One-time shot-noise unit calibration method for continuous-variable quantum key distribution

Yichen Zhang\textsuperscript{1}, Yundi Huang\textsuperscript{1}, Ziyang Chen\textsuperscript{2}, Zhengyu Li\textsuperscript{2}, Song Yu\textsuperscript{1}, \textsuperscript{*} and Hong Guo\textsuperscript{2\dag}

\textsuperscript{1}State Key Laboratory of Information Photonics and Optical Communications, Beijing University of Posts and Telecommunications, Beijing 100876, China
\textsuperscript{2}State Key Laboratory of Advanced Optical Communication Systems and Networks, Department of Electronics, and Center for Quantum Information Technology, Peking University, Beijing 100871, China

(Dated: August 20, 2019)

The shot-noise unit in continuous-variable quantum key distribution plays an important and fundamental role in experimental implementation as it is used as a normalization parameter that contribute to perform security analysis and distill the key information. However, the traditional calibration procedure and detector model can not cover all system noise in practical application, which will result in some loopholes and influence the practical security. What’s more, the traditional procedure is also rather complicated and has difficulty in compatible with automatic operating system. In this paper we propose a calibration model based on the proposed trusted detector model, which could naturally close the loopholes in practical application. It can help identify the shot-noise unit in only one step, which can not only effectively simplify the evaluation process but also reduce the statistical fluctuation, while two steps are needed in traditional method. We prove its feasibility and derive the complete version of the corresponding entanglement-based model. Detailed security analysis against arbitrary collective attacks and numerous simulation results in both the asymptotic limit regime and the finite-size regime are provided. A proof-of-principle experiment has been implemented and the results indicate that the one-time-calibration model can be employed as a powerful substitution to calibrate the shot-noise unit. Our method paves the way for the deployment of continuous-variable quantum key distribution with real time calibration and automatic operation.

I. INTRODUCTION

Quantum key distribution (QKD) \cite{1,2,3} is designed with the aim of realizing a physical-principle guaranteed secure key distribution between the two legitimate parties: Alice and Bob. Continuous variable (CV) QKD \cite{4,5} is developed little posterior to discrete variable QKD but becomes more appealing by virtue of its adaptability of implementing in existing commercial telecom systems. CV-QKD protocols using coherent states \cite{6,7} is considerably simple to implement and reverse reconciliation of CV-QKD protocols can break through the “3dB” limitation in reconciliation process \cite{8} thus they are generally applied in most of the experiment demonstrations. Moreover, finite-size effect has also been extensively studied as its impact commonly influences the practical CV-QKD system performance \cite{10,11,12}. The maximum achievable secret key rate of QKD has also been investigate as the PLOB bound\cite{13,14}.

CV-QKD protocol using Gaussian modulation coherent states can achieve a relatively higher secret key rate and its security has been proved against arbitrary attacks in both asymptotic regime and finite-size regime \cite{10,11,12,15,16,17,18}, thus is getting more popular in recent years. Experimental demonstrations based on laboratory conditions have been conducted to prove its feasibility and field tests based on real-life environmental conditions are carried out subsequently for the future practical applications \cite{19,20,21,22,23,24,25}. The longest distance of the practical field experiments that has been reported is 50km \cite{26}.

Recently, great efforts made in the proving of the security of CV-QKD with discrete modulation and several progress has achieved. \cite{23,24}. In all CV-QKD system, the shot-noise unit (SNU) plays an important and fundamental role because the calibrated SNU will be treated as a normalization parameter to quantize the quadrature measurement results which will eventually contributes to estimate the secret key rate.

However, previous experiment demonstrations usually applied the two-time-evaluation (TTE) procedure \cite{20,22}, which requires first measuring electronic noise of the practical homodyne detector then measuring the output of homodyne detector with the local oscillator (LO) path taken on. In this way, the SNU is calibrated by using the results of the second measurement results minus the electronic noise from the first measurement results which is obviously a rather complicated procedure. And since the SNU is not measured directly, it will certainly bring in more inaccuracy. Notwithstanding, such calibration scheme can open security loopholes that the eavesdropper Eve can utilize to procure the key information \cite{28,29}. Eve can take actions to change the SNU during the key distribution procedure, then the SNU used to normalize the measured quadratures will not be the same as the real SNU, in this way Alice and Bob are prone to underestimate the channel excess noise that further threatens the security of the CV-QKD system. Also, the imperfections of the homodyne detection can also affect the evaluation of SNU. Adopting SNU monitoring is a commonly used countermeasure against such attack, while local LO
scheme where the LO is generated by Bob using an independent laser can effectively resist attacks against the calibration of the SNU [30, 31].

In this paper, we propose a one-time-calibration model that uses two beamsplitters to imitate the imperfections of homodyne detector in the corresponding entanglement-based (EB) model. The new calibration model can simplify the calibration procedures as it does not require measuring the electronic noise for each use of the practical systems. We simply measure the output of the homodyne detector with the LO path connected, and take that measurement result as a new SNU. Also, the statistical fluctuation of SNU introduced by the calibration procedures can be reduced by applying the one-time-calibration model. Detailed analysis on the secret key rate calculations and performances of the proposed model are fully provided. Finally, we consider the proposed model in finite-size regime to testify its performance in a more practical environment. We remark that the one-time-calibration model can basically approach the system performance to the original two-time calibration model in both asymptotic regime and finite-size regime. A demonstration experiment is conducted in order to indicate its eventuality and the results proves that the one-time-calibration model provides us a better substitution when performing calibration procedures.

The rest of the paper is organized as follows: In Sec. II, we review the definition of SNU then provide introduction of the conventional method applied in estimating SNU and the limitations exist under such method. In Sec. III we propose the complete one-time-calibration procedure where we start from the practical output of the homodyne detector. In Sec. IV, we mainly focus on the performance of the one-time-calibration model, where we present the key rate calculation of the model in detail, and then analyze the model behaviour under finite-size regime. We also provide multiple simulation results and give meticulous discussions in this section. We provide experiment details in Sec. V and the conclusions are drawn in Sec. VI.

II. CALIBRATION OF SHOT-NOISE UNIT

In this section we first review the conventional trusted noise and trusted modelling of the homodyne and heterodyne detector, then describe the conventional approach of calibrating the SNU. Lastly, we point out the limitations in the existing SNU calibration method.

A. Conventional trusted detector modelling

We start by reviewing the trusted noise modelling of the homodyne and heterodyne detector. Usually a homodyne detector or a heterodyne detector has two main imperfections: a finite detection efficiency \( \eta \), and electronic noise \( \epsilon_{ele} \) [20]. In the untrusted modelling, the imperfections of the practical homodyne and heterodyne detector contribute to the channel loss or the channel excess noise that controlled by the eavesdropper Eve. While another way of modelling the homodyne or heterodyne detector is trusted modelling, ground on which the assumption is made that the apparatus of Bobs set up is not accessible to Eve [32]. This way we can consider the imperfections of the homodyne or heterodyne detector as trusted loss and trusted noise. The trusted modelling can improve the system performance as it slightly restricts Eves ability.

The EB version of the trusted model of the homodyne and heterodyne detector is depicted in Fig. 1. In this model, the limited detection efficiency is modeled by a beamsplitter whose transmittance is used to imitate the detection efficiency, while the electronic noise is modeled by an EPR source whose one mode is coupled into the quantum signal coming from the channel through the beamsplitter, and the variance added by this coupling is used to imitate the electronic noise.

