of random switching is provided by the terminal random bits. Measuring the squeezed noise level not only allows for the assessment of the quality of the squeezed state but

Optics EXPRESS

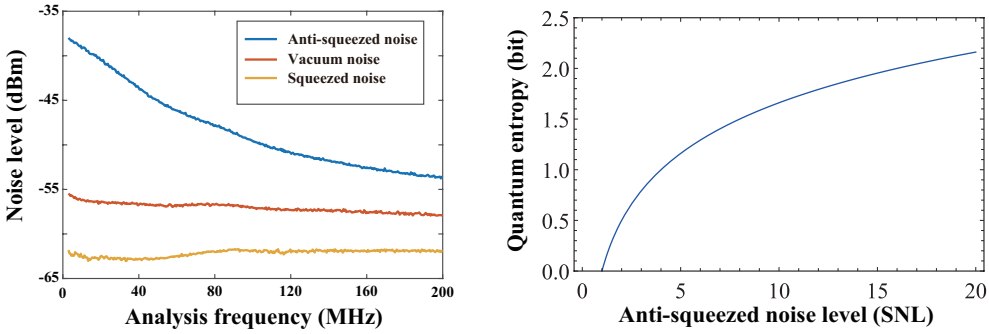

Fig. 3. Experimental results. (a) The measured noise power spectra, spanning a frequency range from 3 MHz to 200 MHz. (b) The entropy rate of quantum random numbers varies with the level of anti-squeezed noise. Here, the quadrature noise of coherent states (or vacuum state) is defined as 1. When the anti-squeezed noise level is 1, no targeted quantum random numbers can be extracted.

also enables the observation of the effects of other factors on the system. The latter may lead to an increase in undesired randomness. Finally, the amount of the targeted quantum randomness is evaluated using Eqs. (4)–(8), followed by further randomness extraction. If squeezing disappears, or if strong noise interference causes the noise level of the squeezed quadrature to surpass vacuum noise, the protocol is aborted.

4. Experimental results

The prepared squeezed state of light is measured using a spectrum analyzer, and the power spectra are shown in Fig. 3(a). The anti-squeezed noise, ranging from 3 MHz to 203 MHz, is selected for random number generation. The estimated amount of targeted quantum randomness for the squeezed quadrature is based on the squeezed quadrature data. The signals are initially acquired at a rate of 1 GSamples/s and then downsampled to 200 MSamples/s.

In order to estimate the generation rate, the amount of quantum random numbers based on different anti-squeezing levels can be obtained using the theory described in Theory and Protocol, as shown in Fig. 3(b). Based on the measured squeezing level and the selected squeezing bandwidth, the squeezing ranges from 6.3 dB at 3 MHz to 4.1 dB at 203 MHz. We chose a conservative squeezing level of 4.1 dB. Based on the estimated quantum conditional min-entropy, each measurement result contains approximately 0.68 targeted quantum random bits.

In the subsequent randomness extraction, Toeplitz-Hash processing is performed on the 10^6 samples obtained from a round of experiments. The randomness extraction involves a security parameter ϵ, which is set as 10^{-12}. A Toeplitz matrix, composed of $m \times l - 1$ computer-generated random numbers, is used to extract randomness from the raw random bits, where m and l represent the number of input raw random bits and output terminal random bits respectively, with $m>l$. The smooth min-entropy is further obtained using Eq. (8), and $H_{\min}^{\epsilon}(P_{\delta p}|E) = 0.48$ bit. Furthermore, the amount of targeted quantum random numbers or the smooth min-entropy obtained at different squeezing levels under the same extraction conditions is shown in Fig. 3(b). Considering that the time required for randomly switching and measuring the check quadrature constitutes 5% of the total measurement time, along with the consumption of random seed at a rate of 156.25 kbps, our random number generation rate is approximately 92.8 Mbps. A extracted random string of 5 Mbit from raw random data is tested with the NIST suite [65], and the results are shown in Table 1. In the case of multiple tests in a category, the smallest have been reported.

Optics EXPRESS

Table 1. Results of NIST test suite on the extracted random numbers.

