



Impact of an imperfect sampling device on the security of a continuous-variable source-independent quantum random-number generator with a phase-randomized local oscillator

Yuanhao Li , Yangyang Fei *, Weilong Wang, Xiangdong Meng, Hong Wang, Qianheng Duan, Yu Han, and Zhi Ma
Henan Key Laboratory of Network Cryptography Technology, Zhengzhou, Henan 450001, China



(Received 15 January 2024; accepted 15 April 2024; published 1 May 2024)

Continuous-variable source-independent quantum random-number generators (CV-SI-QRNGs) generate high-speed secure random numbers without any assumptions about source. Recently, Smith *et al.* [*Phys. Rev. A* **99**, 062326 (2019)] proposed a CV-SI-QRNG with phase-randomized local oscillator (LO) protocol, which does not require additional active optical components, thus reducing the complexity of the CV-SI-QRNG setup and attracting widespread attention. However, the trusted but imperfect sampling device used in CV-SI-QRNG has not yet been fully investigated, which will lead to performance degradation and security problems. In this work, we investigate the influence of imperfect sampling devices on the CV-SI-QRNG with phase-randomized LO, including the finite-sampling bandwidth, finite-sampling precision, and finite-size effect. Simulation results show that practical imperfections in the sampling device will affect the estimation of lower bound on the conditional min-entropy and reduce the extractable randomness. To improve the performance of CV-SI-QRNG and prevent such information leakages, we also provide some corresponding countermeasures. Our work highlights the influences of imperfect sampling devices on the performance and security of practical CV-SI-QRNG systems, which helps to improve their robustness and practicality.

DOI: [10.1103/PhysRevA.109.052401](https://doi.org/10.1103/PhysRevA.109.052401)

I. INTRODUCTION

Random numbers are considered an important resource in various tasks, especially in the field of quantum communication [1–8]. Quantum random-number generators (QRNGs) based on the uncertainty principle of quantum mechanics can generate unpredictable and secure random numbers [9,10], which have attracted lots of attention and many of them are proposed based on various sources [11–21]. According to the randomness reliability levels, QRNGs can be classified into three categories, i.e., practical QRNGs, device-independent (DI) QRNGs, and semi-device-independent (SDI) QRNGs. Practical QRNGs completely trust their well-characterized devices and typically have a fast generation speed [13,18,19]. DI-QRNGs have no assumptions about the source of randomness or the measurement device [22–24], whose security relies on the violation of a Bell inequality. However, the stringent device requirements in DI-QRNGs are highly challenging and limit the randomness generation speed, which can hardly meet actual demands. SDI-QRNGs achieve a tradeoff between the randomness generation speed and the randomness reliability that exists in practice [25–41], which generated random numbers with certain assumptions of device implementations. Several SDI-QRNG protocols have been proposed, such as measurement-device-independent (MDI) QRNGs [27,28] and source-independent (SI) QRNGs [29–39]. In particular, SI-QRNGs can generate secure random numbers with well-characterized measurements but an untrusted randomness source, while the randomness source is usually a complicated

physical system. Therefore, SI-QRNGs have gained public concern.

SI-QRNGs exploiting discrete-variable methods and continuous-variable (CV) methods have been proposed and experimentally demonstrated, respectively. Differing from discrete-variable SI-QRNGs [35–39], CV-SI-QRNGs have been demonstrated to achieve faster random number generation speed up to Gbps [29–34]. To guarantee the security of the generated random numbers immune to an untrusted source, CV-SI-QRNGs use optical homodyne detection or heterodyne detection to measure alternately and randomly two quadrature observables of an input untrusted quantum state, where the quadrature is selected by the phase of a continuous-wave laser, the so-called local oscillator (LO). However, most homodyne-based and heterodyne-based CV-SI-QRNG protocols require the addition of a phase modulator to change the phase of the LO emitted by the continuous-wave laser [29–32,34], especially the homodyne-based CV-SI-QRNG protocols require external initial randomness, which increases the complexity of the CV-SI-QRNG setup and may lead to new security problems. Fortunately, taking advantage of the fact that the gain-switched laser emits each pulse with a random phase, Smith *et al.* proposed a new CV-SI-QRNG scheme without a phase modulator, where a gain-switched laser is used as LO instead of a continuous-wave laser [33], thus reducing the complexity of the CV-SI-QRNG setup and attracting a lot of attention.

Although the CV-SI-QRNG protocol removes all source assumptions, the measurement and sampling devices must be well characterized. In practice, there are inevitably imperfections in measurement and sampling devices that make it difficult to characterize them accurately. Concentrating on

*Corresponding author: fei_yy@foxmail.com

CV-SI-QRNGs, the impacts of different imperfect factors on the security of CV-SI-QRNGs have been studied, such as LO fluctuation, imperfect beam splitter (BS), imperfect phase modulator, and finite-size effect [42–44]. Nevertheless, there is still a lack of study on the effects of imperfect sampling devices on the practical security of CV-SI-QRNG. In the CV-SI-QRNG with phase-randomized LO, the output measurements of homodyne detector are sampled by the sampling device, i.e., analog-to-digital converter (ADC). Ideally, the sampling bandwidth, sampling range, and sampling resolution of the ADC are infinite, but the opposite is true in practice. The finite-sampling bandwidth effect may cause the maximum sampled value of the output signal to deviate from the peak value, which would influence the evaluation of lower bound of the extractable randomness and the performance of CV-SI-QRNG. In addition, finite-sampling range and sampling resolution determine that the sampling precision of ADC is also finite. The finite-sampling precision leads to a partial loss of information of the output continuous signal, which may also affect the evaluation of lower bound of the extractable randomness. To guarantee the security of CV-SI-QRNG, the precise estimation of parameters associated with the lower bound of the extractable randomness requires an infinite data size. However, the data size in practice is finite, which inevitably results in statistical fluctuations of the estimated parameters [45–51], and thus overestimating or underestimating the lower bound of the extractable randomness. Therefore, the impact of finite-size effect on the practical security of CV-SI-QRNG should be studied.

In this paper, we investigate the influences of imperfect sampling devices and finite-size effect on the practical security of the CV-SI-QRNG with phase-randomized LO. Moreover, we also give the corresponding solutions to eliminate these influences and improve the performance of CV-SI-QRNG. This paper is organized as follows. In Sec. II, we describe and model the CV-SI-QRNG with phase-randomized LO. Then, the impacts of finite-sampling bandwidth effect on the evaluation of available randomness are investigated in Sec. III. Considering the finite-sampling precision effect, the influences of different sampling precisions on the evaluation of available randomness are studied in Sec. IV. In Sec. V, we analyze the influences of finite-size effect on the practical security of CV-SI-QRNG with phase-randomized LO. Finally, the conclusion is drawn in Sec. VI.

II. CV-SI-QRNG WITH PHASE-RANDOMIZED LO

In the CV-SI-QRNG with phase-randomized LO, the source is an untrusted party that can be arbitrary and controlled by an adversarial party (Eve), and the user (Alice) trusts the measurement devices. Unlike other CV-SI-QRNGs with continuous-wave lasers, the LO is generated by a gain-switched laser. Due to the phase diffusion process in gain-switched lasers, the LO is phase randomized, which allows CV-SI-QRNG to randomly measure quadratures of the input field without requiring a phase modulator and an initial random number to drive it. By estimating the lower bound for min-entropy conditioned on the quantum side information, secure random numbers can be extracted from the original data using the randomness extraction method.

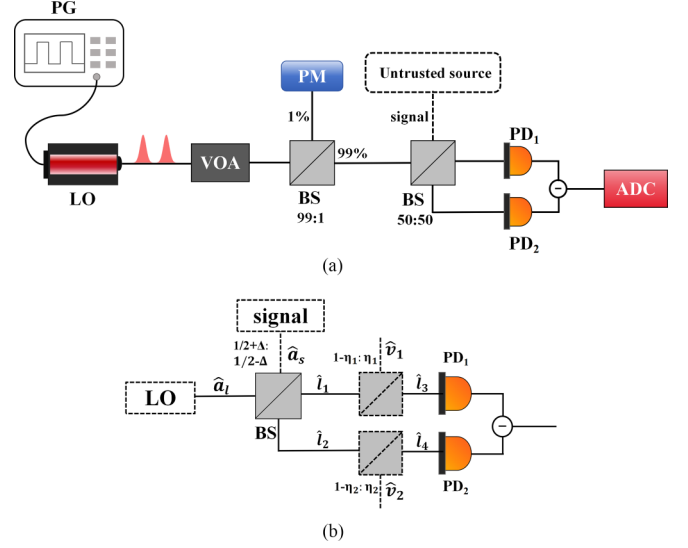


FIG. 1. (a) A schematic of the phase-randomized CV-SI-QRNG setup. The LO is pulsed and gain switched. LO: local oscillator; PG: pattern generator; VOA: variable optical attenuator; PM: power meter; BS: beam splitter; PD: photodiode; ADC: analog-to-digital converter. (b) Physical model of the phase-randomized CV-SI-QRNG.

Figure 1(a) shows the schematic of phase-randomized CV-SI-QRNG setup. The laser is driven above threshold by applying an ac voltage from a pattern generator (PG). It operates in gain-switching mode to produce phase-randomized LO, where the connected VOA can adjust the power level of LO. Then, the attenuated LO is split by a 99:1 BS. The 1% output is connected to a power meter to monitor the LO power. The 99% output is split by a 50:50 BS, and the other input of the 50% BS is completely open and controlled by Eve. The signal beam and LO beam are mixed at 50:50 BS, which is detected and amplified by a balanced homodyne detector. An ADC samples the subtracted photocurrent signal of the homodyne detector. The finite-sampling range $[-N + \delta_{\text{ADC}}/2, N - 3\delta_{\text{ADC}}/2]$ and finite-sampling resolution n lead to the finite-sampling precision $\delta_{\text{ADC}} = N/2^{n-1}$.

