Security bound of continuous-variable measurement-device-independent quantum key distribution with imperfect phase reference calibration

Hong-Xin Ma,[1,2,3] Peng Huang,[3,*] Tao Wang,[3] Dong-Yun Bai,[3] Shi-Yu Wang,[3] Wan-Su Bao,[1,2] and Gui-Hua Zeng[3]

[1]*Henan Key Laboratory of Quantum Information and Cryptography, Zhengzhou Information Science and Technology Institute, Zhengzhou, Henan 450001, China*

[2]*Synergetic Innovation Center of Quantum Information and Quantum Physics, University of Science and Technology of China, Hefei, Anhui 230026, China*

[3]*State Key Laboratory of Advanced Optical Communication Systems and Networks and Center of Quantum Information Sensing and Processing, Shanghai Jiao Tong University, Shanghai 200240, China*

(Received 23 April 2019; published 25 November 2019)

Phase reference calibration is a necessary procedure in practical continuous-variable measurement-device-independent quantum key distribution (CV-MDI-QKD) for the need of Bell-state measurement. However, the phase reference calibration may become imperfect in practical applications. We explored the practical security of CV-MDI-QKD with imperfect phase reference calibration under realistic conditions of lossy and noisy quantum channels. Specifically, a comprehensive framework is developed to model and characterize the imperfection of the practical phase reference calibration operation, which is mainly caused by the nonsynchronization of two remote lasers in senders. Security analysis shows that the imperfect phase reference calibration has significant side effects on the performance and security of the CV-MDI-QKD protocol. A tight security bound to thermal excess noise introduced by imperfect phase reference calibration is derived for reverse reconciliation against one-mode collective Gaussian attack in the asymptotic limit, and the upper threshold of this imperfection tolerated by the system is obtained. This security analysis framework can eliminate the security hazards caused by imperfect phase reference calibration without changing the existing CV-MDI-QKD system structure. In addition, this work will improve the practical security framework of CV-MDI-QKD protocol and provide theoretic instruction for the experimental implementation of CV-MDI-QKD protocol.

DOI: 10.1103/PhysRevA.100.052330

I. INTRODUCTION

Quantum key distribution (QKD) [1] allows two distant authenticated users, Alice and Bob, to establish a secure key through an untrusted environment, which is based on the principles of quantum mechanics. There are mainly two categories of QKD: discrete-variable (DV) QKD protocols [2–4] and continuous-variable (CV) QKD protocols [5–9]. CVQKD utilizes the quadrature components of quantum states to distribute the secure key, which has unique potentials of being compatible with standard telecommunication systems and no request on single-photon detectors. Furthermore, CVQKD protocols allow one to approach the ultimate limit of repeaterless communication, known as the PLOB bound [10].

Theoretically, the Gaussian-modulated CVQKD protocol using coherent states [6] has been proved to be secure against arbitrary collective attacks [11] and coherent attacks [12], even with finite-size regime [13,14] and composable security [15] taken into account. Experimentally, this protocol has been proved to be feasible both in laboratory [7,16] and field tests [17]. The Gaussian-modulated CVQKD protocol has extended the secure transmission over 100 km optical fiber in the laboratory [18], which shows its potential of applying in metropolitan quantum networks.

The security analysis of CVQKD relies on some ideal assumptions, which are hard to satisfy in practice [19–21]. These deviations will bring specific security vulnerabilities to the CVQKD system, and the eavesdroppers can utilize this imperfection to implement attack strategies, such as local oscillator fluctuation attack [22], calibration attack [23], wavelength attack [24], and detector saturation attack [25]. Obviously, most of these attack strategies mainly focus on the imperfect detectors. In order to remove these attacks, one solution is to find and describe these security vulnerabilities, and then propose corresponding countermeasures. But characterizing all vulnerabilities is quite difficult, and the countermeasures will increase the complexity of the system.

Inspired by the idea of entanglement swapping, measurement-device-independent (MDI) QKD has been proposed by two groups [26,27] independently, where Ref. [26] solves the problem of side-channel attack against detectors in full generality and Ref. [27] is limited to qubit systems. Continuous-variable MDI-QKD (CV-MDI-QKD) has been proposed and verified both theoretically and experimentally [28]. Some theoretical schemes of CV-MDI-QKD have been put forward one after another in the same period [29–32]. In the theoretic research of CV-MDI-QKD, some tremendous results have been achieved in recent years

[*] Corresponding author: huang.peng@sjtu.edu.cn

[33–41]. In CV-MDI-QKD protocols, Alice and Bob are both senders, and measurement operations are performed by an untrustworthy third party, Charlie. Charlie performs Bell-state measurement (BSM) based on signals sent by Alice and Bob, where the measurement result is communicated publicly and used for generating the secure keys. Since measurement operations are performed by an untrusted terminal, the security of CV-MDI-QKD does not depend on the detectors. In other words, CV-MDI-QKD can eliminate all side-channel attacks against detectors, whether known or unknown.

In a practical system of CV-MDI-QKD, the light sources of Alice and Bob are mutually independent. Therefore, the initial optical pulses they emit are also independent of each other and may not stay in the same phase reference frame. For the need of BSM, we need to calibrate the phase reference frames between Alice, Bob, and Charlie [28]. The basic idea of phase reference calibration in CV-MDI-QKD is described as follows. First, we measure the phase difference between the local oscillator pulses emitted by Alice and Bob. Then, we take relative phase estimation and correction, adding the phase difference to one side's quantum signal pulse. After these operations, Alice and Bob's quantum signal pulses stay in the same phase reference frame, and Charlie carries out BSM based on this unified phase reference frame.

Obviously, phase reference calibration is of vital importance for the construction of experimental framework for CV-MDI-QKD. Unfortunately, in practical implementation, the phase reference calibration operation is not as perfect as theory. Due to the nonsynchronization of two independent lasers in Alice's and Bob's sides, which are mainly caused by the separate spectral linewidths of two lasers, and the uncertainty of the channel and detection environment, the practical phase reference calibration operation will become imperfect. If the imperfection is not taken into account in security analysis, the security key rate obtained will be higher than the actual value, which may lead to security hazards. For the accuracy of security analysis, in other words, in order to get a tight bound of security key rate, we need to precisely characterize the impact of imperfect phase reference calibration in the security analysis process.

Some latest breakthroughs [42,43] overcome the nonideality brought about by the practical phase reference calibration to a certain extent through the new optical path design, which simplifies the phase reference calibration process. However, these schemes may increase the complexity of other aspects of the system, such as detection, optical path, and so on. In addition, these schemes may also introduce additional thermal excess noise, such as the phase noise between signal pulse and reference pulse. In this paper, we choose to deal with this problem from another point of view, that is, to quantitatively characterize the imperfection of practical phase reference calibration operation through reasonable modeling, which develops a comprehensive security framework of CV-MDI-QKD protocol with imperfect phase reference calibration. In other words, we provide an appropriate theoretical solution to the problem. The exact formula for calculating excess noise caused by the imperfect phase reference calibration is obtained, and then a more compact and accurate security key rate is derived under one-mode collective Gaussian attack.

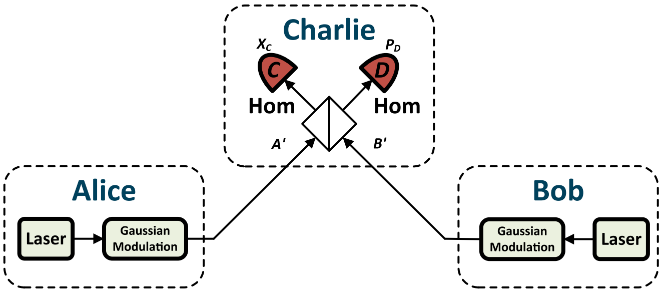

FIG. 1. PM version of the CV-MDI-QKD protocol. Hom is homodyne detection.

