Extracting More Quantum Randomness With Non-Uniform Quantization

Bai-Xiang Ji, Jian Li, and Qin Wang

***Abstract*—Random numbers generated via quantum process is indeterministic, which are of essential to the cryptographic communication and the large-scale computer modeling. However, in realistic scenarios, classical noises can inevitably contaminate the raw sequences of a quantum randomness number generator (QRNG), and then compromise the security of the QRNG. Min-entropy is a useful approach that can quantify the randomness independent of side-information. To enhance the extractable randomness of the raw sequences arising from the QRNG, we propose a new method which exploits non-uniform quantization methods instead of uniform sampling methods and effectively enhances the extractable randomness from the QRNG at a high quantum-to-classical-noise ratio (QCNR). Given a QCNR as 50 dB and a 16-bit analog-to-digital converter (ADC), the worst-case conditional min-entropy of the non-uniform quantization scheme is improved by nearly 11% compared with that of the uniform sampling scheme.**

***Index Terms*—Quantum random-number generation, Min-entropy.**

I. Introduction

RANDOM numbers are of importance for a wide range of applications in scientific and commercial fields [1], such as numerical simulations, lottery games and cryptography. The requirement for true and unique randomness in these applications has triggered several proposals for generating random numbers which must be genuinely unpredictable and sufficiently secure [2], [3], [4].

Pseudo random number generators (PRNGs) based on the computational algorithms, have been widely used in modern information systems. However, by reason of the deterministic and predictable features of these algorithms, PRNGs can not be applied in some applications where true randomness is required. Different from the PRNG, true random number generators (TRNGs) extract randomness from physical random process [5]. As an important type of TRNGs, the QRNG [26] is based on the intrinsic randomness of fundamental quantum processes including quantum phase fluctuations [6], [7], [8], [9], [10], photon arrival times [11], [12], [13], stimulated Raman scattering [14], vacuum fluctuations [11], [15], spontaneous emission noise [16], [17], [18] and photon polarization state [19], [20].

A typical QRNG is composed of three components: quantum entropy source, measurement of quantum states, and extraction of random numbers. QRNGs can be mainly divided into two categories according to the quantum entropy source used: discrete variable (DV) QRNGs and continuous variable (CV) QRNGs. Compared with the DV QRNG, the CV QRNG is characterized by high generation rates because of the use of fast photodiodes instead of (slow) single photon detectors. To obtain true randomness independent of classical noises from a practical QRNG, the implementation of the QRNG should be properly modeled. Ma et al. proposed a framework for evaluating the quantum randomness with the min-entropy [21]. Haw et al. presented an approach to maximize the conditional min-entropy when being given a QCNR [22].

In the conventional measurement model where the extractable randomness is quantified by the min-entropy, and the ADC is used to uniformly sample the output signal of the detector. However, the extractable randomness of a single sample is relatively small and the performance utilization of the ADC is insufficient under some circumstances.

In this work, we proposed a new method to enhance the extractable randomness in a QRNG based on quantum vacuum fluctuations. By using non-uniform quantization methods instead of uniform sampling methods, when being given a high QCNR, 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.

II. Randomness and Conditional Min-Entropy

For the QRNG in Ref. [28], a homodyne measurement of the vacuum state is performed. This measures X, the quadrature values of the vacuum state. The theory of quantum mechanics states that these values are random. The min-entropy of variable X with a distribution $P_X(x_i)$, in unit of bits, is given by [23]

$$H_{\min}(X) = -\log_2 \left[\max_{x_i \in X} P_X\left(x_i\right) \right], \tag{1}$$

Manuscript received 24 July 2022; accepted 12 August 2022. Date of publication 17 August 2022; date of current version 25 August 2022. This work was supported in part by the National Key R&D Program of China under Grants 2018YFA0306400 and 2017YFA0304100, in part by the National Natural Science Foundation of China under Grants 12074194 and U19A2075, in part by the Leading-edge technology Program of Jiangsu Natural Science Foundation under Grant BK20192001, and in part by Industrial Prospect and Key Core Technology Projects of Jiangsu provincial key R & D Program under Grant BE2022071. *(Bai-Xiang Ji and Jian Li contributed equally to this work.) (Corresponding author: Qin Wang.)*

The authors are with the Institute of Quantum Information and Technology, Broadband Wireless Communication and Senser Network Technology Key Lab of Ministry of Education, Telecommunication and Networks National Engineering Research Center, Nanjing University of Posts and Telecommunications, Nanjing 210003, China (e-mail: 1715549917@qq.com; jianli@njupt.edu.cn; qinw@njupt.edu.cn).