As shown in Fig. 1(b), a physical model of the phase-randomized CV-SI-QRNG is illustrated by describing optical modes with annihilation and production operators. Notably, for simplicity, the mentioned LO does not include the part measured by the power meter but only denotes the part that interferes with the input state in the following analysis. The LO power incident on PD can be calculated from the power meter measurements in the real experiment. The signal and LO are described by the mode operators \hat{a}_s and \hat{a}_l , respectively. In our physical model, the splitting ratio of the BS may deviate from the ideal value by Δ . The interference of the signal beam \hat{a}_s and LO beam \hat{a}_l can be described as follows:

$$\begin{bmatrix} \hat{l}_1 \\ \hat{l}_2 \end{bmatrix} = \begin{bmatrix} \sqrt{\frac{1}{2} - \Delta} & \sqrt{\frac{1}{2} + \Delta} \\ \sqrt{\frac{1}{2} + \Delta} & -\sqrt{\frac{1}{2} - \Delta} \end{bmatrix} \begin{bmatrix} \hat{a}_s \\ \hat{a}_l \end{bmatrix}. \quad (1)$$

The nonideal efficiencies of photodiodes (PDs) with quantum efficiencies η_1 and η_2 are modeled by a virtual BS with a transmission coefficient equal to the quantum efficiency of the

real PD followed by an ideal PD. As a result, the modes that are detected by PD₁ and PD₂ are given by

$$\hat{l}_3 = \sqrt{\eta_1} \left(\sqrt{\frac{1}{2} - \Delta} \hat{a}_l + \sqrt{\frac{1}{2} + \Delta} \hat{a}_s \right) + \sqrt{1 - \eta_1} \hat{v}_1, \quad (2)$$

$$\hat{l}_4 = \sqrt{\eta_2} \left(\sqrt{\frac{1}{2} - \Delta} \hat{a}_s - \sqrt{\frac{1}{2} + \Delta} \hat{a}_l \right) + \sqrt{1 - \eta_2} \hat{v}_2. \quad (3)$$

The PD converts the photons into photoelectrons, and the subtracted photoelectrons number per LO pulse \hat{N}_r can be given by

$$\begin{aligned} \hat{N}_r = \hat{l}_3^\dagger \hat{l}_3 - \hat{l}_4^\dagger \hat{l}_4 = & (\eta_1 + \eta_2) \sqrt{\frac{1}{4} - \Delta^2} (\hat{a}_s^\dagger \hat{a}_l \\ & + \hat{a}_l^\dagger \hat{a}_s) + \left[\eta_1 \left(\frac{1}{2} - \Delta \right) - \eta_2 \left(\frac{1}{2} + \Delta \right) \right] \hat{a}_l^\dagger \hat{a}_l \\ & + \sqrt{\eta_1(1 - \eta_1)} \left(\frac{1}{2} - \Delta \right) (\hat{v}_1^\dagger \hat{a}_l + \hat{a}_l^\dagger \hat{v}_1) \\ & + \sqrt{\eta_2(1 - \eta_2)} \left(\frac{1}{2} + \Delta \right) (\hat{v}_2^\dagger \hat{a}_l + \hat{a}_l^\dagger \hat{v}_2), \end{aligned} \quad (4)$$

where small terms have been neglected due to the photon flux per LO pulse in the range of $10^8 \sim 10^9$. Treating the strong LO beam as a classical field, we obtain $\hat{a}_l = |\beta| e^{i\theta_l}$, where $|\beta|$ represents the amplitude of LO, $|\beta|^2$ is the photon flux, and θ_l is the phase of LO beam. For convenience, we assume the BS and homodyne detector are in the ideal case with $\Delta = 0$ and $\eta_1 = \eta_2 = 1$, Eq. (4) can be rewritten as

$$\begin{aligned} \hat{N}_r = \hat{l}_3^\dagger \hat{l}_3 - \hat{l}_4^\dagger \hat{l}_4 = & \hat{a}_s^\dagger \hat{a}_l + \hat{a}_l^\dagger \hat{a}_s \\ = & |\beta| (\hat{a}_s^\dagger e^{i\theta_l} + \hat{a}_s e^{-i\theta_l}) = |\beta| \hat{X}_{\theta_l}, \end{aligned} \quad (5)$$

where \hat{X}_{θ_l} is the quadrature. The homodyne detector only needs to acquire the peak point for each detected signal pulse. After amplification by an amplifier with gain G , the peak value of the output voltage at the homodyne detector U_p is given by

$$U_p = G|\beta| \hat{X}_{\theta_l}, \quad (6)$$

and the quadrature of the signal field is linearly proportional to the peak value of the output voltage. The variance of the measured quantum noise can be expressed as

$$\sigma_{QS}^2 = G^2 |\beta|^2 \langle \Delta^2 \hat{X}_{\theta_l} \rangle, \quad (7)$$

where the variance $\langle \Delta^2 \hat{X}_{\theta_l} \rangle = \langle \Delta^2 \hat{X}_Q \rangle + \langle \Delta^2 \hat{X}_{QN} \rangle$ represents the initial variance of the quadrature of the measured quantum noise composed of two independent signals of vacuum fluctuation \hat{X}_Q and quantum side information \hat{X}_{QN} . When the input quantum state is a pure vacuum state, with $\langle \Delta^2 \hat{X}_Q \rangle = \frac{1}{2}$, the variance of the measured vacuum fluctuation is

$$\sigma_Q^2 = \frac{1}{2} G^2 |\beta|^2. \quad (8)$$

Hence, the variance σ_Q^2 has linearity dependence with the photon number per LO pulse $|\beta|^2$ with the slope $1/2G^2$. In the practical experiment, the power meter monitors the LO power. The relationship between the optical power P_{LO} of LO

and the photon number N_i is given by

$$P_{LO} = \frac{h\nu}{t_0} N_i, \quad (9)$$

where h is the Planck constant, ν is the optical wavelength, and t_0 is the duration of LO pulse. Based on Eqs. (8) and (9), the variance σ_Q^2 is also linear with the optical power P_{LO} . Due to the imperfections of the practical devices, the classical noise with variance σ_E^2 , such as electronic noise and thermal noise, will be introduced in the measurement results. The total variance of measured signal in the input vacuum state has a linear relationship with the optical power and can be expressed as

$$\sigma_t^2 = \sigma_Q^2 + \sigma_E^2 = a_g P_{LO} + c, \quad (10)$$

where $a_g = G^2 t_0 / 2h\nu$ and $c = \sigma_E^2$ are two constant parameters.

For the CV-SI-QRNG with phase-randomized LO, the finite precision of the ADC leads to discretization of the measurements with the precision of δ . The discretized version of the positive-operator-valued measure (POVM) element is given by $\hat{Q}_\delta^j = \int_{I_\delta^j} dq |q\rangle \langle q|$, where the I_δ^j are the half-open intervals $I_\delta^j = (j - \frac{\delta}{2}, j + \frac{\delta}{2}]$ with the bin index j . Specifically, Alice performs the coarse-gained quadrature operator \hat{Q}_δ on the input quantum state ρ_A , storing the discretized measurement outcomes q_j with a certain probability $p(q_j) = \text{Tr}[\rho_A \hat{Q}_\delta^j]$ in a classical register Q_δ . If the input state is a trusted vacuum state, $\rho_A = |0\rangle \langle 0|$, the extractable randomness per measurement is given by the min-entropy $H_{\min}(Q_\delta)_{|0\rangle}$. In the presence of source controlled by an eavesdropper, the input state may be correlated with the state of a malicious party Eve (E) and is mixed, $\rho_A = \text{Tr}_E[\rho_{AE}]$. The maximal number of extractable randomness is given by the conditional min-entropy $H_{\min}(Q_\delta|E)$. It has been demonstrated that Eve's best attack is to input the vacuum state with phase-randomized LO [33], i.e., $H_{\min}(Q_\delta|E) \geq H_{\min}(Q_\delta)_{|0\rangle}$. Assuming the variance of vacuum state is $\sigma_{|0\rangle}^2 = \frac{1}{2}$, the lower bound of $H_{\min}(Q_\delta|E)$ satisfies with [33]

$$H_{\min}(Q_\delta|E) \geq H_{\min}(Q_\delta)_{|0\rangle} = -\log_2 \text{erf}\left(\frac{\delta}{2}\right), \quad (11)$$

where δ denotes the measurement precision in vacuum units. Therefore, to bound of $H_{\min}(Q_\delta|E)$, the precision δ should be accurately estimated, which can be evaluated from the variance of measured vacuum fluctuation and sampling precision of ADC δ_{ADC} . Exploiting the linear relationship between the variance of measured vacuum fluctuation and the LO power on the homodyne detection, the variance σ_Q^2 can be calculated if one knows the LO power P_{LO} . As a result, a calibration procedure is performed before running the experiment of CV-SI-QRNG with phase-randomized LO. First, the signal and LO ports are both blocked, and the variance of classical noise is recorded. Then, only the signal port is blocked to provide a reference vacuum state input and the variances of the measured signal at different LO powers P_{LO} are measured to fit a calibration line. The intercept of the calibration line corresponds to the contribution of the classical noise to the overall variance, whereas the gradient a_g can be used to estimate the variance of vacuum fluctuation. In the process of generating

random numbers, the LO power P_{LO} can be calculated from power meter measurements and the corresponding variance of vacuum fluctuation can be obtained with $a_g P_{LO}$. In this case, the corresponding measurement precision in vacuum units is expressed as [33]

$$\delta = \frac{\delta_{ADC}}{\sqrt{2a_g P_{LO}}}. \quad (12)$$

Therefore, the lower bound of the extractable randomness can be evaluated with Eqs. (11) and (12). To accurately evaluate the conditional min-entropy $H_{\min}(Q_\delta|E)$, it is of importance to obtain the real power of LO and calibrate the real linear relationship between the variance of measured vacuum fluctuation and the LO power. However, the imperfect sampling device may influence the fitted calibration line, resulting in the linear relationship that deviates from the real value, which affects the evaluation of the conditional min-entropy $H_{\min}(Q_\delta|E)$. In the following, we will analyze the impacts of finite-sampling bandwidth, finite-sampling precision, and finite-size effect on the performances and security of CV-SI-QRNG with phase-randomized LO.