In addition, the upper threshold of this imperfection tolerated by the system is obtained in the form of the variance of the relative phase drift between two free-running lasers. Based on this, we can qualitatively and quantitatively analyze the impact of imperfect phase reference calibration on the performance and security of CV-MDI-QKD protocol. This security analysis framework can eliminate the security hazards caused by imperfect phase reference calibration without changing the existing CV-MDI-QKD system structure.

The remainder of this paper is structured as follows. In Sec. II, we first review the structure of CV-MDI-QKD protocol, then introduce phase reference calibration in CV-MDI-QKD protocol and develop a comprehensive framework to obtain the thermal excess noise introduced by imperfect phase reference calibration. In Sec. III, we derive the secret key rate of the CV-MDI-QKD protocol with imperfect phase reference calibration, which is more precise and compact than the original one. In Sec. IV,we give the numerical simulation and performance analysis. Conclusion and discussions are drawn in Sec. V.

II. CV-MDI-QKD PROTOCOL WITH IMPERFECT PHASE REFERENCE CALIBRATION

In this section, we first review the CV-MDI-QKD protocol, especially the prepare-and-measure (PM) version. Then, we introduce the phase reference calibration operation in CV-MDI-QKD protocol and its imperfection in practical implementation. On the basis of these reviews, we describe and calculate the thermal excess noise caused by imperfect phase reference calibration by precise modeling.

A. CV-MDI-QKD protocol

The construction of CV-MDI-QKD protocol is illustrated in Fig. 1, which is based on the PM version. The main steps of the PM version can be depicted as follows.

Step 1. Alice and Bob each prepare coherent states and send them to third-party Charlie through two different quantum channels with length L_{AC} and L_{BC}, respectively. The coherent state prepared by Alice is $|x_A + ip_A\rangle$, where x_A and p_A are Gaussian distributed with modulation variance V_{AM}. The coherent state prepared by Bob is $|x_B + ip_B\rangle$, where x_B and p_B are Gaussian distributed with modulation variance V_{BM}.

Step 2. Charlie performs BSM by interfering the two incoming coherent states on a beam splitter and obtaining two output modes C and D. Then, Charlie uses two homodyne

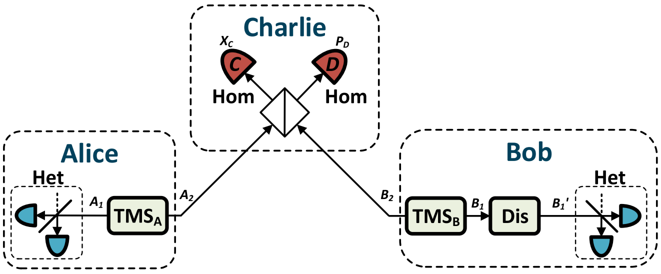

FIG. 2. EB version of the CV-MDI-QKD protocol. Het is heterodyne detection, Dis is displacement operation, and $\mathrm{TMS_A}$ and $\mathrm{TMS_B}$ are two-mode squeezed states.

detections to measure the x quadrature of mode C and p quadrature of mode D and announces the measurement results $\{X_C, P_D\}$ publicly.

Step 3. After receiving Charlie's measurement results, Alice keeps her data unchanged, where $X_A = x_A$, $P_A = p_A$, while Bob modifies his data to $X_B = x_B + \kappa X_C$, $P_B = p_B - \kappa P_D$. κ is an optimization parameter associated with quantum channel loss.

Step 4. Alice and Bob extract a string of secret key after carrying out parameter estimation, information reconciliation, and privacy amplification steps through an authenticated public channel.

In the equivalent entanglement-based (EB) version, which is shown in Fig. 2, Alice and Bob prepare two-mode squeezed states independently and each send one mode to Charlie for BSM. After Charlie announces the measurement results, Bob displaces his retained mode according to the measurement results, where the gain of the displacement operation is g, while Alice keeps her mode unchanged. Then, Alice and Bob measure their modes to obtain the raw data. After the date postprocessing, Alice and Bob obtain the final secret keys.

Before these steps, Alice and Bob implement the phase reference calibration by measuring the phase difference between the local oscillator pulses emitted by Alice and Bob, which makes sure that the prepared coherent states (or two-mode squeezed states) of Alice and Bob stay in the same phase reference frame.

B. Phase reference calibration in CV-MDI-QKD

This subsection mainly discusses the definition and operation of phase reference calibration between Alice, Bob, and Charlie in CV-MDI-QKD protocol.

Practically, local oscillator pulses, as the phase reference light of signal pulse, can be a strong classical light. Therefore, by interfering two classical local oscillator lights on a beam splitter, the phase difference of the two local oscillator pulses can be obtained by measuring the intensity of one output beam with a photodetector.

We assume that the measurements of phase difference and phase reference calibration are performed by Bob. Alice sends her local oscillator pulse to the untrusted third party Charlie. The schematic diagram of apparatus for measuring the phase difference of the local oscillator pulses is given in Fig. 3. Alice divides its local oscillator pulse $\mathrm{LO_A}$ into two beams, one sent to Charlie and the other one sent to Bob. Charlie divides the received beam into two beams as the reference lights of two balanced homodyne detectors for BSM. After receiving the local oscillator pulse sent by Alice, Bob divides the received local oscillator pulse and his own local oscillator pulse $\mathrm{LO_B}$ into two beams, respectively, and interferences these beams through $\mathrm{BS_1}$ and $\mathrm{BS_2}$. In order to measure the phase difference accurately, $\pi/2$ phase has been added to one of the local oscillator beams. Then, the phase difference of the two local oscillator pulses can be obtained by measuring the output interference intensity of one port of $\mathrm{BS_1}$ and $\mathrm{BS_2}$ respectively with $\mathrm{PD_1}$ and $\mathrm{PD_2}$.

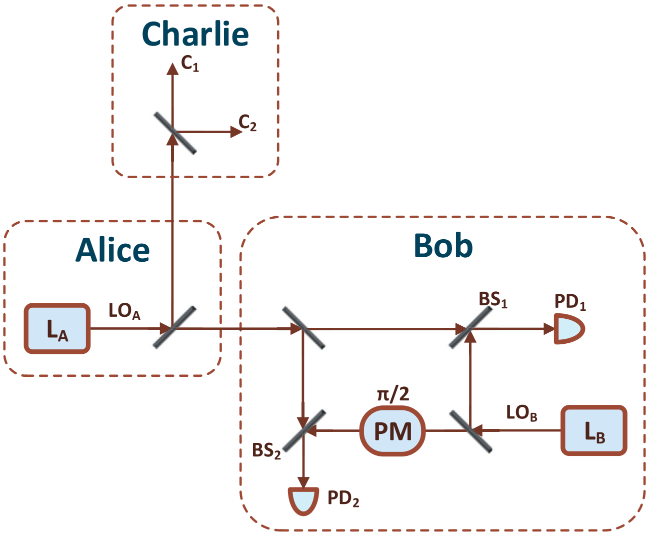

FIG. 3. Schematic structure of measuring the phase difference between the local oscillators sending by Alice and Bob in CV-MDI-QKD protocol. PM is phase modulator. L_A is the laser in Alice's side; L_B is the laser in Bob's side. $\mathrm{LO_A}$ and $\mathrm{LO_B}$ are local oscillator pulses. $\mathrm{PD_1}$ and $\mathrm{PD_2}$ are photo detectors. $\mathrm{C_1}$ and $\mathrm{C_2}$ are the reference lights of two balanced homodyne detectors for BSM. $\mathrm{BS_1}$ and $\mathrm{BS_2}$ are beam splitters. The ratio of all the beam splitters is 50:50.