Digital Object Identifier 10.1109/JPHOT.2022.3199376

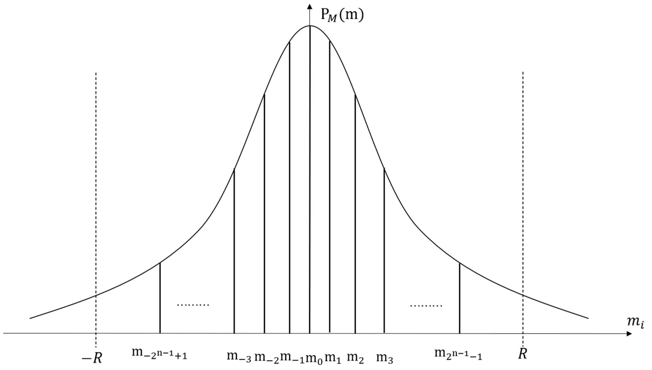

Fig. 1. The schematic diagram of the non-uniform quantization. The probability distribution of the output signal of the homodyne detector is binned into 2^n equal parts (the same area per bin).

which is widely used to quantify the randomness and related to the maximum guessing probability of an adversary on variable X.

In practical QRNGs, the conditional min-entropy which depends on the specific attacks that how the adversary interacts with the classical side-information can be used to evaluate the randomness of the entropy source. We make an assumption on the adversary that she has no restriction on computational power and fully knows the classical noise with arbitrary precision. Only the attack in the worst-case scenario is considered hereafter. In this case, the adversary can fully control the classical noise to maximize her capability to predict random sequences. The maximum conditional probability is used to evaluate the amount of information she successfully captured. The worst-case conditional min-entropy of random sequences conditioned on the classical side-information is defined by [24]

$$H_{\min}(X \mid E) = -\log_2 \left[\max_{e_j \in [e_{\min}, e_{\max}]} \max_{x_i \in X} P_{X|E}\left(x_i \mid e_j\right) \right]. \tag{2}$$

where $e_{\min}$ and $e_{\max}$ are the minimum and maximum values that the classical noise can take, respectively.

According to (2), we can know that extractable secure randomness is limited by the worst-case conditional min-entropy, which is directly associated with the maximum guessing probability of an adversary conditioned on the classical noise. A smaller maximum conditional probability implies a lower amount of an adversary's knowledge on random sequences and more secure randomness that can be extracted. When the entropy source is given, the guessing probability of an adversary is strongly dependent on the measurement model, as we will demonstrate in the following part.

For the QRNG which is based on vacuum fluctuations, the output signal M of the homodyne detector consists of vacuum fluctuations noise Q and classical electronic noise E [25]. The theory of quantum mechanics states that the values of Q are random and have a probability density function (PDF) P_Q which follows a Gaussian distribution and is centered at zero with variance σ_Q^2. Practically, these values can't be measured in complete separation from the classical noise E. The PDF of the classical noise E is then denoted by P_E. An assumption is made that the classical noise follows a Gaussian distribution centered at zero with variance σ_E^2. Then the QCNR is defined as $QCNR = 10\log_{10}(\sigma_Q^2/\sigma_E^2)$ dB.

The PDF of vacuum fluctuations Q and the classical noise E are given by [22]

$$P_Q(q) = \frac{1}{\sqrt{2\pi}\sigma_Q} \exp\left(-\frac{q^2}{2\sigma_Q^2}\right),$$

$$P_E(e) = \frac{1}{\sqrt{2\pi}\sigma_E} \exp\left(-\frac{e^2}{2\sigma_E^2}\right). \tag{3}$$

By convolving P_Q and P_E, the PDF of the measurements M can be expressed as

$$\begin{aligned} P_M(m) &= \frac{1}{\sqrt{2\pi}\sigma_M} \exp\left(-\frac{m^2}{2\sigma_M^2}\right) \\ &= \frac{1}{\sqrt{2\pi\left(\sigma_Q^2+\sigma_E^2\right)}} \exp\left(-\frac{m^2}{2\left(\sigma_Q^2+\sigma_E^2\right)}\right). \end{aligned} \tag{4}$$

Then the PDF of the measurements M conditioned on the classical noise E is

$$\begin{aligned} P_{M|E}(m \mid e) &= \frac{1}{\sqrt{2\pi\left(\sigma_M^2-\sigma_E^2\right)}} \exp\left(-\frac{(m-e)^2}{2\left(\sigma_M^2-\sigma_E^2\right)}\right) \\ &= \frac{1}{\sqrt{2\pi}\sigma_Q} \exp\left(-\frac{(m-e)^2}{2\sigma_Q^2}\right). \end{aligned} \tag{5}$$