The availability of both the untrust and trust modelling relays on the equivalence of the EB model and the prepare-and-measure (PM) model. So, we subsequently write out the output of a practical homodyne detector in the corresponding PM model:

\[
X_{out} = AX_{LO} \left( \sqrt{\eta \hat{x}_B} + \sqrt{1 - \eta \hat{x}_v} \right) + X_{ele}. \tag{1}
\]

where \( X_{ele} \) is a Gaussian variable with variance \( \nu_{ele} \) which normally has a Gaussian distribution, \( A \) is the circuit amplification parameter.

While however, sequence of the result from the homodyne detection can not be used directly. To the purpose of analyzing Eve’s information from the output \( X_{out} \), we need to quantize this value using the SNU:

\[
x_{SNU}^{'out} = \frac{X_{out}}{\sqrt{SNU}} = \left( \sqrt{\eta \hat{x}_B} + \sqrt{1 - \eta \hat{x}_v} \right) + \frac{X_{ele}}{AX_{LO}}. \tag{2}
\]
The output sequence of $x_{out}^{SNU}$ corresponds to output of its EB model, which is depicted in Fig. 1.

The inspiring method of using local local oscillator to interference with the quantum signal in the detection stage can defend all kinds of attacks against the local oscillator. Albeit, the local laser has fluctuations itself, and the electronic noise of the detector also suffers from the undulation due to the environment change for example the temperature change. Thus even adopting the local local oscillator scheme the calibration procedure is certainly required. The proposed measurement-device-independent protocols also are dedicated to defend all kinds of attacks against the homodyne detector, requires proper calibration of the SNU [33–35].

B. Conventional shot-noise unit calibration: two-time-calibration method

In this subsection we review the conventional way of calibrating the SNU.

Typically, two step are required to perform the SNU calibration. Step 1, Calculate the variance of the homodyne detector output with both quantum signal and LO taken off as the electronic noise $V_{ele}$. Step 2, Calculate the variance of the homodyne detector output $V_{tot}$ with only the LO path connected, as a total noise of electronic noise as well as shot-noise unit. After these two steps, one could calculate the shot-noise unit through the equation:

$$SNU = V_{tot} - V_{ele}.$$  \hfill (3)

In the following we also use $SNU^{TTE}$ to refer this kind of calibration method. In practice, even under the assumptions of untrusted modelling, the electronic noise is still known from the corresponding PM model regardless of the EB scenario adopted in the security analysis in order to obtain the SNU. Thus, the trusted modelling is more reasonable in the EB scenario.

C. Limitations with the conventional calibration

First and foremost, the $V_{tot}$ in Eq. (3) is more than the vacuum noise plus the electronic noise, other noises including the relative intensity noise (RIN) should be included. So $V_{tot}$ should be rewritten as $V_{tot} = SNU + V_{ele} + V_{RIN}$, as is described in Eq. (3), the SNU calculated is $SNU^{TTE} = SNU + V_{RIN}$. More precisely, the output of the practical homodyne detector should be rewrite as:

$$X_{out} = AX_{LO} \left( \sqrt{\eta_d} \hat{x}_B + \sqrt{1 - \eta_d} \hat{x}_{\nu 1} \right) + X_{ele} + X_{RIN}.$$ \hfill (4)

The sequence of the raw key after the SNU normalization is thus given by:

$$x_{out}^{SNU^{TTE}} = \frac{X_{out}}{\sqrt{SNU + V_{RIN}}} = \frac{AX_{LO}}{\sqrt{SNU + V_{RIN}}} \left( \sqrt{\eta_d} \hat{x}_B + \sqrt{1 - \eta_d} \hat{x}_{\nu 1} \right) + \frac{X_{ele} + X_{RIN}}{\sqrt{SNU + V_{RIN}}}.$$ \hfill (5)

Thus, the equivalence between the PM model with the EB version of the model does not hold anymore.

Yet, as can be seen from Eq. (2), any incorrect estimated SNU will cause the false approximation of the statistics, furthermore, security analysis suggests that slightly error in the SNU estimation can greatly decrease the secret key rate.

In a realistic scenario, the inaccuracies of the SNU can result in drastically decreasing in the estimated secret key rate through the security analysis. The simulation result is displayed in Fig. 2. It can be seen that even with an 0.1% deviation from the real SNU, the secret key rate can significantly drop to zero when the transmission distance is over 50km.

Moreover, attacks against the SNU can severely threat the security of the practical CV-QKD systems. For instance, the response curve of the homodyne detector is normally calibrated before the distribution stage, so Eve can launch an attack that controls the LO signal [29], which can delay the trigger of the detector. This way, the actual slope of the response curve will be decreased, then if Bob still employs the original response curve to evaluate the SNU, the SNU will be overestimated, which further will lead to the underestimate of the excess noise. Also, attack against the intensity of the LO [28] during the key distribution stage can also cause the misestimate of the SNU, the noise induced by Eve’s attack may be underestimated if Bob applies the calibrated SNU to normalise its data. Thus a security loophole may be turned on.

Under the conventional implementation, each optical path of signal and LO will require an optical switch, which will inevitably increase costs, complicate the SNU calibration procedure as well as data processing procedures. While adding optical switch in the LO path also decreases the optical power, which is no good to the homodyne detection that demand a sufficient amplification on the LO signal.

Since the variance of the electronic noise and the total noise variance are measured separately, the SNU is not directly evaluated. According to Eq. (3), using subtraction to calculate the calibrated SNU introduces more statistical fluctuations since both the electronic and the total noise variance suffers from the finite-size effects.
In this model, we still consider the electronic noise and the limited detection efficiency as the main imperfections of the practical homodyne detector. Two beamsplitters are applied to represent the electronic noise and the limited detection efficiency respectively in the corresponding EB model. In this scenario, the electronic noise is modeled by the transmittance of the beamsplitter. As is depicted in Fig. 3, the transmittance $\eta_d$ of the first beamsplitter $D_1$ equals to the efficiency of the detector, while the transmittance $\eta_e$ of the second beamsplitter $D_2$ models the electronic noise.

In order to keep consistent with the previous SNU calibration of the experimental demonstrations, in the following we still do not consider the RIN specifically, where we recognize the RIN is included in the $SNU^{TEE}$ of the conventional calibration model. We only need to measure one time to identify the SNU when we exploit this model. The new SNU is measured as the output when the LO signal is on, so the new SNU can be rewritten as:

$$SNU' = V_{tot} = SNU + V_{ele},$$

where $SNU'$ is the new calibrated shot-noise unit, $SNU$ is the shot-noise unit measured from two-time evaluation procedure.

Under this modeling, certain advantages can be procured: Firstly, we only need one optical switch in signal path in our system. Secondly, only one-time calibration is required in this model, which makes it a more utility model applying in practical systems. Thirdly, since we only need one-time period to calculate the shot-noise unit, the statistic fluctuation is minimized compared with original calibration model with two-time evaluation.

To analyze the one-time-calibration model in detail, certain assumptions about the homodyne detector are made in the first place:
1. The loss in Bob’s side will not leak any information to Eve.
2. The electronic noise is not caused by Eve, and will not leak any information to Eve.
3. The electronic noise is an additive Gaussian noise.

We draw the complete EB version of the one-time evaluation model for particular analysis. The beamsplitter $B1$ is utilized to stimulate the electronic noise of the practical homodyne detector. Detailed analysis of the derivation are described as follows: We start with considering the ideal homodyne detection, let us take $x$-quadrature for instance:

$$\hat{x}_{hom} = \sqrt{\eta_e} \left( \sqrt{\eta_d} \hat{x}_B + \sqrt{1 - \eta_d} \hat{x}_{e1} \right) + \sqrt{1 - \eta_e} \hat{x}_{e2},$$

where $\hat{x}_{e1}, \hat{x}_{e2}$ indicate the vacuum coupled-in by the two beamsplitters. Vacuum state $\hat{x}_{e1}, \hat{x}_{e2}$ are two Gaussian variables.
FIG. 3. (Color online) The entanglement-based model of one-time evaluation model. The model is based on coherent states and homodyne detection where Alice applies an heterodyne measurement on one mode of the EPR states, the other mode is sent to the quantum channel and measured by homodyne detection. The two other beamsplitters are used to imitate the electronic noise and the limited detection efficiency.