The local oscillator pulses $\mathrm{LO_A}$ and $\mathrm{LO_B}$ can be denoted as $\alpha_{\mathrm{LO}}^{A} e^{i\theta_A}$ and $\alpha_{\mathrm{LO}}^{B} e^{i\theta_B}$, respectively. $|\alpha_{\mathrm{LO}}^{A}|$ and $|\alpha_{\mathrm{LO}}^{B}|$ are the amplitudes of each local oscillator pulse. θ_A and θ_B are the phases of $\mathrm{LO_A}$ and $\mathrm{LO_B}$, respectively. We suppose $\alpha_{\mathrm{LO}}^{A} = \alpha_{\mathrm{LO}}^{B} = \alpha_{\mathrm{LO}}$. After local oscillator pulses interfere on these beam splitters, the amplitude of the light measured by PD1 can be expressed as

$$\beta_1 = \frac{1}{\sqrt{2}}(\alpha_{\mathrm{LO}} e^{i\theta_A} + \alpha_{\mathrm{LO}} e^{i\theta_B}) \\ = \sqrt{2}\alpha_{\mathrm{LO}} e^{\frac{i(\theta_A+\theta_B)}{2}} \cos\left(\frac{\theta_A - \theta_B}{2}\right), \tag{1}$$

and then the intensity of the light measured by PD1 can be calculated as

$$|\beta_1|^2 = 2|\alpha_{\mathrm{LO}}|^2 \cos^2\left(\frac{\theta_A - \theta_B}{2}\right) \\ = |\alpha_{\mathrm{LO}}|^2[1 + \cos(\theta_A - \theta_B)]. \tag{2}$$

Similarly, the intensity of the light measured by PD2 is obtained as

$$\begin{aligned}|\beta_2|^2 &= |\alpha_{\mathrm{LO}}|^2[1+\cos(\theta_A-\theta_B-\pi/2)]\\ &= |\alpha_{\mathrm{LO}}|^2[1+\sin(\theta_A-\theta_B)].\end{aligned} \tag{3}$$

According to Eqs. (2) and (3), we can obtain the phase difference between Alice's and Bob's local oscillator, φ_{cal}, which is calculated as

$$\varphi_{\mathrm{cal}} = \theta_A - \theta_B. \tag{4}$$

After the phase reference calibration operation, the correlation between $(X_{\mathrm{LO}}^A, P_{\mathrm{LO}}^A)$ and $(X_{\mathrm{LO}}^B, P_{\mathrm{LO}}^B)$ can be obtained by

$$\begin{aligned}X_{\mathrm{LO}}^B &= X_{\mathrm{LO}}^A \cos\varphi_{\mathrm{cal}} - P_{\mathrm{LO}}^A \sin\varphi_{\mathrm{cal}},\\ P_{\mathrm{LO}}^B &= X_{\mathrm{LO}}^A \sin\varphi_{\mathrm{cal}} + P_{\mathrm{LO}}^A \cos\varphi_{\mathrm{cal}}.\end{aligned} \tag{5}$$

Assuming Alice's local oscillator has a zero-phase angle, which means $P_{\mathrm{LO}}^A = 0$, the expression of φ_{cal} can be obtained as

$$\varphi_{\mathrm{cal}} = \tan^{-1}\left(P_{\mathrm{LO}}^B/X_{\mathrm{LO}}^B\right). \tag{6}$$

Relative to local oscillator pulses, the initial quantum signal pulses modulated by Alice and Bob can be expressed as $\alpha_S^A e^{i(\theta_A+\theta_{AM})}$ and $\alpha_S^B e^{i(\theta_B+\theta_{BM})}$, respectively. α_S^A and α_S^B are the intensities of their respective signal pulses; θ_{AM} and θ_{BM} are their initial modulated phases, respectively. Based on the phase difference φ_{cal} between Alice's and Bob's local oscillator pulses, when Bob modulates his quantum signal pulses, the phase difference φ_{cal} and the initial modulated phase θ_{BM} should be added as the modulated phase of his ultimate modulated quantum signal pulse, which can be expressed as

$$\alpha_S^B e^{i(\theta_B+\theta_{BM}+\varphi_{\mathrm{cal}})} = \alpha_S^B e^{i(\theta_A+\theta_{BM})}. \tag{7}$$

Obviously, Bob's ultimate modulated quantum signal pulse is defined in Alice's quantum signal modulation reference frame. At this time, Alice's and Bob's quantum signal pulses share the same phase reference frame.

C. Thermal excess noise introduced by imperfect phase reference calibration

Theoretically, after local oscillator reference quadrature measurement, relative phase estimation, and correction, Alice and Bob's quantum signal pulses are expected to stay in the same phase reference frame with the phase difference φ_{cal}. However, in practice, the phase reference calibration operation is not as perfect as in theory, and the estimator $\hat{\varphi}_{\mathrm{cal}}$ always has estimation error, which will introduce thermal excess noise. Here we assume that the modulation variance of Alice and Bob $V_{AM} = V_{BM} = V_M$ in shot noise units. This is an ideal setting to simplify calculation. In the case of Gaussian-modulated protocol, we assume the thermal excess noise introduced by imperfect phase reference calibration is Gaussian, which is similar with the specific phase noise denoted in Refs. [44,45], and can be written as

$$\varepsilon_{\mathrm{prc}} = 2V_M(1-e^{-V_{\mathrm{prc}}/2}), \tag{8}$$

where $V_M = V_{AM} = V_{BM}$ is the modulation variance of both Alice and Bob and V_{prc} is the variance of the thermal excess noise introduced by imperfect phase reference calibration, which is expressed as [46,47]

$$V_{\mathrm{prc}} = \mathrm{var}(\varphi_{\mathrm{cal}} - \hat{\varphi}_{\mathrm{cal}}). \tag{9}$$

Assume that the laser in Alice's side, L_A, has spectral linewidth $\Delta\nu_A$, and the laser in Bob's side, L_B, has spectral linewidth $\Delta\nu_B$. Both lasers are centered around the same optical frequency. f is the repetition rate of the system. The thermal excess noise V_{prc} is constituted by three terms

$$V_{\mathrm{prc}} = V_{\mathrm{laser}} + V_{\mathrm{measure}} + V_{\mathrm{path}}. \tag{10}$$

The term V_{laser} represents the variance of the relative phase drift between two free-running lasers L_A and L_B, which can be obtained as

$$V_{\mathrm{laser}} = \frac{2\pi}{f}(\Delta\nu_A + \Delta\nu_B). \tag{11}$$

Obviously, V_{laser} is caused by the fact that the pulses of L_A and L_B are nonsynchronization, which mainly leads by the separate spectral linewidths of two lasers. In the specific system of the CV-MDI-QKD protocol, V_{laser} is a fixed parameter.

The term V_{measure} corresponds to the noise that is caused by the measurement error of the local oscillator phase. In the CV-MDI-QKD protocol, V_{measure} can be expressed as

$$\begin{aligned}V_{\mathrm{measure}} &= \frac{\chi_A+1}{\left|\alpha_{\mathrm{LO}}^A\right|^2} + \frac{\chi_B+1}{\left|\alpha_{\mathrm{LO}}^B\right|^2}\\ &= \frac{\chi_A+\chi_B+2}{|\alpha_{\mathrm{LO}}|^2},\end{aligned} \tag{12}$$

where χ_A is the total noise imposed on the local oscillator $\mathrm{LO_A}$, which is sent by Alice to Charlie, and χ_B is the total noise imposed on the local oscillator $\mathrm{LO_B}$, which is sent by Bob to Charlie. $|\alpha_{\mathrm{LO}}^A|$ and $|\alpha_{\mathrm{LO}}^B|$ are the amplitude of the local oscillators $\mathrm{LO_A}$ and $\mathrm{LO_B}$, respectively, and $\alpha_{\mathrm{LO}}^A = \alpha_{\mathrm{LO}}^B = \alpha_{\mathrm{LO}}$. χ_A and χ_B are defined in Eq. (15).

