Article:
Zhou, H, Zeng, P, Razavi, M orcid.org/0000-0003-4172-2125 et al. (1 more author) (2018) Randomness quantification of coherent detection. Physical Review A, 98 (4). ARTN 042321. ISSN 1050-2947

https://doi.org/10.1103/PhysRevA.98.042321

Randomness quantification of coherent detection

Hongyi Zhou,[1] Pei Zeng,[1] Mohsen Razavi,[2] and Xiongfeng Ma[1]

[1] *Center for Quantum Information, Institute for Interdisciplinary Information Sciences, Tsinghua University, Beijing, 100084 China*

[2] *School of Electronic and Electrical Engineering, University of Leeds, Leeds, LS2 9JT, UK*

Continuous-variable quantum cryptographic systems, including random number generation and key distribution, are often based on coherent detection. The essence of the security analysis lies in the randomness quantification. Previous analyses employ a semi-quantum picture, where the strong local oscillator limit is assumed. Here, we investigate the randomness of homodyne detection in a full quantum scenario by accounting for the shot noise in the local oscillator, which requires us to develop randomness measures in the infinite-dimensional scenario. Similar to the finite-dimensional case, our introduced measure of randomness corresponds to the relative entropy of coherence defined for an infinite-dimensional system. Our results are applicable to general coherent detection systems, in which the local oscillator is inevitably of finite power. As an application example, we employ the analysis method to a practical vacuum-fluctuation quantum random number generator and explore the limits of generation rate given a continuous-wave laser.

I. INTRODUCTION

Quantum cryptography, the most practical field in quantum information science, has two major tasks — key distribution and randomness generation. Quantum key distribution (QKD) allows communication partners to share private keys in the presence of an eavesdropper, Eve, whose power is only limited by quantum mechanics [1, 2]. Quantum random number generation (QRNG) aims at providing unpredictable random numbers [3, 4]. The main theoretical focus of both cryptographic tasks lies in the security analysis, which ensures that Eve cannot predict the key or random numbers. Mathematically, the definitions of privacy in the key bits and unpredictability in the random numbers are the same. Thus, it is expected that security analyses in QKD can also be applied to QRNG and vice versa.

There are mainly two categories of schemes for quantum cryptographic systems, namely, discrete variable and continuous variable. Continuous-variable cryptography [5, 6] employs Gaussian modulation and coherent detection, e.g., homodyne detection and heterodyne detection. These are standard techniques in classical telecommunications, which could make continuous-variable optical components robust and economic. From the theoretical point of view, it is crucial to study the mechanism of coherent detection for the security analysis of continuous-variable cryptography. Without loss of generality, we will focus on continuous-variable QRNG systems below. Similar results should also be applicable to QKD systems.

Continuous-variable QRNG schemes [7–26] offer some advantage over conventional discrete-variable ones [27–30] in both performance and practicality, especially the ones exploiting quadrature fluctuations of optical fields [7–17] or laser phase fluctuations [20–26], pushing the generation rate from Mbps to the Gbps regime. The substantial improvement in randomness generation performance is mainly attributed to the coherent detection technique, which replaces single-photon detectors with high-performance photodetectors, gets rid of the restriction of detector dead time, and yields a higher sampling rate.

For these continuous-variable QRNG schemes based on coherent detection, a physical model from the first principle along with rigorous randomness quantification is still missing. Former models of coherent detection QRNGs assumed that the local oscillator in use behaves classically [7–17, 31, 32]. In that case, by controlling the phase of the local oscillator ϕ, different quadratures $\hat{x}(\phi) = 1/2(\hat{a}e^{-i\phi} + \hat{a}^\dagger e^{i\phi})$ of the incoming mode of light, with annihilation operator $\hat{a}$, can then be measured. This leads to a continuum of measurement outcomes implying that the amount of randomness extracted from single round of detection is divergent with high detection resolution, which is rather counter-intuitive. Another issue lies in randomness quantification, where conventional approaches are based on classical min-entropy function [7, 8, 20, 21, 23, 24]. Such quantifiers may suffer from side information in the measurement outcomes, i.e., the quantum state before measurement may be entangled with some ancillary systems held by the adversary. Though the nominal output randomness can be calculated by the measurement statistics, the intrinsic randomness that comes from quantum measurement stays unknown.

In this work, we properly model the coherent detection and provide a rigorous analysis of the randomness origin, quantification, and fundamental limits. By modelling the local oscillator quantum mechanically with a pure coherent state, we can look more closely at the mechanism of the coherent detection. What a coherent detection would effectively measure is the photon number difference between different legs. In this case, we can argue that the randomness in the outcome is a result of the shot-noise effect in the photodetection. For that reason, we refer to the continuous-variable QRNG scheme with coherent detection by shot-noise driven QRNG, whose measurement outcomes form a *discrete*, rather than continuous, infinite-dimensional space.