III. IMPACTS OF FINITE-SAMPLING BANDWIDTH

In the CV-SI-QRNG system, the analog output of the homodyne detector is sampled by an ADC with sampling frequency f_{samp} . Theoretically, it is usually assumed that the sampling device ADC is perfect with infinite-sampling bandwidth, i.e., the ADC can accurately sample the peak value of the output pulse. However, the sampling bandwidth of commercial ADC is finite, which may affect the acquisition of peak values and the performance of CV-SI-QRNG.

Generally, to ensure the peak values of all pulses are accurately sampled, the ADC usually oversample the electric pulses of homodyne detector [52–54], that is to say, ADC samples a large number of data points in each pulse period, as shown in Fig. 2. The time interval between sampling points is $t_s = 1/f_{\text{samp}}$. The clock of the pattern generator used to drive the laser is accurately synchronized with the sampling clock of the ADC for high relative stability. Once the maximal sampled point is determined, the resulting oversampled data are subsampled according to the determined point, taking one point for every laser pulse. For a practical homodyne detector, it is necessary to sample each pulse and integrate them together if the pulse duration of the incident light is longer than the response time of detection device, where the quadrature value of input optical field is proportional to the area under each output electric pulse [52]. In order to reduce the system complexity and challenges for data processing, one may assume that the pulse duration of the optical pulse is much smaller than the response time of detection device. Notably, to guarantee the preferable detection response, the bandwidth of the available homodyne detector is much higher than the laser repetition rate in the practical QRNG systems [33]. In this case, the homodyne detector can be assumed to operate in the linear region, and the quadrature value of the input optical field is linearly proportional to the peak value of the homodyne detector [53].

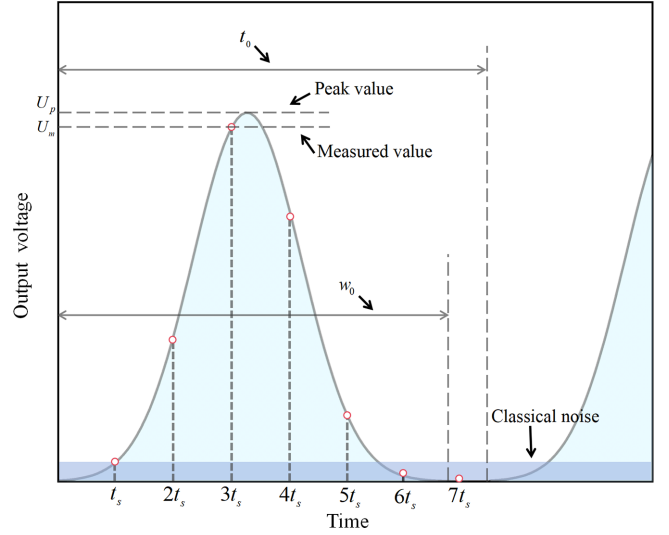


FIG. 2. The sampling process of the output signal pulse from the homodyne detector in time domain. Red circles denote the sampled points; t_s : sampling period; t_0 : pulse period; w_0 : pulse width; U_p : peak value; U_m : maximal measured value.

Without loss of the generality, the shape of output pulse signal of homodyne detector is assumed to be Gaussian with the following shape function [55,56]:

$$r(t) = U_p e^{-\frac{(t-\mu)^2}{2\sigma^2}}, \quad (13)$$

where U_p is the peak value, μ and σ^2 denote the mean value and variance of the Gaussian pulse, respectively. For simplicity, we choose the mean value $\mu = w_0/2$ and variance $\sigma^2 = (w_0/8)^2$, where w_0 is the pulse width. The relationship between the pulse width w_0 and pulse period $t_0 = 1/f_{\text{rep}}$ can be given by $R_{\text{duty}} = w_0/t_0$, where R_{duty} denotes the duty cycle of pulse and f_{rep} is the repetition rate of laser pulse. In the following analysis, the value of R_{duty} is assumed to be 50%. However, for an ADC with finite-sampling bandwidth, the maximal measured value will inevitably deviate from the peak value, as shown in Fig. 2. Moreover, the clock jitter also prevents accurate sampling to the maximum value. In this case, the difference between the maximal measured value U_m and peak value U_p can be expressed as

$$\Delta U = U_p - U_m = U_p \left(1 - e^{-\frac{(\Delta t)^2}{w_0^2/32}}\right), \quad (14)$$

with $\Delta t \in [-t_s/2, t_s/2]$. Based on Eq. (14), the sampling error reaches the maximal value when $\Delta t = -t_s/2(t_s/2)$ and can be denoted as

$$\Delta U = U_p \left(1 - e^{-\frac{32f_{\text{rep}}^2}{f_{\text{samp}}^2}}\right). \quad (15)$$

In order to highlight the effect of finite-sampling bandwidth, the difference between U_m and U_p is taken to the maximum value at each sampling bandwidth in the following analysis. Thus, the ratio between the measured value U_m and peak value U_p can be given by

$$k = \frac{U_m}{U_p} \in \left[\exp\left(-\frac{32f_{\text{rep}}^2}{f_{\text{samp}}^2}\right), 1 \right]. \quad (16)$$

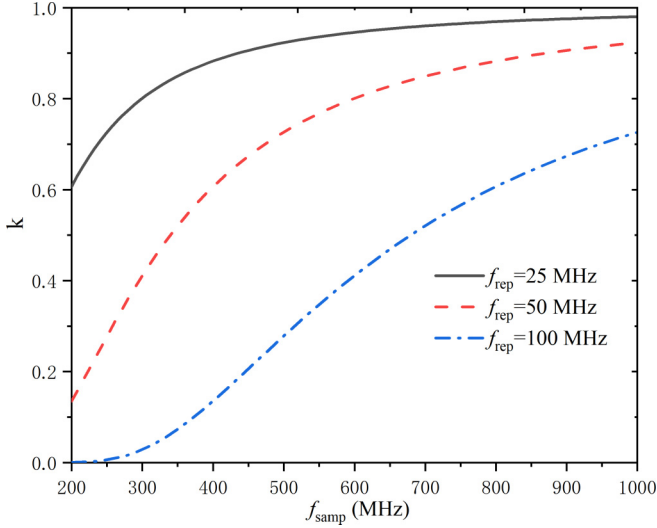


FIG. 3. The ratio k between the measured value U_m and peak value U_p as a function of the sampling bandwidth f_{samp} at different repetition rates f_{rep} .

The value of k depends on both the sampling bandwidth f_{samp} and the repetition rate f_{rep} . The larger the ratio of sampling bandwidth to repetition rate, the closer the value of k is to 1, i.e., the smaller the sampling error. Figure 3 shows the effect of sampling bandwidth on the value of k at different repetition rates. At a fixed repetition rate f_{rep} , k increases with the sampling bandwidth f_{samp} . Compared to different repetition rates, the high-speed CV-SI-QRNG system is more sensitive to the finite-sampling bandwidth.

In the phase-randomized CV-SI-QRNG system, it is essential to perform a calibration procedure to obtain the linear relationship between the LO power and variance of measured vacuum fluctuation. Actually, the measurement results of homodyne detector can be divided into two parts, the maximal measured value and the classical noise. The maximal measured value U_m could be deemed as $U_m = kU_p$, while the classical noise would not be changed. Based on Eqs. (6), (8), and (16), the total variance of measured signal in the input vacuum state can be given by

$$\sigma_t^2 = k^2 \sigma_Q^2 + \sigma_E^2 = \frac{1}{2} k^2 G^2 |\beta|^2 + \sigma_E^2, \quad (17)$$

and the lower bound of $H_{\min}(Q_\delta|E)$ can be rewritten as

$$H_{\min}(Q_\delta|E) = -\log_2 \text{erf} \left(\frac{\delta_{\text{ADC}}}{2G\beta \exp \left(-\frac{32f_{\text{rep}}^2}{f_{\text{samp}}^2} \right)} \right). \quad (18)$$

As shown in Eq. (17), the total variance σ_t^2 is affected by the value of k associated with the sampling bandwidth. Because the measured value U_m deviates from the peak value U_p , the real linear relationship will be changed compared to the ideal case, and thus the gradient of the calibration line will be affected. According to Eqs. (11) and (12), the lower bound of $H_{\min}(Q_\delta|E)$ is determined by the measurement precision in vacuum units, which is related to the gradient of the calibration line. Hence, the calculated extractable randomness $H_{\min}(Q_\delta|E)$ changes with the value of gradient.