Nevertheless, we can consider the electronic noise as another “optical mode”, then we can define a joint shot-noise unit called $SNU_{OT E}$, which counts both the quantum signal and the optical mode. The new joint SNU will be:

$$SNU_{OT E} = A^2 X_{LO}^2 + \langle \Delta X_{ele}^2 \rangle = A^2 X_{LO}^2 + v_{cl}. \quad (8)$$

So the data after quantization using new joint $SNU_{OT E}$ is:

$$X_{\text{out}}^{SNU_{OT E}} = \frac{X_{\text{out}}}{\sqrt{SNU_{OT E}}} = \frac{A X_{LO}}{\sqrt{A^2 X_{LO}^2 + v_{cl}}} \left( \sqrt{\eta_d \hat{x}_B} + \sqrt{1 - \eta_d \hat{x}_{v1}} \right) + \frac{X_{ele}}{\sqrt{A^2 X_{LO}^2 + v_{cl}}} \hat{x}_{v2}. \quad (9)$$

Considering $X_{ele}$ is a Gaussian variable and it is immune to Eve, accordingly we can replace it with a Gaussian operator: $\sqrt{v_{cl}} \hat{x}_{v2}$, in which $\hat{x}_{v2}$ has the variance of 1. Then:

$$X_{\text{out}}^{SNU_{OT E}} = \frac{A X_{LO}}{\sqrt{A^2 X_{LO}^2 + v_{cl}}} \left( \sqrt{\eta_d \hat{x}_B} + \sqrt{1 - \eta_d \hat{x}_{v1}} \right) + \frac{\sqrt{v_{cl}}}{\sqrt{A^2 X_{LO}^2 + v_{cl}}} \hat{x}_{v2}. \quad (10)$$

Now if we define $\eta_e = \frac{A^2 X_{ele}^2}{A^2 X_{LO}^2 + v_{cl}}$, then equation(8) can be rewrite as equation(3), then $x_{\text{new}}^{\text{out}} = \hat{x}_{\text{hom}}$.

Thus we have also derived the corresponding EB version of the model and the equivalence between the PM model and the EB model is built. The PM model is used for actual implementation in the system while the EB model is used for security analysis. Our derivation guarantees that the measurement results of mode $B_3$ in the EB scheme are the same as the output of the PM scheme. Therefore, in this EB scheme, we never change the unit of the vacuum, the variance of the vacuum is always 1. This implies the EB model can describe the practical PM scheme where the measurement output is quantized by the $SNU_{OT E}$.

In this scheme the dissipation incurred by the imperfections of the homodyne detector can be observed intuitively. When the electronic noise is not too big, it can simply be modelled as an extra loss at the receiver’s side. For example, we assume the detection efficiency is 0.65, the clearance between the SNU and the electronic noise is normally required above 10dB, which in total a 2.3dB loss is acquired, which is equivalent to a 11km fiber loss. For those homodyne detectors that employ higher SNU over electronic noise like 15dB, the total loss of the homodyne detector is around 2dB which is about 10km fiber loss, which is quite acceptable in a realistic set up.

Next we quickly review the case where the RIN is taking into the consideration: In this case we identify the $SNU_{OT E}$ as:

$$SNU_{OT E} = SNU + V_{ele} + V_{RIN}. \quad (11)$$

To build the equivalence between the PM model and the corresponding EB model, we start by the output of the practical detector of the PM model in equation(1), next we quantize the output sequence of the detector by this $SNU_{OT E}$ as:

$$x_{\text{out}} = \frac{X_{\text{out}}}{\sqrt{SNU + V_{ele} + V_{RIN}}} = \frac{A X_{LO}}{\sqrt{SNU + V_{ele} + V_{RIN}}} \left( \sqrt{\eta_d \hat{x}_B} + \sqrt{1 - \eta_d \hat{x}_{v1}} \right) + \frac{X_{ele} + X_{RIN}}{\sqrt{SNU + V_{ele} + V_{RIN}}}. \quad (12)$$
In this scenario if we define \( \sqrt{\eta_e} = \frac{\Delta X_{\text{EB}}}{\sqrt{\text{V}_{\text{ele}}+\sqrt{\text{V}_{\text{RIN}}}}} \), then the output of the PM model equals to that of the EB model in Fig.3, thus the equivalence between the EB model and the PM model holds, which proves that the one-time calibration model can extended the security analysis in the trusted modelling and the SNU calibration process when any other addictive noise is considered.

B. One-time shot-noise unit calibration method

From a perspective of practical security, real time calibration can defense most attacks against LO or detectors but it would demand seamless switching between the SNU evaluation and the key distribution. Thus one optical switch is needed in the signal path, when the optical switch is connected, the system performs key distribution, when the optical switch is taken off, the system performs SNU calibration.

With our intuition of solving problems appeared in subsection 2.3, adopting one-time-calibration process we can circumvent the usage of the optical switch on the LO path. It makes the real time calibration possible since the optical switch on the LO side can decide whether the system is in key distribution scheme or in SNU calibration scheme. The optical power is maximally to be retained thus it also helps amplifying the quantum signal.

Furthermore, the data used to perform calibration is rather limited especially when more data are required to distill key information. So the finite-size effect need to be carefully considered to help understand the effect caused by the finite data. For the one-time-calibration model the SNU in this scenario is directly measured thus the statistical fluctuation is suppressed. In Fig.4 we provide the simulation result that explores the SNU behaviour of the one-time calibration model as well as the conventional model. In order to maximally imitate the practical realization we take the total noise variance as 2.3768 and the electronic noise variance 0.421. The simulation result shows the normalized SNU as a function of block length. In order to intuitively observe the deviation owing to the finite-size effects, we define another variable that measures the difference between the ideal calibration and the practical normalization. The simulation result is drawn in the right Y axis as a function of block length. Although the two model behave quite the same when the block length is over \( 10^8 \), from the deviation compared to the ideal calibration the one-time evaluation model has better performance than the conventional calibration model against finite-size effect.

IV. SECURITY ANALYSIS AND NUMERICAL SIMULATION

The proposed one-time-calibration model that helps reduce the system complexity and achieve seamless real time SNU calibration is distinctly more compliance with practical key distribution scenario. Further, we have extended the security analysis where the equivalence of the PM model and the EB model is built up in a more practical implementations where noises like RIN can be taken into consideration. In this chapter we give exhaustive analysis on the performance of one-time-calibration model. Secret key rate calculations in both asymptotic regime and finite-size regime are provided while numerous simulation results are illustrated to show their behaviours compared to the original calibration model.