The term V_{path} represents the relative phase drift which is caused by the accumulation of the phase difference between the quantum signal pulse and the local oscillator pulse. Practically, it is caused by the different optical path lengths between two kinds of pulses. In CV-MDI-QKD protocol, the quantum signal pulse and the local oscillator pulse transmit through the same optical path each for Alice and Bob. Thus we have $V_{\mathrm{path}} = 0$, and the thermal excess noise V_{prc} is caused by two major components: $V_{\mathrm{prc}} = V_{\mathrm{laser}} + V_{\mathrm{measure}}$.

When the deviation of $\hat{\varphi}_{\mathrm{cal}}$ is quite small, V_{prc} stays in a relatively low range. Under this condition, the thermal excess noise introduced by imperfect phase reference calibration can be approximated as [46]

$$\begin{aligned}\varepsilon_{\mathrm{prc}} &= V_M V_{\mathrm{prc}}\\ &= 2\pi\frac{V_M(\Delta\nu_A+\Delta\nu_B)}{f} + \frac{V_M(\chi_A+\chi_B+2)}{|\alpha_{\mathrm{LO}}|^2}.\end{aligned} \tag{13}$$

We denote the transmittance of the quantum channel between Alice (Bob) and Charlie is T_A (T_B), and both quantum channel losses are $l = 0.2$ dB/km; then the transmittance can be given as $T_A = 10^{\frac{-lL_{AC}}{10}}$, $T_B = 10^{\frac{-lL_{BC}}{10}}$. The thermal excess noise introduced by two separate quantum channels are ε_A and ε_B, respectively. ε_c is the equivalent thermal excess noise introduced by all quantum channels, which is obtained as

$$\varepsilon_c = 1 + \chi_A + \frac{T_B}{T_A}(\chi_B - 1) + \frac{T_B}{T_A}\left(\sqrt{\frac{2}{T_B g^2}}\sqrt{V_B - 1} - \sqrt{V_B + 1}\right)^2, \tag{14}$$

where $V_B = V_{BM} + 1$, g is the amplification coefficient of the Bob's displacement in the EB version, and

$$\chi_A = \frac{1}{T_A} - 1 + \varepsilon_A, \quad \chi_B = \frac{1}{T_B} - 1 + \varepsilon_B. \tag{15}$$

As g is an optimization parameter, we denote $g^2 = \frac{2(V_B-1)}{\eta_B(V_B+1)}$ to minimize ε. Then the optimized equivalent thermal excess noise introduced by all quantum channels can be calculated as

$$\varepsilon_c = \frac{T_B}{T_A}(\varepsilon_B - 2) + \varepsilon_A + \frac{2}{T_A}. \tag{16}$$

We suppose the homodyne detectors in Charlie are ideal apparatuses; then the total added noise expressed in shot noise units is

$$\chi_t = \frac{1}{\eta} - 1 + \varepsilon_c + \varepsilon_{\text{prc}}, \tag{17}$$

where $\eta = \frac{1}{2}g^2 T_A$ is a normalized parameter associated with the total quantum channel transmittance [30].

III. CALCULATION OF THE SECRET KEY RATE

In this section, we will derive the secret key rate of the CV-MDI-QKD protocol against one-mode collective Gaussian attack [29–31,34,37–39,41–43] with considering the imperfection of practical phase reference calibration operation.

In order to facilitate the analysis, we restrict the quantum channels to two Markovian memoryless Gaussian quantum channels, which do not interact with each other. Under this assumption, the quantum channels of CV-MID-QKD protocol can be reduced to a one-mode channel [48], and the optimal attack turns into one-mode collective Gaussian attack, where Eve takes entangling cloner collective Gaussian attacks on each quantum channel independently. All the simulations in this paper are under one-mode collective Gaussian attack. We should point out that Eve's attack strategy described here is not the optimal and general one. In addition, when TMS_B and the displacement operation are regarded as manipulated by Eve, the EB version of CV-MDI-QKD protocol can be simplified to an equivalent one-way CVQKD protocol. Then we can use the secret key rate of equivalent one-way protocol to obtain the lower bound of the secret key rate of our protocol

Considering the lossy and noisy quantum channel and imperfection of practical phase reference calibration, the covariance matrix of $\rho_{A_1 B'_1}$ in the EB version can be expressed as

$$\gamma_{A_1 B'_1} = \begin{pmatrix} a\text{I}_2 & c\sigma_z \\ c\sigma_z & b\text{I}_2 \end{pmatrix} = \begin{pmatrix} V\text{I}_2 & \sqrt{\eta(V^2-1)}\sigma_z \\ \sqrt{\eta(V^2-1)}\sigma_z & \eta(V+\chi_t)\text{I}_2 \end{pmatrix}, \tag{18}$$

where I_2 is 2×2 identity matrix, $\sigma_z = \text{diag}(1, -1)$, and $V = V_A = V_B = V_M + 1$.

The secret key rate of the CV-MDI-QKD protocol with imperfect phase reference calibration under reverse reconciliation can be calculated as

$$K_{\text{prc}} = \beta I_{AB} - \chi_{BE}, \tag{19}$$

where β is the reconciliation efficiency, χ_{BE} is the Holevo bound [49] which defines the maximum information available to Eve on Bob's key, and I_{AB} is the mutual information between Alice and Bob, which can be calculated by [49]

$$I_{AB} = 2 \times \frac{1}{2}\log_2\left[\frac{a+1}{a+1-c^2/(b+1)}\right]. \tag{20}$$

The Holevo bound χ_{BE} is given as

$$\chi_{BE} = S(\rho_E) - \int dm_B p(m_B) S(\rho_E^{m_B}), \tag{21}$$

where S is the Von Neumann entropy of the quantum state ρ, m_B represents the measurement of Bob, $p(m_B)$ is the probability density of the measurement, and $\rho_E^{m_B}$ is Eve's state conditional on Bob's measurement result. Based on the fact that $\rho_{A_1}^{m_B}$ is independent of m_B for Gaussian protocols, and Eve purifies the system $A_1 B'_1$, χ_{BE} can be obtained as

$$\chi_{BE} = S(\rho_{A_1 B'_1}) - S(\rho_{A_1}^{m_B}), \tag{22}$$

where $S(\rho_{A_1 B'_1})$ is a function of the symplectic eigenvalues $\lambda_{1,2}$ of $\gamma_{A_1 B'_1}$ characterizing the state $\rho_{A_1 B'_1}$, with the form

$$S(\rho_{A_1 B'_1}) = G[(\lambda_1 - 1)/2] + G[(\lambda_2 - 1)/2], \tag{23}$$

and $S(\rho_{A_1}^{m_B})$ is a function of the symplectic eigenvalues λ_3 of $\gamma_{A_1}^{m_B}$ characterizing the state $\rho_{A_1}^{m_B}$, with the form

$$S(\rho_{A_1}^{m_B}) = G[(\lambda_3 - 1)/2], \tag{24}$$

where the Von Neumann entropy

$$G(x) = (x+1)\log_2(x+1) - x\log_2 x. \tag{25}$$

The symplectic eigenvalues $\lambda_{1,2}$ can be calculated by

$$\lambda_{1,2}^2 = \tfrac{1}{2}(A \pm \sqrt{A^2 - 4B^2}), \tag{26}$$

with the notations

$$A = a^2 + b^2 - 2c^2 = V^2 + \eta^2(V+\chi_t)^2 - 2\eta(V^2 - 1),$$
$$B = ab - c^2 = \eta(V\chi_t + 1). \tag{27}$$

The covariance matrix of the state $\rho_{A_1}^{m_B}$ can be calculated as

$$\gamma_{A_1}^{m_B} = a\text{I}_2 - c\sigma_z(b\text{I}_2 + \text{I}_2)^{-1}c\sigma_z = [a - c^2/(b+1)]\text{I}_2, \tag{28}$$

and then the symplectic eigenvalue λ_3 is given by

$$\lambda_3 = a - c^2/(b+1) = \frac{\eta V\chi_t + V + \eta}{\eta(V+\chi_t)+1}. \tag{29}$$