Test	P-value	Result
ApproximateEntropy	0.741933	Pass
BlockFrequency	0.927454	Pass
CumulativeSums	0.873457	Pass
FFT	0.686381	Pass
Frequency	0.896566	Pass
LinearComplexity	0.118981	Pass
LongestRun	0.264913	Pass
NonOverlappingTemplate	0.597707	Pass
OverlappingTemplate	0.547525	Pass
RandomExcursions	0.079253	Pass
RandomExcursionsVariant	0.215725	Pass
Rank	0.677375	Pass
Runs	0.572743	Pass
Serial	0.423874	Pass
Universal	0.916456	Pass

5. Summary

In this work, we choose the anti-squeezing noise completely introduced by the squeezing operation as the targeted quantum entropy source for random number generation. By exploiting the entropic uncertainty principle and a prepared broadband squeezed light, we achieve a SI QRNG with the generation rate of approximately 92.8 Mbps. In this protocol, the vacuum noise and other untrusted noise are treated separately and differently. The generated random numbers can be used to demonstrate some quantum information protocols [60,66–70]. Furthermore, recent advancements in waveguide-based squeezed light suggest that the squeezing bandwidth can be significantly improved [71,72], indicating the potential for further enhancement in the generation rate of such a QRNG. The demonstrated quantum random number scheme represents a novel scheme that enriches the research on QRNGs.

Funding. National Natural Science Foundation of China (61925503, 62122044, 62135008); Program for the Outstanding Innovative Teams of Higher Learning Institutions of Shanxi; Program for the Innovative Talents of Higher Education Institutions of Shanxi; Fund for Shanxi Key Subjects Construction (1331 Project).

Acknowledgment. The authors thank for Xiongfeng Ma and Hongyi Zhou for useful discussions.

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.

References

1. M. Herrero-Collantes and J. C. Garcia-Escartin, "Quantum random number generators," Rev. Mod. Phys. **89**(1), 015004 (2017).
2. X. Ma, X. Yuan, Z. Cao, *et al.*, "Quantum random number generation," npj Quantum Inf. **2**(1), 16021 (2016).
3. B. Shen, H. Shu, W. Xie, *et al.*, "Harnessing microcomb-based parallel chaos for random number generation and optical decision making," Nat. Commun. **14**(1), 4590 (2023).
4. M. Eaton, A. Hossameldin, R. J. Birrittella, *et al.*, "Resolution of 100 photons and quantum generation of unbiased random numbers," Nat. Photonics **17**(1), 106–111 (2023).
5. S. Li, X. Zhu, J. Fan, *et al.*, "5-bit all-optical quantum random number generator based on a time-multiplexed optical parametric oscillator," Opt. Express **31**(23), 38939–38948 (2023).
6. Y. Zhang, H.-P. Lo, A. Mink, *et al.*, "A simple low-latency real-time certifiable quantum random number generator," Nat. Commun. **12**(1), 1056 (2021).