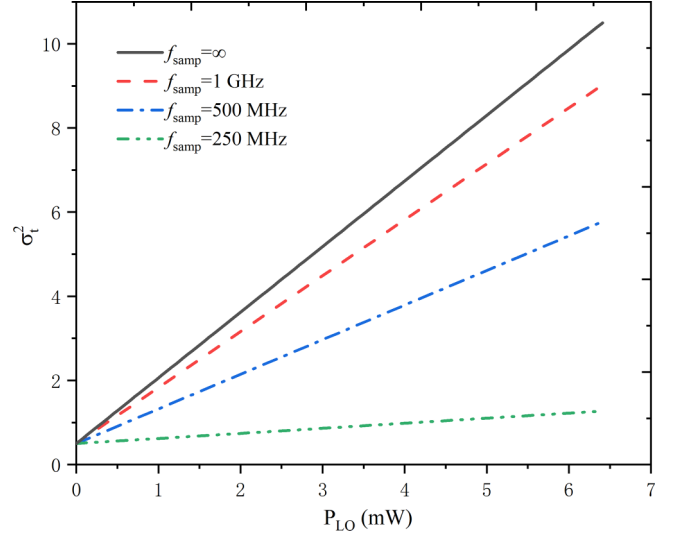


FIG. 4. Calibration linear relationship between the variance of the homodyne detection measurements and the LO power under different sampling bandwidths. The system repetition rate is set as $f_{\text{rep}} = 50$ MHz.

In addition, the sampling clock of the sampling device is one of the important factors to determine the accuracy of the pulse peak value. However, the imperfect sampling clock with clock jitter would cause the maximum measured value to deviate from the peak value, similar to the finite-sampling bandwidth effect. Due to the presence of clock jitter Δt_j , the sampling time of the peak value will deviate from Δt_j , so that the actual maximum measured value becomes $U_m = r(t \pm \Delta t_j)$. In this case, the sampling error can be expressed as

$$\Delta U = U_p - U_m = U_p \left(1 - e^{-\frac{(\Delta t_j)^2}{w_0^2/32}} \right). \quad (19)$$

Therefore, the sampling error due to the finite-sampling bandwidth effect can also be seen as an effect of clock jitter. The analytical methods and theoretical models for the impact of finite-sampling bandwidth on the calculated condition min-entropy are also applicable to clock jitter.

To demonstrate the influence of the finite-sampling bandwidth effect on the CV-SI-QRNG, we perform some numerical simulations. Without loss of generality, the center wavelength of LO is assumed to be 1550 nm, and the other parameters used for simulations are set as $\hbar = 6.626 \times 10^{-34}$, $\nu = 193.5$ THz, $G = \sqrt{2} \times 10^{-7}$ V/A, $\sigma_E^2 = 0.5$, $N = 10$, and $n = 8$. Figure 4 shows the calibration linear relationship between the variance of the homodyne detection measurements and the LO power under different sampling bandwidths, in which the LO is pulsed at 50 MHz with a duty cycle of 50%. We find that the gradient of calibration line is strongly affected by the finite-sampling bandwidth effect and decreases with the sampling bandwidth.

Then we further simulate the influence of finite-sampling bandwidth on the calculated extractable randomness. Figure 5(a) shows the simulation results for the calculated extractable randomness $H_{\min}(Q_\delta|E)$ as a function of sampling

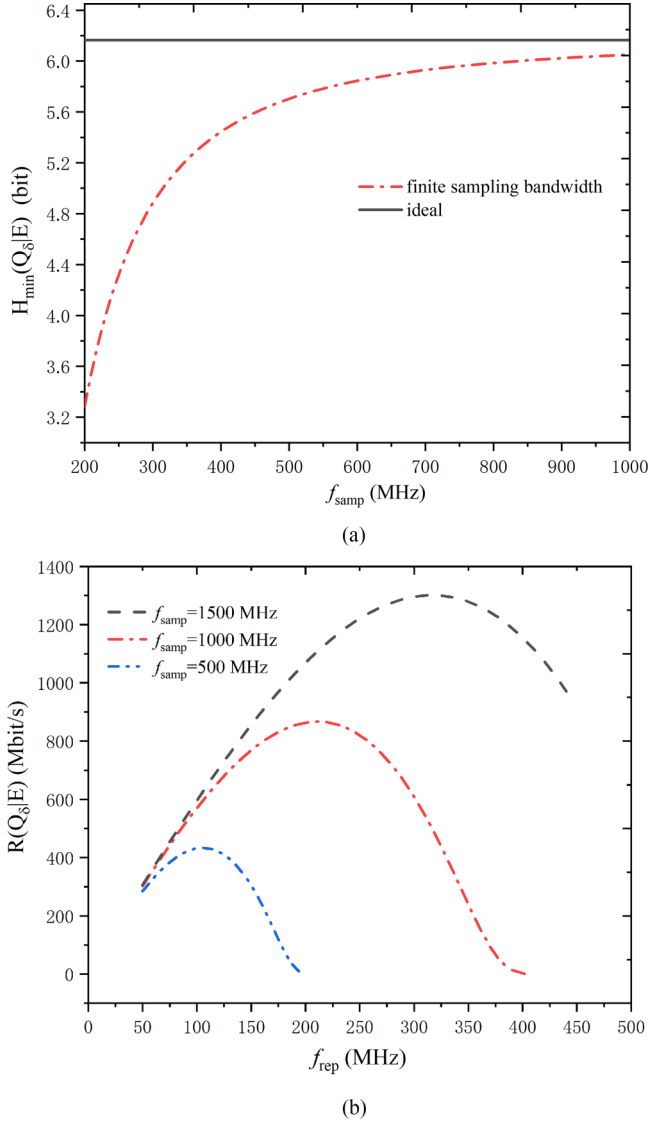


FIG. 5. The extractable randomness of CV-SI-QRNG with finite-sampling bandwidth effects. The photon number $|\beta|^2$ is set as 5×10^8 . (a) Simulation results for the calculated extractable randomness $H_{\min}(Q_\delta|E)$ as a function of sampling bandwidth f_{samp} . The system repetition rate is set as $f_{\text{rep}} = 50$ MHz. (b) Simulation results for the secure generation rate $R(Q_\delta|E)$ as a function of system repetition rate f_{rep} at different sampling bandwidths.

bandwidth f_{samp} . The red dotted line represents the results $H_{\min}(Q_\delta|E)$ under finite-sampling bandwidth effect, while the black solid line is the ideal result under infinite-sampling bandwidth. As shown in Fig. 5(a), the calculated $H_{\min}(Q_\delta|E)$ increases with the sampling bandwidth. Compared with the ideal case, the calculated $H_{\min}(Q_\delta|E)$ considering the finite-sampling bandwidth has a very slight deviation even with a sampling bandwidth of ADC up to 1000 GHz. In the practical experiment, although the finite-sampling bandwidth effect does not cause the calculated $H_{\min}(Q_\delta|E)$ to be overestimated affecting the security of generated random numbers, it would reduce the amount of extractable randomness from the raw data, which degrades the performance of CV-SI-QRNG. Furthermore, based on Eq. (11), the secure generation rate

$R(Q_\delta|E)$ can be given by

$$R(Q_\delta|E) = H_{\min}(Q_\delta|E)f_{\text{rep}}. \quad (20)$$

The relationships between the secure generation rate $R(Q_\delta|E)$ and system repetition rate f_{rep} under different sampling bandwidths are shown in Fig. 5(b). The secure generation rate of CV-SI-QRNG at different sampling bandwidths reaches a maximal value at a certain repetition rate. The generation rate does not always increase with the repetition rate. In other words, when the sampling bandwidth is finite, increasing the repetition rate is not always beneficial to improving the performance of CV-SI-QRNG. Therefore, due to the finite-sampling bandwidth effect, the repetition rate of laser should be selected to a suitable value for high-speed CV-SI-QRNG system.

We have demonstrated that the finite-sampling bandwidth influences the fitted calibration line and the evaluation of extractable randomness. To eliminate the finite-sampling bandwidth effect and improve the performance of CV-SI-QRNG, some countermeasures can be taken with reference to the countermeasures in continuous-variable quantum key distribution [55,57,58]. In the phase-randomized CV-SI-QRNG, the variance of measured vacuum fluctuation can be estimated from the LO power measured by a power meter. Although the shift of the pulse signal does not change the measured LO power, it still affects the measurement results of the variance, which results in a mismatch between the measured variance and the corresponding LO power. One method is to replace the power meter with a positive intrinsic-negative (PIN) detector and connect another ADC that is identical to the ADC at the end of the homodyne detector. The same electronic circuits trigger these two ADCs. In this case, the measured LO power and variance of measured signal are also matched, even if the shift of the pulse signal in the time domain causes a deviation in the measured values of the two ADCs. Another approach is to find out the peak value of the output voltage from homodyne detector using postprocessing methods, such as the peak-valley seeking combined with Gaussian postselection method [58], and the dynamic delay adjusting module combined with a statistical power feedback-control algorithm [57].

IV. IMPACTS OF FINITE-SAMPLING PRECISION

In the practical phase-randomized CV-SI-QRNG, the homodyne measurement is coarse grained with imperfect characteristics, which may influence the calculation of measured signal variance, compromising the security of extracted random numbers. The output pulse signal of homodyne detector is sampled by an ADC, which must be imperfect with finite-sampling range $[-N + \delta_{\text{ADC}}, N - 3\delta_{\text{ADC}}/2]$ and sampling resolution n , leading to finite-sampling precision $\delta_{\text{ADC}} = N/2^{n-1}$. Without considering the finite-sampling bandwidth effect, we assume that the peak value of output pulse can be perfectly measured. The peak value is a continuous variable, denoted as a , following probability density distribution $p(a)$. Then, the ADC digitizes the continuous data a into a_i over 2^n bins following probability distribution $p(a_i)$. Thereby, the interval between every adjacent digitized results

a_i is δ_{ADC} and the digitized results a_i can be expressed as

$$a_i = \begin{cases} -N, & a < -N + \frac{\delta_{\text{ADC}}}{2}, i = i_{\min} \\ -N + (2^{n-1} + i)\delta_{\text{ADC}}, & -N + \frac{(2^n + 2i - 1)\delta_{\text{ADC}}}{2} \leq a \\ -N + \frac{(2^n + 2i + 1)\delta_{\text{ADC}}}{2}, & i_{\min} < i < i_{\max} \\ N - \delta_{\text{ADC}}, & a \geq N - \frac{3\delta_{\text{ADC}}}{2}, i = i_{\max} \end{cases} \quad (21)$$

where $i \in \{-2^{n-1}, \dots, 2^{n-1} - 1\}$. The same digitized result a_i represents many continuous outputs a , as long as a is in the corresponding digitized interval. Consequently, during the sampling process of the ADC, partial information about the continuous variable a is lost. Based on the digitized results a_i , one may not get the proportional quadrature of the input state correctly.

