Imperfect state preparation in continuous-variable quantum key distribution

Wenyuan Liu,[1] Xuyang Wang,[1,2] Ning Wang,[1] Shanna Du,[1] and Yongmin Li[1,2,*]

[1]*State Key Laboratory of Quantum Optics and Quantum Optics Devices, Institute of Opto-Electronics, Shanxi University, Taiyuan 030006, China*

[2]*Collaborative Innovation Center of Extreme Optics, Shanxi University, Taiyuan 030006, China*

(Received 11 July 2017; published 11 October 2017)

In continuous-variable quantum key distribution, the loss and excess noise of the quantum channel are key parameters that determine the secure key rate and the maximal distribution distance. We investigate the imperfect quantum state preparation in Gaussian modulation coherent-state protocol both theoretically and experimentally. We show that the Gaussian distribution characteristic of the prepared states in phase space is broken due to the incorrect calibration of the working parameters for the amplitude modulator and phase modulator. This further causes a significant increase of the excess noise and misestimate of the channel loss. To ensure an accurate estimate of the quantum channel parameters and achieve a reliable quantum key distribution, we propose and demonstrate two effective schemes to calibrate the working parameters of the modulators.

DOI: 10.1103/PhysRevA.96.042312

I. INTRODUCTION

Quantum key distribution (QKD) can achieve secret key sharing between two legitimate parties over an unsafe quantum channel with the help of a public, authenticated classical channel [1,2]. The unconditional security relies on the basic properties of the quantum physics, for instance, the quantum no-cloning theorem and uncertainty principle. Continuous-variable (CV) QKD protocols encode the secret keys into continuous-spectrum quantum observables (quadratures of the light field) and employ homodyne detectors instead of single photon detectors. One potential of the CV protocols is that we can achieve high key rates at a relatively short distance due to the multiphoton feature of the signal states. Recently, the research of CV QKD has made great progress in experimental aspects as well as the theoretical analysis [3–18].

In real scenarios, the experimental imperfections of QKD systems may threaten their security. Such imperfections mainly include the light source, the preparation of the signal state, and the measurement of the received states [19–29]. These side-channel attacks can be countered in principle by characterizing the system carefully; for instance, a real-time measurement of the shot noise or generating the local oscillator (LO) locally in Bob's side disables the attacks on the LO [30,31]. Measurement-device-independent QKD is another powerful countermeasure to address the imperfect measurement process [32–34]. In a prepare-and-measure (PM) implementation of Gaussian-modulated protocols, waveguide electro-optic amplitude and phase modulators are usually exploited to achieve the desired bivariate Gaussian modulation. It has been shown that approximating the theoretical Gaussian modulation with a discrete one is sufficient in practice [24]. Waveguide electro-optic modulators are currently the most popular modulating device utilized in high-speed optical communication systems. The adoption of this type of device in QKD lies in consideration of its high bandwidth, low driving voltage, and its ease of further integration in a QKD system. Lithium niobate–based phase modulators and Mach-Zehnder (MZ) intensity modulators are the most common devices commercially available. However, it is known that the initial bias point and half-wave voltage drift over time due to environmental perturbations and aging effects. Such drift leads to deterioration of the modulation fidelity, and further causes the incorrect parameter evaluations and opens a security loophole for CV QKD systems, an issue that has not been investigated in depth previously.

In this paper, we investigate the imperfect state preparation issue theoretically and verify the predicted results in experiment. In Sec. II we give a theoretical analysis of imperfect amplitude and phase modulation in CV QKD. In Sec. III, we verify the theoretically predicted results in experiment and analyze the experimental results in detail. Then in Sec. IV we propose two efficient schemes to calibrate the working parameters of the modulators and demonstrate a reliable CV QKD. In Sec. V, we give a conclusion, and discuss the issue of calibration errors during the calibration procedures.

II. THEORETICAL ANALYSIS OF IMPERFECT AMPLITUDE AND PHASE MODULATION IN CV QKD

A. Imperfect amplitude and phase modulation due to incorrect calibration of the modulators

In the Gaussian-modulated coherent-state CV QKD protocol, Alice randomly generates a coherent state $|\alpha_A\rangle$ with $\alpha_A = |\alpha_A|e^{i\theta} = x_A + i\,p_A$. Here α_A is the complex amplitude of the coherent state, x_A and p_A represent two independent Gaussian variables with the same variance V_A in shot-noise units (SNUs). According to the Box-Muller transform [35], x_A and p_A can be generated from a pair of uniformly distributed random numbers (U_1 and U_2) over the interval [0,1]:

$$\begin{aligned} x_A &= \sqrt{-2V_A \ln U_1}\cos(2\pi U_2), \\ p_A &= \sqrt{-2V_A \ln U_1}\sin(2\pi U_2). \end{aligned} \tag{1}$$

In the corresponding polar coordinates ($|\alpha_A|$, θ), Eq. (1) can be rewritten as

$$\begin{aligned} |\alpha_A| &= \sqrt{x_A^2 + p_A^2} = \sqrt{-2V_A \ln U_1}, \\ \theta &= \arccos\left(x_A/\sqrt{x_A^2 + p_A^2}\right) = 2\pi U_2, \end{aligned} \tag{2}$$

*yongmin@sxu.edu.cn

 ©2017 American Physical Society

where θ has a uniform distribution on $[0,2\pi]$, and $|\alpha_{\rm A}|$ obeys the Rayleigh distribution

$$P(|\alpha_{\rm A}|) = \frac{|\alpha_{\rm A}|}{V_{\rm A}} e^{-|\alpha_{\rm A}|^2/(2V_{\rm A})}. \tag{3}$$

Therefore, an amplitude modulator together with a phase modulator is sufficient to achieve above bivariate Gaussian modulation.