Hereafter the quantum noise is used to normalize all the relevant quantities, $\sigma_Q^2 = 1$. The output signal of the homodyne detector is sampled by an n-bit ADC with dynamical range $[-R+\delta/2, R-3\delta/2]$ where the R represents the sampling boundary of the ADC. Upon measurement, the sampled signal is discretized into 2^n bins with bin width $\delta = R/2^{n-1}$. The conditional probability distribution of measurements M conditioned on the classical noise E can be expressed as [22]

$$\begin{aligned} &P_{M_{\text{dis}}|E}\left(m_i \mid e\right) \\ &= \begin{cases} \int_{-\infty}^{-R+\delta/2} p_{M|E}(m \mid e)\mathrm{d}m, & i = i_{\min}, \\ \int_{m_i-\delta/2}^{m_i+\delta/2} p_{M|E}(m \mid e)\mathrm{d}m, & i_{\min} < i < i_{\max}, \\ \int_{R-3\delta/2}^{\infty} p_{M|E}(m \mid e)\mathrm{d}m, & i = i_{\max}. \end{cases} \end{aligned} \tag{6}$$

where the i are integers $\in \{-2^{n-1}, \ldots, 2^{n-1}-1\}$.

By combining (2) with (6), the worst-case conditional min-entropy is given by

$$H_{\min}(X \mid E) = -\log_2\left[\max\left(p_1, p_2\right)\right], \tag{7}$$

where p_1 represents the maximum conditional probability of the boundary bins $(i = i_{\min}, i_{\max})$ and p_2 denotes the maximum conditional probability within the sampling range $(i_{min} < i < i_{max})$. According to (7) and given the QCNR, it can be easily found that p_1 and p_2 are two key factors that the maximum conditional min-entropy depends on [22]. In addition to this, the classical noise e in (2) should be limited for practical purposes in the worst-case scenario. When the value range of the variable e is limited in $[-5\sigma_E, 5\sigma_E]$, it is valid for 99.9999%

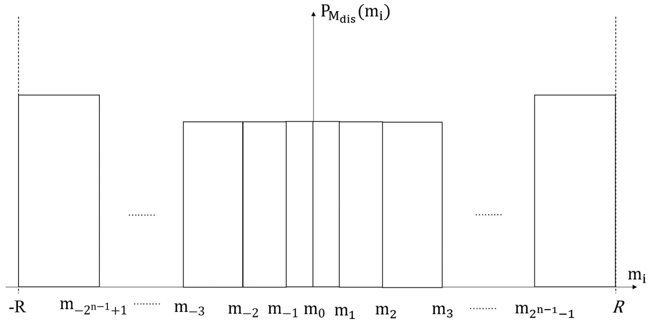

Fig. 2. The non-uniform quantization model. The output signal of the homodyne detector is discretized into 2^n sampling bins by a non-uniform quantizer with 2^n quantization intervals and dynamical range $[-\mathrm{R}, \mathrm{R}]$. The bin width δ_i changes dynamically satisfying $\delta_i = \mathrm{m_i} - \mathrm{m_{i-1}}$ and the right boundary of the i-th is $\mathrm{m_i}$ where $\mathrm{i_{min}} = -2^{\mathrm{n}-1} + 1$ and $\mathrm{i_{max}} = 2^{\mathrm{n}-1}$.

of the time and sufficient for the practical scenario. Hereafter, the range $[-5\sigma_E, 5\sigma_E]$ is chosen as the smallest confidence interval of the classical noise e. The dynamic ADC range R can be optimized to maximize the worst-case conditional min-entropy, which is obtained when $p_1 = p_2$.

III. Non-Uniform Sampling Model

In this part, we introduce a modified model of entropy quantification for a practical QRNG. We will show that the proposed model using non-uniform quantization methods effectively enhances the extractable randomness from the entropy source compared with the conventional model of entropy quantification using uniform sampling methods.

From previous part, we can know that the maximum conditional min-entropy depends on the maximum conditional probability of the boundary bin p_1 and within the sampling range p_2. In the uniform sampling scheme, the first bin $i = i_{\text{min}}$ and the last bin $i = i_{\text{max}}$ of an ADC respectively cover the input signal in a range of $[-\infty, -R + \delta/2]$ and $[R - 3\delta/2, \infty]$. In the non-uniform quantization scheme, we use non-uniform quantization methods instead of uniform sampling methods. The sampling is performed with a non-uniform quantizer as shown in Fig 5(a) with dynamical range $[-R, R]$. Upon measurement, the sampled signal is discretized into 2^n bins with a dynamical bin width δ_i. The dynamical bin width δ_i is chosen to make sure that the maximum conditional probability of each bin expressed as $P_i = 1/2[\text{erf}(m_i/\sqrt{2}\sigma_M) - \text{erf}(m_{i-1}/\sqrt{2}\sigma_M)]$ is equal. The schematic of the non-uniform quantization is depicted in Fig 2 and m_i represents the right boundary of the i-th bin where the $i \in \{-2^{n-1} + 1, \ldots, 2^{n-1}\}$. The value of m_0 is set to zero and the relationship between m_i can be expressed as