Meanwhile, in order to accurately calculate the intrinsic randomness in such a QRNG, we apply the rigorous

and powerful tool of quantum coherence [33], which has been related to quantum randomness in [34]. For instance, in the quantum information context, the Z-basis measurement on the qubit $(|0\rangle + |1\rangle)/\sqrt{2}$ would result in either basis states with equal probability. The result of such a measurement is unpredictable. A simple implementation of this idea is based on measuring the relative phase or polarization of a single photon [28]. One can get a similar result if, instead of a superposed state, a mixed state $(|0\rangle\langle 0| + |1\rangle\langle 1|)/2$ is measured. In the latter case, however, we cannot rule out the possibility of the input state being entangled with another external system. In fact, we can purify our mixed state into a Bell state, in which case, an adversary party, who may hold the other part of the Bell state, can fully predict the outcome of the measurement. There is, in fact, no intrinsic (unpredictable) quantum randomness in this mixed-state case, and it only represents sheer classical randomness. The transition from fully random in the case of the superposition state to no quantum randomness for the mixed state indicates a correspondence between coherence of a state and how much quantum randomness can be extracted from it. In fact, it has been shown that, for finite-dimensional states, the relative entropy of coherence is an intrinsic randomness quantifier [35]. In this paper, we extend this result to the infinite dimensional case and quantify the randomness in shot-noise driven QRNG with the help of infinite dimensional coherence [36]. We believe such an analysis should be a standard approach for randomness quantification of QRNGs based on coherent detection, and be further widely employed in other continuous-variable cryptography systems.

The rest of this paper is organised as follows. In Sec. II A, we review the shot-noise driven QRNG structure and show that to properly quantify its generated randomness, we need to employ relevant measures for discrete infinite dimensional variables. Such measures are derived in Sec. II C and their correspondence with infinite dimensional coherence on Fock basis is shown. We then quantify the randomness in shot-noise driven QRNGs and find practical rate bounds for its realistic implementations in Sec. III before concluding the paper in Sec. IV.

II. SHOT-NOISE DRIVEN QRNG

A. Physical model of homodyne detection

Here we first focus on a shot-noise driven QRNG model which is based on homodyne detection of a vacuum state. A slightly modified version of this model can also be applied to other coherent detections, such as heterodyne detection. A schematic diagram of homodyne detection is shown in Fig. 1(a). A local oscillator (LO) in coherent state $|\alpha_{\mathrm{LO}}\rangle$ is coupled to a vacuum state at a 50:50 beam splitter (BS). The two output modes are then measured by two identical photodetectors. The resulting currents are subtracted from each other and converted to bits by an analogue-to-digital converter (ADC).

Such a process is expected to introduce random numbers. In previous analyses [7–9, 11], the LO is modelled classically as a plane wave (in the limit of strong LOs). We show the detailed classical description in Appendix A. This device practically measures $\hat{x}(\phi)$ quadrature of the vacuum state following Gaussian distribution, where ϕ is the modulated phase of the LO. In phase space, such a measurement is a cross-section of the Wigner function of the vacuum state (Fig. 1(c)).

Now, more precisely, we quantum mechanically characterize the LO as a pure coherent state

$$|\alpha_{\mathrm{LO}}\rangle = e^{-\frac{|\alpha_{\mathrm{LO}}|^2}{2}} \sum_n \frac{\alpha_{\mathrm{LO}}^n}{\sqrt{n!}} |n\rangle, \tag{1}$$

where α_{LO} is a complex number and $|n\rangle$ is a Fock state with n photons. Then we can model the module in Fig. 1(a) by that of Fig. 1(b). Each photodetector performs a Fock basis measurement on $\left|\alpha_{\mathrm{LO}} e^{i\phi}/\sqrt{2}\right\rangle$. Because of the shot-noise effect, the output of both Fock basis measurements would follow a Poisson distribution

$$\begin{aligned} p_j^{\mathcal{P}}(\mu) &= |\langle j|\alpha_{\mathrm{LO}} e^{i\phi}/\sqrt{2}\rangle|^2 \\ &= e^{-\mu}\frac{\mu^j}{j!}, \end{aligned} \tag{2}$$

with a mean of $\mu = |\alpha_{\mathrm{LO}}|^2/2$ and independent of the modulated phase ϕ. If we denote the measured photon number by detector D_i, $i = 0, 1$, by N_i, the input to the ADC would then be proportional to the photon number difference $N_d = N_0 - N_1$. It can be shown that N_d, as a difference of two independent Poisson distributions, follows Skellam distribution [37] given by

$$\begin{aligned} p_j^{\mathcal{S}}(\mu) &= \Pr(N_d = j) \\ &= \begin{cases} e^{-2\mu} I_j(2\mu) & j > 0 \\ e^{-2\mu} I_{-j}(2\mu) & j < 0 \end{cases} \end{aligned} \tag{3}$$

where $I_j(2\mu)$ is the modified Bessel function given by [38]

$$I_j(2\mu) = \sum_{m=0}^{\infty} \frac{1}{m!\Gamma(m+j+1)} \mu^{2m+j}. \tag{4}$$

Figure 2 shows the Skellam distribution at $\mu = 50$. It can be seen that it has a symmetric form getting its maximum value at $j = 0$. For sufficiently large values of μ, the Skellam distribution can be well approximated by a Gaussian distribution.

B. Generalizations of the physical model

Our physical model of shot-noise driven QRNG can be generalized to different input states including coherent