To estimate the lower bound of extractable randomness, the calibration linear relationship between the variance of the homodyne detection measurement and the LO power should be obtained in the CV-SI-QRNG, where the input signal is in vacuum state. In the ideal digitization with infinite-sampling precision, the total variance σ_t^2 of the homodyne detection measurement can be perfectly calculated, and the ideal total variance is equal to the result calculated in Eq. (10). However, the ADC has finite-sampling precision. Each output a of the homodyne detection is upper and lower bounded by its digitization interval, i.e., $a_i - \delta_{\text{ADC}}/2 \leq a \leq a_i + \delta_{\text{ADC}}/2$. The total variance σ_t^2 calculated from the discrete results a_i may be overestimated or underestimated, which leaves a security loophole. For a relatively large sampling range, the probability that a is outside the sampling range is negligible. Considering finite-sampling precision effect, the total variance σ_t^2 has an upper and lower bound. The upper bound $\bar{\sigma}_t^2$ and lower bound $\underline{\sigma}_t^2$ can be expressed as

$$\begin{aligned} \bar{\sigma}_t^2 &= p_{\text{dis}}(a_{i_{\min}})(a_{\min} - \bar{a})^2 + p_{\text{dis}}(a_{i_{\min}})(a_{\max} - \bar{a})^2 \\ &+ \sum_{i=i_{\min}+1}^0 p_{\text{dis}}(a_i) \left(a_i - \bar{a} - \frac{1}{2}\delta_{\text{ADC}} \right)^2 \\ &+ \sum_{i=1}^{i=i_{\max}+1} p_{\text{dis}}(a_i) \left(a_i - \bar{a} + \frac{1}{2}\delta_{\text{ADC}} \right)^2, \end{aligned} \quad (22)$$

$$\begin{aligned} \underline{\sigma}_t^2 &= p_{\text{dis}}(a_{i_{\min}})(a_{\min} - \bar{a})^2 + p_{\text{dis}}(a_{i_{\min}})(a_{\max} - \bar{a})^2 \\ &+ \sum_{i=i_{\min}+1}^0 p_{\text{dis}}(a_i) \left(a_i - \bar{a} + \frac{1}{2}\delta_{\text{ADC}} \right)^2 \\ &+ \sum_{i=1}^{i=i_{\max}+1} p_{\text{dis}}(a_i) \left(a_i - \bar{a} - \frac{1}{2}\delta_{\text{ADC}} \right)^2, \end{aligned} \quad (23)$$

where $p_{\text{dis}}(a_i)$ denotes the probability of a_i and can be calculated based on the Gaussian distribution, \bar{a} is the mean value of measurement result, a_{\min} and a_{\max} are the minimal and maximum values of the sampling range, respectively. As shown in Eqs. (22) and (23), the upper bound $\bar{\sigma}_t^2$ is estimated from the boundary of the discrete interval farther from 0 point, while the lower bound $\underline{\sigma}_t^2$ is estimated from the boundary of the discrete interval closer from 0 point.

The finite-sampling precision of the ADC influences the estimation of total variance σ_t^2 , which further affects the

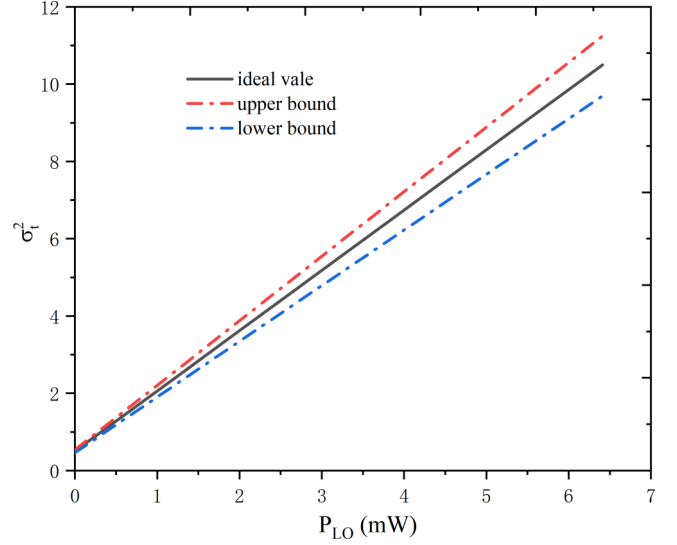


FIG. 6. Calibration linear relationship between the variance of the homodyne detection measurements and the LO power taking into the finite-sampling precision effect. The black solid line represents the expected ideal value of total variance σ_t^2 . The red (upper) dotted line and blue (bottom) dotted line represent the upper and lower bounds of total variance σ_t^2 , respectively. Parameters are set as $h = 6.626 \times 10^{-34}$, $\nu = 193.5$ THz, $G = \sqrt{2} \times 10^{-7}$ V/A, $\sigma_E^2 = 0.5$, $f_{\text{rep}} = 50$ MHz, $N = 10$, and $n = 8$.

calibration line used to estimate the variance of measured vacuum fluctuation. Figure 6 shows the influence of finite-sampling precision on the calibration linear relationship between the variance of the homodyne detection measurements and the LO power. The black solid line represents the expected ideal value of total variance, and the red (upper) dotted line and blue (bottom) dotted line represent the upper and lower bounds of total variance based on digitized measurement results, respectively. It is clear that the difference between the upper and lower bounds of measured total variance and the ideal measured total variance increases with LO power. The gradient a_g of the calibration line would be overestimated or underestimated. According to Eqs. (11) and (12), we obtain that an overestimation of the gradient a_g would cause the calculated extractable randomness $H_{\min}(Q_\delta|E)$ to be overestimated, whereas an underestimation of the gradient a_g would cause the calculated extractable randomness $H_{\min}(Q_\delta|E)$ to be underestimated.

The sampling range and sampling resolution determine the sampling precision of the ADC. If the sampling resolution is fixed, the sampling precision increases with the sampling resolution. To further investigate the impacts of sampling precision on phase-randomized CV-SI-QRNG system, we simulate the influence of sampling resolution n on the total variance σ_t^2 and calculated extractable randomness $H_{\min}(Q_\delta|E)$. As shown in Fig. 7(a), the upper and lower bounds of the total variance σ_t^2 are closer to the expected ideal value as the increase of sampling resolution n . It means that the influence of finite-sampling precision on the estimated variance σ_t^2 based on digitized measurement results becomes smaller with higher sampling precision. Figure 7(b) is the simulation result for the calculated extractable

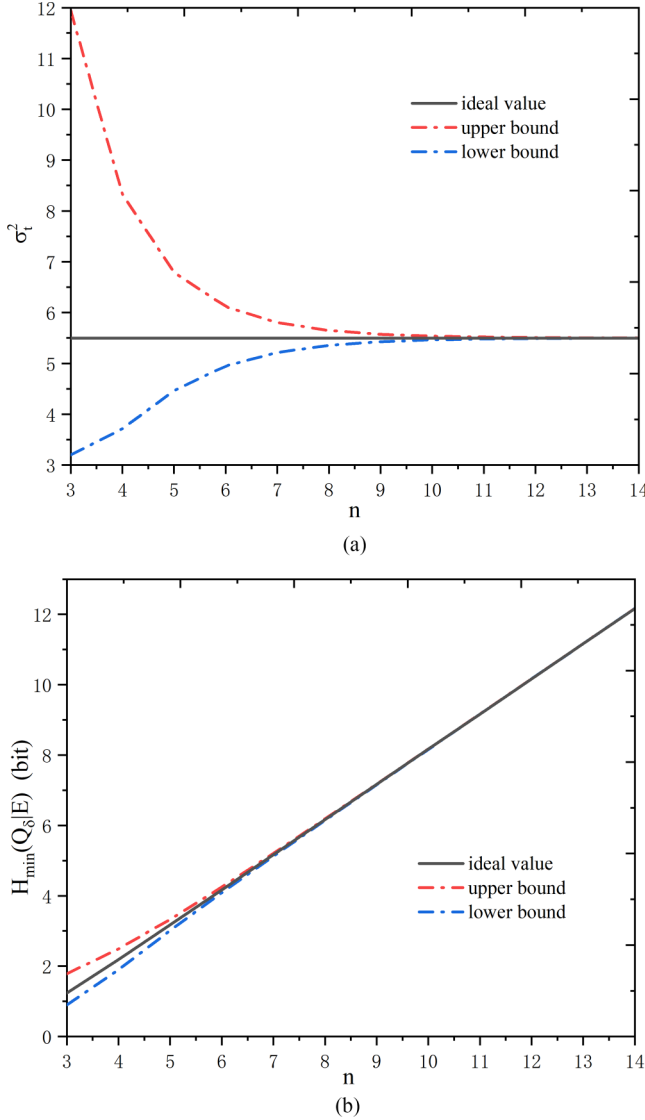


FIG. 7. Parameters are set as $h = 6.626 \times 10^{-34}$, $\nu = 193.5$ THz, $G = \sqrt{2} \times 10^{-7}$ V/A, $\sigma_E^2 = 0.5$, $f_{\text{rep}} = 50$ MHz, $|\beta|^2 = 5 \times 10^8$, and $N = 10$. (a) Simulation results for the variance σ_t^2 of the homodyne detection measurements based on digitized measurement results as a function of sampling resolution n . The black solid line represents the expected ideal value of total variance σ_t^2 . The red (upper) dotted line and blue (bottom) dotted line represent the upper and lower bounds of total variance σ_t^2 , respectively. (b) Simulation results for the calculated extractable randomness $H_{\min}(Q_\delta|E)$ as a function of sampling resolution n . The black solid line represents the ideal value of $H_{\min}(Q_\delta|E)$. The red (upper) dotted line and blue (bottom) dotted line represent the upper and lower bounds of $H_{\min}(Q_\delta|E)$, respectively.

randomness $H_{\min}(Q_\delta|E)$ as a function of sampling resolution n . As the sampling precision becomes higher, the impact of finite-sampling precision on calculated $H_{\min}(Q_\delta|E)$ becomes smaller. At relatively small n , i.e., relatively low sampling precision, the value of $H_{\min}(Q_\delta|E)$ would be overestimated or underestimated. Therefore, in a real experiment system, finite-sampling precision of the ADC not only may cause the evaluated extractable randomness to be underestimated,

reducing the performance of CV-SI-QRNG, but also compromise the evaluated extractable randomness, threatening the security of CV-SI-QRNG. To prevent security loopholes associated with finite-sampling precision, the sampling resolution n should use a relatively large value to provide high sampling precision. In addition, the security of practical CV-SI-QRNG could be guaranteed by exploiting the lower bound of total variance to estimate the extractable randomness, but it would reduce the random-number generation rate.