$$\text{erf}\left(\frac{m_i}{\sqrt{2}\sigma_M}\right) - \text{erf}\left(\frac{m_{i-1}}{\sqrt{2}\sigma_M}\right) = \frac{\text{erf}\left(\frac{R}{\sqrt{2}\sigma_M}\right)}{2^{n-1}}, \tag{8}$$

where $\text{erf}(x) = 2/\sqrt{\pi}\int_0^x e^{-t^2}dt$ is the error function. According to (8), we can know that the dynamical bin width δ_i of the i-th bin is determined by m_i and m_{i-1}. In the non-uniform quantization scheme, the first bin $i = i_{\text{min}}$ and the last bin $i = i_{\text{max}}$ of a non-uniform quantizer respectively cover the input signal in a range of $[-\infty, -R]$ and $[R, \infty]$. The maximum conditional probability in the non-uniform quantization scheme will be lower than it in the uniform sampling scheme, which means a higher conditional min-entropy. The basic reason is the maximum entropy principle where for a discrete source with q symbols, the entropy of the source reaches its maximum value when the probability of each symbol is equal.

Based on the non-uniform quantization, the conditional probability of measurements M_{dis} on the classical noise E can be expressed by

$$\begin{aligned} &P_{M_{\text{dis}}|E}(m_i \mid e) \\ &= \begin{cases} \int_{-\infty}^{m_i} p_{M|E}(m \mid e)\text{d}m, & i = i_{\text{min}}, \\ \int_{m_{i-1}}^{m_i} p_{M|E}(m \mid e)\text{d}m, & i_{\text{min}} < i < i_{\text{max}}, \\ \int_{m_i-1}^{\infty} p_{M|E}(m \mid e)\text{d}m, & i = i_{\text{max}}. \end{cases} \end{aligned} \tag{9}$$

From Fig 2, the maximum conditional probability distribution can be rewritten as

$$\begin{aligned} &\max_{m_i \in M_{dis}} P_{M_{dis}|E}(m_i \mid e) \\ &= \max\left\{P_{M_{dis}|E}(m_{i_{\text{min}}} \mid e), P_{M_{dis}|E}(m_{i_{\text{max}}} \mid e)\right\}. \end{aligned} \tag{10}$$

Given a bound of the classical noise e as $[e_{\text{min}}, e_{\text{max}}]$, which can be fully controlled by an adversary, (10) can be rewritten as

$$\begin{aligned} &\max_{e\epsilon[e_{\text{min}}, e_{\text{max}}]} \max_{m_i \in M_{\text{dis}}} P_{M_{dis}|E}(m_i \mid e) \\ &= \max\Bigg\{\max_{e\epsilon[e_{\text{min}}, e_{\text{max}}]} \max_{m_i \in M_{dis}} P_{M_{dis}|E}(m_{i_{\text{min}}} \mid e), \\ &\max_{e\epsilon[e_{\text{min}}, e_{\text{max}}]} \max_{m_i \in M_{dis}} P_{M_{dis}|E}(m_{i_{\text{max}}} \mid e)\Bigg\}. \end{aligned} \tag{11}$$

Combine (2) and (11), the worst-case conditional min-entropy can be expressed as

$$\begin{aligned} &H_{\text{min}}(M_{dis} \mid E) \\ &= -\log_2\left[\max_{e\epsilon[e_{\text{min}}, e_{\text{max}}]} \max_{m_i \in M_{\text{dis}}} P_{M_{dis}|E}(m_i \mid e)\right]. \end{aligned} \tag{12}$$

From (12), the worst-case conditional min-entropy of the non-uniform quantization scheme can be calculated. In Fig 3, we plot the worst-case conditional min-entropy with optimized R for the conventional measurement model using uniform sampling methods (Fig 3(a)) and the worst-case conditional min-entropy with R=5 for the non-uniform quantization scheme (Fig 3(b)). In the non-uniform quantization scheme, all the input signals outside [-R, R] will be accumulated in the first and last bins, with the increment of R, the effect of the input signals outside [-R, R] on the first and last bins is reduced. Considering that when R=5, the probability of the out-of-bounds input signals is only 5.7330×10^{-7} which can be almost ignored, then we reasonably choose R=5 in the following numerical simulations. Both Fig 3(a) and Fig 3(b) show that the worst-case conditional min-entropy will be enhanced accordingly with the increase in the resolution and the QCNR. Compared Fig 3(a) with Fig 3(b), when n is 16 b and QCNR respectively takes 10 dB, 20 dB, 30 dB, 40 dB, 50 dB, the worst-case conditional min-entropy for the uniform sampling scheme is 13.86 b, 13.92 b, 14.29 b, 14.34 b and 14.17 b accordingly and the worst-case conditional