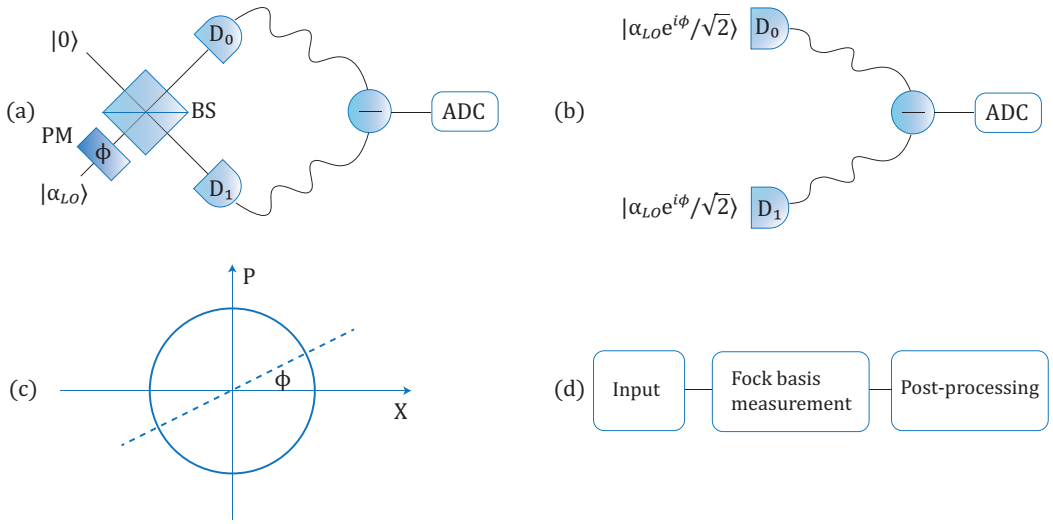

FIG. 1. (a) Schematic diagram of a shot-noise driven QRNG. A homodyne receiver measures a certain quadrature $x(\phi)$ of the vacuum state, which is controlled by the phase modulator. (b) Equivalent setting of (a). The two input coherent states $\left|\alpha_{\rm LO}e^{i\phi}/\sqrt{2}\right\rangle$ have the same phase, but their intensities are independent. The output is proportional to the photon-number difference measured by the two detectors. Here, the randomness originates from the shot-noise effect. (c) Phase space presentation of classical modelled homodyne detection measuring $x(\phi)$ quadrature of a vacuum state. (d) Generalized flow chart of a shot-noise driven QRNG. The whole process can be divided into a quantum phase performing Fock basis measurement on certain input states and a classical phase performing a post-processing on the Fock basis measurement outcomes. LO: local oscillator; PM: phase modulator; BS: beam splitter; $D_{0,1}$: photo detector; ADC: analogue-to-digital converter.

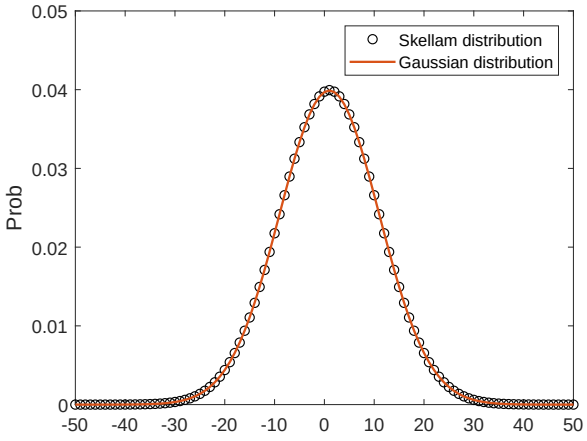

FIG. 2. Comparison of a Skellam distribution, given in Eq. (3), and a Gaussian distribution, with the same mean 0 and variance $2\mu = 100$.

states, Fock states and their mixtures, and general coherent detections (homodyne detection and heterodyne detection).

Coherent state input. If we replace the vacuum state to a general coherent state $|\beta\rangle$, the output state of the beam splitter is a product state of $|\Psi_\beta\rangle = \left|(\beta+\alpha_{\rm LO})/\sqrt{2}\right\rangle\left|(\beta-\alpha_{\rm LO})/\sqrt{2}\right\rangle$ when we consider an X quadrature measurement, which leads to a biased Skellam distribution of

$$p_j(\mu_1,\mu_2) = e^{-(\mu_1+\mu_2)}\left(\frac{\mu_1}{\mu_2}\right)^{j/2} I_j(2\sqrt{\mu_1\mu_2}), \quad (5)$$

after postprocessing, where μ_1 and μ_2 are given by,

$$\begin{aligned}\mu_1 &= \frac{|\beta+\alpha_{\rm LO}|^2}{2},\\ \mu_2 &= \frac{|\beta-\alpha_{\rm LO}|^2}{2}.\end{aligned} \quad (6)$$

For a mixed coherent state input $\int P(\beta)|\beta\rangle\langle\beta|d^2\beta$, the output state will also be a mixture given by

$$\rho_{coh} = \int P(\beta)|\Psi_\beta\rangle\langle\Psi_\beta|d^2\beta \quad (7)$$

followed by a joint Fock basis measurement of $|n_0\rangle\langle n_0|\otimes|n_1\rangle\langle n_1|$.

Fock state input. It is also interesting to consider a Fock state input $|k\rangle$ in our scenario. The corresponding output state can be expressed as

$$|\Psi_k\rangle = e^{-\frac{1}{2}|\alpha_{\rm LO}|^2}\frac{(a_0^\dagger+a_1^\dagger)^k}{2^{k/2}\sqrt{k!}}e^{\frac{\alpha_{\rm LO}(a_0^\dagger-a_1^\dagger)}{\sqrt{2}}}|0\rangle_{01} \quad (8)$$

where $a_0^\dagger$ and $a_1^\dagger$ are creation opeators of the output optical modes of the beam splitter. The Fock state input can lead to a high-dimension entanglement in the output state. For a mixed Fock state input $\sum_k P(k)|k\rangle\langle k|$, the output state will also be a mixture given by $\rho_{Fock} = \sum_k P(k)|\Psi_k\rangle\langle\Psi_k|$.