The transfer function of a MZ intensity modulator is represented as

$$t_{\rm A} = \frac{\alpha_{\rm out}}{\alpha_{\rm in}} = t_{\rm A0} \sin\left(\frac{\pi}{2}\frac{V_{\rm min} - V_{\rm AM}}{V_\pi^{\rm AM}}\right), \tag{4}$$

where $1 - t_{\rm A0}^2$ is the inserting loss, $\alpha_{\rm in}$ and $\alpha_{\rm out}$ are the input and output optical fields, respectively, $V_{\rm AM}$ is the modulation voltage signal, $V_{\rm min}$ is the voltage corresponding to a minimum transmission of modulator, and $V_\pi^{\rm AM}$ is the half-wave voltage. The transfer function of a phase modulator is

$$t_{\rm P} = \frac{\alpha_{\rm out}}{\alpha_{\rm in}} = t_{\rm P0} e^{i\pi(V_{\rm PM}/V_\pi^{\rm PM})}, \tag{5}$$

where $1 - t_{\rm P0}^2$ is the inserting loss, $V_{\rm PM}$ is the modulation voltage signal, and $V_\pi^{\rm PM}$ is the half-wave voltage. From Eqs. (4) and (5), the total transfer function is given by

$$t = \frac{\alpha_{\rm out}}{\alpha_{\rm in}} = t_{\rm A} t_{\rm P} = t_{\rm A0} t_{\rm P0} \sin\left(\frac{\pi}{2}\frac{V_{\rm min} - V_{\rm AM}}{V_\pi^{\rm AM}}\right) e^{i\pi(V_{\rm PM}/V_\pi^{\rm PM})}. \tag{6}$$

Starting from Eqs. (2) and (6) and letting $\alpha_{\rm out} = \alpha_{\rm A}$, under the condition of $0 \leqslant (V_{\rm min} - V_{\rm AM})/V_\pi^{\rm AM} \leqslant 1$, the modulation voltage signal $V_{\rm AM}$ and $V_{\rm PM}$ are given by

$$V_{\rm AM} = V_{\rm min} - \frac{2}{\pi} V_\pi^{\rm AM} \arcsin(\sqrt{-2V_{\rm A} \ln U_1}/h), \tag{7}$$

$$V_{\rm PM} = 2U_2 V_\pi^{\rm PM}, \tag{8}$$

where $h = |\alpha_{\rm in}| t_{\rm A0} t_{\rm P0}$. Equations (7) and (8) show the idealized modulation voltages required for the amplitude and phase modulators to achieve a bivariate Gaussian modulation.

However, when the modulators are incorrectly calibrated, that means the adopted values of $V_{\rm min}$, $V_\pi^{\rm AM}$, and $V_\pi^{\rm PM}$ deviate from their true values

$$V'_{\rm min} = V_{\rm min} + \delta_{\rm min} V_\pi^{\rm AM}, \quad V_\pi^{\rm AM'} = V_\pi^{\rm AM}\left(1 + \delta_\pi^{\rm AM}\right),$$
$$V_\pi^{\rm PM'} = V_\pi^{\rm PM}\left(1 + \delta_\pi^{\rm PM}\right), \tag{9}$$

where δ denotes the deviation coefficient. In this case, the actual $|\alpha'_{\rm A}|$ and θ' will differ from the true values of $|\alpha_{\rm A}|$ and θ which are defined by Eq. (2). This further leads to the modulation errors

$$x'_{\rm A} = h \sin\left\{-\frac{2}{\pi}\delta_{\rm min} + \left(1 + \delta_\pi^{\rm AM}\right) \arcsin[\sqrt{-2V_{\rm A} \ln U_1}/h]\right\} \times \cos\left[2\pi U_2\left(1 + \delta_\pi^{\rm PM}\right)\right], \tag{10}$$

$$p'_{\rm A} = h \sin\left\{-\frac{2}{\pi}\delta_{\rm min} + \left(1 + \delta_\pi^{\rm AM}\right) \arcsin[\sqrt{-2V_{\rm A} \ln U_1}/h]\right\} \times \sin\left[2\pi U_2\left(1 + \delta_\pi^{\rm PM}\right)\right], \tag{11}$$

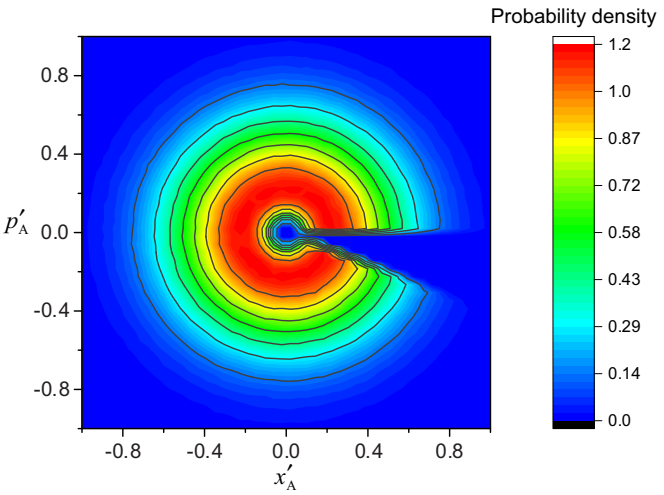

FIG. 1. The contour map of the probability density $P(\alpha'_{\rm A})$ for imperfect amplitude and phase modulation with parameters $V_{\rm A} = 1/3$, $\delta_{\rm min} = -0.06$, $\delta_\pi^{\rm AM} = -0.06$, and $\delta_\pi^{\rm PM} = -0.06$.