A. Asymptotical regime

The complete EB version of the one-time evaluation model is pictured in Fig.1. In our proposed model, the electronic noise \( \eta_e \) is not directly measured, thereby the secret key rate calculation may not be so straightforward. As a preliminary consideration, Alice’s data and Bob’s data are directly accessible from the experiment in the PM scheme thus mode A and mode B are what we can at least conclude in the corresponding EB model. Although mode C and mode D are not controlled by Eve, we merely ignore them at the moment. In this scenario the covariance matrix used to calculate the key rate is a four-order covariance matrix:
\[
\gamma_{AB_3} = \begin{pmatrix} \gamma^A_{AB_3} & \Gamma^A \\
\phi^A_{AB_3} & \gamma^B_{B_3} \end{pmatrix}.
\]

The covariance matrix of \(AB'\) can be deduced as:

\[
\gamma_{AB_3} = \begin{pmatrix} V I_2 & V \sqrt{T C_{\eta d} \eta e (V^2 - 1) \sigma_Z} \\
\sqrt{T C_{\eta d} \eta e (V^2 - 1) \sigma_Z} & T C_{\eta d} \eta e (V - 1 + \kappa e) + 1 \end{pmatrix},
\]

where \(V\) is the variance of EPR state in EB model, \(T C\) indicates channel transmissivity and \(\kappa e\) is the channel excess noise. \(I_2\) is second-order identity matrix and \(\sigma_Z\) is a 2*2 matrix:

\[
\begin{pmatrix} 1 & 0 \\
0 & -1 \end{pmatrix}.
\]

The main focus of secret key rate calculation is how to evaluate the upper bound of the information that Eve can procure. According to equation (10), we can derive the uncertainty on Bob’s variance after the measurement on Alice’s side. According to equation (10), we can calculate \(I_{AB}\):

\[
I_{AB_3} = H(B_3) - H(B_3|A),
\]

where \(H(B)\) can be calculated as \(\frac{1}{2} \log_2 V_B\), \(H(B|A)\) is the conditional Shannon entropy that can be calculated as \(\frac{1}{2} \log_2 V_B|A\), the conditional variance \(V_B|A\) means the remaining uncertainty on Bob’s variance after the measurement on Alice’s side. According to equation (10), we can derive \(I_{AB}\) as:

\[
I_{AB_3} = 1 \log_2 \left( V + \chi \right) / \chi + 1,
\]

where we define \(\chi\) as \(\chi = 1 / T C_{\eta d} \eta e - 1 + \kappa e\) for conciseness.

Now we derive the mutual information between Bob and Eve, the maximum information between Eve and Bob is decided by the Holevo interval [37] \(\chi_{B,E}\):

\[
\chi_{B,E} = S(\rho_{E}) - \int dm_{B_3} p(m_{B_3}) S(\rho_{E_{m_{B_3}}}).
\]

According to the Fig.1, eavesdropper Eve and the measurement will both purify the system \(AB'\), then \(\chi_{B,E}\) should be written as:

\[
\chi_{B,E} = S(\rho_{AB_3}) - S(\rho_{A_{m_{B_3}}}),
\]

where \(S(\rho_{AB_3})\) and \(S(\rho_{A_{m_{B_3}}})\) can be figured out by calculating the symplectic eigenvalues of the correspondence covariance matrix \(\gamma_{AB_3}\) and \(\gamma_{A_{m_{B_3}}}\), where \(\gamma_{A_{m_{B_3}}}\) is the covariance matrix of modes A and \(B_3\) after Bob performing detections:

\[
\chi_{B,E} = \sum_{i=1}^{3} G \left( \frac{\lambda_i - 1}{2} \right) - \sum_{i=3}^{4} G \left( \frac{\lambda_i - 1}{2} \right),
\]

where \(G(x) = (x + 1) \log_2 (x + 1) - x \log_2 x\), and \(\lambda_i\) are the symplectic eigenvalues. We have already derived the covariance matrix of \(AB_3\), so its symplectic eigenvalues \(\lambda_1, \lambda_2\) can be subsequently derived:

\[
\lambda^2_{1,2} = \frac{1}{8} \left[ A ± \sqrt{A^2 - 4B} \right],
\]

\[
A = V^2 (1 - 2 T C_{\eta d} \eta e) + 2 T C_{\eta d} \eta e + (T C_{\eta d} \eta e)^2 (V + \chi)^2,
\]

\[
B = (T C_{\eta d} \eta e)^2 (V + 1)^2.
\]

Next we calculate the symplectic eigenvalues of the covariance matrix of \(\gamma_{A_{m_{B_3}}}\). After the quantum signals arrive at Bob’s side, Bob can take whether homodyne detection or heterodyne detection to measure the quantum states. Considering most practical systems would use homodyne detection at present, in this paper we analyze the symplectic eigenvalues after Bob performs homodyne detection.

Bob performs homodyne detection on mode B, measuring whether its coordinate x or momentum p. After detection, mode A will be projected to new Gaussian state, where the covariance matrix will become:

\[
\gamma_{A_{m_{B_3}}} = \gamma_A - \sigma_{AB_3} (X \gamma_{B_3} X) M P^T \sigma_{AB_3}^T,
\]

where \(\gamma_A, \gamma_{B_3}, \sigma_{AB_3}\) are corresponded with equation (9), and we find that \(\gamma_{A_{m_{B_3}}}\) takes the form:

\[
\gamma_{A_{m_{B_3}}} = \begin{pmatrix} \chi_3 + 1 & 0 \\
0 & V \end{pmatrix},
\]

The symplectic eigenvalue of this matrix is:

\[
\lambda^2_3 = V (\chi_3 + 1) / \chi_3 + V \chi_3.
\]

Now we can calculate the upper bound of information that Eve can procure. Combining with the equation (11) and equation (14), the secret key rate is calculable.

In the above scenario we include mode A and mode \(B_3\) into our security analysis, we call it two-mode EB model. However, we scarcely exploit the features of the two beamsplitters that represent the homodyne detector imperfections in the EB model which may result in the underestimate of the secret key rate. In the following we manage to take these imperfections into trusted losses. By permuting the two beamsplitters, we can take the mode C that models the detector efficiency into Bob’s side. The feasibility of the permuting operation is based on the trusted homodyne detector assumption.
The eavesdropper Eve cannot take control of the homodyne detector, the permuting operation will not affect detected mode $B_3$, thus it will not influence Eve’s knowledge about Bob’s result. After the permuting of the beamsplitters, we obtain a new EB model and since mode $B_3$ remains unchanged, this new EB scheme is still a match with the PM scheme that uses $SU^{OTE}_N$ to quantise the measurement output. The complete EB version of this scenario is traced out in Fig. 3 and in total modes $A$, $B_3$, and $C$ are comprised into consideration. In this case mode $D$ that represents the electronic noise is still unknown to us, but the detection efficiency is a known quantity. Thus we may obtain the covariance matrix with there mode $A$, $B_3$, and $C$, we call it three-mode EB model, and it should take the form of:

$$\gamma_{ABCB_3} = \begin{pmatrix} \gamma_A & \phi_{AC} & \phi_{AB_3} \\ \phi_{AC}^T & \gamma_C & \phi_{CB_3} \\ \phi_{AB_3}^T & \phi_{CB_3}^T & \gamma_{B_3} \end{pmatrix}. \quad (25)$$

Alice first generate two-mode squeezed state then send one of its mode to the quantum channel, before it goes through the first BS, the state of the system $AB_1'$ is a pure state with the expectation of 0, the covariance matrix of modes $A$ and $B_1'$ is:

$$\gamma_{AB_1'} = \begin{pmatrix} VI_2 & \sqrt{T(V^2 - 1)\sigma_z} \\ \sqrt{T(V^2 - 1)\sigma_z} & [T(V - 1 + \varepsilon_c) + 1]I_2 \end{pmatrix}. \quad (26)$$

