Optics EXPRESS

Quantum random number generator with discarding-boundary-bin measurement and multi-interval sampling

ZHENGUO LU,[1,2] JIANQIANG LIU,[1,2] XUYANG WANG,[1,2] PU WANG,[1,2] YONGMIN LI,[1,2,*] 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*

**yongmin@sxu.edu.cn*

Abstract: A quantum random number generator (QRNG) provides a reliable means for the generation of true random numbers. The inherent randomness of the vacuum fluctuations makes the quantum vacuum state a superior source of entropy. However, in practice, the raw sequences of QRNG are inevitably contaminated by classical technical noise, which compromises the security of the QRNG. Min-entropy conditioned on the classical noise is a useful method that can quantify the side-information independent randomness. To improve the extractable randomness from the raw sequences arising from the quantum vacuum-based QRNG, we propose and experimentally demonstrate two approaches, discarding-boundary-bin measurement and multi-interval sampling. The first one increases the conditional min-entropy at a low quantum-to-classical-noise ratio. The latter exploits parallel sampling using multiple analog-to-digital converters (ADCs) and effectively overcomes the finite resolution limit and uniform sampling of a single ADC. The maximum average conditional min-entropy can reach 9.2 per sample when combining these two approaches together in contrast to 6.93 with a single 8-bit ADC.

1. Introduction

Quantum random number generator (QRNG) plays an essential role in various applications, such as simulation, cryptography, and fundamental science [1,2]. For instance, quantum key distribution requires a reliable randomness source to guarantee its information-theoretical security [3–7]. If the quantum states are not prepared in a truly random manner, the quantum key distribution protocol will inevitably suffer from attacks, which has been shown for the BB84 protocol [8]. Therefore, in such applications, the random sequence must be genuinely unpredictable and has sufficient security.

The quality of the entropy source fundamentally determines the performance of a random number generator. Random number generators based on noise in electronic circuits can be used to generate high-speed random numbers and easily integrated into application systems [9,10]. However, the randomness of most of the noise in electronic circuits is not theoretically provable. More precisely, noise in such systems come basically from two types, shot noise and thermal noise. Shot noise arises from quantum effects due to the discrete charges nature of the current, which shows quantum fluctuations. In contrast, thermal noise arises from the thermal agitation of the carriers and is subject to thermally activated statistical motion. In practice, it is difficult to characterize precisely the amount of quantum fluctuations inside electric noise.

QRNG offers a perfect source of entropy due to the inherent randomness of quantum mechanics [11–14]. At present, various optical QRNGs have been proposed and implemented, such as vacuum fluctuations [15–18], phase noise [19–21], stimulated Raman scattering [22], photon arrival times [23–26], photon path [27], and photon number counting [28,29]. These QRNGs

#419756
Journal © 2021

https://doi.org/10.1364/OE.419756
Received 13 Jan 2021; revised 24 Mar 2021; accepted 30 Mar 2021; published 7 Apr 2021

can generate information-theoretical randomness only when model assumptions fulfill practical implementation. The imperfection of the practical devices of a QRNG, such as classical noise in detector, the unused port of the interferometer, may leak side-information correlated with the random sequence [2]. Such side-information could be exploited by a potential attacker to guess the measurement outcomes and compromise the security.

To address the security issues, several protocols have been proposed. The device-independent (DI) QRNG utilizes the violation of loophole-free Bell inequality to generate true randomness in a self-testing way [30–33]. However, the extremely low rate and the sophisticated experimental setup of DI-QRNG severely limit its practical applications. The semi-device-independent (SDI) QRNG [11,18,34–40] relies on weaker assumptions to bound the side information and can achieve a higher generation rate than DI-QRNG. Different from the DI-QRNGs and SDI-QRNGs, the practical QRNGs calibrate the devices in a fully trusted way to bound the classical side-information and ensure the security of random sequence [41,42].

A typical QRNG consists of three parts: quantum entropy source, measurement of quantum states, and extraction of true random numbers. To extract genuine randomness independent of classical noise from a practical QRNG, one should properly model the implementation of the QRNG. Ma et al. presented a framework for quantifying the quantum randomness by min-entropy and provided information-theoretically provable randomness extractors for post-processing [43]. Haw et al. proposed a method to maximize the conditional min-entropy from a given quantum-to-classical-noise ratio [42]. Huang et al. systematically analyzed the effects of the local oscillator fluctuation under imbalanced homodyne detection on the security of QRNG [44].

In this work, we proposed and demonstrated two approaches to improve the extractable randomness in a quantum vacuum fluctuations based QRNG. The first one is the discarding-boundary-bin measurement (DBBM), which increases the upper bound of the conditional min-entropy. The other one is the multi-interval sampling (MIS) technique, which uses parallel sampling based on multiple Analog-to-Digital Converters (ADCs) and effectively overcomes the finite resolution limit and uniform sampling of a single ADC. By combining these two methods together, we show that the conditional min-entropy is significantly improved, and more secure randomness can be extracted from the output signal of the homodyne detector.

2. Randomness and conditional min-entropy

2.1. Randomness quantification

The min-entropy of variable X with a probability distribution $P_X(x_i)$ is defined by [45]

$$H_{\min}(X) = -\log_2[\overset{\max}{_{x_i\in X}} P_X(x_i)], \tag{1}$$

which is widely used for quantifying the randomness and associated with the maximum guessing probability for an adversary about variable X.

In practical QRNGs, the randomness of the entropy source can be evaluated by the conditional min-entropy, which depends on the specific attacks that how the adversary interacts with the classical side-information. We assume that the adversary has no limit on computational power and fully knows the classical noise with arbitrary precision. Two attack scenarios (worst-case scenario and average-case scenario) are considered hereafter. In the worst-case scenario, the adversary has full control of the classical noise to maximize his ability to predict random sequences. In this case, the maximum conditional probability is exploited to estimate the amount of information she successfully captured, and the worst-case min-entropy of random sequences conditioned on the classical side-information is given by [46]

$$\tilde{H}_{\min}(X|E) = -\log_2[\overset{\max}{_{e_j\in[e_{\min},e_{\max}]}}\overset{\max}{_{x_i\in X}} P_{X|E}(x_i|e_j)]. \tag{2}$$

In the average-case scenario, the adversary can freely monitor the classical noise with infinite sampling range and digitization resolution but cannot modify it. Therefore, we estimate the extractable randomness of the device using the average conditional min-entropy

$$\bar{H}_{\min}(X|E) = -\log_2[P_{guess}(X_{dis}|E)], \tag{3}$$

where $P_{guess}(X_{dis}|E)$ is the average guessing probability of an adversary that can correctly guess the bit information with the best strategy [45],

$$P_{guess}(X_{dis}|E) = \int_{-\infty}^{\infty} P_E(e)^{\max}_{x_i \in X_{dis}} P_{X_{dis}|E}(x_i|e) de. \tag{4}$$

According to Eqs. (2)–(4), we know that extractable secure randomness is bounded by the worst-case conditional min-entropy or the average conditional min-entropy, which directly relates to the maximum (average) guessing probability of an adversary conditioned on the classical noise. A smaller maximum conditional probability means a lower amount of an adversary's knowledge on the random sequence and therefore more extractable randomness. Given the entropy source, the guessing probability of an adversary strongly depends on the measurement model, as we will show in the following section.