where $x'_{\rm A}$ and $p'_{\rm A}$ are the actual variables generated from the imperfect amplitude and phase modulation process. In this case, the mixed coherent states prepared by Alice are modified from $\rho_{\rm ideal}$ to $\rho_{\rm real}$,

$$\rho_{\rm ideal} = \int P(\alpha_{\rm A})|\alpha_{\rm A}\rangle\langle\alpha_{\rm A}|d^2\alpha_{\rm A},$$
$$\rho_{\rm real} = \int P(\alpha'_{\rm A})|\alpha'_{\rm A}\rangle\langle\alpha'_{\rm A}|d^2\alpha'_{\rm A}, \tag{12}$$

where $P(\alpha_{\rm A})$, $P(\alpha'_{\rm A})$ are the probability density of being in the state $|\alpha_{\rm A}\rangle$ and $|\alpha'_{\rm A}\rangle$, respectively. In general, not only the variance of $x'_{\rm A}$ and $p'_{\rm A}$ changes; furthermore, $P(\alpha'_{\rm A})$ is no longer a Gaussian distribution. Such a phenomenon is plotted in Fig. 1. For a minus deviation of the MZ intensity modulator's null point $\delta_{\rm min} = -0.06$, a hole appears in the center of the contour map. Meanwhile, a gap also emerges due to the minus deviation of the phase modulator's half-wave voltage $\delta_\pi^{\rm PM} = -0.06$.

B. Estimation of quantum channel parameters

Consider Alice has randomly prepared a set of quantum states $\{|\alpha_{\rm A}\rangle\}_i$ $(i = 1,...,N)$, the quadratures of the modulated coherent states can be represented as

$$\hat{x}_{\rm A} = x_{\rm A} + \hat{x}_{\rm V1}, \tag{13}$$

where $x_{\rm A}$ is the Gaussian modulation signal and $\hat{x}_{\rm V1}$ is the quadrature of a vacuum field. The prepared states transmit through a quantum channel which is characterized by its transmittance T and excess noise ε, and successively detected by Bob's homodyne detector

$$\hat{x}_{\rm B} = \sqrt{\eta T}(\hat{x}_{\rm A} + \hat{x}_\varepsilon) + \sqrt{1 - \eta T}\hat{x}_{\rm V2} + x_{\rm el}, \tag{14}$$

where $\hat{x}_\varepsilon$ is the quadrature of the added auxiliary mode due to the eavesdropping, which satisfies $\langle\hat{x}_\varepsilon\rangle = 0$ and $\langle\hat{x}_\varepsilon^2\rangle = \varepsilon$, η and $\upsilon_{\rm el} = \langle x_{\rm el}^2\rangle$ are the detection efficiency and the electronic noise of Bob's homodyne detector, respectively; $\hat{x}_{\rm V2}$ is the quadrature of a vacuum field which simulates the

detection noise due to the nonideal quantum efficiency of the photodetector.

After Alice and Bob complete the state preparation and measurement stage, a key sifting procedure is followed to ensure they can share correlated variables $\{x_{\mathrm{A}}^{i}, x_{\mathrm{B}}^{i}\}$, $i = 1,\ldots,N$. In order to estimate the parameters of the quantum channel, a sampling of the obtained raw keys is declared to calculate the variance of Alice's and Bob's, $\langle x_{\mathrm{A}}^2\rangle$ and $\langle x_{\mathrm{B}}^2\rangle$, and the covariance between them $\langle x_{\mathrm{A}} x_{\mathrm{B}}\rangle$. From Eqs. (13) and (14), the channel parameters for transmittance T and excess noise ε are related to these values through the following equations [5]:

$$\langle x_{\mathrm{A}}^2\rangle = V_{\mathrm{A}}, \tag{15}$$

$$\langle x_{\mathrm{B}}^2\rangle = \eta T(V_{\mathrm{A}} + \varepsilon) + 1 + \upsilon_{\mathrm{el}}, \tag{16}$$

$$\langle x_{\mathrm{A}} x_{\mathrm{B}}\rangle = \sqrt{\eta T} V_{\mathrm{A}}, \tag{17}$$

where the parameters η and υ_{el} of the homodyne detector are calibrated in advance, and the shot noise can be monitored in real time at Bob's side. It is noted that all the parameters in the above equations are expressed in SNUs. From Eqs. (15), (16), and (17), the parameters for T and ε have the form

$$T = \frac{\langle x_{\mathrm{A}} x_{\mathrm{B}}\rangle^2}{\eta \langle x_{\mathrm{A}}^2\rangle^2}, \tag{18}$$

$$\varepsilon = \frac{\langle x_{\mathrm{B}}^2\rangle - 1 - \upsilon_{\mathrm{el}}}{\left(\langle x_{\mathrm{A}} x_{\mathrm{B}}\rangle / \langle x_{\mathrm{A}}^2\rangle\right)^2} - \langle x_{\mathrm{A}}^2\rangle. \tag{19}$$

In the above analysis, we have assumed that Alice performs a perfect Gaussian modulation. In the case of imperfect Gaussian modulation, one should replace x_{A} with x'_{A} in Eq. (13). Consequently, Eqs. (18) and (19) should be rewritten as

$$T' = \frac{\langle x_{\mathrm{A}} x'_{\mathrm{A}}\rangle^2}{\langle x_{\mathrm{A}}^2\rangle^2} T, \tag{20}$$

$$\varepsilon' = \frac{\langle x'^2_{\mathrm{A}}\rangle + \varepsilon}{\left(\langle x_{\mathrm{A}} x'_{\mathrm{A}}\rangle / \langle x_{\mathrm{A}}{}^2\rangle\right)^2} - \langle x_{\mathrm{A}}^2\rangle. \tag{21}$$

It is evident from the above equations that the estimated excess noise ε' differs from its true value ε. In particular, the transmittance T is mistakenly estimated due to the modulation error.