IV. PERFORMANCE ANALYSIS

In this section, we give the numerical simulation and provide the sufficient analysis of the CV-MDI-QKD protocol with imperfect phase reference calibration compared with

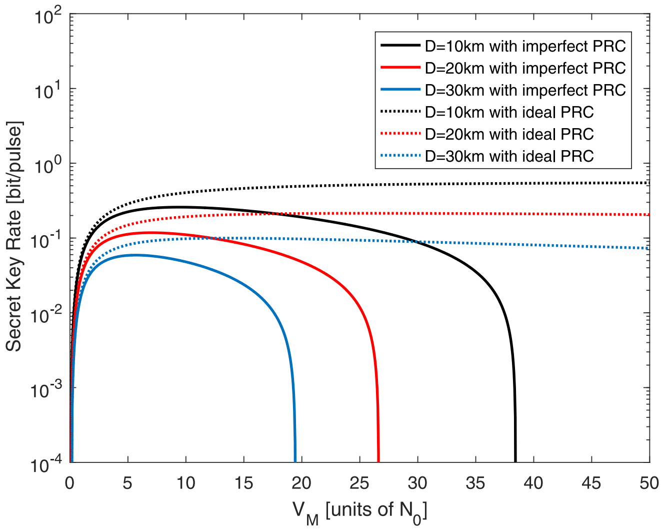

FIG. 4. Secret key rates as a function of V_M in the extreme asymmetric case, where Charlie is extremely close to Bob. Transmission distances $D = L_{AC}$ are set to 10 km, 20 km, and 30 km. N_0 is the shot noise variance. PRC is phase reference calibration. The solid lines denote the CV-MDI-QKD protocol with ideal phase reference calibration; the dashed lines denote the CV-MDI-QKD protocol with imperfect phase reference calibration. Parameters are fixed as follows: $\varepsilon_A = \varepsilon_B = 0.002$ [7], $V_{\text{laser}} = 0.005$, $|\alpha_{\text{LO}}|^2/V_M = 10^8$, and reconciliation efficiency $\beta = 96\%$.

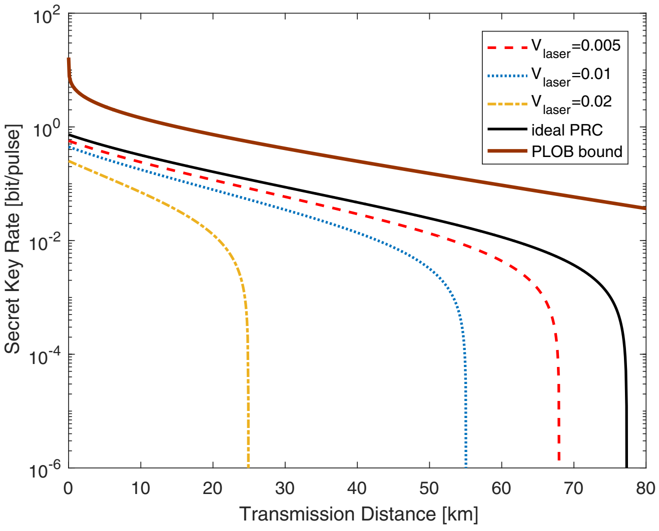

FIG. 5. Secret key rates as a function of the transmission distance in the extreme asymmetric case, where Charlie is extremely close to Bob. The uppermost heavy solid line denotes the PLOB bound. The thin solid lines denote the CV-MDI-QKD protocol with ideal phase reference calibration. The dashed lines denote the CV-MDI-QKD protocol with imperfect phase reference calibration, where V_{laser} are set to 0.005, 0.01, and 0.02 with the units of shot noise (N_0). Parameters are fixed as follows: $\varepsilon_A = \varepsilon_B = 0.002$, $|\alpha_{\text{LO}}|^2/V_M = 10^8$, modulation variance $V_M = 6$, and reconciliation efficiency $\beta = 96\%$.

previous works which do not consider the impact of imperfect phase reference calibration.

In CV-MDI-QKD protocols, the asymmetric case, where $L_{AC} \neq L_{BC}$, has obvious advantage in performance compared with the symmetric case, where $L_{AC} = L_{BC}$ [28], and the extreme asymmetric case, where Charlie is extremely close to Bob [30], has the optimal performance. In other words, the shorter the distance between Bob and Charlie, the better the performance we can obtain. Employing the same parameters, the extreme asymmetric case can obtain the maximal transmission distance, which is more suitable for point-to-point communications. In short-range network applications where the relay needs to be in the middle of the legitimate communication parties, the symmetric case is more suitable and has unique potentials. Our following analysis is based on two cases: the extreme asymmetric case and the symmetric case.

A. Performance analysis in the extreme asymmetric case

The modulation variance V_M is critical to the performance and security of CV-MDI-QKD protocol. Before obtaining the secret key rate of the CV-MDI-QKD protocol with imperfect phase reference calibration as a function of transmission distance in the extreme asymmetric case, we need to know how the secret key rate changes with the modulation variance in order to obtain the optimal modulation variance. We plot the secret key rates as a function of the modulation variance V_M with different transmission distance in the extreme asymmetric case, for both the CV-MDI-QKD protocol with ideal phase reference calibration and the protocol with imperfect phase reference calibration, which is shown Fig. 4.

There are two key parameters, V_{laser} and $|\alpha_{\text{LO}}|^2/V_M$, directly deciding the impact of imperfect phase reference calibration on the protocol. V_{laser} is related with the spectral linewidth of two free-running lasers and the repetition rate of the system. We denote $V_{\text{laser}} = 0.005$ based on the parameters of the practical equipment. $|\alpha_{\text{LO}}|^2/V_M$ is related with the light intensity of the local oscillator pulse. We choose $|\alpha_{\text{LO}}|^2/V_M = 10^8$, which is the value commonly used in practical CV systems.

Obviously, when considering the imperfection of practical phase reference calibration, the practicable V_M values are much lower than the one without taking this imperfection into account, which means that we need to set the modulation variance more strictly under the condition of imperfect phase reference calibration. In addition, when transmission distance increases, the optional areas of V_M are gradually compressed and the secret key rate decreases evidently. There is a noteworthy phenomenon that, under the fixed parameters, the optimal value of V_M for the CV-MDI-QKD protocol with imperfect phase reference calibration, which leads to the best performance, is always about six in short noise units. Hence, in the next analysis of the extreme asymmetric case, we always denote $V_M = 6$.