2.2. Conventional measurement model

For QRNG based on the vacuum fluctuations noise, the output signal M of the balanced homodyne detector (BHD) is a mixture of vacuum fluctuations noise Q and classical electronic noise E [15]. We suppose both the noises are time-independent and follow Gaussian distributions centered at zero, $N(0, \sigma_E^2)$ and $N(0, \sigma_Q^2)$, where σ_Q^2 is the variance of quantum noise and σ_E^2 is the variance of classical electronic noise. The quantum-to-classical noise ratio is defined as QCNR, i.e., QCNR $= 10\log_{10}(\sigma_Q^2/\sigma_E^2)$ dB.

The probability density functions (PDF) of the vacuum quantum noise Q and the classical noise E can be expressed as

$$p_Q(q) = \frac{1}{\sqrt{2\pi}\sigma_Q} \exp\left[-\frac{q^2}{2\sigma_Q^2}\right], p_E(e) = \frac{1}{\sqrt{2\pi}\sigma_E} \exp\left[-\frac{e^2}{2\sigma_E^2}\right]. \tag{5}$$

By performing a convolution of p_Q and p_E, the PDF of the measurements M is

$$p_M(m) = \frac{1}{\sqrt{2\pi}\sigma_M} \exp\left[-\frac{m^2}{2\sigma_M^2}\right] = \frac{1}{\sqrt{2\pi(\sigma_Q^2+\sigma_E^2)}} \exp\left[-\frac{m^2}{2(\sigma_Q^2+\sigma_E^2)}\right]. \tag{6}$$

Then the PDF of the measurements M conditional on the classical noise E is given by

$$p_{M|E}(m|e) = \frac{1}{\sqrt{2\pi}\left(\sigma_M^2-\sigma_E^2\right)} \exp\left[-\frac{(m-e)^2}{2\left(\sigma_M^2-\sigma_E^2\right)}\right] = \frac{1}{\sqrt{2\pi}\sigma_Q} \exp\left[-\frac{(m-e)^2}{2\sigma_Q^2}\right]. \tag{7}$$

Hereafter we normalize all the relevant quantities by the quantum noise ($\sigma_Q^2 = 1$). When we sample the output signal of BHD with an n-bit ADC with dynamical range $[-R+\delta, R-3\delta/2]$, the conditional probability distribution of measurements M on classical noise E is [42]

$$P_{M_{dis}|E}(m_i|e) = \begin{cases} \int_{-\infty}^{-R+\delta/2} p_{M|E}(m|e)\, d_m, & i = i_{\min}, \\ \int_{m_i-\delta/2}^{m_i+\delta/2} p_{M|E}(m|e)\, d_m, & i_{\min}+1 \le i \le i_{\max}-1, \\ \int_{R-3\delta/2}^{\infty} p_{M|E}(m|e)\, d_m, & i = i_{\max}. \end{cases} \tag{8}$$

Combine Eqs. (2) and (8), the worst-case min-entropy can be expressed by

$$\tilde{H}_{\min}(M_{dis}|E) = -\log_2[\max(c_1, c_2)], \tag{9}$$

where c_1 is the maximum conditional probability of the boundary bins ($i = i_{\max}, i_{\min}$) and c_2 is the maximum conditional probability within the sampling range ($i_{\min}+1 \le i \le i_{\max}-1$).

Starting from Eq. (9) and given the QCNR, we find that c_1 and c_2 are two key parameters to determine the maximum conditional min-entropy [42]. Besides, the classical noise e in Eq. (2) can be bounded for practical purposes in the worst-case scenario. When the value range of the variable e is bounded by $[-5\sigma_E, 5\sigma_E]$, it is valid for 99.9999% of the time and enough for the practical scenario. Here, we chose the range $[-5\sigma_E, 5\sigma_E]$ as the smallest confidence interval of the classical noise e. By optimizing the dynamic ADC range R, we can maximize the worst-case conditional min-entropy, which is obtained when $c_1 = c_2$.

3. Modified model of entropy quantification

In this section, we present a modified model of entropy quantification for a practical QRNG. Two approaches are employed in the modified model, DBBM and MIS. We will show that the proposed methods effectively improve the extractable randomness from the entropy source in comparison with the conventional model (CM) of entropy quantification.

3.1. Discarding-boundary-bin measurement

From previous section, we know that the maximum conditional min-entropy relies on the maximum conditional probability of the boundary bins c_1 and the maximum conditional probability within the sampling the range c_2. In the CM, the first bin $i = i_{\min}$ and last bin $i = i_{\max}$ of an ADC cover the input signals with a range of $[-\infty, -R+\delta/2]$ and $[R-3\delta/2, \infty]$, respectively. If we discard the boundary bins, the conditional probability distribution of measurements M on classical noise E will change from Eqs. (8) to (10). By further optimizing R, we can set the maximum conditional probability of the boundary bins c_1 equal to c_2. In this case, the new c_1 will be lower than before, which results in a higher maximum conditional min-entropy. The basic reason is that the boundary bins cover an infinite range of input signals. If we discard them, we can decrease the optimized R, which results in a lower maximum conditional probability and therefore a higher maximum conditional min-entropy can be obtained. The schematic of DBBM is depicted in Fig. 1.

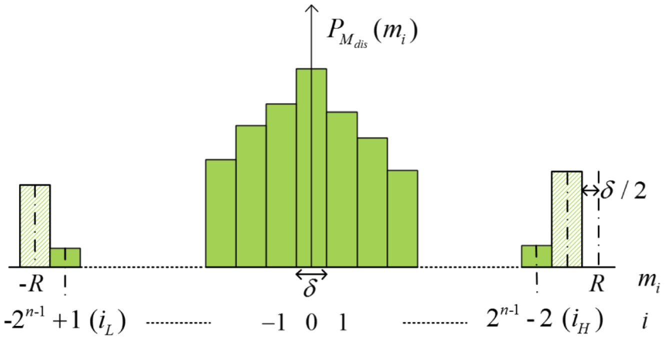

Fig. 1. Discarding-boundary-bin measurement model. The output signal of the BHD is discretized into 2^n sampling bins by n-bit ADC with dynamical range $[-R-\delta/2, R-\delta/2]$. The bin width and discrete measurement outcomes are $\delta = R/2^{n\text{-}1}$ and $m_i = \delta \times i$. The measured data that distributed in the boundary bins (shaded) are discarded. Therefore, the first bin i_L and the last bin i_H of the remaining bins centered round $-R+\delta$ and $R-2\delta$, respectively.