C. Calculation of secret key rate

In the asymptotic limit on infinite samples, the collective attack has been proven to the optimal attack [36], and the corresponding secret key rate for protocols with reverse reconciliation is given by

$$\Delta I^{\mathrm{Holevo}} = \beta I_{\mathrm{AB}} - \chi_{\mathrm{BE}}, \tag{22}$$

where β is the reconciliation efficiency, I_{AB} is the mutual information between the legitimate parties' measurement results, and χ_{BE} denotes the Holevo quantity between Eve's quantum states and Bob's data. Start from the experimental accessible parameters V_{A}, η, T, ε, and β, one can calculate the secret key rate $\Delta I^{\mathrm{Holevo}}$ [5].

According to the results in Sec. II B, if the working parameters of the modulators are not calibrated correctly and the legitimate users are not aware of that, they will get incorrect channel parameters T' and ε'. Based on these incorrect parameters, the security key rate will be overestimated or underestimated. For the former case, it can open a security loophole, while for the latter case, the system performance is sacrificed.

To resolve such problems, two countermeasures can be considered. The first one is to build a model for such imperfect amplitude and phase modulation protocol and figure out the accurate secret key rate. As we have shown above, the mixed coherent states prepared by Alice, ρ_{real}, under the imperfect modulation no longer satisfy a Gaussian distribution. To simplify the theoretical calculation of the key rates, in principle, such PM scheme can be transformed into an equivalent entanglement-based scheme. However, except for the Gaussian-modulated Gaussian states or some symmetric discrete modulation types such as four-state modulation protocol [37], the equivalent entangled states for the present nonideal PM scheme are difficult to find. The second countermeasure used to solve the imperfect modulation issue is to calibrate the relevant parameters of the modulators precisely; in this case, the security analysis approach of the Gaussian-modulated coherent states protocol can be used.

III. EXPERIMENTAL RESULTS AND ANALYSIS

Figure 2 depicts the sketch of our experimental setup for fiber-based Gaussian-modulated coherent-state CVQKD. Optical pulses 100 ns wide and with a repetition rate of 500 kHz are generated from a 1550-nm continuous-wave single frequency semiconductor laser by using MZ intensity modulators (AM1). A fiber coupler with a splitting ratio of 99:1 separates the optical pulses into two parts where the weak one serves as the signal field and the intense one acts as the LO. A combination of a MZ intensity modulator (AM2) and a phase modulator (PM1) is adopted to modulate the coherent states with bivariate Gaussian modulation as described in Sec. II A). To ensure a real-time shot-noise calibration, we use a third intensity modulator (AM3) to block the signal path regularly. The intensity of the signal is monitored in real time by splitting a small portion of the signal field with a splitter of 90:10. A variable attenuator (VA) further attenuates the intensity of the signal field to the desired values.

At Bob's side, the amplitude or phase quadrature of the received signal quantum states is randomly measured by using a pulsed balanced homodyne detector (BHD). The random

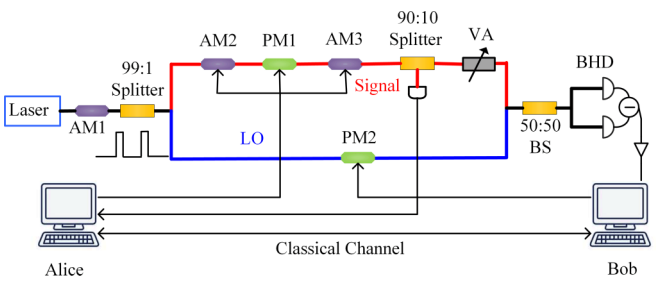

FIG. 2. The schematic diagram of the experimental setup. AM, MZ amplitude modulator; PM, phase modulator; VA, variable attenuator; BS, 50:50 beam splitter; LO, local oscillator; BHD, balanced homodyne detector.

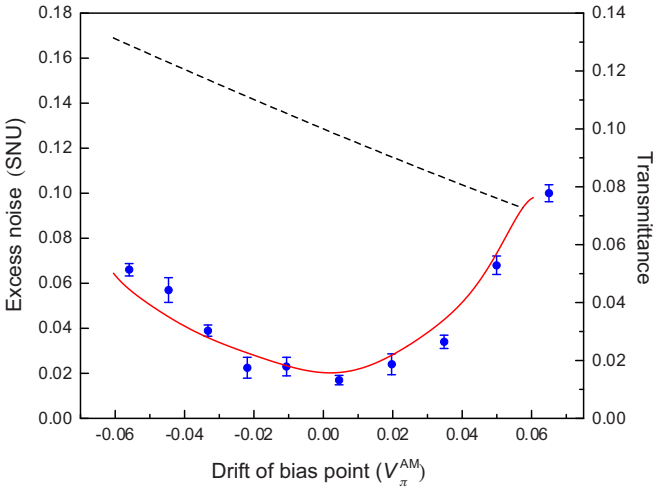

FIG. 3. The estimated excess noise and transmittance versus the drift of the amplitude modulator's bias point (normalized to the half-wave voltage). The filled circle and the solid line are the experimental data and the theoretical simulation for the excess noise, respectively. The theoretically predicted transmittance is depicted by a dashed line.