The secret key rates as a function of the transmission distance in the extreme asymmetric case are shown in the plot of Fig. 5, for both the CV-MDI-QKD protocol with imperfect phase reference calibration and the one with ideal phase reference calibration. Besides, different values of V_{laser} are taken into account for the CV-MDI-QKD protocol with imperfect phase reference calibration, and the PLOB bound is plotted as a reference for performance comparison. Here

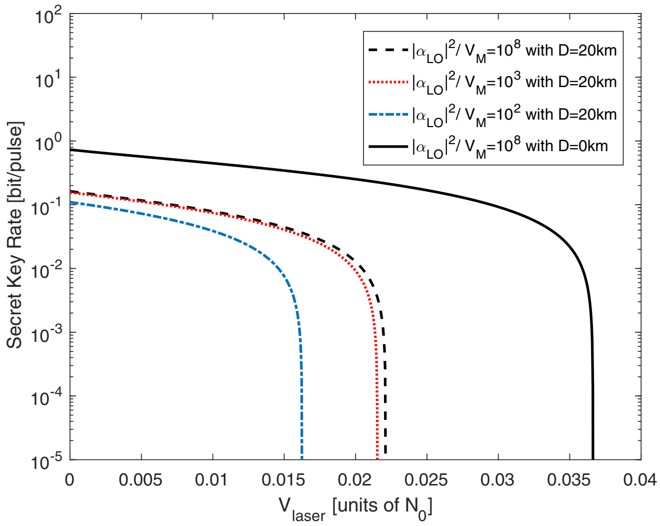

FIG. 6. Secret key rates as a function of V_{laser} in the extreme asymmetric case, where Charlie is extremely close to Bob. The dashed lines denote the CV-MDI-QKD protocol with imperfect phase reference calibration, where transmission distances $D = L_{AC}$ are set to 20 km and $|\alpha_{\text{LO}}|^2/V_M$ are set to 10^8, 10^3, and 10^2. The solid line denotes the initial secret key rate of CV-MDI-QKD protocol with imperfect phase reference calibration, where transmission distances $D = L_{AC} = 0$ km and $|\alpha_{\text{LO}}|^2/V_M = 10^8$. Parameters are fixed as follows: $\varepsilon_A = \varepsilon_B = 0.002$, modulation variance $V_M = 6$, and reconciliation efficiency $\beta = 96\%$.

we denote $|\alpha_{\text{LO}}|^2/V_M = 10^8$ as a fixed value. As shown in the figure, the performance curve of the CV-MDI-QKD protocol with imperfect phase reference calibration is always lower than that of the one without considering this imperfection, and the gap between the former curve and the PLOB bound is always larger than that between the later curve and the PLOB bound. Furthermore, the gap between these two performance curves will become larger and larger as the value of V_{laser} increases, and the performance of the CV-MDI-QKD protocol with imperfect phase reference calibration reduces rapidly as V_{laser} increases.

On the one hand, the figure shows that the imperfect phase reference calibration will seriously affect the performance and security of the CV-MDI-QKD protocol, and the reduction is more obvious with the larger V_{laser}. On the other hand, a tight bound of the secret key rate is given with considering this imperfection in security analysis. Specifically, this imperfection will introduce additional thermal excess noise into the formula of the secret key rate under the one-mode collective Gaussian attack, which will weaken the performance of the CV-MDI-QKD protocol. Therefore, a tight bound of the secret key rate can be obtained, which is closer to the practical situation.

Figure 6 depicts the secret key rates as a function of V_{laser} in the extreme asymmetric case, for the CV-MDI-QKD protocol with imperfect phase reference calibration. The lower dashed lines denote the case of the secret key rate changing with V_{laser} under fixed transmission distance and different value of $|\alpha_{\text{LO}}|^2/V_M$. On one hand, when the local oscillator pulse is too weak, the coherent detectors cannot work effectively. On the other hand, when the local oscillator pulse is too strong, it will exceed the performance of the coherent detectors. Therefore, in the practical system, we take the intensity of the local oscillator pulse as a fixed range, which leads the value of $|\alpha_{\text{LO}}|^2/V_M$ to be always around 10^8.

Although the value of $|\alpha_{\text{LO}}|^2/V_M$ has been limited in the practical system, we still need to consider its impact on system security, as it is an important parameter in the calculation formula of ε_{prc}. According to the figure, we can obtain that the value of $|\alpha_{\text{LO}}|^2/V_M$ and the performance of the protocol are negatively correlated. However, when $|\alpha_{\text{LO}}|^2/V_M$ is larger than 10^4, its effect on the performance of the protocol is negligible. Therefore, in practical systems, even if the value of $|\alpha_{\text{LO}}|^2/V_M$ fluctuates around 10^8, it will not have a significant impact on the security key rate. In other words, the effect of $|\alpha_{\text{LO}}|^2/V_M$ on the performance of the protocol is not obvious in practice. Hence, in the extreme asymmetric case, the most important parameter affecting the impact of imperfect phase reference calibration in practical CV-MDI-QKD systems is V_{laser}.

The upper black solid line, which is denoted as "$|\alpha_{\text{LO}}|^2/V_M = 10^8$ with $D = 0$ km," gives the upper bound of tolerance threshold for the CV-MDI-QKD protocol to the imperfection of practical phase reference calibration in the extreme asymmetric case. The upper bound is obtained in the form of the specific values of V_{laser}, which is calculated as $\tilde{V}_{\text{laser}}^{\text{asy}} = 0.0367$ in shot noise units. This means that there is just no secret key extracted when the variance of the relative phase drift between two free-running lasers V_{laser} is greater than 0.0367 in the extreme asymmetric case. Under this situation, the CV-MDI-QKD system will not be secure.

From the point of view of the thermal excess noise introduced by the imperfect phase reference calibration, the upper bound of tolerance threshold for ε_{prc} is 0.2202 in shot noise units under the fixed parameters.

B. Performance analysis in the symmetric case

In the symmetric case, the untrusted third party Charlie is right in the middle of Alice and Bob, which is quite suitable for the applications where two legitimate parties are roughly equidistant from a public server [32]. Same as the previous subsection, we should obtain the optimal value of V_M before simulating the secret key rate of the CV-MDI-QKD protocol with imperfect phase reference calibration in the symmetric case. The plot of Fig. 7 shows the secret key rates as a function of the modulation variance V_M with different transmission distance in the symmetric case, for both the CV-MDI-QKD protocol with ideal phase reference calibration and the protocol with imperfect phase reference calibration. The feasible range of V_M in the latter is much smaller than that in the former. Considering the imperfection of phase reference calibration, with transmission distance increases, the optional areas of V_M are gradually compressed, which is similar to what is shown in Fig. 4. Under the fixed parameters, the optimal value of V_M in the symmetric case is about 12.

The secret key rate as a function of the transmission distance in the symmetric case is shown in the plot of Fig. 8, for both the CV-MDI-QKD protocol with imperfect phase reference calibration and the one with ideal phase reference

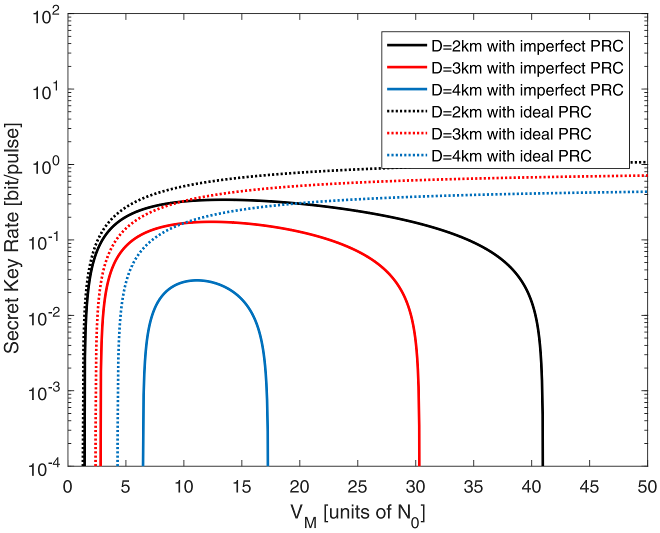

FIG. 7. Secret key rates as a function of V_M in the symmetric case, where Charlie is in the middle of Alice and Bob. Transmission distances $D = L_{AC} + L_{BC}$ are set to 2 km, 3 km, and 4 km. N_0 is the shot noise variance. PRC is phase reference calibration. The solid lines denote the CV-MDI-QKD protocol with ideal phase reference calibration; the dashed lines denote the CV-MDI-QKD protocol with imperfect phase reference calibration. Parameters are fixed as follows: $\varepsilon_A = \varepsilon_B = 0.002$, $V_{\text{laser}} = 0.005$, $|\alpha_{\text{LO}}|^2/V_M = 10^8$, and reconciliation efficiency $\beta = 96\%$.