Based on the DBBM, the conditional probability of measurements M_{dis} on classical noise E is given by

$$P_{M_{dis}|E}(m_i|e) = \int_{m_i-\delta/2}^{m_i+\delta/2} p_{M|E}(m|e)\, d_m, \quad i_L \le i \le i_H, \tag{10}$$

where $i_L = -2^{n-1} + 1$ and $i_H = 2^{n-1} - 2$.

For each measurement, there will be a probability that the measurement results fall in the boundary bins ($i_{\min}$ and $i_{\max}$). Those results are discarded and the total conditional probability of effective measurements is

$$P_T(M_{dis}|e) = 1 - P_{M_{dis}|E}\left(m_{i_{\max}}|e\right) - P_{M_{dis}|E}\left(m_{i_{\min}}|e\right), \tag{11}$$

where $i_{\min} = -2^{n-1}$ and $i_{\max} = 2^{n-1} - 1$. Then, the normalized conditional probability of the effective measurements is

$$P^T_{M_{dis}|E}\left(m_i|e\right) = P_{M_{dis}|E}\left(m_i|e\right)/P_T(M_{dis}|e). \tag{12}$$

In terms of Eq. (12), the maximum conditional probability distribution is written as

$$\max_{m_i\in M_{dis}} P^T_{M_{dis}|E}\left(m_i|e\right) = \max\{P^T_{M_{dis}|E}\left(m_{i_{mid}}|e\right), P^T_{M_{dis}|E}\left(m_{i_L}|e\right), P^T_{M_{dis}|E}\left(m_{i_H}|e\right)\}, \tag{13}$$

where $P^T_{M_{dis}|E}\left(m_{i_{mid}}|e\right) = \begin{cases} erf[\delta/2\sqrt{2}]/P_T(e,R), & i_L<i_{mid}<i_H, \\ 0, & other. \end{cases}$

Given the bound of the classical noise $[e_{\min}, e_{\max}]$, which can be manipulated by an adversary, Eq. (13) can be rewritten as

$$\begin{aligned} &\max_{e\in[e_{min},e_{max}]}\max_{m_i\in M_{dis}} P^T_{M_{dis}|E}\left(m_i|e\right) = \max\{ \\ &\max_{e\in[e_{min},e_{max}]} P^T_{M_{dis}|E}\left(m_{i_{mid}}|e\right), \\ &\max_{e\in[e_{min},e_{max}]} P^T_{M_{dis}|E}\left(m_{i_L}|e\right), \\ &\max_{e\in[e_{min},e_{max}]} P^T_{M_{dis}|E}\left(m_{i_H}|e\right)\}. \end{aligned} \tag{14}$$

Notice that the DBBM approach decreases the number of effective measurements, we should carefully choose the optimal R to achieve the balance between the conditional min-entropy and the amount of effective data to maximize the throughput of our QRNG. To resolve this problem, we introduce the concept of equivalent conditional min-entropy.

In the worst-case scenario, the equivalent conditional min-entropy is expressed as

$$\tilde{H}^T_{eq\,\min}(M_{dis}|E) = \tilde{H}^T_{\min}(M_{dis}|E) \times \tilde{P}_T(M_{dis}|E), \tag{15}$$

where $\tilde{P}_T(M_{dis}|E)$ is the total probability of the effective measurements corresponding to the maximum conditional min-entropy $\tilde{H}^T_{\min}(M_{dis}|E)$,

$$\tilde{H}^T_{\min}(M_{dis}|E) = -\log_2\{\max_{e\in[e_{min},e_{max}]}\max_{m_i\in M_{dis}} P^T_{M_{dis}|E}(m_i|e)\}. \tag{16}$$

In the average-case scenario, the equivalent conditional min-entropy is

$$\bar{H}^T_{eq\,\min}(M_{dis}|E) = \bar{H}^T_{\min}(M_{dis}|E) \times \bar{P}_T(M_{dis}|E), \tag{17}$$

where $\bar{P}_T(M_{dis}|E)$ is the mean of the total probability of valid measurements changing with e,

$$\bar{P}_T(M_{dis}|E) = \int_{-\infty}^{+\infty} P_T(M_{dis}|e)de, \tag{18}$$

and

$$\bar{H}^T_{\min}(M_{dis}|E) = -\log_2[\int_{-\infty}^{+\infty} p_E(e)\max_{m_i\in M_{dis}} P^T_{M_{dis|}E}(m_i|e)de]. \tag{19}$$

From Eqs. (14), (15), and (16), we can optimize the ADC dynamical range R and obtain the maximum value of the worst-case equivalent conditional min-entropy in the DBBM. When the confidence interval of the classical noise e is $[-10\delta_E, 10\delta_E]$ ($[-20\delta_E, 20\delta_E]$), the worst-case equivalent conditional min-entropy of DBBM is 14.43 (14.06) for $n = 16$ and QCNR = 20 dB. In Fig. 2, we plot the discretized conditional probability distribution $P_{M_{dis}|E}(m_i|e)$ with optimized dynamical range R for the CM (Fig. 2(a)) and the DBBM (Fig. 2(b)). Compared to the CM, the maximum conditional probability distribution in the DBBM can be effectively reduced from 5.91×10^{-5} to 4.05×10^{-5}, which increases the worst-case conditional min-entropy from 14.05 to 14.43. Furthermore, we notice that unlike the CM, the maximum conditional probability c_1 of the boundary bins is no longer equal to the maximum conditional probability c_2 within the sampling range for the DBBM. Instead, the amount of effective data and the conditional min-entropy are balanced to maximize the throughput of the QRNG.