V. IMPACTS OF FINITE-SIZE EFFECT

In fact, the CV-SI-QRNG system can run for only finite time during the calibration process. However, the precise parameters' estimation of measured variance of the homodyne detection requires infinite-size data, which is used to calculate the extractable randomness. Finite data size will lead to statistical fluctuations of the estimated parameters [45–51], which may cause the calculated extractable randomness to be overestimated or underestimated, leaving security loopholes. Thus, it is important to estimate the parameters in the finite-size regime for the final random-number security. Here, we only consider the influences of finite-size effect on the estimation of total variance σ_t^2 as well as the calculated $H_{\min}(Q_\delta|E)$.

With the input vacuum state, the total variance σ_t^2 of the homodyne detection measurements consists of vacuum fluctuation σ_Q^2 and electronic noise σ_E^2 . In practice, the total variance σ_t^2 is calculated from the sampled measurement results a_i of homodyne detection, where the maximum-likelihood estimator $\hat{\sigma}_t^2$ is known for the normal linear model [45]

$$\hat{\sigma}_t^2 = \frac{1}{m} \sum_{i=1}^m (a_i - \bar{a})^2, \quad (24)$$

where m is the data length used to estimate the total variance and \bar{a} is the mean value assumed to be 0. Moreover, $\hat{\sigma}_t^2$ is independent estimator with the following distribution:

$$\frac{m\hat{\sigma}_t^2}{\sigma_t^2} \sim \chi^2(m-1), \quad (25)$$

where $\hat{\sigma}_t^2$ denotes the experimental value and σ_t^2 denotes the expected ideal value. The χ^2 distribution converges to a normal distribution in the limit large of m . Hence, the confidence intervals of $\hat{\sigma}_t^2$ with confidence probability ε_{PE} ,

$$\sigma_t^2 \in [\hat{\sigma}_t^2 - \Delta\sigma_t^2, \hat{\sigma}_t^2 + \Delta\sigma_t^2], \quad (26)$$

where

$$\Delta\sigma_t^2 = z_{\varepsilon_{\text{PE}}/2} \frac{\hat{\sigma}_t^2 \sqrt{2}}{\sqrt{m}}. \quad (27)$$

ε_{PE} represents the probability that the estimated parameter outside the confidence interval $z_{\varepsilon_{\text{PE}}/2}$ is a coefficient such that $1 - \text{erf}(z_{\varepsilon_{\text{PE}}/2}/\sqrt{2}) = \varepsilon_{\text{PE}}/2$ and $\text{erf}(x)$ is the error function defined as

$$\text{erf}(x) = \frac{2}{\sqrt{\pi}} \int_0^x e^{-t^2} dt. \quad (28)$$

In order to ensure the security of CV-SI-QRNG, one should consider the most pessimistic case that the lower bound of extractable randomness may be underestimated. Therefore,

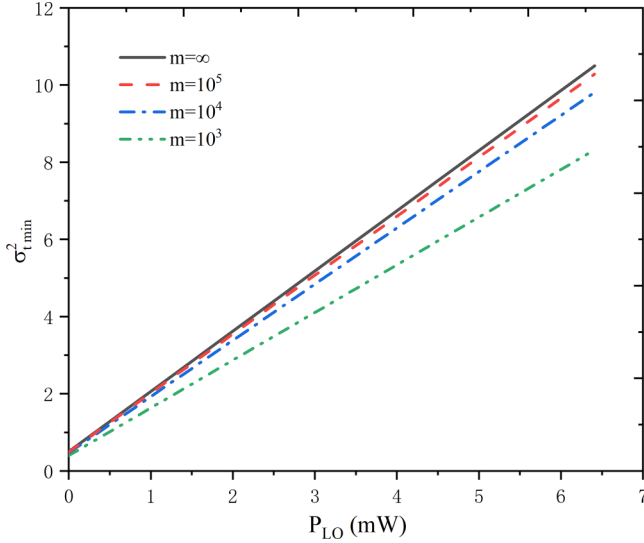


FIG. 8. Calibration linear relationship between the variance of the homodyne detection measurements and the LO power considering finite-size effect, which from bottom to top line correspond to $m = 10^3$, 10^4 , 10^5 and ideal value. Parameters are set as $h = 6.626 \times 10^{-34}$, $\nu = 193.5$ THz, $G = \sqrt{2} \times 10^{-7}$ V/A, $\sigma_E^2 = 0.5$, $f_{\text{rep}} = 50$ MHz, $N = 10$, $n = 8$, and $\varepsilon_{\text{PE}} = 10^{-10}$.

we need to make sure the true value of σ_t^2 is underestimated and can be calculated with

$$\sigma_{t\text{min}}^2 \approx \hat{\sigma}_t^2 - \Delta\sigma_t^2 = \hat{\sigma}_t^2 - z_{\varepsilon_{\text{PE}}/2} \frac{\hat{\sigma}_t^2 \sqrt{2}}{\sqrt{m}}. \quad (29)$$

To demonstrate the influence of finite-size effect on the security of CV-SI-QRNG, we present and discuss the results of some numerical simulations. The infinite-size condition corresponds to the data length $m \rightarrow \infty$. Figure 8 shows the impacts of different data sizes on the calibration linear relationship between the variance of the homodyne detection measurements and the LO power considering finite-size effect. We can find that the data length significantly impacts the estimated total variance. The calibration line is closer to the ideal one with a longer data length. Besides, as LO power increases, the difference between ideal total variance and total variance with finite-size effect increases.

Deviations from the calibration line ultimately affect the evaluation of extractable randomness. In Fig. 9, we investigate the impacts of finite-size effect on the calculated $H_{\min}(Q_\delta|E)$. The relationship between extractable randomness $H_{\min}(Q_\delta|E)$ and data length m is shown in Fig. 9(a). The red dotted line is the extractable randomness with finite-size effect, and the blue solid line is the ideal extractable randomness in infinite-size case. The gap between the ideal extractable randomness $H_{\min}(Q_\delta|E)$ and the $H_{\min}(Q_\delta|E)$ calculated by considering the finite-size effect decreases with the increase of data length m . Moreover, the finite-size effect remarkably influences the extractable randomness when data length reduces under 10^4 . Nevertheless, when data length is larger than 10^6 , the finite-size line is very close to the ideal line, which reveals the finite-size effect has a negligible impact on extractable randomness in this case. Therefore, the length of data used to

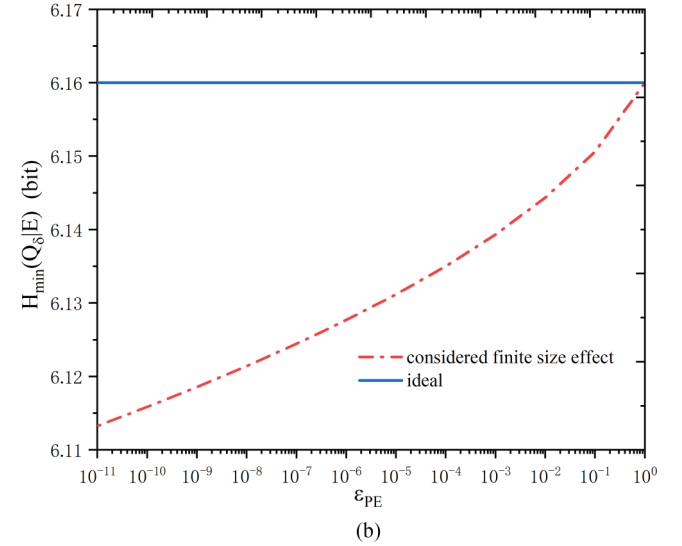
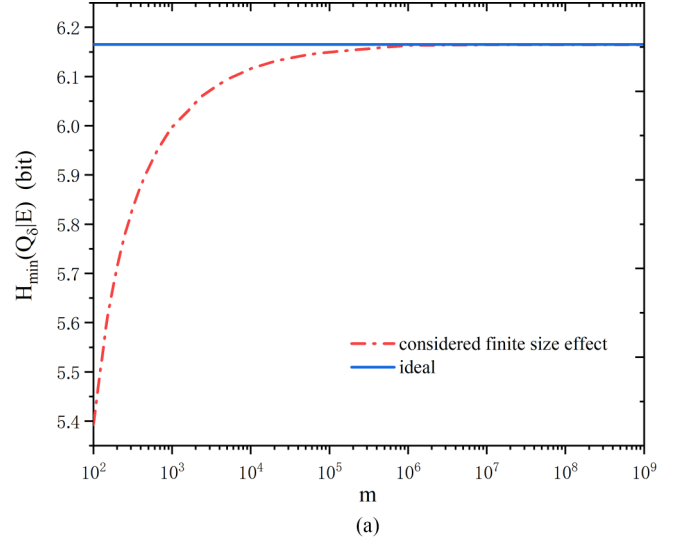