Heterodyne detection. If we replace homodyne detection with heterodyne detection, and consider a coherent state input $|\beta\rangle$, there will be two output Skellam distributions $p_j(\mu_3, \mu_4)$ and $p_j(\mu_5, \mu_6)$ where

$$\begin{aligned} \mu_{3,4} &= |\frac{\beta}{2} \pm \frac{\alpha_{\mathrm{LO1}}}{\sqrt{2}}|^2 \\ \mu_{5,6} &= |\frac{\beta}{2} \pm \frac{\alpha_{\mathrm{LO2}}}{\sqrt{2}}|^2 \end{aligned} \tag{9}$$

Here $|\alpha_{\mathrm{LO1}}\rangle$ and $|\alpha_{\mathrm{LO2}}\rangle$ are local oscillators in heterodyne detection.

For simplicity, we analyze the vacuum input and homodyne detection in the following discussions, but the methods can be applied for other cases. To fundamentally study the quantum randomness generated by the shot-noise driven QRNG, we have to separate classical sources of randomness from the underlying quantum phenomena. In our case, the electric noise of the receiver, for instance, would contribute to classical randomness and needs to be extracted out using distillation techniques. True intrinsic randomness comes from the photon number difference explained above. We then deal with an infinite dimensional, but discrete, random variable. In the next section, we derive a proper measure of randomness for such cases.

C. Randomness origin and quantification: infinite dimensional coherence

Now we consider the randomness origin and quantification in the shot-noise driven QRNG based on coherent detection. Figure. 1(d) schematically shows its mechanism, including a quantum phase performing Fock basis measurement on certain input states and a classical phase performing a post-processing on the Fock basis measurement outcomes. Same as finite dimensional case, the true randomness origins from the Fock basis measurement breaking the infinite dimensional coherence, which cannot be directly detected as raw data since the classical noises dominates. The post-processing, subtracting the two measurement results, is able to mitigate the classical noises and let the proportion of quantum signals high enough to be detected.

We begin the randomness quantification with the quantum version of min entropy function and show that, in the asymptotic limit, when an experiment is repeated infinitely many times, the average randomness per round approaches the Shannon entropy function. Consider an arbitrary state ρ_A, after a projective measurement $|i\rangle\langle i|$ on A, ρ_A is dephased to $\rho'_A = \sum_i p_i |i\rangle\langle i|$ in the measurement basis. In the worst case, the adversary is access to the most side information of the measurement outcomes by holding a purification of $\rho_{AE} = |\Psi\rangle_{AE}\langle\Psi|_{AE}$. And the state after measurement is $\rho_{A'E} = \sum_i p_i |i\rangle\langle i| \otimes \rho_E^i$. The one-shot randomness in the measurement outcome against such an adversary is given by conditional min-entropy [39]

$$S_{min}(A'|E) = \max_{\sigma_E} \sup\{\lambda \in \mathcal{R} : \rho_{A'E} \leq 2^{-\lambda} I_A \otimes \sigma_E\}, \tag{10}$$

where the dimension of σ_E is not higher than that of $\rho_E = \mathrm{tr}_E(\rho_{AE})$. In Appendix B, we prove that when ρ_A is pure, this formula will reduce to the classical min-entropy function $H_{min} = -\log_2(\max_i p_i)$. The ϵ-smooth version of Eq. (10), removing extreme events, is also a one-shot randomness quantifier,

$$S^{\epsilon}_{min}(A'|E) = \max_{\rho_{\tilde{A}E}} S_{min}(A'|E) \tag{11}$$

satisfying $\sqrt{1 - F^2(\tilde{\rho}_{AE}, \rho_{AE})} \leq \epsilon$, where fidelity function is defined as $F(\tilde{\rho}_{AE}, \rho_{AE}) = \mathrm{tr}(\tilde{\rho}_{AE}\rho_{AE})$.

If the measurement is conducted n times, in an independent and identical way, then the outputs are also independent and identically distributed (i.i.d) variables whose randomness is given by $S^{\epsilon}_{min}(A'^n|E^n)$. In the limit of $n \to \infty$, for any $0 < \epsilon < 1$

$$\lim_{n\to\infty} \frac{1}{n} S^{\epsilon}_{min}(A'^n|E^n) = S(A'|E) = S(A') - S(A) \tag{12}$$

where the first equation is the asymptotic equipartition property [39], the second equation is referred to Ref. [35] for finite dimensional cases, but it still holds for infinite dimensional cases since the relative entropy of coherence is a well-defined coherence measure for infinite dimensional states [36]. Therefore, we can conclude that the randomness after the Fock basis measurement can be quantified with relative entropy of coherence. Fortunately, in our shot-noise driven QRNG, the state ρ_A is a pure coherent state, the relative entropy of coherence reduce to Shannon entropy of the probability distribution of the measurement results,

$$\begin{aligned} R_0 &= C(\rho_A) = H(\{p_j^{\mathcal{P}}(\mu)\}) \\ &= -\sum_{j=-\infty}^{\infty} p_j^{\mathcal{P}}(\mu) \log_2 p_j^{\mathcal{P}}(\mu), \end{aligned} \tag{13}$$

where $p_j^{\mathcal{P}}(\mu)$ is given by Eq. (2) and $C(\cdot)$ is the relative entropy of coherence. After the post-processing of subtraction, the final randomness becomes

$$\begin{aligned} R_1 &= H(\{p_j^{\mathcal{S}}(\mu)\}) \\ &= -\sum_{j=-\infty}^{\infty} p_j^{\mathcal{S}}(\mu) \log_2 p_j^{\mathcal{S}}(\mu), \end{aligned} \tag{14}$$

which is less than the total randomness $2R_0$ and $p_j^{\mathcal{S}}(\mu)$ is given by Eq. (3). We compare the randomness before and after the subtraction, i.e., $2R_0$ and R_1 respectively, with respect to the intensity of the local oscillator in Fig. 3.