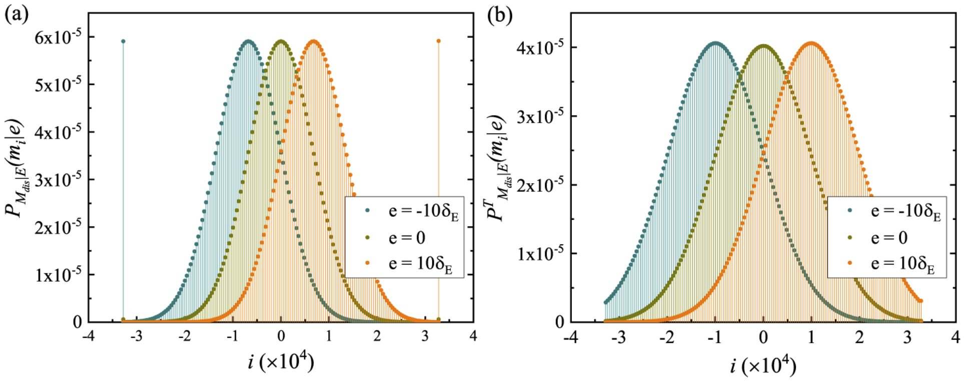

Fig. 2. The discretized worst-case conditional probability distribution $P_{M_{dis}|E}(m_i|e)$ with optimized dynamical range R for (a) CM and (b) DBBM. The parameter used are $e = \{-10\delta_E, 0, 10\delta_E\}$ (from left to right), QCNR = 20 dB, and $n = 16$. Given the optimized dynamic range $R = 4.85$, the maximum conditional probability of the CM is 5.91×10^{-5} and the corresponding condition min-entropy is 14.05. Given the optimized dynamic range $R = 3.3$, the maximum conditional probability of the DBBM is 4.05×10^{-5}, and the optimized equivalent conditional min-entropy is 14.43.

Combining Eqs. (17)–(19), we calculate the optimized equivalent conditional min-entropy for DBBM with $n = 8$ and $n = 16$ (average-case scenario). The simulated results are listed in Table 1. For a 16-bit ADC and QCNR = 20 dB, the equivalent conditional min-entropy can reach 14.79 for DBBM instead of 14.28 with the CM. In the case of QCNR = 0 dB, the equivalent conditional min-entropy obtained using the DBBM is 14.30, which is an improvement of 5.38% compared to the CM. Note that the improvement on average min-entropy decreases with the increasing QCNR, and the improvement is better for a higher resolution ADC. The above results indicate that more secure randomness can be extracted using the DBBM approach.

Table 1. Optimized $\bar{H}_{\min}(M_{dis}|E)$ (and R) for 8-bit and 16-bit ADCs.

		$n = 8$			$n = 16$	
QCNR (dB)	DBBM	CM	Improvement	DBBM	CM	Improvement
20	6.93 (2.2)	6.93 (2.59)	0.00%	14.79 (2.5)	14.28 (4.09)	+3.57%
10	6.87 (2.3)	6.72 (2.93)	+2.23%	14.73 (2.6)	14.11 (4.55)	+4.39%
0	6.44 (3.1)	6.11 (4.33)	+5.41%	14.30 (3.5)	13.57 (6.48)	+5.38%

3.2. Multi-interval sampling model

Figure 3 shows the schematic of our MIS model. The output signal of the BHD is divided into L measurement intervals and sampled synchronously by L parallel ADCs with the total sampling range $2R = \sum\limits_{w=1}^{L} 2R_w$. By using the MIS model, an equivalent ADC resolution of n_{eq} can be obtained, where $2^{n_{eq}} = \sum\limits_{w=1}^{L} 2^{n_w}$ and n_w is the ADC resolution of each channel. In this way, we can overcome the finite resolution limit of a single ADC.

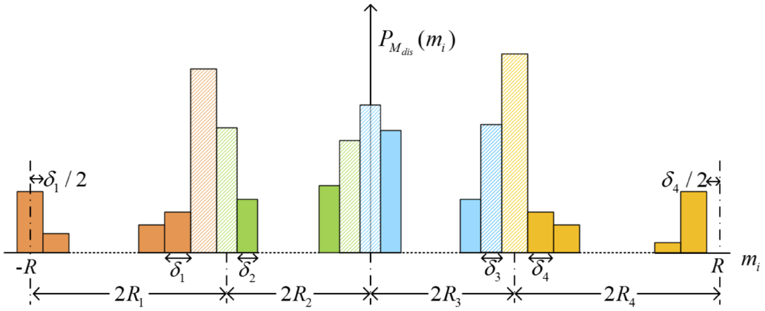

Fig. 3. The multi-interval sampling model. The output signal of the BHD is divided into L measurement ranges (In our experiment we set $L = 4$) and sampled synchronously by L parallel ADCs with the total sampling range $2R = \sum\limits_{w=1}^{L} 2R_w$. The total equivalent ADC resolution is $2^{n_{eq}} = \sum\limits_{w=1}^{L} 2^{n_w}$, where n_w is ADC resolution of each channel.

Notice that the conditional min-entropy is directly related to the conditional probability distribution function, which is associated with the PDF of the sampling signal and the sampling bin δ. According to Eq. (19), for a given QCNR and sampling range R, a larger bin width will lead to a higher conditional probability and thus a lower conditional min-entropy. To suppress the conditional min-entropy and enhance the randomness, it is desired that one has a small bin width in the high probability density region and a large bin width in the low probability density region. Such unequal bin width sampling configuration can be implemented using the MIS and is impossible using the CM where only equal bin sampling is feasible.

For MIS, the conditional probability distribution function $P^1_{M_{dis}|E}(m_i|e)$ of the measurement outcomes for the first sampling range is given by

$$P^1_{M_{dis}|E}(m_i|e) = \begin{cases} \int_{-\infty}^{-R+\delta/2} p_{M|E}(m|e)dm, & i = i^1_{\min}, \\ \int_{m^1_i-\delta/2}^{m^1_i+\delta/2} p_{M|E}(m|e)dm, & i^1_{\min}<i<i^1_{\max}, \\ 0 & i = i^1_{\max}. \end{cases} \tag{20}$$

Accordingly, the conditional probability distribution function $P^L_{M_{dis}|E}(m_i|e)$ of the measurement outcomes for the last sampling interval is

$$P^L_{M_{dis}|E}(m_i|e) = \begin{cases} 0 & i = i^L_{\min}, \\ \int_{m^L_i-\delta/2}^{m^L_i+\delta/2} p_{M|E}(m|e)dm, & i^L_{\min}<i<i^L_{\max}, \\ \int_{R-3\delta/2}^{+\infty} p_{M|E}(m|e)dm, & i = i^L_{\max}. \end{cases} \tag{21}$$

For other sampling ranges, the conditional probability distribution function can be modeled as the DBBM.

Finally, the worst-case (average) conditional min-entropy of the MIS model can be expressed as

$$\tilde{H}_{\min}(M_{dis}|E) = -\log_2[\max_{w\in[1,L]}\max_{e\in[e_{\min},e_{\max}]}\max_{m_i\in M_{dis}} P^w_{M_{dis}|E}(m_i|e)], \tag{22}$$

and

$$\bar{H}_{\min}(M_{dis}|E) = -\log_2[\int_{-\infty}^{+\infty} p_E(e)\max_{w\in[1,L]}\max_{m_i\in M_{dis}} P^w_{M_{dis}|E}(m_i|e)de]. \tag{23}$$

Based on the MIS, we calculate the conditional min-entropy when $L = 4$ and the corresponding digitization resolutions are $\{n_1 = n_2 = n_3 = n_4 = 8\}$. We have maximized the extractable min-entropy by optimizing the total sampling range R and the scale factor k of the measurement interval $R_2 = R_3 = k \times R_1 = k \times R_4$.