FIG. 9. The impacts of finite-size effect on the calculated extractable randomness $H_{\min}(Q_\delta|E)$. Parameters are set as $h = 6.626 \times 10^{-34}$, $\nu = 193.5$ THz, $G = \sqrt{2} \times 10^{-7}$ V/A, $\sigma_E^2 = 0.5$, $f_{\text{rep}} = 50$ MHz, $|\beta|^2 = 5 \times 10^8$, $N = 10$, and $n = 8$. (a) Simulation results for calculated extractable randomness $H_{\min}(Q_\delta|E)$ as a function of data length m with confidence probability $\varepsilon_{\text{PE}} = 10^{-10}$. (b) Simulation results for the calculated extractable randomness $H_{\min}(Q_\delta|E)$ as a function of confidence probability ε_{PE} with data length $m = 10^4$.

estimate the total variance should be chosen as an appropriate value to reduce the influence of finite-size effect, obtain enough extractable randomness, and use fewer computing resources. Additionally, the parameter of confidence probability ε_{PE} has an impact on the calculated $H_{\min}(Q_\delta|E)$, as shown in Fig. 9(b). The curve of $H_{\min}(Q_\delta|E)$ considering finite-size effect becomes more smoother as confidence probability ε_{PE} increases. When $\varepsilon_{\text{PE}} = 1$, the finite-size effect on $H_{\min}(Q_\delta|E)$ disappears since the estimation for confidence interval of variance converges toward its ideal value. In practice, confidence probability can be regarded as a security parameter to satisfy the security requirements of the CV-SI-QRNG systems.

VI. CONCLUSION

In conclusion, we have pointed out and evaluated the influence of imperfect sampling devices on the phase-randomized CV-SI-QRNG system, including the finite-sampling bandwidth, finite-sampling precision, and finite-size effect. Moreover, we also provide methods to improve the performance and security of CV-SI-QRNG in practical applications. It is of great importance to accurately estimate the calibration linear relationship between the variance of the homodyne detection measurements and the LO power for the calculation of extractable randomness. When disturbances occur on the pulse positions or the synchronizing system, the ADC cannot sample the peak value of the output signal due to the finite-sampling bandwidth effect. This leads to the estimated gradient of calibration line deviating from the ideal value, which reduces the extractable randomness and performance of CV-SI-QRNG system. Furthermore, the random-number generation rate will achieve a maximal value but not always increase with the system repetition rate. To solve the impacts of finite-sampling bandwidth effect, one can refer to methods in continuous-variable quantum key distribution that use a double-sampling system or the postprocessing algorithm for finding peak values.

By analyzing the finite-sampling precision effect, we find that the gradient of the calibration line will be overestimated or underestimated. The overestimated gradient leads to an overestimation of the calculated extractable randomness, which compromises the security of CV-SI-QRNG system, whereas the underestimated gradient leads to an underestimation of the calculated extractable randomness, which reduces the performance of CV-SI-QRNG. To prevent security loopholes associated with finite-sampling precision, the

sampling resolution n should use a relatively large value to provide high sampling precision, or the lower bound of total variance should be used to calculate the lower bound of extractable randomness.

Finally, we demonstrate the influences of finite-size effect on the CV-SI-QRNG. Simulation results show that the finite-size effect leads to statistical fluctuations of estimated total variance of homodyne detection measurements and influences the evaluation of extractable randomness. With the increased data length and confidence probability, the calculated extractable randomness is closer to the ideal value. Therefore, we should consider the finite-size effect in practical CV-SI-QRNG systems, especially for small data length and confidence probability. In addition, choosing an appropriate value of data length helps to reduce the influence of finite-size effect. Compared to previous works [29–32], our work investigates the effects of practical imperfections on the calculated extractable randomness, which has not been considered before, and further improves the practical security and robustness of SI-QRNG. Our work highlights the influences of imperfect sampling devices on the performance and security of phase-randomized CV-SI-QRNG system and provides corresponding countermeasures to prevent information leakages and improve its performance.

ACKNOWLEDGMENTS

This work was supported by National Natural Science Foundation of China (Grants No. 61901525, No. 61972413, and No. 62002385), National Key R&D Program of China (Grant No. 2021YFB3100100).

-
- [1] H.-L. Yin, Y. Fu, C.-L. Li, C.-X. Weng, B.-H. Li, J. Gu, Y.-S. Lu, S. Huang, and Z.-B. Chen, Experimental quantum secure network with digital signatures and encryption, *Natl. Sci. Rev.* **10**, nwac228 (2023).
 - [2] L. Zhou, J. Lin, Y.-M. Xie, Y.-S. Lu, Y. Jing, H.-L. Yin, and Z. Yuan, Experimental quantum communication overcomes the rate-loss limit without global phase tracking, *Phys. Rev. Lett.* **130**, 250801 (2023).
 - [3] X.-Y. Cao, B.-H. Li, Y. Wang, Y. Fu, H.-L. Yin, and Z.-B. Chen, Experimental quantum e-commerce, *Sci. Adv.* **10**, eadk3258 (2024).
 - [4] J.-P. Chen, C. Zhang, Y. Liu, C. Jiang, D.-F. Zhao, W.-J. Zhang, F.-X. Chen, H. Li, L.-X. You, Z. Wang, Y. Chen, X.-B. Wang, Q. Zhang, and J.-W. Pan, Quantum key distribution over 658 km fiber with distributed vibration sensing, *Phys. Rev. Lett.* **128**, 180502 (2022).
 - [5] W.-X. Xie, G.-J. Fan-Yuan, Z.-H. Wang, F.-Y. Lu, J.-X. Li, S. Wang, Z.-Q. Yin, W. Chen, D.-Y. He, G.-C. Guo, and Z.-F. Han, Higher key rate in asymmetric quantum-classical integrated measurement-device-independent quantum-key-distribution systems, *Phys. Rev. Appl.* **20**, 054042 (2023).
 - [6] F.-Y. Lu, Z.-H. Wang, V. Zapatero, J.-L. Chen, S. Wang, Z.-Q. Yin, M. Curty, D.-Y. He, R. Wang, W. Chen, G.-J. Fan-Yuan, G.-C. Guo, and Z.-F. Han, Experimental demonstration of fully passive quantum key distribution, *Phys. Rev. Lett.* **131**, 110802 (2023).
 - [7] S. Wang, Z.-Q. Yin, D.-Y. He, W. Chen, R.-Q. Wang, P. Ye, Y. Zhou, G.-J. Fan-Yuan, F.-X. Wang, Y.-G. Chen, Weiland Zhu, P. V. Morozov, A. V. Divochiy, Z. Zhou, G.-C. Guo, and Z.-F. Han, Twin-field quantum key distribution over 830-km fibre, *Nat. Photonics* **16**, 154 (2022).
 - [8] S.-F. Shao, X.-Y. Cao, Y.-M. Xie, J. Gu, W.-B. Liu, Y. Fu, H.-L. Yin, and Z.-B. Chen, Phase-matching quantum key distribution without intensity modulation, *Phys. Rev. Appl.* **20**, 024046 (2023).
 - [9] X. Ma, X. Yuan, Z. Cao, B. Qi, and Z. Zhang, Quantum random number generation, *npj Quantum Inf.* **2**, 16021 (2016).
 - [10] M. Herrero-Collantes and J. C. Garcia-Escartin, Quantum random number generators, *Rev. Mod. Phys.* **89**, 015004 (2017).
 - [11] M. Ren, E. Wu, Y. Liang, Y. Jian, G. Wu, and H. Zeng, Quantum random-number generator based on a photon-number-resolving detector, *Phys. Rev. A* **83**, 023820 (2011).
 - [12] B. Qi, Y.-M. Chi, H.-K. Lo, and L. Qian, High-speed quantum random number generation by measuring phase noise of a single-mode laser, *Opt. Lett.* **35**, 312 (2010).