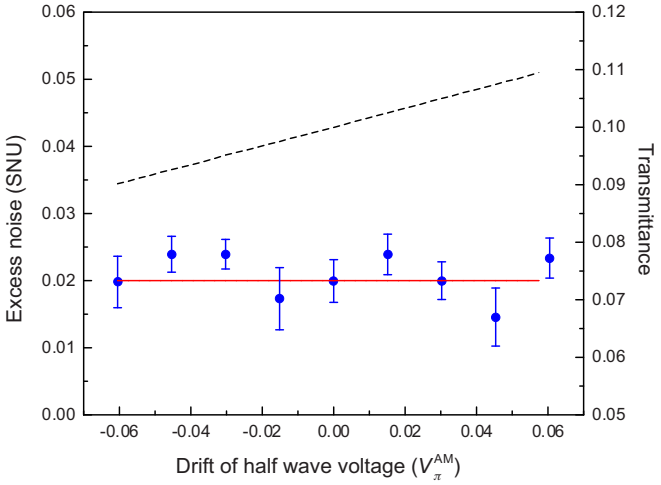

FIG. 4. The estimated excess noise and transmittance of the quantum channel versus the drift of the amplitude modulator's half-wave voltage (normalized to the half-wave voltage). The filled circle and the solid line are the experimental data and the theoretical simulation for the excess noise, respectively. The theoretically predicted transmittance is depicted by a dashed line.

basis switch and relative phase stabilization between the signal and the LO are fulfilled with a phase modulator (PM2). A bidirectional classical communication link between Alice and Bob used for synchronization and parameter estimation is created using two optical small form-factor pluggable fiber switches on each side.

For all the implementations below, the modulation variance and the channel transmittance are set to $V_A = 5.6$ and $T = 0.1$ respectively, where the channel loss is simulated by setting an appropriate modulation voltage to the intensity modulator (AM3). The phase noise between the signal and the LO is determined to be around $\pm 0.5°$, which induces an excess noise less than 0.001 SNU.

Figure 3 plots the estimated excess noise ε' and transmittance T' as a function of the normalized drift $\delta_{\min}$ of the amplitude modulator's bias point. We can see that the drift of the amplitude modulator's bias point (both negative and positive) leads to an increase of the estimated excess noise. The dependence of ε' on the drift $\delta_{\min}$ is asymmetric, where ε' gradually increases to around 0.06 (0.08) SNU when $\delta_{\min}$ reaches -0.06 (0.06). The experimental results exhibit an excess noise of 0.02 even if the bias point of the amplitude modulator is correctly calibrated (no drift); such excess noise is due to other factors rather than the drift of the bias point and not included in the theoretical model presented in Sec. II. To compare the theoretical simulations with the experimental data, a constant value (0.02) is added in the theoretical values. One also observes that the estimated channel transmittance T' varies linearly with the drift of the bias point, and the T' is lower (higher) than the real value of $T = 0.1$ for positive (minus)$\delta_{\min}$. This is due to the fact that the drift of the bias point results in a nonlinear dependence between x_A and x_B, whereas the linear relationship is a precondition for the correct evaluation of the channel parameters T and ε by using Eqs. (18) and (19).

The estimated excess noise ε' and transmittance T' versus the normalized drift of the amplitude modulator's half-wave voltage δ_π^{AM} is depicted in Fig. 4. Similar to the drift of the bias point, the estimated channel transmittance T' varies linearly with the drift of δ_π^{AM}. In contrast with Fig. 3, T' is higher (lower) than the real T (0.1) for positive (minus) δ_π^{AM}. However, the graph shows that estimated excess noise ε' is immune to the drift of the amplitude modulator's half-wave voltage. This phenomenon is due to the error cancellation mechanism between the parameters T' and $\langle (x'_A)^2 \rangle$, which are used to determine the excess noise ε'.

The drift of the phase modulator's half-wave voltage δ_π^{PM} (normalized to V_π^{PM}) also affects the estimated excess noise and channel transmittance, as shown in Fig. 5. The dependence

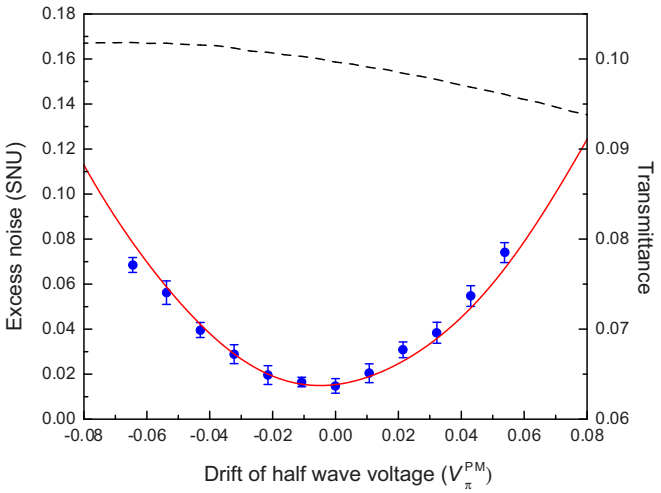

FIG. 5. The estimated excess noise and transmittance of the quantum channel versus the drift of the phase modulator's half-wave voltage (normalized to the half-wave voltage). The filled circle and the solid line are the experimental data and the theoretical simulation for the excess noise, respectively. The theoretically predicted transmittance is depicted by a dashed line.

of ε' on the drift $\delta_{\min}$ exhibits slight asymmetry, where ε' gradually increases to around 0.056 (0.074) SNU when $\delta_{\min}$ reaches -0.054 (0.054). In contrast with the relevant phenomenon caused by the drift of the amplitude modulator's bias point and half-wave voltage, the estimated channel transmittance T' exhibits a nonlinear relation along with δ_π^{PM}. In Figs. 3–5, the main origin of the excess noise fluctuations is statistical due to the finite samples (1.5×10^7) for the parameters estimation.

IV. CALIBRATION OF THE MODULATORS' WORKING PARAMETERS

In above sections we have shown that the incorrect calibration of the parameters can result in a significant increase of the estimated excess noise and misestimate of the channel loss. To solve these problems, we proposed two effective methods to calibrate the parameters of the modulators.