After the quantum signal goes through the first BS, $AB_2'D$ is a pure state, it can be described with covariance matrix $\gamma_{AB_2'D}$:

$$\gamma_{AB_2'D} = (Y^{BS})^T[\gamma_{AB_1'} \oplus I_2](Y^{BS}). \quad (27)$$

The covariance matrix $\gamma_{AB_1'}$ performs kronecker product with vacuum state since no other signal is needed to couple in the beamsplitter in this scenario. $Y^{BS}$ is the transformation matrix of the first beamsplitter, which models the electronic noise of the practical homodyne detector:

$$Y^{BS} = I_2 \oplus Y_{\eta_e}^{BS}, \quad (28)$$

where $Y_{\eta_e}^{BS}$ is the symplectic matrix of the beamsplitter:

$$Y_{\eta_e}^{BS} = -\frac{\sqrt{\eta_e I_2}}{\sqrt{1 - \eta_e I_2}}, \quad \frac{\sqrt{1 - \eta_e I_2}}{\sqrt{\eta_e I_2}}. \quad (29)$$

However we do not measure the electronic noise directly which implies we do not know the mode $D$ in this one-time evolution model. For the rest, the covariance matrix $\gamma_{AB_2'C}$ is:

$$\gamma_{AB_2'C} = (Y^{BS'})^T[\gamma_{AB_2'} \oplus I_2](Y^{BS'}), \quad (31)$$

where $Y^{BS'}$ is the transformation matrix that imitate the limited detection efficiency of the practical beam splitter:

$$Y^{BS'} = I_2 \oplus Y_{\eta_d}^{BS}. \quad (32)$$

$Y_{\eta_d}^{BS}$ is the symplectic matrix of the beamsplitter:

$$Y_{\eta_d}^{BS} = \begin{pmatrix} \sqrt{\eta_d I_2} & \sqrt{1 - \eta_d I_2} \\ -\sqrt{1 - \eta_d I_2} & \sqrt{\eta_d I_2} \end{pmatrix}. \quad (33)$$

Now the covariance matrix of three modes $A$, $B_3$, and $C$ can be calculated using equation (29). And it is supposed to achieve a higher secret key rate compare to the two-modes model aforementioned.

$$\gamma_{ABC} = \begin{pmatrix} VI_2 & \sqrt{T_{\eta_e} \eta_d (V^2 - 1)\sigma_z} & \sqrt{T_{\eta_e} \eta_d (1 - \eta_d) (V^2 - 1)\sigma_z} \\ \sqrt{T_{\eta_e} \eta_d (1 - \eta_d) (V^2 - 1)\sigma_z} & [T_{\eta_e} \eta_d (V - 1 + \varepsilon_c) + 1]I_2 & \sqrt{T_{\eta_e} \eta_d (1 - \eta_d) \eta_e (V - 1 + \varepsilon_c) I_2} \\ \sqrt{T_{\eta_e} \eta_d (1 - \eta_d) \eta_e (V - 1 + \varepsilon_c) I_2} & \sqrt{T_{\eta_e} \eta_d (1 - \eta_d) \eta_e (V - 1 + \varepsilon_c) I_2} & [T_{\eta_e} \eta_d (1 - \eta_d) (V - 1 + \varepsilon_c) + 1]I_2 \end{pmatrix}. \quad (34)$$

In this case, the secret key rate is calculated the same way as Eq. (13). The mutual information between Alice and Bob is figured as Eq. (14) with the variance of EPR state at Alice’s side $V$, variance at Bob’s side $(T_{\eta_e} \eta_d (V - 1 + \varepsilon_c) + 1)$ and covariance between Alice and Bob $(T_{\eta_e} \eta_d (V^2 - 1))$ which gives exactly the same results as the two-mode model scenario as Eq. (15).

Next we estimate the upper bound of information between Eve and Bob, according to Eq. (16), $\chi_{BE}$ is now rewritten as:

$$\chi_{BE} = S(\rho_{ABC}) - S(\rho_0^{ABC}). \quad (35)$$

$S(\rho_{ABC})$ is Eve’s Von Neumann entropy, since Eve
purifies the system $AB_3C$. It can be figured out with the symplectic eigenvalues of the corresponding covariance matrix $\gamma_{AB_3C}$, but there is one eigenvalue that constantly equals to one, which means it contains no information, while the other symplectic eigenvalues contribute to the entropy. $S(\rho_{AB_3})$ is the Von Neumann entropy of the remaining quantum states have after Bob performs homodyne detection. So over all, the mutual information between Eve and Bob can be can be further exploit as the same as Eq. (18).

$\lambda_1$ and $\lambda_2$ are derived from covariance matrix $S(\rho_{AB_3C})$:

$$\lambda_{1,2}^2 = \frac{1}{2}[A \pm \sqrt{A^2 - 4B}],$$

where parameter $A$ and $B$ are:

\[
\begin{align*}
A &= C(2 + C) + D + 1, \\
B &= V^2[(1 - \eta_d)\eta_d C^2 + C + 1]^2 - \\
&\quad V[(1 - \eta_d)\eta_d^2 C^2 D - (1 - \eta_d)\eta_d[(1 - \eta_d)\eta_d C^2 + C + 1]^2 - D^2. \\
\end{align*}
\]

(37)

Here we note $C = T\eta_e(V - 1 + \varepsilon_e)$, $D = T\eta_e(V^2 - 1)$ for shortness.

Next we figure out the symplectic eigenvalues of matrix $\gamma_{m_{AB_3}}$ to calculate $S(\rho_{AB_3C})$. $\gamma_{m_{AB_3}}$ is the covariance matrix after Bob applies homodyne detection which can be derived from:

$$\gamma_{m_{AB_3}} = \gamma_{AC} - \phi_{ACB_3}(X\gamma_{B_3X})M^P\phi_{ACB_3}^T.$$  

(38)

It has two non-zero symplectic eigenvalues so the symplectic eigenvalues should have form of:

$$\lambda_{3,4}^2 = \frac{1}{2}[E^2 \pm \sqrt{E^2 - 4F^2}],$$

where $E$, $F$ are defined as:

\[
\begin{align*}
E &= G\sqrt{V^2 - 2(1 - \eta_d)D + (C + 1)[(1 - \eta_d)C + 1]} \\
F &= \frac{(n_dG + V)}{\eta_d C} - (1 - \eta_d)D\left(\frac{n_dC}{\eta_d C + 1} - 1\right)^2[(1 - \eta_d)G + V].
\end{align*}
\]

(40)

where $C$ and $D$ have been defined previously. We noted symbol $G$ as $G = T\eta_e[V(\varepsilon_e - 1) + 1]$ for shortness.

While we are still not satisfy that mode $D$ is practically controlled by Eve as we do not know the electronic noise at this stage. The electronic noise is viewed as the transmittance of the beamsplitter which can be treated as a loss. In realistic experiments, this loss may be calculated from the data of Alice’s and Bob’s, it will express as the product of the channel transmittance $T$ and the transmittance of the beamsplitter $\eta_e$. To the purpose of ultimately finding out the value of $\eta_e$, we can find some restrictions to limit the possible values of $\eta_e$:

$$\begin{align*}
\text{const.} &\leq T \leq 1, \\
\text{const.} &\leq \eta_e \leq 1, \\
T\eta_e &\text{ const.}
\end{align*}$$

(41)

where we assume that const. is the transmittance that represents the total loss from channel and electronic noise. Although it seems that there are plenty of valid values that $\eta_e$ may take, we still have to limit ourselves by the lowest secret key rate can be achieved. And we note that the value is when the channel transmittance $T$ takes the value of const. thereafter $\eta_e$ will only take the value of 1. It suggests that there is no electronic noise existed, all the loss is contributed by the untrusted channel, essentially, this resultant is realised because the lowest secret key rate may be obtained when the untrusted party controls all the loss. It will no longer have mode $D$ and the EB model virtually retrogrades to the scenario where we only consider $A, B_3$ and $C$ aforementioned. Therefore, we may not consider Eve purifies $A, B_3, D$ and $C$ as $S(\rho_{AE}) = S(\rho_{ACDB_3})$ in the EB model, but as $S(\rho_{AE}) = S(\rho_{ACB_3})$, in the form of equation (31).