- [13] H. Guo, W. Tang, Y. Liu, and W. Wei, Truly random number generation based on measurement of phase noise of a laser, *Phys. Rev. E* **81**, 051137 (2010).
- [14] W. Wei, G. Xie, A. Dang, and H. Guo, High-speed and bias-free optical random number generator, *IEEE Photonics Technol. Lett.* **24**, 437 (2011).
- [15] Y. Li, Y. Fei, W. Wang, X. Meng, H. Wang, Q. Duan, and Z. Ma, Analysis of the effects of temperature increase on quantum random number generator, *Eur. Phys. J. D* **75**, 1 (2021).
- [16] Y. Li, Y. Fei, W. Wang, X. Meng, H. Wang, Q. Duan, and Z. Ma, Experimental study on the security of superluminescent led-based quantum random generator, *Optical Engineering* **60**, 116106 (2021).
- [17] C. Gabriel, C. Wittmann, D. Sych, R. Dong, W. Maurer, U. L. Andersen, C. Marquardt, and G. Leuchs, A generator for unique quantum random numbers based on vacuum states, *Nat. Photonics* **4**, 711 (2010).
- [18] 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**, 063814 (2010).
- [19] C. Bruynsteen, T. Gehring, C. Lupo, J. Bauwelinck, and X. Yin, 100-gbit/s integrated quantum random number generator based on vacuum fluctuations, *PRX Quantum* **4**, 010330 (2023).
- [20] Y.-H. Li, Y.-Y. Fei, W.-L. Wang, X.-D. Meng, H. Wang, Q.-H. Duan, Y. Han, and Z. Ma, Effect of external magnetic fields on practical quantum random number generator, *EPJ Quantum Technol.* **10**, 49 (2023).
- [21] Y.-Y. Hu, X. Lin, S. Wang, J.-Q. Geng, Z.-Q. Yin, W. Chen, D.-Y. He, W. Huang, B.-J. Xu, G.-C. Guo, and Z.-F. Han, Quantum random number generation based on spontaneous raman scattering in standard single-mode fiber, *Opt. Lett.* **45**, 6038 (2020).
- [22] S. Pironio, A. Acín, S. Massar, A. B. de La Giroday, D. N. Matsukevich, P. Maunz, S. Olmschenk, D. Hayes, L. Luo, T. A. Manning, and C. Monroe, Random numbers certified by Bell's theorem, *Nature (London)* **464**, 1021 (2010).
- [23] Y. Liu, X. Yuan, M.-H. Li, W. Zhang, Q. Zhao, J. Zhong, Y. Cao, Y.-H. Li, L.-K. Chen, H. Li, T. Peng, Y.-A. Chen, C.-Z. Peng, S.-C. Shi, Z. Wang, L. You, X. Ma, J. Fan, Q. Zhang, and J.-W. Pan, High-speed device-independent quantum random number generation without a detection loophole, *Phys. Rev. Lett.* **120**, 010503 (2018).
- [24] W.-Z. Liu, M.-H. Li, S. Ragy, S.-R. Zhao, B. Bai, Y. Liu, P. J. Brown, J. Zhang, R. Colbeck, J. Fan *et al.*, Device-independent randomness expansion against quantum side information, *Nat. Phys.* **17**, 448 (2021).
- [25] T. Lunghi, J. B. Brask, C. C. W. Lim, Q. Laviagne, J. Bowles, A. Martin, H. Zbinden, and N. Brunner, Self-testing quantum random number generator, *Phys. Rev. Lett.* **114**, 150501 (2015).
- [26] 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**, 062338 (2019).
- [27] Y.-Q. Nie, J.-Y. Guan, H. Zhou, Q. Zhang, X. Ma, J. Zhang, and J.-W. Pan, Experimental measurement-device-independent quantum random-number generation, *Phys. Rev. A* **94**, 060301(R) (2016).
- [28] Z. Cao, H. Zhou, and X. Ma, Loss-tolerant measurement-device-independent quantum random number generation, *New J. Phys.* **17**, 125011 (2015).
- [29] D. G. Marangon, G. Vallone, and P. Villoresi, Source-device-independent ultrafast quantum random number generation, *Phys. Rev. Lett.* **118**, 060503 (2017).
- [30] T. Michel, J. Y. Haw, D. G. Marangon, O. Thearle, G. Vallone, P. Villoresi, P. K. Lam, and S. M. Assad, Real-time source-independent quantum random-number generator with squeezed states, *Phys. Rev. Appl.* **12**, 034017 (2019).
- [31] 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**, 025013 (2019).
- [32] M. Avesani, D. G. Marangon, G. Vallone, and P. Villoresi, Source-device-independent heterodyne-based quantum random number generator at 17 Gbps, *Nat. Commun.* **9**, 5365 (2018).
- [33] 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**, 062326 (2019).
- [34] J. Cheng, J. Qin, S. Liang, J. Li, Z. Yan, X. Jia, and K. Peng, Mutually testing source-device-independent quantum random number generator, *Photon. Res.* **10**, 646 (2022).
- [35] Z. Cao, H. Zhou, X. Yuan, and X. Ma, Source-independent quantum random number generation, *Phys. Rev. X* **6**, 011020 (2016).
- [36] W.-B. Liu, Y.-S. Lu, Y. Fu, S.-C. Huang, Z.-J. Yin, K. Jiang, H.-L. Yin, and Z.-B. Chen, Source-independent quantum random number generator against tailored detector blinding attacks, *Opt. Express* **31**, 11292 (2023).
- [37] X. Lin, S. Wang, Z.-Q. Yin, G.-J. Fan-Yuan, R. Wang, W. Chen, D.-Y. He, Z. Zhou, G.-C. Guo, and Z.-F. Han, Security analysis and improvement of source independent quantum random number generators with imperfect devices, *npj Quantum Inf.* **6**, 100 (2020).
- [38] X. Lin, R. Wang, S. Wang, Z.-Q. Yin, W. Chen, D.-Y. He, Z. Zhou, G.-C. Guo, and Z.-F. Han, Imperfection-insensitivity quantum random number generator with untrusted daily illumination, *Opt. Express* **30**, 25474 (2022).
- [39] X. Lin and R. Wang, Quantum random number generation with partial source assumptions, *arXiv:2312.03333*.
- [40] X. Lin, R. Wang, S. Wang, Z.-Q. Yin, W. Chen, G.-C. Guo, and Z.-F. Han, Certified randomness from untrusted sources and uncharacterized measurements, *Phys. Rev. Lett.* **129**, 050506 (2022).
- [41] H. Wang, K. Chen, M. Gao, Z. Ma, W. Wang, C. Li, and C. Ma, Randomness expansion with a one-sided trusted device, *Phys. Rev. A* **91**, 052308 (2015).
- [42] H. Zhou, Z. Zheng, L. Huang, X. Wang, Z. Chen, and S. Yu, Eavesdropping attack on a continuous-variable source-independent quantum random number generator with fluctuating local oscillator, *J. Phys. B: At. Mol. Opt. Phys.* **55**, 065502 (2022).
- [43] Y. Li, Y. Fei, W. Wang, X. Meng, H. Wang, Q. Duan, Y. Han, and Z. Ma, Practical security analysis of a continuous-variable source-independent quantum random number generator based on heterodyne detection, *Opt. Express* **31**, 23813 (2023).
- [44] J. Zhang, Y. Zhang, Z. Zheng, Z. Chen, B. Xu, and S. Yu, Finite-size analysis of continuous variable source-independent quantum random number generation, *Quantum Inf. Proc.* **20**, 15 (2021).

- [45] P. Jouguet, S. Kunz-Jacques, E. Diamanti, and A. Leverrier, Analysis of imperfections in practical continuous-variable quantum key distribution, *Phys. Rev. A* **86**, 032309 (2012).
- [46] M.-Y. Li, X.-Y. Cao, Y.-M. Xie, H.-L. Yin, and Z.-B. Chen, Finite-key analysis for coherent one-way quantum key distribution, *Phys. Rev. Res.* **6**, 013022 (2024).
- [47] F.-Y. Lu, Z.-Q. Yin, R. Wang, G.-J. Fan-Yuan, S. Wang, D.-Y. He, W. Chen, W. Huang, B.-J. Xu, G.-C. Guo, and Z.-F. Han, Practical issues of twin-field quantum key distribution, *New J. Phys.* **21**, 123030 (2019).
- [48] Z. Li, X.-Y. Cao, C.-L. Li, C.-X. Weng, J. Gu, H.-L. Yin, and Z.-B. Chen, Finite-key analysis for quantum conference key agreement with asymmetric channels, *Quantum Sci. Technol.* **6**, 045019 (2021).
- [49] H. Jiang, M. Gao, B. Yan, W. Wang, and Z. Ma, Universally-composable finite-key analysis for efficient four-intensity decoy-state quantum key distribution, *Eur. Phys. J. D* **70**, 78 (2016).
- [50] W. Wang, X. Meng, Y. Fei, and Z. Ma, Finite-key security analysis of the 1-decoy state QKD protocol with a leaky intensity modulator, *Quantum Inf. Proc.* **19**, 196 (2020).
- [51] W. Wang, K. Tamaki, and M. Curty, Finite-key security analysis for quantum key distribution with leaky sources, *New J. Phys.* **20**, 083027 (2018).
- [52] Y.-M. Chi, B. Qi, W. Zhu, L. Qian, H.-K. Lo, S.-H. Youn, A. I. Lvovsky, and L. Tian, A balanced homodyne detector for high-rate Gaussian-modulated coherent-state quantum key distribution, *New J. Phys.* **13**, 013003 (2011).
- [53] H. Hansen, T. Aichele, C. Hettich, P. Lodahl, A. I. Lvovsky, J. Mlynek, and S. Schiller, Ultrasensitive pulsed, balanced homodyne detector: application to time-domain quantum measurements, *Opt. Lett.* **26**, 1714 (2001).
- [54] W.-B. Liu, C.-L. Li, Y.-M. Xie, C.-X. Weng, J. Gu, X.-Y. Cao, Y.-S. Lu, B.-H. Li, H.-L. Yin, and Z.-B. Chen, Homodyne detection quadrature phase shift keying continuous-variable quantum key distribution with high excess noise tolerance, *PRX Quantum* **2**, 040334 (2021).
- [55] C. Wang, P. Huang, D. Huang, D. Lin, and G. Zeng, Practical security of continuous-variable quantum key distribution with finite sampling bandwidth effects, *Phys. Rev. A* **93**, 022315 (2016).
- [56] C. Xie, Y. Guo, Q. Liao, W. Zhao, D. Huang, L. Zhang, and G. Zeng, Practical security analysis of continuous-variable quantum key distribution with jitter in clock synchronization, *Phys. Lett. A* **382**, 811 (2018).
- [57] H. Li, C. Wang, P. Huang, D. Huang, T. Wang, and G. Zeng, Practical continuous-variable quantum key distribution without finite sampling bandwidth effects, *Opt. Express* **24**, 20481 (2016).
- [58] P. Huang, J. Huang, T. Wang, H. Li, D. Huang, and G. Zeng, Robust continuous-variable quantum key distribution against practical attacks, *Phys. Rev. A* **95**, 052302 (2017).