To illustrate the improvement of the conditional min-entropy using MIS in the worst-case scenario, we plot the conditional probability distributions of both the CM and MIS with optimized R and k in Fig. 4. The optimized worst-case conditional min-entropy is obtained when the maximum conditional probability of the right-hand boundary-bin is equal to that in the middle interval. We can see that the maximum conditional probability of the MIS (Fig. 4(c)) is smaller than that of the CM sampling of a single ADC (Figs. 4(a) and 4(b)). Notice that the optimized bin width of the measurement intervals from left to right are 0.0083, 0.0066, 0.0066, and 0.0083. This verifies that non-uniform sampling is superior to uniform sampling.

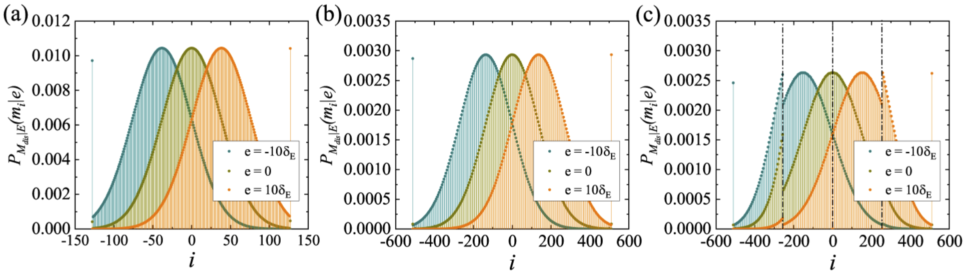

Fig. 4. The worst-case $P_{M_{dis}|E}(m|e)$ for (a) the CM ($n = 8$) and (b) the CM ($n = 10$) and (c) the MIS ($n_{eq} = 10$) with $e = \{-10\delta_E, 0, 10\delta_E\}$, QCNR = 20 dB, and optimized R. In (a), the maximum conditional probability is 0.0104 and the corresponding optimized conditional min-entropy is 6.58 (the optimized dynamical range R is 3.35). In (b), the optimized maximum conditional probability reaches 0.0104 and the maximum conditional min-entropy can be extracted is 8.41 (the optimized dynamical range R is 3.77). In (c), with the optimized total sampling range R of 3.39 and the scale factor $k = R_2/R_1$ ($R_1 = R_4, R_2 = R_3$) of 0.8, the maximum conditional probability is 0.00265 and the corresponding conditional min-entropy is 8.56, which is higher than that in the CM with a single 8 or 10-bit ADC.

Table 2 lists the simulation results of the optimized average conditional min-entropy of the CM ($n = 8$ and $n = 10$) and MIS ($n_{eq} = 10$). It shows that the optimized average conditional min-entropy of our MIS is larger than that of the CM with a single 8 or 10-bit ADC. For example, when QCNR = 20 dB, the average conditional min-entropy that can be extracted by MIS ($n_{eq} = 10$) can reach 9.11, which is higher than 6.93 by CM ($n = 8$), and about 31.46% improvement is achieved. Compared with the average conditional min-entropy in CM ($n = 10$), our MIS ($n_{eq} = 10$) also improves the average conditional min-entropy by 4.47%. Therefore, MIS not only breaks the finite resolution limit of a single ADC but also improves the robustness of QRNG against the potential attacks, and more randomness independent of classical noise can be extracted. Note that the improvement on average min-entropy by MIS decreases with QCNR.

Similar to the worst-case scenario, non-uniform sampling is beneficial to the extraction of the randomness in the average-case scenario.

Table 2. Optimized $\bar{H}_{\min}(M_{dis}|E)$ (and k, R) for n = 8-bit, 10-bit.

QCNR (dB)	MIS (n_{eq} = 10)	CM (n = 8)	Improvement	CM (n = 10)	Improvement
50	9.22 (0.57, 2.95)	7.03 (2.45)	+31.15%	8.81 (2.86)	+4.65%
20	9.11 (0.58, 3.09)	6.93 (2.59)	+31.46%	8.72 (3.01)	+4.47%
10	8.84 (0.60, 3.47)	6.72 (2.93)	+31.54%	8.52 (3.39)	+3.76%
0	8.14 (0.62, 5.13)	6.11 (4.33)	+33.22%	7.93 (4.95)	+2.65%

4. Experimental implementation and results

To verify our proposed approaches, we experimentally demonstrate the QRNG with both the DBBM and MIS (DBB + MIS). As shown in Fig. 5(a), the continuous-wave laser from a fiber-coupled laser at 1550 nm is acted as the local oscillator (LO) and injected into one port of the 50:50 fiber beam splitter (BS). The vacuum fluctuations are interfered with the LO beam and amplified, and the output beams are coupled to a fiber-based BHD and converted into random electric signals. When the LO is physically blocked, the output signal of the BHD is classical electronic noise. In contrast, it is a mixture of quantum vacuum fluctuations and classical electronics noise if the LO is active. Figure 5(b) shows the power spectral density of the electric signal with the LO active and not. To accurately estimate the QCNR of the output signal of the BHD and reduce the interference of low-frequency signals on the randomness, we select a 200 MHz sideband signal centered around 300 MHz, and the average QCNR is approximately 10 dB.

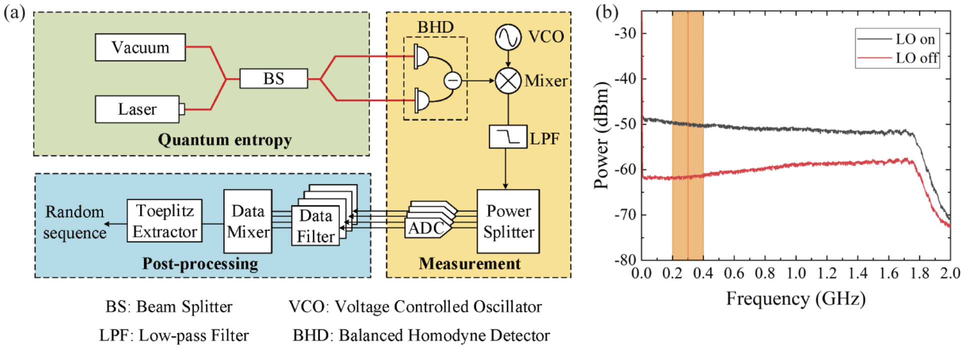

Fig. 5. (a) Schematic diagram of our QRNG based on quantum vacuum fluctuations. (b) Spectrum of the technical noise and vacuum fluctuation noise obtained from the balanced homodyne detector (BHD). The spectrum range highlighted in orange with clearance of 10 dB between the vacuum noise and technical noise is used for the generation of random numbers.