B. Finite-size regime

In this section, we analyze the finite-size regime on the proposed models as well as the original model and mainly focus on the effect on shot-noise calibration. We first
analyze its influence on shot-noise calibration procedure, then calculate the secret key rate of the proposed models based on covariance matrices.

As is discussed in section III, the original calibration procedure needs two steps to obtain the SNU result. Regarding the new model however, we define the measurement results of the output when the LO path is connected as shot-noise unit, as in equation (3). According to the theory of finite-size analysis [38], the finite-size block will bring in more statistical fluctuations compare to the asymptotic regime, which will lead to the decreasing of the secret key rate. The importance of conducting finite-size analysis in CV-QKD systems has been extensively demonstrated. Succeedingly the secret key rate calculation needs to be revised:

\[
R = \frac{n}{N} \left[ \beta I(A : B) - I_{\varepsilon PE}(B : E) - \Delta(n) \right],
\]

(42)

where \( N \) is the block length and \( n \) is the number of data that used to distill the key information.

We now consider the influence on shot-noise unit of finite-size regime. Maximum likelihood estimation is applied and we can describe the shot-noise unit as:

\[
\hat{V}_{tot} = \frac{1}{m} \sum_{i=1}^{m} (y_{im})^2.
\]

(43)

The ‘hat’ in the above equation suggests that it is an estimated value. We then apply law of large numbers to acquire the approximate distribution of the shot-noise unit:

\[
m\hat{V}_{tot}/V_{tot} \sim \chi^2(m - 1),
\]

(44)

where \( V_{tot} \) is the actual value of the variance of the SNU, \( \chi^2 \) means chi-square distribution. By combining the failure probability during the parameter estimation process \( \varepsilon_{PE} \), we can compute the fluctuation interval for an identified confidence interval. Then by traversing through the confidence interval, we can seek out the worst case. Here, we set the confidence interval as \( \varepsilon_{PE}/2 \), so the range of the fluctuated shot-noise unit can be calculated as:

\[
\Delta V_{tot} = z_{\varepsilon PE/2} \frac{\hat{V}_{tot} \sqrt{\varepsilon}}{\sqrt{m}},
\]

(45)

where \( z_{\varepsilon PE/2} \) satisfies \( 1 - \text{erf}(z_{\varepsilon PE/2}/\sqrt{2})/2 = \varepsilon_{PE}/2 \), and \( \text{erf} \) is the error function that defined as:

\[
\text{erf}(x) = \frac{2}{\sqrt{\pi}} \int_{0}^{x} e^{-t^2} dt.
\]

(46)

Therefore, the final shot-noise unit \( SNU' \) is:

\[
SNU' \in [\hat{V}_{tot} - \Delta V_{tot}, \hat{V}_{tot} + \Delta V_{tot}].
\]

(47)

Based on the explication above, the confidence interval of shot-noise unit of the original two-time evaluation model under finite-size effect should be described as:

\[
SNU = [\hat{V}_{tot} - \Delta V_{tot} - V_{ele} - \Delta V_{ele}, \hat{V}_{tot} - \Delta V_{tot} + V_{ele} + \Delta V_{ele}].
\]

(48)

\( \hat{V}_{ele} \) is the estimated electronic noise which is corresponding to the system output when both the quantum signal path and LO path are turned off. And consequently \( \Delta V_{ele} \) is the statistical fluctuation that this measurement brings in.

Since the influence of finite-size effect on shot-noise unit has already been studied in detail, next we exploit how it changes the secret key rate calculation. We noted the shot-noise-unit as \( N_0 \) for simplicity. For the two-mode model scenario, the variance of mode \( B_3 \) and covariance \( AB_3 \) vary as the shot-noise unit changes. So the covariance matrix needs to be rewritten in order to take consideration of the effect of shot-noise unit:

\[
\gamma_{AB_3} = \left( \frac{VI_2}{\sqrt{T_{\eta e} \eta_d(V^2 - 1)/N_0 \sigma_z}} \right) \{ [T_{\eta e} \eta_d(V - 1 + \varepsilon_{c}) + 1]/N_0 \} I_2.
\]

(49)

With the derived covariance matrix \( \gamma_{AB_3} \), following procedure on secret key rate calculation is quite similar as the case in asymptotic limit regime and by traversing through the confidence interval, the lower bound of the secret key rate under finite-size effect can be figured.

The derivation of three-mode covariance matrix is little complicated. We need to take reconsideration of elements which are varying because of the shot-noise unit fluctuations of the covariance matrix. As is described above, the variance of Bob is modified as \( [T_{\eta e} \eta_d(V - 1 + \varepsilon_{c}) + 1]/N_0 \), the variance of mode \( C \) can be modified by using the element \( V_{B_3} \) subsequently as:

\[
V_C = \frac{(V_{B_3} - 1)}{\eta_d}(1 - \eta_d) + 1.
\]

(50)

Further the covariance elements of the matrix also alter as:

\[
< AB_3 > = \sqrt{T_{\eta e} \eta_d(V^2 - 1)/N_0},
< AC > = - < AB_3 > \sqrt{(1 - \eta_d)/\eta_d},
< B_3 C > = -(V_{B_3} - 1)\sqrt{(1 - \eta_d)\eta_d/\eta_d}.
\]

(51)
So the elements in covariance matrix \( \gamma_{ACB_3} \) which the

\[
\gamma_{ACB_3} = \begin{pmatrix}
-VI_2 & \sqrt{T\eta_c(1-\eta_d)(V^2-1)/N_0\sigma_z} & \sqrt{T\eta_c\eta_d(V^2-1)/N_0\sigma_z} \\
\sqrt{T\eta_c\eta_d(V^2-1)/N_0\sigma_z} & (V_{B_3}-1)(1-\eta_d)/\eta_dI_2 & -(V_{B_3}-1)\sqrt{\eta_d(1-\eta_d)/\eta_d}\sigma_z \\
\sqrt{T\eta_c\eta_d(V^2-1)/N_0\sigma_z} & -(V_{B_3}-1)\sqrt{\eta_d(1-\eta_d)/\eta_d}\sigma_z & V_{B_3}I_2
\end{pmatrix}.
\]

(52)

By setting failure probability of parameter estimation, the confidence interval is able to be identified. Then the lower bound of the secret key rate under finite-size effect can be procured by traversing the shot-noise unit value through the confidence interval. With the modified covariance matrix \( \gamma_{ACB_3} \), further procedures to calculate secret key rate can be followed.

C. Numerical simulation and discussion

In this subsection, we give numerical simulation results of firstly the two one-time-calibration model aforementioned as well as the original two-time-calibration model to make comparison. The comparisons between these models under finite-size regime are also provided subsequently.

Fig.6 shows the secret key rate as a function of the transmission distance for different SNU calibration models. Solid line, dashed line and pointed line represent simulation results under different variance \( V \) of 40, 20 and 4 respectively. Red lines represents the three-mode one-time-calibration model, blue lines represents the two-mode one-time-calibration model and black lines represents original evaluation model. The secret key rates among these three models can be exceedingly close under variance \( V = 4 \), for the scenarios of variance \( V = 20 \) and \( V = 40 \), the secret key rate of three-mode one-time-calibration model and original evaluation model are still very close while the secret key rate of the two-mode model is slightly lower than the other two models. This implies that the one-time evaluation models we proposed are suitable in estimating the secret key rate especially for the three-mode one-time evaluation model, which is considerably approaching to the original two-time evaluation model.