Optics EXPRESS

7. Y. Okawachi, B. Y. Kim, Y. Zhao, *et al.*, "Dynamic control of photon lifetime for quantum random number generation," Optica **8**(11), 1458–1461 (2021).
8. A. Quirce and A. Valle, "Random polarization switching in gain-switched vcsels for quantum random number generation," Opt. Express **30**(7), 10513–10527 (2022).
9. Q. Luo, Z. Cheng, J. Fan, *et al.*, "Quantum random number generator based on single-photon emitter in gallium nitride," Opt. Lett. **45**(15), 4224–4227 (2020).
10. H. Zhou, P. Zeng, M. Razavi, *et al.*, "Randomness quantification of coherent detection," Phys. Rev. A **98**(4), 042321 (2018).
11. S. Pironio, A. Acín, S. Massar, *et al.*, "Random numbers certified by bell's theorem," Nature **464**(7291), 1021–1024 (2010).
12. Q. Zhang, D. Kong, Y. Wang, *et al.*, "Dual-entropy-source quantum random number generation based on spontaneous emission," Opt. Lett. **45**(2), 304–307 (2020).
13. R. Shakhovoy, D. Sych, V. Sharoglazova, *et al.*, "Quantum noise extraction from the interference of laser pulses in an optical quantum random number generator," Opt. Express **28**(5), 6209–6224 (2020).
14. M.-H. Li, X. Zhang, W.-Z. Liu, *et al.*, "Experimental realization of device-independent quantum randomness expansion," Phys. Rev. Lett. **126**(5), 050503 (2021).
15. W.-Z. Liu, M.-H. Li, S. Ragy, *et al.*, "Device-independent randomness expansion against quantum side information," Nat. Phys. **17**(4), 448–451 (2021).
16. Y. Liu, Q. Zhao, M.-H. Li, *et al.*, "Device-independent quantum random-number generation," Nature **562**(7728), 548–551 (2018).
17. L. K. Shalm, Y. Zhang, J. C. Bienfang, *et al.*, "Device-independent randomness expansion with entangled photons," Nat. Phys. **17**(4), 452–456 (2021).
18. B. Bai, J. Huang, G.-R. Qiao, *et al.*, "18.8 Gbps real-time quantum random number generator with a photonic integrated chip," Appl. Phys. Lett. **118**(26), 264001 (2021).
19. C. Bruynsteen, T. Gehring, C. Lupo, *et al.*, "100-gbit/s integrated quantum random number generator based on vacuum fluctuations," PRX Quantum **4**(1), 010330 (2023).
20. Y.-Q. Nie, L. Huang, Y. Liu, *et al.*, "The generation of 68 Gbps quantum random number by measuring laser phase fluctuations," Rev. Sci. Instrum. **86**(6), 063105 (2015).
21. V. Tamma and S. Laibacher, "Boson sampling with random numbers of photons," Phys. Rev. A **104**(3), 032204 (2021).
22. M. A. Smirnov, K. Petrovnin, V I. Fedotov, *et al.*, "Quantum random numbers from a fiber-optic photon-pair source," Laser Phys. Lett. **16**(11), 115402 (2019).
23. T. Michel, J. Y. Haw, D. G. Marangon, *et al.*, "Real-time source-independent quantum random-number generator with squeezed states," Phys. Rev. Appl. **12**(3), 034017 (2019).
24. X. Guo, C. Cheng, M. Wu, *et al.*, "Parallel real-time quantum random number generator," Opt. Lett. **44**(22), 5566–5569 (2019).
25. J.-R. Álvarez, S. Sarmiento, J. A. Lázaro, *et al.*, "Random number generation by coherent detection of quantum phase noise," Opt. Express **28**(4), 5538–5547 (2020).
26. D. Rusca, H. Tebyanian, A. Martin, *et al.*, "Fast self-testing quantum random number generator based on homodyne detection," Appl. Phys. Lett. **116**(26), 264004 (2020).
27. J. Cheng, S. Liang, J. Qin, *et al.*, "Semi-device-independent quantum random number generator with a broadband squeezed state of light," npj Quantum Inf. **10**(1), 20 (2024).
28. R. Shakhovoy, M. Puplauskis, V. Sharoglazova, *et al.*, "Phase randomness in a semiconductor laser: Issue of quantum random-number generation," Phys. Rev. A **107**(1), 012616 (2023).
29. F. Raffaelli, P. Sibson, J. E. Kennard, *et al.*, "Generation of random numbers by measuring phase fluctuations from a laser diode with a silicon-on-insulator chip," Opt. Express **26**(16), 19730–19741 (2018).
30. Y.-Y. Hu, X. Lin, S. Wang, *et al.*, "Quantum random number generation based on spontaneous raman scattering in standard single-mode fiber," Opt. Lett. **45**(21), 6038–6041 (2020).
31. K. Aungskunsiri, R. Amarit, K. Wongpanya, *et al.*, "Random number generation from a quantum tunneling diode," Appl. Phys. Lett. **119**(7), 074002 (2021).
32. H. Zhou, J. Li, W. Zhang, *et al.*, "Quantum random-number generator based on tunneling effects in a Si diode," Phys. Rev. Appl. **11**(3), 034060 (2019).
33. H. Tebyanian, M. Zahidy, M. Avesani, *et al.*, "Semi-device independent randomness generation based on quantum state's indistinguishability," Quantum Sci. Technol. **6**(4), 045026 (2021).
34. V. Lovic, D. Marangon, M. Lucamarini, *et al.*, "Characterizing phase noise in a gain-switched laser diode for quantum random-number generation," Phys. Rev. Appl. **16**(5), 054012 (2021).
35. A. Quirce and A. Valle, "Phase diffusion in gain-switched semiconductor lasers for quantum random number generation," Opt. Express **29**(24), 39473–39485 (2021).
36. F. Raffaelli, G. Ferranti, D. H. Mahler, *et al.*, "A homodyne detector integrated onto a photonic chip for measuring quantum states and generating random numbers," Quantum Sci. Technol. **3**(2), 025003 (2018).
37. Z. Zheng, Y. Zhang, W. Huang, *et al.*, "6 Gbps real-time optical quantum random number generator based on vacuum fluctuation," Rev. Sci. Instrum. **90**(4), 043105 (2019).