For the MZ amplitude modulator, one can scan its bias voltage over $[0, 2V_\pi^{\mathrm{AM}}]$ and record the bias voltage and transmitted optical power (x_i, y_i) at the same time. In this way, the null point $V_{\min}$ and half-wave voltage V_π^{AM} can be conveniently determined in principle. However, for a high extinction ratio modulator (>40 dB in our experiment), the required dynamic range should be larger than the value of the extinction ratio; this is usually well beyond the conventional photodetectors. Such an obstacle can be overcome subtly by utilizing a fitting method. More precisely, a high-order polynomial fitting is employed to fit the measured data, which is acquired by a conventional photodetector. In this way, we can acquire the null point and half-wave voltage in spite of the insufficient dynamic range and dark noises of the photodetector.

In our experiment, we fit the measured data (x_i, y_i) to a 13th-order polynomial function

$$f(x_i) = \sum_{j=0}^{13} a_j x_i^j, \tag{23}$$

where $f(x_i)$ represents the best polynomial fit of the transmitted optical power and a_j is the polynomial coefficient, which is found by using the least-square method, i.e., minimizing the residue using the following equation:

$$R = \frac{1}{N}\sum_{i=0}^{N-1}[f(x_i) - y_i]^2, \tag{24}$$

where N is the number of the recorded data (x_i, y_i).

In order to calibrate the half-wave voltage of the phase modulator, we proposed a noninvasive method here. From Eqs. (13) and (14), the mean value of $\hat{x}_{\mathrm{B}}$ is given by

$$\langle \hat{x}_{\mathrm{B}} \rangle = \sqrt{\eta T}(\langle x'_{\mathrm{A}} \rangle + \langle \hat{x}_{\mathrm{V1}} \rangle + \langle \hat{x}_\varepsilon \rangle) + \sqrt{1-\eta T}\langle \hat{x}_{\mathrm{V2}} \rangle + \langle x_{\mathrm{el}} \rangle. \tag{25}$$

For a sufficient amount of measurements, the quadrature of the excess noise, vacuum fields, and electronic noise should average out to be close to zero,

$$\langle \hat{x}_{\mathrm{V1}} \rangle \approx 0, \quad \langle \hat{x}_\varepsilon \rangle \approx 0, \quad \langle \hat{x}_{\mathrm{V2}} \rangle \approx 0, \quad \langle x_{\mathrm{el}} \rangle \approx 0. \tag{26}$$

In this case, Eq. (25) can be simplified to be

$$\langle \hat{x}_{\mathrm{B}} \rangle \approx \sqrt{\eta T}\langle x'_{\mathrm{A}} \rangle. \tag{27}$$

By using Eqs. (1), (2), (3), and (27), the mean value of $\hat{x}_{\mathrm{B}}$ can be determined as

$$\begin{aligned}\langle \hat{x}_{\mathrm{B}} \rangle &\approx \sqrt{\eta T}\int_0^{\infty}\int_0^{2\pi(1+\delta_\pi^{\mathrm{PM}})} \frac{r^2}{V_{\mathrm{A}}} e^{-r^2/2V_{\mathrm{A}}}\cos(\theta) dr d\theta \\ &= \sqrt{\frac{\eta T V_{\mathrm{A}}}{8\pi}}\sin\left(2\pi\delta_\pi^{\mathrm{PM}}\right).\end{aligned} \tag{28}$$

Thus, the drift of the phase modulator's half-wave voltage δ_π^{PM} is found to be equal to

$$\delta_\pi^{\mathrm{PM}} = \frac{1}{2\pi}\arcsin\left(\frac{\langle \hat{x}_{\mathrm{B}} \rangle}{\sqrt{(\eta T V_{\mathrm{A}})/(8\pi)}}\right). \tag{29}$$

We assume $\delta_\pi^{\mathrm{PM}} \ll 1$, which is justified in practice; the expression of δ_π^{PM} can be approximately given by

$$\delta_\pi^{\mathrm{PM}} \approx \frac{\langle \hat{x}_{\mathrm{B}} \rangle}{\sqrt{(\pi \eta T V_{\mathrm{A}})/2}}. \tag{30}$$

By using Eq. (30), the drift of the phase modulator's half-wave voltage δ_π^{PM} can be determined in real time by using $\langle \hat{x}_{\mathrm{B}} \rangle$, V_{A}, and ηT. The determination of δ_π^{PM} only refers to the raw signal data and no other additional modulations are required; this approach ensures a noninvasive calibration and keeps the secret key rate intact. In practice, $\langle \hat{x}_{\mathrm{B}} \rangle$ can be determined with a precision of less than 0.1%, and V_{A} is the ideal modulation variance. The calibration period is chosen so that the drift of the phase modulator's normalized half-wave voltage is less than ± 0.01. In this case, T can be determined with a precision of less than 1% from Fig. 5. Therefore, the calibration error of δ_π^{PM} for the phase modulator is within 0.5% using Eq. (30).

By using the above methods, we can determine the working parameters of the modulators including the bias point $\delta_{\min}$ and half-wave voltage δ_π^{AM} of the amplitude modulator, the half-wave voltage δ_π^{PM} of the phase modulator. In order to calibrate the working parameters of the modulators in real time, the QKD system automatically measures and corrects the corresponding parameters regularly. A feedback control period of 2 min is adopted so that the drifts of the parameters are small and tolerable.