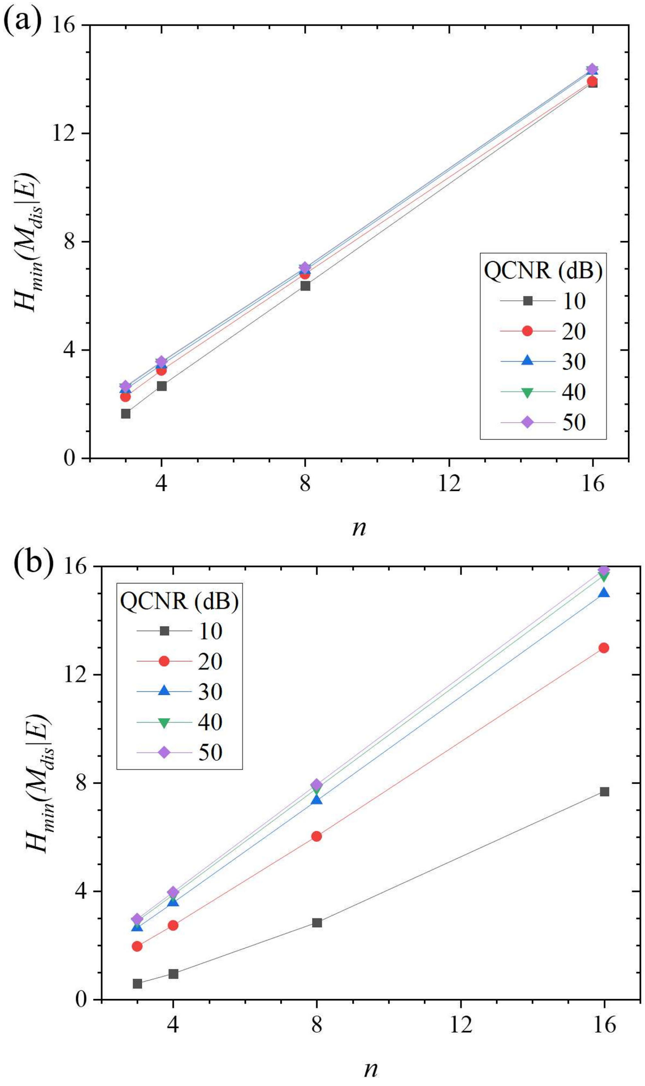

Fig. 3. The worst-case conditional min-entropy $H_{\min}(M_{dis} \mid E)$ with the resolution n for (a) the uniform sampling scheme and (b) the non-uniform quantization scheme. The parameters are $\text{QCNR} = \{10\,\text{dB}, 20\,\text{dB}, 30\,\text{dB}, 40\,\text{dB}, 50\,\text{dB}\}$, where we optimize R in the uniform sampling scheme, and reasonably set $R = 5$ in the non-uniform quantization scheme.

min-entropy for the non-uniform quantization scheme is 7.68 b, 12.98 b, 14.99 b, 15.66 b, 15.87 b correspondingly. We can find that the worst-case conditional min-entropy for the non-uniform quantization scheme changes more significantly than that for the uniform sampling scheme in the case where n is the same value but the QCNR is different. As shown in Fig 4, we take the resolution n as 4 b, 8 b and 16 b respectively. It can be seen in the Fig 4(a), Fig 4(b) and Fig 4(c), when the QCNR is relatively low, the worst-case conditional min-entropy for the uniform sampling scheme is higher than that for the non-uniform quantization scheme. However, as the QCNR continues to increase, finally at 30 dB, the worst-case conditional min-entropy for the non-uniform quantization scheme begins to outpace that for the uniform sampling scheme. With further increase of the QCNR,