Fig.7 is the simulation result of tolerable excess noise (TEN) versus the transmission distance: solid line, dashed line and pointed line are results under variance \( V \) of 40, 20 and 4 respectively. Red lines denotes the three-mode one-time-calibration model, blue lines denotes two-mode one-time-calibration model and black lines denotes the original evaluation model. It can be seen that three-mode model and original two-time evaluation model can tolerate the highest excess noise under all three different variances whereas the two-mode one-time evaluation model is not as outperformance as the other two models.

We define a secret key rate disparity as \( |R_{\text{new}} - R_{\text{original}}| \) to intuitively demonstrate the degree of difference between the one-time-calibration models with the original two-time-calibration model. From the previous simulation results we realise that the secret key rates of the one-time-calibration models are not exceeding that of the two-time-calibration model. Thus this disparity can show how close the two one-time-calibration models approach to the two-time-calibration model. The lower percentage suggests a smaller divergence in the secret key rate compares to the two-time-calibration model. As can be seen from Fig.8, the three-mode model is considerably outperformance the two-mode model. The secret key rate of the three-mode model with variance 4 can achieve a as low as 0.64% divergence compare to the two-time-calibration model. On balance, the one-time-evaluation model is rather appropriate to be utilized to estimate the lower bound of the information that Alice and Bob can share and the one-time-calibration model.
The secret key rate of three-mode one-time-calibration is higher than the two-mode one-time-calibration model for about 70 km. The variance of the original two-time-evaluation model is quite close to the three-mode model. In the case of variance $V = 40$, the tolerable excess noise is almost the same for three-mode and original two-time-evaluation model, both higher than the two-mode model. With variance $V = 40$, the original calibration model appears to have little higher tolerable excess noise than the other models.

**V. EXPERIMENTAL DEMONSTRATION**

We implement a proof of principle experiment to verify the feasibility of the one-time-calibration model. Since the three-mode model is outperforming than the two-mode model analysed in Sec. IV, three-mode one-time-evaluation model is used in the following. The schematic diagram of the complete optical layout is delineated in Fig. 11. In the experiment coherent state protocol with homodyne detection technique is adopted where the legitimate party Alice generates coherent states from the laser and the other legitimate party Bob uses homodyne detector to randomly measure one of the quadratures.
of the electromagnetic field. The experiment employs a 49.85 km fiber with the total channel loss 11.62 dB.

In this PM model, the standard 1550 nm telecom laser followed with two high-extinction amplitude modulators supplies 40 ns coherent optical pulses which correspond to a duty circle of 20% with a frequency of 5 MHz. The pulses are then separated by the 1:99 beam splitter where the majority of them is treated as LO, the rest of the pulses are modulated by an amplitude modulator and an phase modulator subsequently so that a centered Gaussian distribution can be achieved. After the proper attenuation which can optimize the modulation variance and delay line, the signal is polarization and time multiplexed with the LO. At Bob’s side, the incoming signal of both the signal pulses and the LO pulses are first compensated by the dynamic polarization controller (DPC) to offset the polarization drifts. The polarization extinction ratio after the DPC maintains at a high level which attributes to separate the signal from the LO. Another delay line is used on Bob’s side to compensate the time delay. The manipulations of the LO can be more complicated on Bob’s side. 10% of the LO is used for clock synchronization, data synchronization and LO monitor. The phase modulator in the LO path is responsible for phase compensation and random selection of the measured optical quadrature. An 80 MHz shot-noise-limited balanced pulsed homodyne detector are then applied to detect the quantum signal.

One optical switch is adopted in the signal path in the receiver side, which corresponds to the corresponding EB model presented in Sec. III. During the experiment, the calibration process and the key distributing process alternatively. When the SNU calibration process is on, the optical switch is disconnected. When the optical switch is switched on, the key distribution process is executed.

In order to investigate the performance between the one-time calibration method and the conventional method, the electronic noise which is not a necessity any more in the one-time-calibration model is specifically measured in which cases another optical switch is put in the LO path of the receiver side. In the process of SNU calibration, the optical switches on both the signal path and the LO path are first both switched off, then switch on the optical switch on the signal path. After the SNU calibration, the optical switch in the signal path also switch on and the key distribution process continues.

The calibration scheme used in this experiment offers several advantages over the conventional calibration procedure. The LO power is surely retained since the optical switch is no longer a necessity in the experiment implementation. This can be crucial when the transmission distance reaches certain distance since the power of the LO is required to attain a certain level so that the quantum signal can be properly amplified during the interference of the homodyne detection. The one-time-calibration scheme also offers simpler implementation easier data control as we only need to control one optical switch to complete the SNU calibration and the key distribution and this is also suitable in the local oscillator scenario.

The basis sifting and parameter estimation of the post-processing are with low computational complexity, thus

FIG. 9. (Color online) Secret key rate as a function of transmission distance with the original two-time-evaluation model and the two one-time-evaluation models under different variances $V = 40, 20, 4$ in the finite-size regime. Electronic noise is set as $\nu_{ele} = 0.01$, the channel excess noise $\epsilon_c = 0.01$, the limited detection efficiency $\eta_d = 0.6$ and the reconciliation efficiency $\eta = 0.956$.

FIG. 10. (Color online) Tolerable excess noise as a function of transmission distance with the original two-time-evaluation model and the two one-time-evaluation models under different variances $V = 40, 20, 4$ in the finite-size regime. The electronic noise $\nu_{ele} = 0.01$, the limited detection efficiency $\eta_d = 0.6$ and the reconciliation efficiency $\eta = 0.956$. 

\begin{align*}
\eta & = 40, \\
\eta & = 20, \\
\eta & = 4.
\end{align*}
FIG. 11. (Color online) Optical layout of the experiment. Alice uses two high extinction ratio modulators and amplitude and phase modulator to prepare Gaussian distributed coherent states. Combined with strong local oscillator, the signals are multiplexed using polarizing beamsplitter and then sent through the quantum channel. The states are demultiplexed on Bob's side after the polarization compensation from the active dynamic polarization controller. The signal and local oscillator interfere on a shot-noise-limited balanced pulsed homodyne detector while the LO also attributes to the clock and data synchronization. Laser: continuous-wave laser; AM: amplitude modulator; PM: phase modulator; BS: beamsplitter; VATT: variable attenuator; PBS: polarizing beamsplitter; DPC: dynamic polarization controller; PD: photodetector.

FIG. 12. (Color online) Secret key rate as a function of channel loss with the conventional two-time-calibration model and the one-time evaluation model in both the asymptotic regime and the finite-size regime. The red solid star is the mean secret key rate in our experiment under the asymptotic regime, while the purple star is the mean secret key rate in our experiment under the finite-size regime.
VI. CONCLUSION

In this paper, we propose a shot-noise unit calibration procedure that only demands one step to calibrate the shot-noise unit. We derive the complete entanglement-based model that corresponds to the proposed one-time-calibration procedure and provide fully analysis on its performance. Complete experiment implementations based on the coherent states homodyne scheme are conducted to experimentally testify its feasibility. We first review the conventional shot-noise unit calibration procedures and sketch the limitations in the existing model while we propose the one-time-calibration method that can extended the security under a more general noise environment where the relative-intensity noise can be addressed properly. It will not only simplify the evaluation environment where the relative-intensity noise can be addressed properly. It will not only simplify the evaluation procedures but also accuates the estimated shot-noise unit, which makes it more close to the actual commercial implementation. We perform security analysis against arbitrary collective attacks and secret key rate calculation on a two-mode version of the entanglement-based model subsequently put forward a three-mode calibration entanglement-based model by permuting the order of beamsplitters that further improving the model behaviour. We further show the performance of the one-time-calibration model under finite-size regime. Our results from both the theoretical and experimental perspectives manifest that the one-time-calibration model can essentially achieve nearly the same performance as the conventional calibration model especially for the three-mode model in both the asymptotic limit regime and the finite-size regime. Our proposal provides a better substitution for the shot-noise unit evaluation procedure.