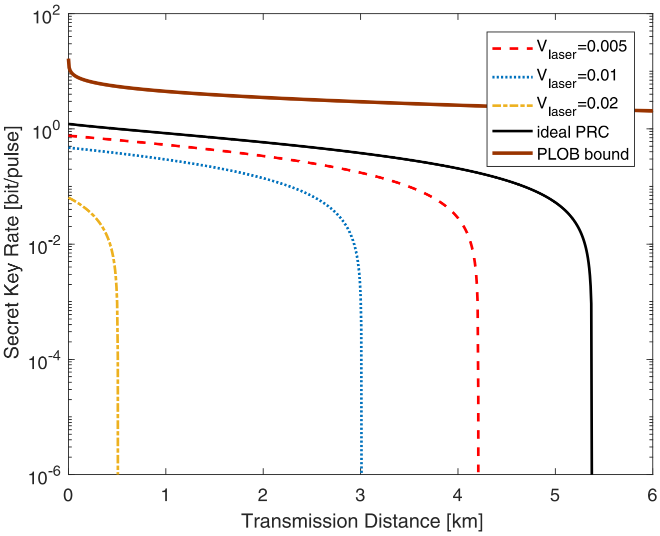

FIG. 8. Secret key rates as a function of the transmission distance in the symmetric case, where Charlie is in the middle of Alice and Bob. The uppermost heavy solid line denotes the PLOB bound. The thin solid lines denote the CV-MDI-QKD protocol with ideal phase reference calibration. The dashed lines denote the CV-MDI-QKD protocol with imperfect phase reference calibration, where V_{laser} are set to 0.005, 0.01, and 0.02 with the units of shot noise (N_0). Parameters are fixed as follows: $\varepsilon_A = \varepsilon_B = 0.002$, $|\alpha_{\text{LO}}|^2/V_M = 10^8$, modulation variance $V_M = 12$, and reconciliation efficiency $\beta = 96\%$.

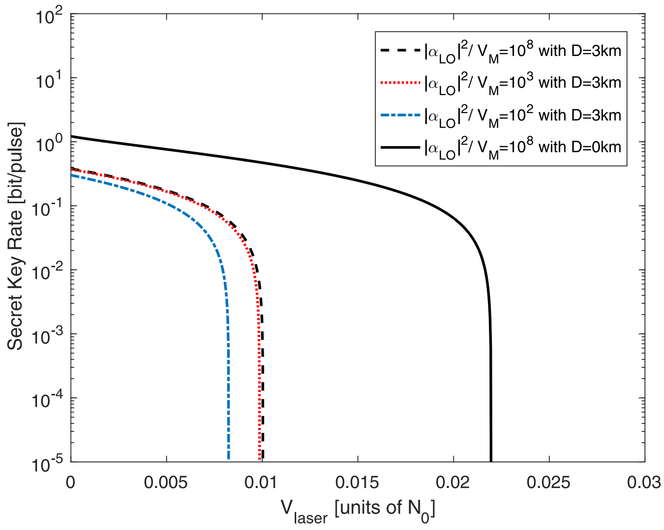

FIG. 9. Secret key rates as a function of V_{laser} in the symmetric case, where Charlie is in the middle of Alice and Bob. The dashed lines denote the CV-MDI-QKD protocol with imperfect phase reference calibration, where transmission distances $D = L_{AC} + L_{BC}$ are set to 3 km and $|\alpha_{\text{LO}}|^2/V_M$ are set to 10^8, 10^3, and 10^2. The solid lines denote the initial secret key rate of CV-MDI-QKD protocol with imperfect phase reference calibration, where transmission distances $D = L_{AC} = 0$ km and $|\alpha_{\text{LO}}|^2/V_M = 10^8$. Parameters are fixed as follows: $\varepsilon_A = \varepsilon_B = 0.002$, modulation variance $V_M = 12$, and reconciliation efficiency $\beta = 96\%$.

calibration. The modulation variance V_M of both protocols are all set to 12; $|\alpha_{\text{LO}}|^2/V_M$ is also fixed as 10^8. Same as the former case, the performance curves of the CV-MDI-QKD protocol with considering imperfect phase reference calibration are always lower than the one without considering this imperfection, and the gap will rise with the increase of V_{laser}. A more compact secret key rate is given with considering this imperfection in the symmetric case.

Furthermore, for both the CV-MDI-QKD protocol with imperfect phase reference calibration and the one with ideal phase reference calibration, the maximal transmission distances of the symmetric case are less than one-tenth of these of the extreme asymmetric case. The secret key rate of the CV-MDI-QKD protocol with imperfect phase reference calibration in the symmetric case looks more sensitive to the change of V_{laser} than that in the extreme asymmetric case, which will be confirmed in Fig. 9.

Figure 9 depicts the secret key rates of the CV-MDI-QKD protocol with imperfect phase reference calibration as a function of V_{laser} in the symmetric case, with different values of $|\alpha_{\text{LO}}|^2/V_M$ and transmission distance. Similar to what is shown in Fig. 6, although $|\alpha_{\text{LO}}|^2/V_M$ and the performance of the protocol have negative correlation, when $|\alpha_{\text{LO}}|^2/V_M$ surpasses 10^4, its effect on the performance of the protocol is not worth mentioning. So the most critical parameter for determining the impact of the imperfect phase reference calibration in practical CV-MDI-QKD systems is still V_{laser} in the symmetric case.

The upper black solid line denoted as "$|\alpha_{\text{LO}}|^2/V_M = 10^8$ with $D = 0$ km" shows the upper bound of tolerance threshold for the CV-MDI-QKD protocol to the imperfection of practical phase reference calibration in the symmetric case, which is obtained as $\tilde{V}^{\text{sy}}_{\text{laser}} = 0.0220$ in shot noise units in the form of the specific values of V_{laser}. It is clear that the upper bound of tolerance threshold for the CV-MDI-QKD protocol to the imperfection of practical phase reference calibration in the symmetric case is lower than that in the extreme asymmetric case. This shows that the symmetric case of the CV-MDI-QKD protocol is more sensitive to V_{laser} than the extreme asymmetric case. In addition, the upper bound of tolerance threshold for ε_{prc} in the symmetric case is 0.2640 in shot noise units, which is higher than that of the extreme asymmetric case. This is mainly caused by the quite higher modulation variance of the former case.

V. CONCLUSION AND DISCUSSIONS

CV-MDI-QKD protocol can ignore the side-channel attacks against imperfect measurement devices, but it is not immune to the imperfection of other parts. Phase reference calibration is of vital importance for the experimental realization of CV-MDI-QKD, as it's a necessary operation for BSM. But in practice, phase reference calibration operation is not as perfect as in theory, which will bring security vulnerabilities to the system. In this paper, we have investigated the imperfection of practical phase reference calibration on the security of CV-MDI-QKD protocol, which is caused by the nonsynchronization of two remote lasers in senders and has not been taken into account in previous security analysis of this protocol. Both the extreme asymmetric case and the symmetric case are taken into account. We developed a comprehensive security framework to model and characterize this imperfection. Through reasonable modeling, the effect of this imperfection on the security of the CV-MDI-QKD protocol is equivalent to the thermal excess noise ε_{prc} introduced by imperfect phase reference calibration. A tight bound of the secret key rate is derived under one-mode collective Gaussian attack, where the tightness is caused by the thermal excess noise introduced by the imperfect phase reference calibration. The security analysis shows that the imperfect phase reference calibration will obviously damage the performance and security of the CV-MDI-QKD protocol. Moreover, based on the variance of the relative phase drift between two free-running lasers V_{laser}, we give the upper bound of tolerance threshold for the CV-MDI-QKD protocol to the imperfection of practical phase reference calibration. This work can effectively eliminate the potential security hazards caused by the imperfect phase reference calibration without changing the protocol structure, and make the security analysis closer to the practical situation. Furthermore, this work will be conducive to further improving the practical security framework of the CV-MDI-QKD protocol, and provide theoretical guidance for the experimental implementation of the CV-MDI-QKD protocol in the next step.