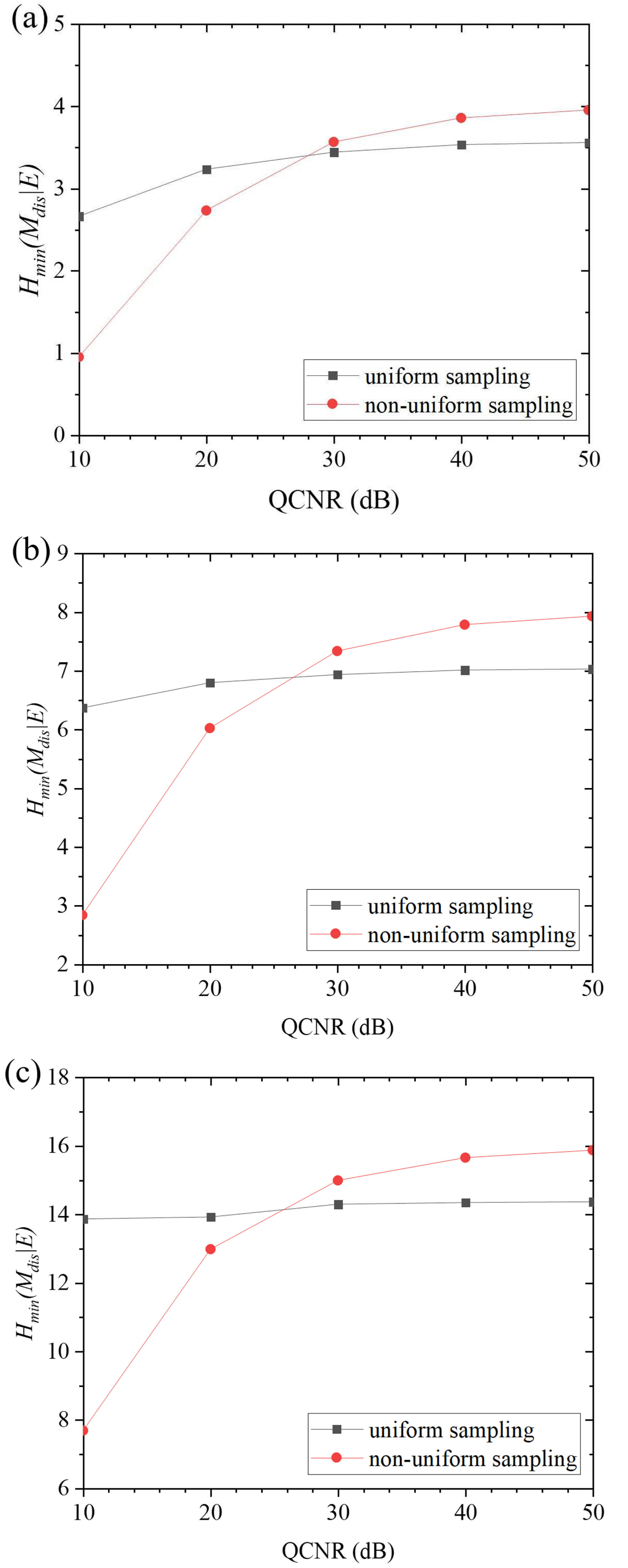

Fig. 4. The worst-case conditional min-entropy $H_{\min}(M_{dis} \mid E)$ under different QCNRs for (a) $\text{n} = 4$ b, (b) $\text{n} = 8$ b and (c) $\text{n} = 16$ b. The parameters are $\text{n} = \{4\,\text{bit}, 8\,\text{bit}, 16\,\text{bit}\}$, where we optimize R in the uniform sampling scheme, and reasonably set $R = 5$ in the non-uniform quantization scheme.

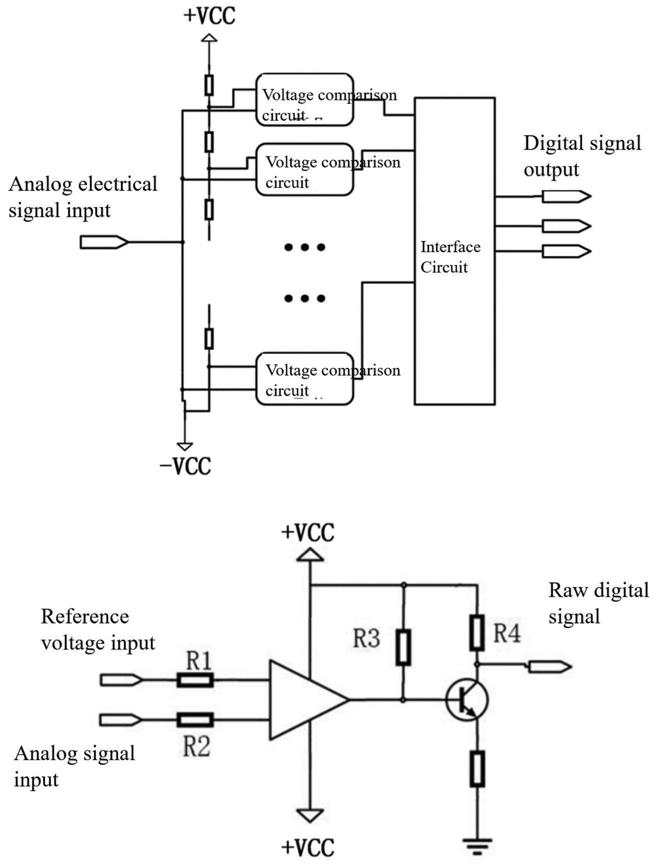

Fig. 5. (a) The non-uniform quantizer and (b) the single-limit comparator circuit. The non-uniform quantizer is mainly composed of a multi-channel single-limit comparator circuits.

the worst-case conditional min-entropy for the non-uniform quantization scheme is expected to reach maximum entropy which is the entropy of the random sequence exactly following a uniform distribution. As a result, we can conclude that at a high QCNR, more secure randomness can be extracted from the QRNG in the non-uniform quantization scheme compared with that in the uniform sampling scheme.