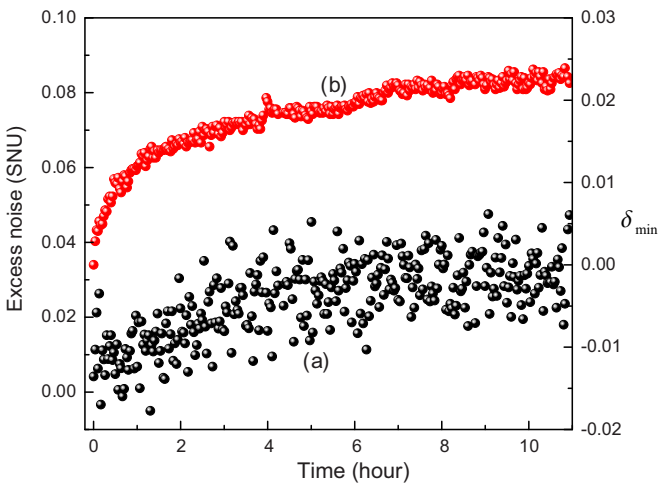

FIG. 6. Excess noises of the CV QKD system when the modulators are free running. (a) Excess noise and (b) the corresponding drift of the amplitude modulator's bias point.

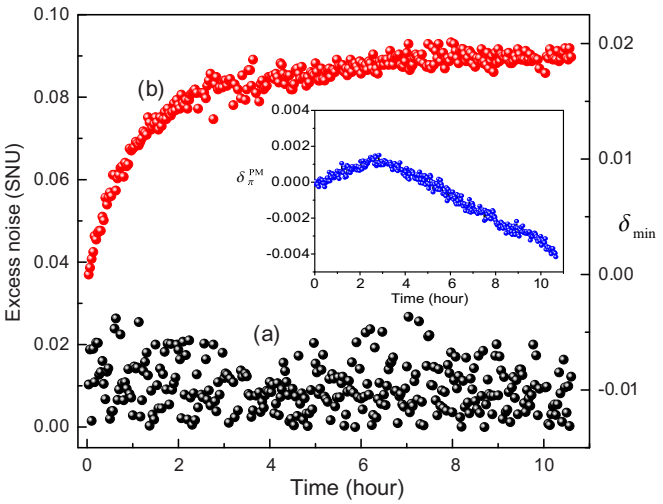

FIG. 7. Excess noises of the CV QKD system when the modulators are feedback controlled. (a) Excess noise and (b) the corresponding drift of the amplitude modulator's bias point. Inset: measured δ_π^{PM} which is used to calibrate the phase modulator's half-wave voltage.

Figure 6(a) illustrates measured excess noises of the CV QKD system when the modulators are free running. Initially, we carefully calibrate the modulators and then use the calibrated parameters repeatedly. It is evident that the measured excess noise of the system stays at a low level at the first stage, and then it starts to increase with time due to the drifts of the modulator's working parameters. Figure 6(b) plots the variation of the amplitude modulator's bias point δ_{min} along with time; the amount of the drift is around 2% for an observation period of 11 h. Meanwhile, we record the drifts of the modulator's half-wave voltages δ_π^{AM} and δ_π^{PM}, which are relatively stable both with fluctuations less than 1%. Due to the finite operating time and stable environment temperature (within 2 °C in our experiment), the observed drifts of the modulator's working parameters are not obvious. It is expected that the drifts will increase for a long-term operation and fluctuating environment temperature.

Figure 7 shows measured excess noises when the working parameters of the modulators are calibrated and feedback controlled regularly. Due to the existence of the active feedback procedure, the excess noise of the system remains stably at a low level during a 10-h observation period. The inset of Fig. 7 shows the δ_π^{PM} measured in real time which is used to calibrate the phase modulator's half-wave voltage. The fluctuations of the excess noise mainly stem from the statistical fluctuations due to the finite size effect, where the parameters estimation is performed on data blocks of size 1.5×10^7. Using the experimental parameters of $\eta = 0.64$, $\upsilon_{\mathrm{el}} = 0.1$, and $\beta = 0.95$, the secret key rate (per pulse) of the system is determined to be $\Delta I^{\mathrm{Holevo}} = 0.02$ bit/pulse.

In the above sections, we have focused on the influence of the imperfect working parameters of both the amplitude and phase modulators on CV QKD, and assume the devices operate perfectly and ideally in other aspects other than the imperfections mentioned above. It is noted that other imperfect factors of the modulators certainly exist and will affect the QKD to some extent. For instance, the modulators may not operate strictly according to Eqs. (4) and (5), and the working parameters obtained during calibration may vary when the device is under continuous and high-speed modulation. We will consider such effects in our future work.

V. CONCLUSION

We have investigated the influences of imperfect amplitude and phase modulation upon continuous-variable quantum key distribution. The imperfect modulations we considered are caused by the incorrect calibration of the half-wave voltage and bias point for the amplitude modulator, and the half-wave voltage for the phase modulator. We show that an accurate modulation is crucial to the performance and security of the QKD system. When imperfect modulations occur, the Gaussian distribution characteristic of the prepared states is destroyed; one cannot estimate correctly the channel loss and excess noise using the conventional approaches. In order to overcome such problems and realize a faithful quantum key distribution, we proposed and demonstrated two effective approaches, which can calibrate the parameters of the modulators at regular intervals. In this way, we demonstrated a stable continuous-variable quantum key distribution without suffering from the imperfect state preparation. However, due to the finite resolution of the experimental techniques, the relevant parameters can only be calibrated as close as possible to their real values. There inevitably exist calibration errors for the calibration procedures. In this scenario, the remaining question is how such slight imperfections affect the security of the QKD system, which requires a further study.

ACKNOWLEDGMENTS

This research was supported by Key Project of the Ministry of Science and Technology of China (Grant No. 2016YFA0301403), National Natural Science Foundation of China (NSFC) (Grants No. 61378010 and No. 11504219), Shanxi 1331KSC, and Program for the Outstanding Innovative Teams of Higher Learning Institutions of Shanxi.