Things become more difficult when considering mixed state input cases, where the output states are also mixed state, and the relative entropy of coherence on the Fock basis cannot reduce to Shannon entropy any more. For

the mixed coherent state and mixed Fock state discussed in Sec. II B, we can still consider the randomness before post-processing, $C(\mathrm{tr}_1(\rho_{coh})) + C(\mathrm{tr}_0(\rho_{coh}))$ and $C(\mathrm{tr}_1(\rho_{Fock})) + C(\mathrm{tr}_0(\rho_{Fock}))$, as an upper bound of the final randomness. The noise of the local oscillator, i.e., phase fluctuation and intensity fluctuation of a coherent state, can also be regarded as effects from a mixed coherent state input. And the above upper bound still holds. We leave the accurate calculation of randomness for mixed state input for future works.

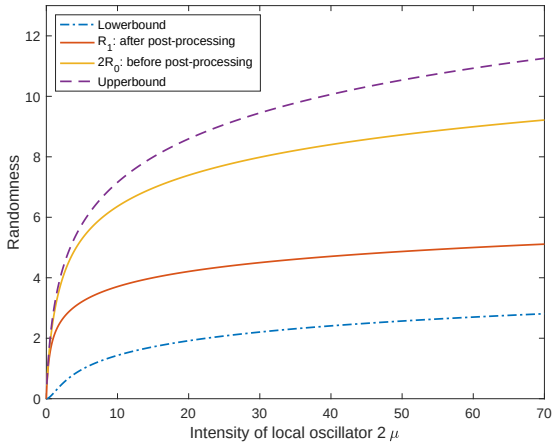

FIG. 3. Dependence of the randomness before and after the post-processing of subtraction on the intensity of LO. In the legend "R_1: after post-processing" refers to Eq. (14) and "$2R_0$: before post-processing" refers to Eq. (13). The dashed line and dot-dashed line are practical upper and lower bound of randomness per sample given in Sec. III, respectively.

III. PRACTICAL BOUNDS FOR REALISTIC IMPLEMENTATIONS

In the last section, we obtained the random number generation rate for the shot-noise driven QRNG in Eq. (14). In this section, we try to find an upper bound R^U and a lower bound R^L on Eq. (14) for practical cases. The upper bound R^U provides a limit on the output randomness per sample, while the lower bound R^L is just randomness quantification in previous works [7, 8]. In the following analysis, we model some experimental parameters relevant to realistic setups. In what follows, the power of the local oscillator, which is assumed to be generated by a continuous-wave laser, by P, central and max frequency of the laser by ν and ν_m, the response time of the photodetectors by τ, the sampling frequency of ADC by f, and the quantization interval of ADC by a.

A. Upper bound

The photon number of the LO within the response time follows Poisson distribution $p_j^{\mathcal{P}}(2\mu)$, where $2\mu = P\tau/(h\nu)$ is the mean photon number. The total randomness comes from two aspects, the randomness in the detection outcomes and the randomness in the Poisson distribution, i.e., $H(AB) = H(A|B) + H(B)$, where A and B stand for the two aspects above respectively. The maximum possible randomness for n-photon input is that the photon number difference $\{-n, -n+2, \cdots, n-2, n\}$ follows a uniform distribution, which corresponds to the max-entropy $\log_2(n+1)$. Then $H(A|B) < \sum_n p_n \log_2(n+1) \leq \log_2[(\sum_n p_n n) + 1]$, where the second inequality is due to the concavity of logarithm function. Therefore we obtain an upper bound of randomness per sample,

$$R^U = \log_2(2\mu + 1) + H(\{p_j^{\mathcal{P}}(2\mu)\}), \tag{15}$$

From the equation above we notice that in the homodyne-detection based shot-noise driven QRNG, the upper bound of the output randomness only depends on the mean photon number and the photon number distribution of the source, and is independent of the specific implementations of measurement settings, such as the ratio of the beam splitter, the post-processing method, etc. A further conjecture on the upper bound of output randomness of an optical QRNG is that, it will only depend on the source and the number of paths in detection (for example, the number of paths in homodyne detection is 2). We leave this generalized case for future works.

The upper bound of randomness generation rate is proportional to R^U, while the sampling frequency is constrained by the response time and Nyquist-Shannon sampling theorem [40, 41]. When the sampling frequency exceeds $1/\tau$ or $2\nu_m$, the information becomes redundant due to high autocorrelation. Therefore, the upper bound of randomness generation rate is given by

$$R_{\mathrm{tot}}^{(\max)} = \min\{\frac{1}{\tau}, 2\nu_m\} R^U. \tag{16}$$

B. Lower bound

In order to find a lower bound on R_1, we can use the relationship $H(\{p_j^{\mathcal{S}}(\mu)\}) \geq H_{min}(\{p_j^{\mathcal{S}}(\mu)\}) = -\log_2(p_0^{\mathcal{S}}(\mu))$. However, in practice, instead of measuring N_d directly, we typically measure kN_d, which represents the voltage/current corresponding to the photon count, where k is a proportionality factor. We also need to account for the effect of quantization in the employed ADC that follows the homodyne receiver. For an ADC with a quantization interval a, we can only tell if the output voltage/current lies in a certain interval with width a. The probability, P_J, that the corresponding output voltage/current to the homodyne receiver will lie in the

interval $[J, J+a]$ is given by

$$P_J = \sum_{\lceil J/k \rceil \le j \le \lfloor (J+a)/k \rfloor} p_j^{\mathcal{S}}(\mu). \tag{17}$$