Optics EXPRESS

38. X. Lin, R. Wang, S. Wang, *et al.*, "Imperfection-insensitivity quantum random number generator with untrusted daily illumination," Opt. Express **30**(14), 25474–25485 (2022).
39. Y.-H. Li, X. Han, Y. Cao, *et al.*, "Quantum random number generation with uncharacterized laser and sunlight," npj Quantum Inf. **5**(1), 97 (2019).
40. D. Drahi, N. Walk, M. J. Hoban, *et al.*, "Certified quantum random numbers from untrusted light," Phys. Rev. X **10**(4), 041048 (2020).
41. B. Sanguinetti, A. Martin, H. Zbinden, *et al.*, "Quantum random number generation on a mobile phone," Phys. Rev. X **4**(3), 031056 (2014).
42. W.-B. Liu, Y.-S. Lu, Y. Fu, *et al.*, "Source-independent quantum random number generator against tailored detector blinding attacks," Opt. Express **31**(7), 11292–11307 (2023).
43. Y. Li, Y. Fei, W. Wang, *et al.*, "Practical security analysis of a continuous-variable source-independent quantum random number generator based on heterodyne detection," Opt. Express **31**(15), 23813–23829 (2023).
44. C. Roch i Carceller, K. Flatt, H. Lee, *et al.*, "Quantum vs noncontextual semi-device-independent randomness certification," Phys. Rev. Lett. **129**(5), 050501 (2022).
45. C. Wang, I. W. Primaatmaja, H. J. Ng, *et al.*, "Provably-secure quantum randomness expansion with uncharacterised homodyne detection," Nat. Commun. **14**(1), 316 (2023).
46. M. Avesani, D. G. Marangon, G. Vallone, *et al.*, "Source-device-independent heterodyne-based quantum random number generator at 17 gbps," Nat. Commun. **9**(1), 5365 (2018).
47. J. Ma, A. Hakande, X. Yuan, *et al.*, "Coherence as a resource for source-independent quantum random-number generation," Phys. Rev. A **99**(2), 022328 (2019).
48. C. Wang, W. Y. Kon, H. J. Ng, *et al.*, "Experimental symmetric private information retrieval with measurement-device-independent quantum network," Light: Sci. Appl. **11**(1), 268 (2022).
49. Z. Zheng, Y. Zhang, M. Huang, *et al.*, "Bias-free source-independent quantum random number generator," Opt. Express **28**(15), 22388–22398 (2020).
50. T. Gehring, C. Lupo, A. Kordts, *et al.*, "Homodyne-based quantum random number generator at 2.9 gbps secure against quantum side-information," Nat. Commun. **12**(1), 605 (2021).
51. J. Cheng, J. Qin, S. Liang, *et al.*, "Mutually testing source-device-independent quantum random number generator," Photonics Res. **10**(3), 646–652 (2022).
52. Y. Zhang, L. K. Shalm, J. C. Bienfang, *et al.*, "Experimental low-latency device-independent quantum randomness," Phys. Rev. Lett. **124**(1), 010505 (2020).
53. G. Gras, A. Martin, J. W. Choi, *et al.*, "Quantum entropy model of an integrated quantum-random-number-generator chip," Phys. Rev. Appl. **15**(5), 054048 (2021).
54. C. Weedbrook, S. Pirandola, R. García-Patrón, *et al.*, "Gaussian quantum information," Rev. Mod. Phys. **84**(2), 621–669 (2012).
55. D. G. Marangon, G. Vallone, and P. Villoresi, "Source-device-independent ultrafast quantum random number generation," Phys. Rev. Lett. **118**(6), 060503 (2017).