ACKNOWLEDGMENTS

This work was supported in part by the Key Program of National Natural Science Foundation of China under Grants 61531003, the National Natural Science Foundation under Grants 61427813, China Postdoctoral Science Foundation under Grant 2018M630116, and the Fund of State Key Laboratory of Information Photonics and Optical Communications.

[1] N. Gisin, G. Ribordy, W. Tittel, and H. Zbinden, Quantum cryptography, Rev. Mod. Phys. 74, 145 (2002).
[2] V. Scarani, et al. The security of practical quantum key distribution, Rev. Mod. Phys. 81, 1301 (2009).
[3] S. Pirandola, et al. Advances in Quantum Cryptography, arXiv preprint arXiv:1906.01645 (2019).
[4] C. Weedbrook, et al, Gaussian quantum information, Rev. Mod. Phys. 84, 621 (2012).
[5] E. Diamanti, & A. Leverrier, Distributing secret keys with quantum continuous variables: principle, security and implementations. Entropy 17(9), 6072-6092 (2015).
[6] F. Grosshans, & P. Grangier, Continuous variable quantum cryptography using coherent states. Phys. Rev. Lett. 88, 057902 (2002).
[7] C. Weedbrook, et al, Quantum cryptography without switching. Phys. Rev. Lett., 93(17), 170504 (2004).
[8] F. Grosshans, et al, Quantum key distribution using Gaussian modulated coherent states, Nature, 421, 238 (2003).
[9] I. Devetak, & A. Winter, Distillation of secret key and entanglement from quantum states. Proceedings of the Royal Society of London A: Mathematical, Physical and Engineering Sciences. Vol. 461. No. 2053. The Royal Society, (2005).
[10] A. Leverrier, et al, Security of continuous-variable quantum key distribution against general attacks. Phys. Rev. Lett. 110, 030502 (2013).
[11] A. Leverrier, Composable security proof for continuous-variable quantum key distribution with coherent states. Phys. Rev. Lett. 114, 070501 (2015).
[12] A. Leverrier, Security of continuous-variable quantum key distribution via a Gaussian de Finetti reduction. Phys. Rev. Lett. 118, 200501 (2017).
[13] Pirandola, S. et al. Fundamental limits of repeaterless quantum communications. Nat. Commun. 8: 15043 (2017).
[14] Pirandola, S. et al. Theory of channel simulation and bounds for private communication. Quantum Sci. Technol. 3.3 035009 (2018).
[15] F. Grosshans, Collective attacks and unconditional security in continuous variable quantum key distribution. Phys. Rev. Lett. 94, 020504 (2005).
[16] M. Navascués, & A. Acín, Security bounds for continuous variables quantum key distribution. Phys. Rev. Lett. 94, 020505 (2005).
[17] P. Pirandola, et al, Characterization of Collective Gaussian Attacks and Security of Coherent-State Quantum Cryptography. Phys. Rev. Lett. 101, 200504 (2008).
[18] R. Renner, & J. I. Cirac, de Finetti representation theorem for infinite-dimensional quantum systems and applications to quantum cryptography. Phys. Rev. Lett. 102, 110504 (2009).
[19] A. M. Lance, et al., No-switching quantum key distribution using broadband modulated coherent light. Phys. Rev. Lett. 95, 180503 (2005).
[20] J. Lodewyck, et al. Quantum key distribution over 25km with an all-fiber continuous-variable system. Phys. Rev. A 76, 042305 (2007).
[21] B. Qi, et al, Experimental study on the Gaussian-modulated coherent-state quantum key distribution over standard telecommunication fibers. Phys. Rev. A 76, 052323 (2007).
[22] I. Khan, et al. Optimal working points for continuous-variable quantum channels. Phys. Rev. A 88, 010302 (2013).
[23] Z. Li, et al, 2018. User-defined quantum key distribution. arXiv preprint arXiv:1805.04249. (2018).
[24] S. Ghorai, et al, Asymptotic security of continuous-variable quantum key distribution with a discrete modulation. Phys. Rev. X, 9(2), p.021059. (2019).
[25] D. Huang, et al, Long-distance continuous-variable quantum key distribution by controlling excess noise. Scientific reports, 6, 19201 (2016).
[26] S. Ghorai, et al, Asymptotic security of continuous-variable quantum key distribution with a discrete modulation. Phys. Rev. X, 9(2), p.021059. (2019).
[27] Y.C. Zhang, et al, Continuous-variable QKD over 50 km commercial fiber. Quantum Sci. Technol., 4(3), p.035006 (2019).
[28] A. Ferenczi, et al, Calibration attack and defense in continuous variable quantum key distribution. In International Quantum Electronics Conference. Optical Society of America (2007).
[29] P. Jouguet, et al, Preventing calibration attacks on the local oscillator in continuous-variable quantum key distribution. Phys. Rev. A, 87(6), p.062313 (2013).
[30] B. Qi, et al, Generating the local oscillator locally in continuous-variable quantum key distribution based on coherent detection. Phys. Rev. X, 5(4), p.041009 (2015).
[31] D.B. Soh, et al, Self-referenced continuous-variable quantum key distribution protocol. Phys. Rev. X, 5(4), p.041010. (2015).
[32] S. Fossier, et al, Improvement of continuous-variable quantum key distribution systems by using optical preamplifiers. J. Phys. B: At. Mol. Opt. Phys, 42(11), p.114014 (2009).
[33] Z. Li, et al, Continuous-variable measurement-device-independent quantum key distribution. Phys. Rev. A, 89(5), 052301 (2014).
[34] Y. C. Zhang, et al, Continuous-variable measurement-device-independent quantum key distribution using squeezed states. Phys. Rev. A, 90.5 052325 (2014).
[35] S. Pirandola, et al, High-rate measurement-device-independent quantum cryptography. Nat. Photon. 9, 397-402 (2015).
[36] X. Wang, et al, High efficiency postprocessing for continuous-variable quantum key distribution: using all raw keys for parameter estimation and key extraction. Quantum Information Processing 18.9, 264 (2019).
[37] M. A. Nielsen, & I. L. Chuang, Quantum Computation and Quantum Communication (Cambridge University Press, Cambridge, 2000).
[38] A. Leverrier, et al, Finite-size analysis of a continuous-variable quantum key distribution. Phys. Rev. A, 81(6), 062343 (2010).
[39] A. Leverrier, et al, Multidimensional reconciliation for a continuous-variable quantum key distribution. Phys. Rev. A, 77(4), 042325 (2008).
[40] T. Richardson, & R. Urbanke. Multi-edge type LDPC codes. presented at the Workshop honoring Prof. Bob McEliece on his 60th birthday, California Institute of Technology, Pasadena, California (2002).
[41] H. Krawczyk, LFSR-based hashing and authentication. Advances in Cryptology - CRYPTO 94: pp. 129-139 (1994).
[42] C. Fung, et al, Practical issues in quantum-key-distribution postprocessing. Phys. Rev. A, 81, 012318 (2010).
[43] X. Wang, et al, Efficient rate-adaptive reconciliation for continuous-variable quantum key distribution. Quantum Inf. Comput., 17 (13&14), pp. 1123-1134 (2017).