Considering the symmetric form of the Skellam distribution, shown in Fig. 2, we can then show that the min entropy for the ADC output is given by $-\log_2(P_J)$ at $J = -a/2$. Given that, at $J = -a/2$, $P_J \ge p_0$, the lower bound on R_0 is given by

$$R^L = -\log_2 \sum_{\lceil -a/(2k) \rceil \le j \le \lfloor a/(2k) \rfloor} p_j^{\mathcal{S}}(\mu). \tag{18}$$

Similarly, the lower bound on the total random number generation rate is given by

$$R_{\text{tot}}^{(\min)} = \min\{\frac{1}{\tau}, 2\nu_m\} R^L \tag{19}$$

Such a lower bound is often used as the randomness generation rate in experiment since it is easy to calculate, corresponding to the worst case with the minimal true randomness. We make a comparison between the randomness upper bound Eq. (15), the lower bound Eq. (18), and the actual randomness Eq. (14) in Fig. 3 with the ADC resolution $a/k = 1$. We further simulate the randomness generation rate lower bound based on Eq. (19) for different resolutions of the ADC and different local oscillator intensities in Fig. 4. Here we neglect the constraint of Nyquist-Shannon sampling theorem and assume the optimal sampling frequency is equal to reciprocal value of the response time of the photo detector $1/\tau$. The simulation result shows the lower bound of random number generation rate has a peak value and becomes convergent when the sampling frequency goes to infinity. This is because when $\tau \to 0$, the variance per sample also goes to zero, and the measurement result will always fall in a certain interval of the ADC, which leads to a fixed sequence with a min-entropy of zero. For practical photodetectors, the response time is at the order of 10^{-10} s which is much larger than the optimal value. Therefore the sampling frequency can be increased to $1/\tau \sim 10^{10}$ Hz in practical implementations.

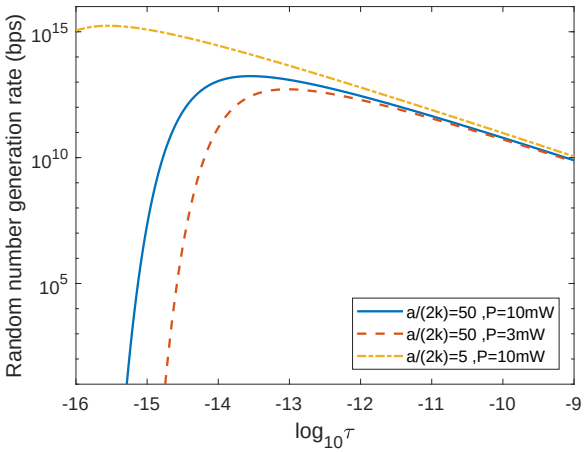

FIG. 4. The lower bound of random number generation rate with different resolutions of the ADC and different local oscillator intensities.

IV. CONCLUSION AND OUTLOOK

In this work, we investigate the randomness quantification in shot-noise driven QRNG based on coherent detection. By characterizing the local oscillator in a quantum way, we find the outcome of homodyne detection is actually an infinite dimensional discrete variable rather than a continuous one, whose randomness is quantified by infinite-dimensional coherence. Considering experimental parameters, we calculate practical upper and lower bounds of the randomness generation rate.

As a beginning, our work provides a new point of view on the coherent detection. For future work, we may take more practical issues into consideration, such as electronic noises, bandwidth of photodetectors, and more important, intensity fluctuations of the local oscillator and input state. These intensity fluctuations will make the coherent states in our model become mixed, which will be exploited by the adversary to extract side information. The randomness quantification in this case is quite challenging.

Moreover, our technique for randomness quantification in coherent detection is applicable to other scenarios that a similar setup is used. One example is phase fluctuation extracting randomness from spontaneous emission. The bottleneck lies in how to characterize the entropy source, i.e., a coherent light carrying a random phase introduced by spontaneous emission.

Another key example is the continuous-variable QKD systems where a Gaussian-modulated coherent state by Alice is measured by a homodyne receiver at Bob's end [5]. The common assumption in the security analysis is to treat the local oscillator classically, or, equivalently, assume that the local oscillator is of infinitely large intensity. If one wants to account for the effect of having a finite-power oscillator, then one can use the techniques we developed in this work, and the security analysis may fall in to the same framework of discrete variable QKD.

The security of QKD is generally based on measurement results from two conjugate bases. In our scenario, the conjugate basis measurement is realized by adjusting the relative phase between the input state and the local oscillator. For example, the local oscillator state can be set as $|\alpha_{\text{LO}}\rangle$ and $|i\alpha_{\text{LO}}\rangle$ for different basis measurement. The key rate calculations will then involve estimating the mutual information between Alice and Bob and upper bounding the Holevo information between Alice/Bob and Eve (depending on whether direct/reverse reconciliation is in use) [42], in other words, lower bounding the local randomness of Alice/Bob eliminating Eve's

side information. To find a lower bound of the local randomness, one can apply the entropic uncertainty relation with the help of the measurement result from another basis. Note that in the current analysis of continuous variable QKD protocols, the uncertainty relation is between measurement results from X and P quadrature measurements [43, 44]. However, the real coherent detection, as modeled in this work, is a discrete-valued POVM measurement. To accurately estimate the local randomness of Alice/Bob eliminating Eve's side information, a different form of uncertainty relation is required, which is left for future research.