The signal generated by BHD is mixed down at 300 MHz and low pass filtered with a cutoff frequency of 100 MHz. By using a power splitter, the filtered signal is split into four output signals which are simultaneously sampled and digitalized by a multi-channel high bandwidth oscilloscope with a sampling rate of 200 MSample/s. For the given number of sampling intervals and digitization resolution in our model, the sampling range of each interval is optimized to improve the maximum conditional min-entropy.

In the data post-processing of DBB + MIS, the data from the boundary bins of each sampling interval is discarded by the data filter unit. The data output from each measurement interval does not include the position information of the sampling intervals, which will result in a data overlap problem and degradation of the randomness. To resolve this issue, a data mixer unit is constructed, which inserts two flag bits before the most significant bit of each data according to the position of the corresponding sampling interval. In this way, the data acquired from different sampling channels is identified and mixed together to generate raw data. Finally, the random bits are extracted with the Toeplitz extractor based on the conditional min-entropy [43].

In our experiment, we investigate two different digitization resolutions, $n_1 = n_2 = n_3 = n_4 = 8$ ($n_{eq} = 10$) and $n_1 = n_2 = n_3 = n_4 = 16$ ($n_{eq} = 18$). Figure 6 plots the extractable randomness independent of classical noise with equivalent conditional min-entropy for the worst-case under the confidence interval of $5\delta_E \leq |e| \leq 20\delta_E$. For comparison, the optimized worst-case conditional min-entropy for the CM is also shown [42]. As we can see from Figs. 6(a) and 6(b), the DBB + MIS method effectively improves the worst-case conditional min-entropy. For both $n = 10$ and $n = 18$, the improvements of the worst-case conditional min-entropy are more obvious at higher QCNR. We also notice that higher digitization resolution n is beneficial to the extractable secure randomness.

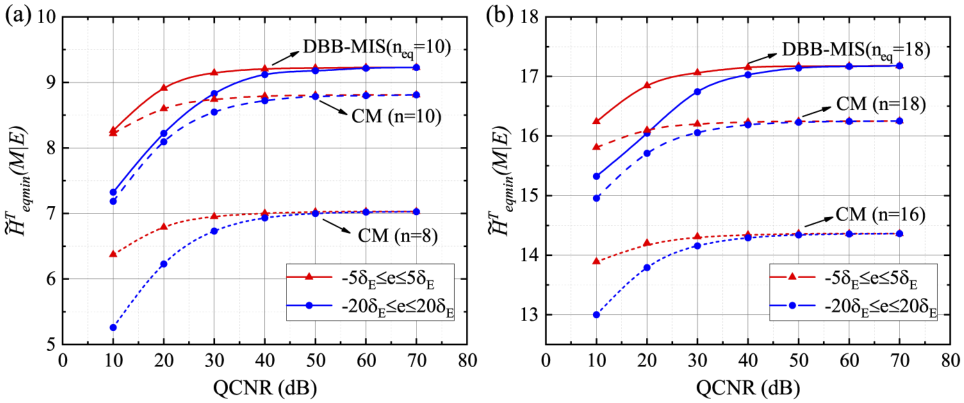

Fig. 6. The extractable secure randomness of CM and DBB + MIS as a function of QCNR for (a) 10-bit measurement and (b) 18-bit measurements in the worst-case under the confidence interval of $5\delta_E \leq |e| \leq 20\delta_E$.

Figure 7 depicts the extractable randomness independent of classical noise with equivalent conditional min-entropy for the average-case. We find that there exist upper bounds for the extractable secure randomness in both the average-case and worst-case at a high QRNG regime, and the two bounds are approximately equal when QCNR→ ∞. Compared with the CM for $n = 8$ ($n = 16$), the upper bound of the conditional min-entropy of the DBB + MIS for $n_{eq} = 10$ ($n_{eq} = 18$) increases approximately by 31.30% (19.62%). For the same digitization resolution , the DBB + MIS method can still achieve improvement of 4.77% for $n = 10$ and 5.71% for $n = 18$, respectively. The final random bit generation rate in our experiment can reach 3.2 Gbits/s with $n_{eq} = 18$ and QCNR = 10 dB.

To evaluate the randomness of the extracted bit sequence from our QRNG, we calculate the autocorrelation coefficients using a typical record of 5×10^7 bits. As shown in Fig. 8, both the average-case and worst-case are plotted for 10-bit ADC and QCNR of 10 dB, and the confidence interval of classical noise is $-5\delta_E \leq e \leq 5\delta_E$. The low autocorrelation coefficients indicate the extracted bitstream from our QRNG has a good randomness and is close to independent and identically distributed.

To further verify the randomness, we employ the NIST SP 800-22 suite [47] for data's statistical tests. The total amount of extracted random numbers used for the test is 1 Gbits. As shown

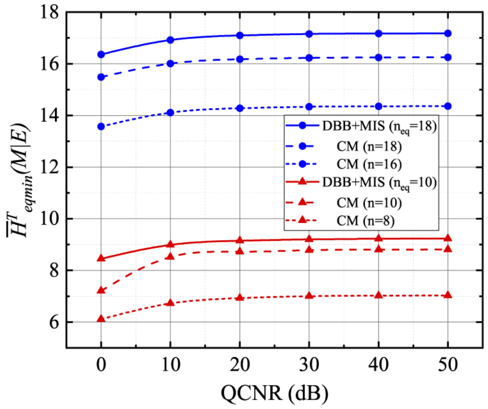

Fig. 7. The extractable secure randomness of CM and DBB + MIS in the average-case.