Fig 5(a) shows the structure of the non-uniform quantizer. As shown in the figure, the non-uniform quantizer is mainly composed of a multi-channel single-limit comparator circuit composed of n-channel voltage comparators. The structure of the single-channel single-limit voltage comparison circuit is shown in Fig 5(b). The non-uniform quantizer includes N voltage comparators and N+1 divider resistors, where N is greater than or equal to 1. The original analog electrical signal output of the homodyne detector is connected to the noninverting input of each voltage comparator as the signal to be measured. After N+1 voltage divider resistors are connected in series, the power supply +Vcc and -Vcc are connected at both ends, respectively. Then, the power supply voltage is divided into N + 1 voltage intervals, resulting in the reference voltage of N quantization intervals, and the voltage intervals are unevenly distributed. A divider resistor is connected to the inverting input of each voltage comparator, and the reference voltage of N quantization intervals is used as the threshold voltage of N voltage comparators. Among them, the resistors R1 and R2 are connected to the two inputs of the comparator as current-limiting resistors, the output termination of the comparator circuit is connected to the pull-up resistor R3 to stabilize the output, the transistor collector is connected to the pull-up resistor R4, and the output of the comparator circuit is also connected to the transistor base, finally, the original digital electrical signal that meets the interface standard of the coding circuit is obtained through the transistor common emitter amplification.

TABLE I
THE WORST-CASE CONDITIONAL MIN-ENTROPY FOR THE UNIFORM SAMPLING SCHEME AND THE NON-UNIFORM QUANTIZATION SCHEME

QCNR(dB)	uniform sampling scheme	non-uniform quantization scheme
30	2.53 (1.76)	2.64 (5)
40	2.62 (1.65)	2.88 (5)
50	2.65 (1.62)	2.96 (5)

Taking 8 quantization intervals as an example and ignoring the electronic noise, each quantization interval corresponds to a voltage comparator. When the output signal follows a Gaussian distribution, in order to make it satisfy a uniform distribution as much as possible, the quantization interval is designed according to (13) as

$$\left(\operatorname{erf}\left(\frac{m_{i+1}}{\sqrt{2}}\right)-\operatorname{erf}\left(\frac{m_i}{\sqrt{2}}\right)\right)=0.25 \tag{13}$$

where $i_{\min}=-2^{n-1}+1$, $i_{\max}=2^{n-1}$ and $n=3$.

From (13), the worst-case conditional min-entropy of the uniform sampling scheme and the non-uniform quantization scheme under different QCNRs is shown in Table I. It can be seen that more secure randomness can be extracted in the non-uniform quantization scheme.

IV. CONCLUSION

In this work, we propose a new method to enhance the extractable secure randomness in the QRNG based on vacuum fluctuations independent of classical noises in the worst-case scenario. By using non-uniform quantization methods instead of uniform sampling methods during discretization of vacuum fluctuations, we make the conditional probability of each bin almost equal and enhance the extractable secure randomness of the output sequence. Because the non-uniform quantization cannot be performed with a conventional ADC, we design a non-uniform quantizer which is mainly composed of a multi-channel single-limit comparator circuit composed of n-channel voltage comparators. Finally, given a QCNR as 50 dB and a 16-bit ADC, the worst-case conditional min-entropy can reach 15.87 per sample when using the non-uniform quantization in contrast with 14.36 per sample when using the uniform sampling. We show that the non-uniform quantization can provide more secure randomness independent of classical noises than the uniform sampling.

For further study, it will be interesting to apply the proposed method to other kinds of QRNGs, such as the source-device-independent QRNGs introduced in Ref. [27], where the bound to the conditional min-entropy of the random numbers is determined by the resolution of the trusted measurement device.

References

[1] B. Hayes, “Computing Science: Randomness as a resource,” *Amer. Scientist*, vol. 89, no. 4, pp. 300–304, 2001.

[2] S. Valerio, B. P. Helle, J. C. Nicolas, D. Miloslav, L. Norbert, and P. Momtchil, “The security of practical quantum key distribution,” *Rev. Modern Phys.*, vol. 81, no. 3, 2009, Art. no. 1301.

[3] G. Nicolas, R. Grégoire, T. Wolfgang, and Z. Hugo, “Quantum cryptography,” *Rev. Modern Phys.*, vol. 74, no. 1, 2002, Art. no. 145.

[4] B. Jan, P. Matej, P. Martin, and W. Colin, “Weak randomness seriously limits the security of quantum key distribution,” *Phys. Rev. A*, vol. 86, no. 6, 2012, Art. no. 2308.

[5] P. Li et al., “Fully photonics-based physical random bit generator,” *Opt. Lett.*, vol. 41, no. 14, pp. 3347–3350, 2016.

[6] 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.*, vol. 35, no. 3, pp. 312–314, 2010.

[7] H. Guo, W. Z. Tang, Y. Liu, and W. Wei, “Truly random number generation based on measurement of phase noise of a laser,” *Phys. Rev. E*, vol. 81, no. 5, 2010, Art. no. 051137.