ACKNOWLEDGMENTS

The authors acknowledge J. Ma, M. Plenio and X. Yuan for the insightful discussions. This work is supported by National Key R&D Program of China (2017YFA0303900, 2017YFA0304004), the National Natural Science Foundation of China Grant No. 11674193, and the UK EPSRC Grant EP/M013472/1. All data generated in this paper can be reproduced by the provided methodology and equations.

Appendix A: Classical model of homodyne detection

Homodyne detection settings, made up of a beam splitter and two photodetectors, have two inputs: a local oscillator (LO), which can be described as a strong coherent state $|\alpha_{LO}\rangle$, and a signal state ρ. After a transformation from photon intensity to current by the photodetector, a subtraction of current is performed to mitigate the classical electronic noise.

The output in the homodyne detection is given by the operator,

$$\delta\hat{i} = \hat{i}_1 - \hat{i}_2 = k(\hat{a}_{LO}^\dagger \hat{a} + \hat{a}^\dagger \hat{a}_{LO}). \tag{A1}$$

where $\hat{a}$ and $\hat{a}_{LO}$ are annihilation operators of the input optical modes. And for a photodetector, we make an assumption that the current is proportional to photon number and the coefficient is k. Note that all the calculation above is in the Heisenberg picture. Hence the expectation value of $\delta\hat{i}$ is $Tr(\delta\hat{i}\rho \otimes |\alpha_{LO}\rangle\langle\alpha_{LO}|)$ and the variance is $Tr(\delta\hat{i}^2\rho \otimes |\alpha_{LO}\rangle\langle\alpha_{LO}|) - (Tr(\delta\hat{i}\rho \otimes |\alpha_{LO}\rangle\langle\alpha_{LO}|))^2$. When the intensity of the LO is strong enough, the homodyne detection can be regarded as a measurement of quadratures as an approximation. Considering the phase of the LO, $\alpha_{LO} = |\alpha_{LO}|e^{i\phi}$, the expectation and variance can be rewritten as

$$\begin{aligned}
&\langle\delta\hat{i}\rangle = 2k|\alpha_{LO}|\mathrm{tr}(\hat{x}(\phi)\rho) \\
&\langle\delta\hat{i}^2\rangle - \langle\delta\hat{i}\rangle^2 \\
&= 4k^2|\alpha_{LO}|^2[\mathrm{tr}(\hat{x}^2(\phi)\rho) - (\mathrm{tr}(\hat{x}(\phi)\rho))^2] + k^2\mathrm{tr}(\hat{a}^\dagger\hat{a}\rho),
\end{aligned} \tag{A2}$$

where $\hat{x}(\phi) = (\hat{a}e^{-i\phi} + \hat{a}^\dagger e^{i\phi})/2$ is a quadrature of the signal state depending on ϕ. When $\phi = 0$ or $\pi/2$, it corresponds to $\hat{x} = (\hat{a} + \hat{a}^\dagger)/2$ or $\hat{p} = (\hat{a} - \hat{a}^\dagger)/2$ quadrature respectively, that is, the quantity measured by the homodyne detection depends on the phase ϕ of the LO.

Appendix B: Quantum min-entropy can reduce to its classical counterpart

In this section we prove the quantum min-entropy will reduce to the classical min-entropy function when the adversary has no side information of the measurement outcomes, i.e, ρ_A is a pure state. We begin with Eq. (10)

$$\begin{aligned}
S_{min}(A'|E) &= \max_{\sigma_E} \sup\{\lambda \in \mathcal{R} : \rho_{A'E} \leq 2^{-\lambda} I_A \otimes \sigma_E\} \\
&= \min_{\sigma_E} \inf\{p \in \mathcal{R} : pI_A \otimes \sigma_E \geq \rho_{A'E}\} \\
&= \min_{\sigma_E} \inf\{p \in \mathcal{R} : pI_A \otimes \sigma_E \geq \rho_{A'} \otimes \rho_E\}
\end{aligned} \tag{B1}$$

where $p = 2^{-\lambda}$, the last equation is because ρ_A is pure and after the measurement on A, $\rho_{A'E}$ is also a product state. Now we need to let p as small as possible such that $pI_A \otimes \sigma_E \geq \rho_{A'} \otimes \rho_E$ which can be rewritten as

$$\sum_i |i\rangle\langle i| \otimes (p\sigma_E - p_i\rho_E) \tag{B2}$$

We only need to consider $p\sigma_E - p_i\rho_E \geq 0$. Note that ρ_E is a pure state with only one non-zero eigenvalue $\eta = 1$ in its spectrum. In order to let p as small as possible, the best choice is to let σ_E also be a pure state $\sigma_E = \rho_E$ and $p \geq p_i$. Consider all decomposition components in Eq. (B2), $p = \max_i p_i$ and $\lambda = -\log_2(\max_i p_i)$ which is just the classical min-entropy function.