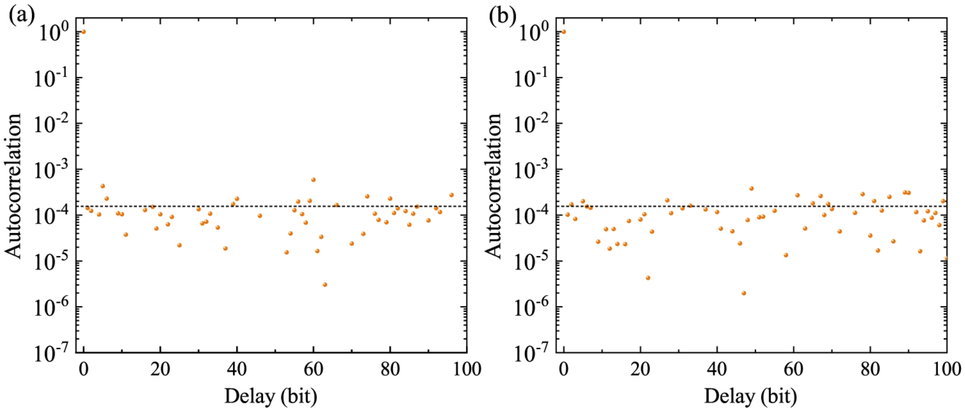

Fig. 8. Autocorrelation coefficients calculated from 5×10^7 extracted random bits for (a) the average-case and (b) the worst-case when QCNR = 10 dB and $-5\delta_E \leq e \leq 5\delta_E$. The theoretical standard deviation of the autocorrelation for truly random 5×10^7 bits is shown as dashed lines.

in Fig. 9, the test results show that the NIST statistical test suite is passed successfully, which indicates that the generated random sequence has a good statistical characteristic.

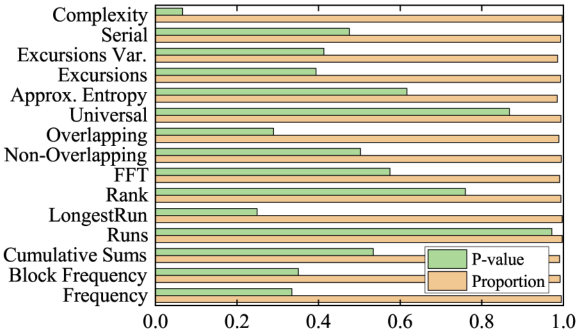

Fig. 9. The NIST test results.

5. Conclusion

In this work, we propose two novel approaches to improve the extractable randomness in a vacuum fluctuations based QRNG independent of classical noise in the worst-case and average-case scenarios. By discarding the boundary bins after discretization of vacuum fluctuations, we suppress the influence of the conditional probability of the boundary bins on the conditional min-entropy and enhance the randomness of the output sequence. It is a challenge to operate an ADC at both high speed and high resolution. We release the bottleneck of the finite resolution limit of a single ADC by adopting a multi-interval sampling. Combine with an unequal-bins-sampling, the conditional probability distributions of different sampling intervals are well balanced. We show that unequal-bins-sampling can provide more randomness independent of classical noise than the equal-bins-sampling. Finally, we apply the above two approaches to quantum vacuum fluctuations based random number generators. The secure random bits generation rate of our QRNG can reach 3.2 Gbits/s. Compared with the previous QRNGs based on a homodyne measurement of vacuum state, our methods can extract more secure randomness from the output signal of the balanced homodyne detector.

For further study, it will be interesting to apply the proposed protocol to other kinds of QRNGs, such as the Source-DI QRNGs introduced in Ref. [38], where the bound to the conditional min-entropy of the random numbers is determined by the resolution of the trusted measurement apparatus.

Funding. Key Research and Development Program of Guangdong Province (2020B0303040002); Key Research and Development Projects of Shanxi Province (201803D121065); Shanxi 1331KSC; National Key Research and Development Program of China (2016YFA0301403); National Natural Science Foundation of China (11774209).

Disclosures. The authors declare that there are no conflicts of interest related to this article.

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, B. Qi, and Z. Zhang, "Quantum random number generation," npj Quantum Inf. **2**(1), 16021 (2016).
3. N. Wang, S. Du, W. Liu, X. Wang, Y. Li, and K. Peng, "Long-distance continuous-variable quantum key distribution with entangled states," Phys. Rev. Appl. **10**(6), 064028 (2018).
4. E. Diamanti, H.-K. Lo, B. Qi, and Z. Yuan, "Practical challenges in quantum key distribution," npj Quantum Inf. **2**(1), 16025 (2016).
5. F. Xu, X. Ma, Q. Zhang, H.-K. Lo, and J.-W. Pan, "Secure quantum key distribution with realistic devices," Rev. Mod. Phys. **92**(2), 025002 (2020).
6. 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**(15), 150502 (2018).
7. S. Pirandola, U. L. Andersen, L. Banchi, M. Berta, D. Bunandar, R. Colbeck, D. Englund, T. Gehring, C. Lupo, C. Ottaviani, J. L. Pereira, M. Razavi, J. S. Shaari, M. Tomamichel, V. C. Usenko, G. Vallone, P. Villoresi, and P. Wallden, "Advances in quantum cryptography," Adv. Opt. Photonics **12**(4), 1012–1236 (2020).
8. H. Li, Z. Yin, S. Wang, Y. Qian, W. Chen, G. Guo, and Z. Han, "Randomness determines practical security of BB84 quantum key distribution," Sci. Rep. **5**(1), 16200 (2015).
9. P. Z. Wieczorek and K. Gołofit, "True random number generator based on flip-flop resolve time instability boosted by random chaotic source," IEEE Trans. Circuits Syst. I **65**(4), 1279–1292 (2018).
10. M. Bucci and R. Luzzi, "Fully digital random bit generators for cryptographic applications," IEEE Trans. Circuits Syst. I **55**(3), 861–875 (2008).
11. B. Xu, Z. Chen, Z. Li, J. Yang, Q. Su, W. Huang, Y. Zhang, and H. Guo, "High speed continuous variable source-independent quantum random number generation," Quantum Sci. Technol. **4**(2), 025013 (2019).
12. M. Fiorentino, C. Santori, S. M. Spillane, R. G. Beausoleil, and W. J. Munro, "Secure self-calibrating quantum random-bit generator," Phys. Rev. A **75**(3), 032334 (2007).
13. Q. Zhang, X. Deng, C. Tian, and X. Su, "Quantum random number generator based on twin beams," Opt. Lett. **42**(5), 895–898 (2017).
14. C. S. Calude, M. J. Dinneen, M. Dumitrescu, and K. Svozil, "Experimental evidence of quantum randomness incomputability," Phys. Rev. A **82**(2), 022102 (2010).
15. C. Gabriel, C. Wittmann, D. Sych, R. Dong, W. Mauerer, U. L. Andersen, C. Marquardt, and G. Leuchs, "A generator for unique quantum random numbers based on vacuum states," Nat. Photonics **4**(10), 711–715 (2010).