56. P. J. Coles, M. Berta, M. Tomamichel, *et al.*, "Entropic uncertainty relations and their applications," Rev. Mod. Phys. **89**(1), 015002 (2017).
57. F. Furrer, M. Berta, M. Tomamichel, *et al.*, "Position-momentum uncertainty relations in the presence of quantum memory," J. Math. Phys. **55**(12), 122205 (2014).
58. M. Berta, M. Christandl, R. Colbeck, *et al.*, "The uncertainty principle in the presence of quantum memory," Nat. Phys. **6**(9), 659–662 (2010).
59. T. Eberle, V. Haendchen, J. Duhme, *et al.*, "Gaussian entanglement for quantum key distribution from a single-mode squeezing source," New J. Phys. **15**(5), 053049 (2013).
60. M. Huo, J. Qin, J. Cheng, *et al.*, "Deterministic quantum teleportation through fiber channels," Sci. Adv. **4**(10), eaas9401 (2018).
61. X. Zuo, Z. Yan, Y. Feng, *et al.*, "Quantum interferometer combining squeezing and parametric amplification," Phys. Rev. Lett. **124**(17), 173602 (2020).
62. J. Yu, Y. Qin, J. Qin, *et al.*, "Quantum enhanced optical phase estimation with a squeezed thermal state," Phys. Rev. Appl. **13**(2), 024037 (2020).
63. Z. Yan, L. Wu, X. Jia, *et al.*, "Establishing and storing of deterministic quantum entanglement among three distant atomic ensembles," Nat. Commun. **8**(1), 718 (2017).
64. S. Liang, J. Cheng, J. Qin, *et al.*, "High-speed quantum radio-frequency-over-light communication," Phys. Rev. Lett. **132**(14), 140802 (2024).
65. L. Bassham, A. Rukhin, J. Soto, *et al.*, "A statistical test suite for random and pseudorandom number generators for cryptographic applications, special publication (nist sp)," National Institute of Standards and Technology (2024).
66. H. Zhang, Z. Sun, R. Qi, *et al.*, "Realization of quantum secure direct communication over 100 km fiber with time-bin and phase quantum states," Light: Sci. Appl. **11**(1), 83 (2022).
67. Y. Zhou, J. Yu, Z. Yan, *et al.*, "Quantum secret sharing among four players using multipartite bound entanglement of an optical field," Phys. Rev. Lett. **121**(15), 150502 (2018).
68. Y. Qin, J. Ma, D. Zhao, *et al.*, "Continuous variable quantum conference network with a greenberger-horne-zeilinger entangled state," Photonics Res. **11**(4), 533–540 (2023).

Optics EXPRESS

69. S. Shen, C. Yuan, Z. Zhang, *et al.*, "Hertz-rate metropolitan quantum teleportation," Light: Sci. Appl. **12**(1), 115 (2023).
70. Z. Yan and X. Jia, "Teleportation goes to hertz rate," Light: Sci. Appl. **12**(1), 167 (2023).
71. T. Kashiwazaki, N. Takanashi, T. Yamashima, *et al.*, "Continuous-wave 6-db-squeezed light with 2.5-thz-bandwidth from single-mode ppln waveguide," APL Photonics **5**(3), 036104 (2020).
72. T. Kashiwazaki, T. Yamashima, K. Enbutsu, *et al.*, "Over-8-dB squeezed light generation by a broadband waveguide optical parametric amplifier toward fault-tolerant ultra-fast quantum computers," Appl. Phys. Lett. **122**(23), 234003 (2023).