[1] C. H. Bennett and G. Brassard, in *Proceedings of the IEEE International Conference on Computers, Systems and Signal Processing* (IEEE Press, New York, 1984) pp. 175–179.
[2] A. K. Ekert, Phys. Rev. Lett. **67**, 661 (1991).
[3] X. Ma, X. Yuan, Z. Cao, B. Qi, and Z. Zhang, npj Quantum Information **2**, 16021 (2016), review Article.
[4] M. Herrero-Collantes and J. C. Garcia-Escartin, Rev. Mod. Phys. **89**, 015004 (2017).
[5] F. Grosshans and P. Grangier, Phys. Rev. Lett. **88**, 057902 (2002).
[6] F. Grosshans, G. Van Assche, J. Wenger, R. Brouri, N. J. Cerf, and P. Grangier, Nature **421**, 238 (2003).
[7] C. Gabriel, C. Wittmann, D. Sych, R. Dong, W. Mauerer, U. L. Andersen, C. Marquardt, and

G. Leuchs, Nature Photonics **4**, 711 (2010).
[8] Y. Shen, L. Tian, and H. Zou, Physical Review A **81**, 063814 (2010).
[9] T. Symul, S. Assad, and P. K. Lam, Applied Physics Letters **98**, 231103 (2011).
[10] M. Jofre, M. Curty, F. Steinlechner, G. Anzolin, J. Torres, M. Mitchell, and V. Pruneri, Optics express **19**, 20665 (2011).
[11] Y. Shi, B. Chng, and C. Kurtsiefer, Applied Physics Letters **109** (2016), http://dx.doi.org/10.1063/1.4959887.
[12] D. G. Marangon, G. Vallone, and P. Villoresi, Phys. Rev. Lett. **118**, 060503 (2017).
[13] B. Xu, Z. Li, J. Yang, S. Wei, Q. Su, W. Huang, Y. Zhang, and H. Guo, arXiv preprint arXiv:1709.00685 (2017).
[14] B. Haylock, D. Peace, F. Lenzini, C. Weedbrook, and M. Lobino, arXiv preprint arXiv:1801.06926 (2018).
[15] X. Guo, R. Liu, P. Li, C. Cheng, M. Wu, and Y. Guo, arXiv preprint arXiv:1805.10506 (2018).
[16] M. Avesani, D. G. Marangon, G. Vallone, and P. Villoresi, arXiv preprint arXiv:1801.04139 (2018).
[17] Z. Zheng, Y.-C. Zhang, W. Huang, S. Yu, and H. Guo, arXiv preprint arXiv:1805.08935 (2018).
[18] H. Fürst, H. Weier, S. Nauerth, D. G. Marangon, C. Kurtsiefer, and H. Weinfurter, Optics express **18**, 13029 (2010).
[19] Q. Yan, B. Zhao, Q. Liao, and N. Zhou, Review of Scientific Instruments **85**, 103116 (2014).
[20] B. Qi, Y.-M. Chi, H.-K. Lo, and L. Qian, Optics letters **35**, 312 (2010).
[21] F. Xu, B. Qi, X. Ma, H. Xu, H. Zheng, and H.-K. Lo, Optics express **20**, 12366 (2012).
[22] Y.-Q. Nie, H.-F. Zhang, Z. Zhang, J. Wang, X. Ma, J. Zhang, and J.-W. Pan, Applied Physics Letters **104**, 051110 (2014).
[23] Y.-Q. Nie, L. Huang, Y. Liu, F. Payne, J. Zhang, and J.-W. Pan, Review of Scientific Instruments **86**, 063105 (2015).
[24] X.-G. Zhang, Y.-Q. Nie, H. Zhou, H. Liang, X. Ma, J. Zhang, and J.-W. Pan, Review of Scientific Instruments **87**, 076102 (2016).
[25] J. Yang, J. Liu, Q. Su, Z. Li, F. Fan, B. Xu, and H. Guo, Optics Express **24**, 27475 (2016).
[26] S.-H. Sun and F. Xu, Phys. Rev. A **96**, 062314 (2017).
[27] T. Jennewein, U. Achleitner, G. Weihs, H. Weinfurter, and A. Zeilinger, Review of Scientific Instruments **71**, 1675 (2000).
[28] A. Stefanov, N. Gisin, O. Guinnard, L. Guinnard, and H. Zbinden, Journal of Modern Optics **47**, 595 (2000).
[29] Z. Cao, H. Zhou, and X. Ma, New Journal of Physics **17**, 125011 (2015).
[30] Z. Cao, H. Zhou, X. Yuan, and X. Ma, Phys. Rev. X **6**, 011020 (2016).
[31] X. Ma, F. Xu, H. Xu, X. Tan, B. Qi, and H.-K. Lo, Phys. Rev. A **87**, 062327 (2013).
[32] H. Zhou, X. Yuan, and X. Ma, Phys. Rev. A **91**, 062316 (2015).
[33] T. Baumgratz, M. Cramer, and M. Plenio, Physical review letters **113**, 140401 (2014).
[34] X. Yuan, H. Zhou, Z. Cao, and X. Ma, Physical Review A **92**, 022124 (2015).
[35] X. Yuan, Q. Zhao, D. Girolami, and X. Ma, arXiv preprint arXiv:1605.07818 (2016).
[36] Y.-R. Zhang, L.-H. Shao, Y. Li, and H. Fan, Physical Review A **93**, 012334 (2016).
[37] J. G. Skellam, Journal of the Royal Statistical Society. Series A (General) **109**, 296 (1945).
[38] M. Abramowitz, I. A. Stegun, *et al.*, Applied mathematics series **55**, 62 (1966).
[39] M. Tomamichel, arXiv preprint arXiv:1203.2142 (2012).
[40] H. Nyquist, Transactions of the American Institute of Electrical Engineers **47**, 617 (1928).
[41] C. E. Shannon, Bell Labs Technical Journal **28**, 656 (1949).
[42] I. Devetak and A. Winter, Proceedings of the Royal Society of London A: Mathematical, Physical and Engineering Sciences **461**, 207 (2005).
[43] F. Furrer, M. Berta, M. Tomamichel, V. B. Scholz, and M. Christandl, Journal of Mathematical Physics **55**, 172 (2014).
[44] A. Hertz and N. J. Cerf, arXiv preprint arXiv:1809.01052 (2018).