[8] M. Jofre et al., “True random numbers from amplified quantum vacuum,” *Opt. Exp.*, vol. 19, no. 21, pp. 20665–20672, 2011.

[9] F. H. Xu, B. Qi, X. F. Ma, H. Xu, H. X. Zheng, and H. K. Lo, “Ultrafast quantum random number generation based on quantum phase fluctuations,” *Opt. Exp.*, vol. 20, no. 11, pp. 12366–12377, 2012.

[10] C. Abellán et al., “Ultra-fast quantum randomness generation by accelerated phase diffusion in a pulsed laser diode,” *Opt. Exp.*, vol. 22, no. 2, pp. 1645–1654, 2014.

[11] W. Michael, L. Matthias, B. Michael, R. Tino, J. R. Hans, and B. Oliver, “An ultrafast quantum random number generator with provably bounded output bias based on photon arrival time measurements,” *Appl. Phys. Lett.*, vol. 98, no. 17, 2011, Art. no. 171105.

[12] A. W. Michael and G. K. Paul, “Low-bias highspeed quantum random number generator via shaped optical pulses,” *Opt. Exp.*, vol. 18, no. 9, pp. 9351–9357, 2010.

[13] H. Q. Ma, Y. J. Xie, and L. G. Wu, “Random number generation based on the time of arrival of single photons,” *Appl. Opt.*, vol. 44, no. 36, pp. 7760–7763, 2005.

[14] J. B. Philip et al., “Quantum random bit generation using energy fluctuations in stimulated Raman scattering,” *Opt. Exp.*, vol. 21, no. 24, pp. 29350–29357, 2013.

[15] Y. Q. Nie et al., “Practical and fast quantum random number generation based on photon arrival time relative to external reference,” *Appl. Phys. Lett.*, vol. 104, no. 5, 2014, Art. no. 1110.

[16] S. Mario and B. M. Rogina, “Quantum random number generator based on photonic emission in semiconductors,” *Rev. Sci. Instrum.*, vol. 78, no. 4, 2007, Art. no. 5104.

[17] R. W. Caitlin, C. S. Julia, X. W. Li, R. Rajarshi, and E. M. Thomas, “Fast physical random number generator using amplified spontaneous emission,” *Opt. Exp.*, vol. 18, no. 23, pp. 23584–23597, 2010.

[18] Y. Liu, M. Y. Zhu, B. Luo, J. W. Zhang, and H. Guo, “Implementation of 1.6 Tb s- 1 truly random number generation based on a super-luminescent emitting diode,” *Laser Phys. Lett.*, vol. 10, no. 4, 2013, Art. no. 5001.

[19] M. Fiorentino, C. Santori, S. M. Spillane, R. G. Beausoleil, and W. J. Munro, “Secure self-calibrating quantum random-bit generator,” *Phys. Rev. A*, vol. 75, no. 3, 2007, Art. no. 2334.

[20] V. Giuseppe, G. M. Davide, T. Marco, and V. Paolo, “Quantum randomness certified by the uncertainty principle,” *Phys. Rev. A*, vol. 90, no. 5, 2014, Art. no. 2327.

[21] 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*, vol. 87, no. 6, 2013, Art. no. 062327.

[22] J. Y. Haw et al., “Maximization of extractable randomness in a quantum random-number generator,” *Phys. Rev. Appl.*, vol. 3, no. 5, 2015, Art. no. 054004.

[23] R. Konig, R. Renner, and C. Schaffner, “The operational meaning of min- and max-entropy,” *IEEE Trans. Inf. Theory*, vol. 55, no. 9, pp. 4337–4347, Sep. 2009.

[24] M. Tomamichel, C. Schaffner, A. Smith, and R. Renner, “Leftover hashing against quantum side information,” *IEEE Trans. Inf. Theory*, vol. 57, no. 8, pp. 5524–5535, Aug. 2011.

[25] C. Gabriel et al., “A generator for unique quantum random numbers based on vacuum states,” *Nature Photon.*, vol. 4, no. 10, pp. 711–715, 2010.

[26] V. Mannalath, S. Mishra, and A. Pathak, “A comprehensive review of quantum random number generators: Concepts, classification and the origin of randomness,” 2022, *arXiv:2203.00261*.

[27] M. Avesani, D. G. Marangon, G. Vallone, and P. Villoresi, “Source-device-independent heterodyne-based quantum random number generator at 17 Gbps,” *Nature Commun.*, vol. 9, no. 1, pp. 1–7, 2018.

[28] S. Thomas, S. M. Assad, and K. L. Ping, “Real time demonstration of high bitrate quantum random number generation with coherent laser light,” *Appl. Phys. Lett.*, vol. 98, no. 23, 2011, Art. no. 1103.