[1] V. Scarani, H. Bechmann-Pasquinucci, N. J. Cerf, M. Dušek, N. Lütkenhaus, and M. Peev, Rev. Mod. Phys. **81**, 1301 (2009).
[2] H. W. Lo, M. Curty, and K. Tamaki, Nat. Photonics **8**, 595 (2014).
[3] C. Weedbrook, S. Pirandola, R. García-Patrón, N. J. Cerf, T. C. Ralph, J. H. Shapiro, and S. Lioyd, Rev. Mod. Phys. **84**, 621 (2012).
[4] L. S. Madsen, V. C. Usenko, M. Lassen, R. Filip, and U. L. Andersen, Nat. Commun. **3**, 1083 (2012).
[5] P. Jouguet, S. Kunz-Jacques, A. Leverrier, P. Grangier, and E. Diamanti, Nat. Photonics **7**, 378 (2013).
[6] B. Heim, C. Peuntinger, N. Killoran, I. Khan, C. Wittmann, C. Marquardt, and G. Leuchs, New J. Phys. **16**, 113018 (2014).

[7] F. Furrer, Phys. Rev. A **90**, 042325 (2014).
[8] T. Gehring, V. Handchen, J. Duhme, F. Furrer, T. Franz, C. Pacher, R. F. Werner, and R. Schnabel, Nat. Commun. **6**, 8795 (2015).
[9] S. Pirandola, C. Ottaviani, G. Spedalieri, C. Weedbrook, S. L. Braunstein, S. Lloyd, T. Gehring, C. S. Jacobsen, and U. L. Andersen, Nat. Photonics **9**, 397 (2015).
[10] A. Leverrier, Phys. Rev. Lett. **114**, 070501 (2015).
[11] D. Huang, D. Lin, C. Wang, W. Q. Liu, S. H. Fang, J. Y. Peng, P. Huang, and G. H. Zeng, Opt. Express **23**, 17511 (2015).
[12] E. Diamanti and A. Leverrier, Entropy **17**, 6072 (2015).
[13] N. Walk, S. Hosseini, J. Geng, O. Thearle, J. Y. Haw, S. Armstrong, S. M. Assad, J. Janousek, T. C. Ralph, T. Symul, H. M. Wiseman, and P. K. Lam, Optica **3**, 634 (2016).
[14] B. Qi, Phys. Rev. A **94**, 042340 (2016).
[15] E. Diamanti, H. K. Lo, B. Qi, and Z. L. Yuan, npj Quantum Inf. **2**, 16025 (2016).
[16] Y. M. Li, X. Y. Wang, Z. L. Bai, W. Y. Liu, S. S. Yang, and K. C. Peng, Chin. Phys. B **26**, 040303 (2017).
[17] Z. Qu and I. B. Djordjevic, Opt. Express **25**, 7919 (2017).
[18] A. Leverrier, Phys. Rev. Lett. **118**, 200501 (2017).
[19] J. Lodewyck, T. Debuisschert, R. Tualle-Brouri, and P. Grangier, Phys. Rev. A **72**, 050303 (2005).
[20] R. García-Patrón and N. J. Cerf, Phys. Rev. Lett. **102**, 130501 (2009).
[21] V. C. Usenko and R. Filip, Phys. Rev. A **81**, 022318 (2010).
[22] Y. J. Shen, X. Peng, J. Yang, and H. Guo, Phys. Rev. A **83**, 052304 (2011).
[23] C. Weedbrook, S. Pirandola, and T. C. Ralph, Phys. Rev. A **86**, 022318 (2012).
[24] P. Jouguet, S. Kunz-Jacques, E. Diamanti, and A. Leverrier, Phys. Rev. A **86**, 032309 (2012).
[25] X. Y. Wang, J. Q. Liu, X. F. Li, and Y. M. Li, IEEE J. Quantum Electron. **51**, 5200206 (2015).
[26] C. S. Jacobsen, T. Gehring, and U. L. Andersen, Entropy **17**, 4654 (2015).
[27] X. C. Ma, S. H. Sun, M. S. Jiang, and L. M. Liang, Phys. Rev. A **88**, 022339 (2013).
[28] P. Jouguet, S. Kunz-Jacques, and E. Diamanti, Phys. Rev. A **87**, 062313 (2013).
[29] J. Z. Huang, S. Kunz-Jacques, P. Jouguet, C. Weedbrook, Z. Q. Yin, S. Wang, W. Chen, G. C. Guo, and Z. F. Han, Phys. Rev. A **89**, 032304 (2014).
[30] S. Kunz-Jacques and P. Jouguet, Phys. Rev. A **91**, 022307 (2015).
[31] B. Qi, P. Lougovski, R. Pooser, W. Grice, and M. Bobrek, Phys. Rev. X **5**, 041009 (2015).
[32] H. K. Lo, M. Curty, and B. Qi, Phys. Rev. Lett. **108**, 130503 (2012).
[33] Z. Y. Li, Y. C. Zhang, F. Xu, X. Peng, and H. Guo, Phys. Rev. A **89**, 052301 (2014).
[34] X. C. Ma, S. H. Sun, M. S. Jiang, M. Gui, and L. M. Liang, Phys. Rev. A **89**, 042335 (2014).
[35] D. W. Scott, Wiley Interdiscip. Rev: Comput. Statist. **3**, 177 (2011).
[36] R. Renner and J. I. Cirac, Phys. Rev. Lett. **102**, 110504 (2009).
[37] A. Leverrier and P. Grangier, Phys. Rev. Lett. **102**, 180504 (2009).