16. Z. Zheng, Y. Zhang, M. Huang, Z. Chen, S. Yu, and H. Guo, “Bias-free source-independent quantum random number generator,” Opt. Express **28**(15), 22388–22398 (2020).
17. Y. Shi, B. Chng, and C. Kurtsiefer, “Random numbers from vacuum fluctuations,” Appl. Phys. Lett. **109**(4), 041101 (2016).
18. D. G. Marangon, G. Vallone, and P. Villoresi, “Source-device-independent ultrafast quantum random number generation,” Phys. Rev. Lett. **118**(6), 060503 (2017).
19. F. Xu, B. Qi, X. Ma, H. Xu, H. Zheng, and H.-K. Lo, “Ultrafast quantum random number generation based on quantum phase fluctuations,” Opt. Express **20**(11), 12366–12377 (2012).
20. C. Abellán, W. Amaya, M. Jofre, M. Curty, A. Acín, J. Capmany, V. Pruneri, and M. W. Mitchell, “Ultra-fast quantum randomness generation by accelerated phase diffusion in a pulsed laser diode,” Opt. Express **22**(2), 1645–1654 (2014).
21. 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**(24), 27475–27481 (2016).
22. 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**(24), 29350–29357 (2013).
23. Y. Nie, H. Zhang, Z. Zhang, J. Wang, X. Ma, J. Zhang, and J. Pan, “Practical and fast quantum random number generation based on photon arrival time relative to external reference,” Appl. Phys. Lett. **104**(5), 051110 (2014).
24. M. Wahl, M. Leifgen, M. Berlin, T. Röhlicke, H.-J. Rahn, and O. Benson, “An ultrafast quantum random number generator with provably bounded output bias based on photon arrival time measurements,” Appl. Phys. Lett. **98**(17), 171105 (2011).
25. L. Nguyen, P. Rehain, Y. M. Sua, and Y.-P. Huang, “Programmable quantum random number generator without postprocessing,” Opt. Lett. **43**(4), 631–634 (2018).
26. P. Bierhorst, E. Knill, S. Glancy, Y. Zhang, A. Mink, S. Jordan, A. Rommal, Y.-K. Liu, B. Christensen, S. W. Nam, M. J. Stevens, and L. K. Shalm, “Experimentally generated randomness certified by the impossibility of superluminal signals,” Nature **556**(7700), 223–226 (2018).
27. T. Jennewein, U. Achleitner, G. Weihs, H. Weinfurter, and A. Zeilinger, “A fast and compact quantum random number generator,” Rev. Sci. Instrum. **71**(4), 1675–1680 (2000).
28. M. R. Coleman, K. G. Ingalls, J. T. Kavulich, S. J. Kemmerly, N. C. Salinas, E. V. Ramirez, and M. Schlosshauer, “Parity-based, bias-free optical quantum random number generation with min-entropy estimation,” J. Opt. Soc. Am. B **37**(7), 2088–2094 (2020).
29. H. Fürst, H. Weier, S. Nauerth, D. G. Marangon, C. Kurtsiefer, and H. Weinfurter, “High speed optical quantum random number generation,” Opt. Express **18**(12), 13029–13037 (2010).
30. T. Lunghi, J. B. Brask, C. C. W. Lim, Q. Lavigne, J. Bowles, A. Martin, H. Zbinden, and N. Brunner, “Self-testing quantum random number generator,” Phys. Rev. Lett. **114**(15), 150501 (2015).
31. Y. Liu, X. Yuan, M. Li, W. Zhang, Q. Zhao, J. Zhong, Y. Cao, Y. Li, L. Chen, H. Li, T. Peng, Y. Chen, C. Peng, S. Shi, Z. Wang, L. You, X. Ma, J. Fan, Q. Zhang, and J. Pan, “High-speed device-independent quantum random number generation without a detection loophole,” Phys. Rev. Lett. **120**(1), 010503 (2018).
32. P. R. Smith, D. G. Marangon, M. Lucamarini, Z. L. Yuan, and A. J. Shields, “Simple source device-independent continuous-variable quantum random number generator,” Phys. Rev. A **99**(6), 062326 (2019).
33. B. G. Christensen, K. T. McCusker, J. B. Altepeter, B. Calkins, T. Gerrits, A. E. Lita, A. Miller, L. K. Shalm, Y. Zhang, S. W. Nam, N. Brunner, C. C. Lim, N. Gisin, and P. G. Kwiat, “Detection-loophole-free test of quantum nonlocality, and applications,” Phys. Rev. Lett. **111**(13), 130406 (2013).
34. Z. Cao, H. Zhou, X. Yuan, and X. Ma, “Source-independent quantum random number generation,” Phys. Rev. X **6**(1), 011020 (2016).
35. P. Mironowicz, G. Cañas, J. Cariñe, E. S. Gómez, J. F. Barra, A. Cabello, G. B. Xavier, G. Lima, and M. Pawłowski, “Quantum randomness protected against detection loophole attacks,” Quantum Inf. Process. **20**(1), 39 (2021).
36. J. B. Brask, A. Martin, W. Esposito, R. Houlmann, J. Bowles, H. Zbinden, and N. Brunner, “Megahertz-rate semi-device-independent quantum random number generators based on unambiguous state discrimination,” Phys. Rev. Appl. **7**(5), 054018 (2017).
37. D. Rusca, T. van Himbeeck, A. Martin, J. B. Brask, W. Shi, S. Pironio, N. Brunner, and H. Zbinden, “Self-testing quantum random-number generator based on an energy bound,” Phys. Rev. A **100**(6), 062338 (2019).
38. 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**(1), 5365 (2018).
39. F. Xu, J. H. Shapiro, and F. N. C. Wong, “Experimental fast quantum random number generation using high-dimensional entanglement with entropy monitoring,” Optica **3**(11), 1266–1269 (2016).
40. 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**(3), 034017 (2019).
41. Y. Shen, L. Tian, and H. Zou, “Practical quantum random number generator based on measuring the shot noise of vacuum states,” Phys. Rev. A **81**(6), 063814 (2010).
42. J. Y. Haw, S. M. Assad, A. M. Lance, N. H. Y. Ng, V. Sharma, P. K. Lam, and T. Symul, “Maximization of extractable randomness in a quantum random-number generator,” Phys. Rev. Appl. **3**(5), 054004 (2015).

43. X. Ma, F. Xu, H. Xu, X. Tan, B. Qi, and H.-K. Lo, "Postprocessing for quantum random-number generators: Entropy evaluation and randomness extraction," Phys. Rev. A **87**(6), 062327 (2013).
44. W. Huang, Y. 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**(1), 012422 (2020).
45. R. Konig, R. Renner, and C. Schaffner, "The operational meaning of min- and max-entropy," IEEE Trans. Inf. Theory **55**(9), 4337–4347 (2009).
46. M. Tomamichel, C. Schaffner, A. Smith, and R. Renner, "Leftover hashing against quantum side information," IEEE Trans. Inf. Theory **57**(8), 5524–5535 (2011).
47. E. Barker and J. Kelsey, "Recommendation for the entropy sources used for random bit generation," NIST Draft Special Publication 800-90B, second draft (2016).