In the analysis of ε_{prc}, we find that the most critical parameter for determining the impact of the imperfect phase reference calibration in practical CV-MDI-QKD systems is V_{laser}, which is a fixed parameter in the specific system and decided by the spectral linewidth of two free-running lasers and the repetition rate f of the system. We usually choose f below 100 MHz with considering the current bandwidth limitation of shot-noise limited coherent detectors. In order to minimize V_{laser}, we can choose low-phase-noise lasers, such as external-cavity lasers (ECL), whose typical spectral linewidth is of a few kHz [44]. In this case, V_{laser} may even be less than 10^{-4}. The participation of such equipment can effectively narrow the impact of the imperfect phase reference calibration on the security and performance of CV-MDI-QKD protocol. In future work, we will strive to design a comprehensive security framework to characterize the overall practical security of CV-MDI-QKD protocol under the optimal attack strategy.

In addition, there is indeed a link between Alice and Bob due to the need for phase reference calibration, and this link transmits the phase reference light that Alice sends to Bob, which is the local oscillator and easily controlled by Eve. Therefore, we must consider the attack strategy that Eve may take on the link. The attack strategy that Eve can adopt is as follows. Eve can work hard to keep the link between Alice and Bob stable, so that Alice's and Bob's lasers are always in synchronization. At the same time, Eve interferes with the link between Alice and Charlie by imitating the fluctuation of Alice's practical laser, thus hiding the thermal excess noise caused by her own eavesdropping. In this way, Eve can successfully steal the key information without being discovered by legitimate users. At this point, Alice and Bob's phase calibration is inaccurate, which will be mistaken by Alice and Bob as being in synchronization, and the secret key rate estimated according to the results of BSM is higher than the practical situation. The system is no longer secure. We can take some countermeasures against Eve's attack strategy on the link between Alice and Bob: real-time phase monitoring of Alice's reference light or Charlie's local preparation of local oscillator. This will be our next research focus.

ACKNOWLEDGMENTS

This work was supported the National key research and development program (Grant No. 2016YFA0302600), the National Basic Research Program of China (Grant No. 2013CB338002), and the National Natural Science Foundation of China (Grants No. 11304397, No. 61332019, No. 61505261, No. 61675235, No. 61605248, and No. 61671287).

[1] N. Gisin, G. Ribordy, W. Tittel, and H. Zbinden, Rev. Mod. Phys. **74**, 145 (2002).

[2] C. H. Bennett and G. Brassard, in *Proceedings of the IEEE International Conference on Computers, Systems and Signal Processing, Bangalore, India* (IEEE, New York, 1984), pp. 175–179.

[3] A. K. Ekert, Phys. Rev. Lett. **67**, 661 (1991).

[4] Q. Cai and H. Lv, Chin. Phys. Lett. **24**, 1154 (2007).

[5] T. C. Ralph, Phys. Rev. A **61**, 010303(R) (1999).

[6] F. Grosshans and P. Grangier, Phys. Rev. Lett. **88**, 057902 (2002).

[7] F. Grosshans, G. V. Assche, J. Wenger, R. Brouri, N. J. Cerf, and P. Grangier, Nature (London) **421**, 238 (2003).
[8] C. Weedbrook, S. Pirandola, R. García-Patrón, N. J. Cerf, T. C. Ralph, J. H. Shapiro, and S. Lloyd, Rev. Mod. Phys. **84**, 621 (2012).
[9] Y. Guo, W. Ye, H. Zhong, and Q. Liao, Phys. Rev. A **99**, 032327 (2019).
[10] S. Pirandola, R. Laurenza, C. Ottaviani, and L. Banchi, Nat. Commun. **8**, 15043 (2017).
[11] M. Navascues, F. Grosshans, and A. Acín, Phys. Rev. Lett. **97**, 190502 (2006).
[12] R. Renner and J. I. Cirac, Phys. Rev. Lett. **102**, 110504 (2009).
[13] A. Leverrier, R. García-Patrón, R. Renner, and N. J. Cerf, Phys. Rev. Lett. **110**, 030502 (2013).
[14] A. Leverrier, Phys. Rev. Lett. **118**, 200501 (2017).
[15] A. Leverrier, Phys. Rev. Lett. **114**, 070501 (2015).
[16] P. Jouguet, S. Kunz-Jacques, A. Leverrier, P. Grangier, and E. Diamanti, Nat. Photon. **7**, 378 (2013).
[17] D. Huang, P. Huang, H. Li, T. Wang, Y. Zhou, and G. Zeng, Opt. Lett. **41**, 3511 (2016).
[18] D. Huang, P. Huang, D. Lin, and G. Zeng, Sci. Rep. **6**, 19201 (2016).
[19] G. Brassard, N. Lutkenhaus, T. Mor, and B. C. Sanders, Phys. Rev. Lett. **85**, 1330 (2000).
[20] Z. L. Yuan, J. F. Dynes, and A. J. Shields, Nat. Photon. **4**, 800 (2010).
[21] Y. Guo, C. Xie, Q. Liao, W. Zhao, G. Zeng, and D. Huang, Phys. Rev. A **96**, 022320 (2017).
[22] X. C. Ma, S. H. Sun, M. S. Jiang, and L. M. Liang, Phys. Rev. A **88**, 022339 (2013).
[23] P. Jouguet, S. Kunz-Jacques, and E. Diamanti, Phys. Rev. A **87**, 062313 (2013).
[24] X. C. Ma, S. H. Sun, M. S. Jiang, and L. M. Liang, Phys. Rev. A **87**, 052309 (2013).
[25] H. Qin, R. Kumar, and R. Alléaume, Phys. Rev. A **94**, 012325 (2016).
[26] S. L. Braunstein and S. Pirandola, Phys. Rev. Lett. **108**, 130502 (2012).
[27] H.-K. Lo, M. Curty, and B. Qi, Phys. Rev. Lett. **108**, 130503 (2012).
[28] S. Pirandola, C. Ottaviani, G. Spedalieri, C. Weedbrook, S. L. Braunstein, S. Lloyd, T. Gehring, C. S. Jacobsen, and U. L. Andersen, Nat. Photon. **9**, 397 (2015).
[29] X.-C. Ma, S.-H. Sun, M.-S. Jiang, M. Gui, and L.-M. Liang, Phys. Rev. A **89**, 042335 (2014).
[30] Z. Li, Y.-C. Zhang, F. Xu, X. Peng, and H. Guo, Phys. Rev. A **89**, 052301 (2014).
[31] Y. C. Zhang, Z. Li, S. Yu, W. Gu, X. Peng, and H. Guo, Phys. Rev. A **90**, 052325 (2014).
[32] C. Ottaviani, G. Spedalieri, S. L. Braunstein, and S. Pirandola, Phys. Rev. A **91**, 022320 (2015).
[33] P. Papanastasiou, C. Ottaviani, and S. Pirandola, Phys. Rev. A **96**, 042332 (2017).
[34] X. Zhang, Y. Zhang, Y. Zhao, X. Wang, S. Yu, and H. Guo, Phys. Rev. A **96**, 042334 (2017).
[35] C. Lupo, C. Ottaviani, P. Papanastasiou, and S. Pirandola, Phys. Rev. A **97**, 052327 (2018).
[36] C. Lupo, C. Ottaviani, P. Papanastasiou, and S. Pirandola, Phys. Rev. Lett. **120**, 220505 (2018).
[37] Z. Chen, Y. Zhang, G. Wang, Z. Li, and H. Guo, Phys. Rev. A **98**, 012314 (2018).
[38] Y. Zhao, Y. Zhang, B. Xu, S. Yu, and H. Guo, Phys. Rev. A **97**, 042328 (2018).
[39] H.-X. Ma, P. Huang, D.-Y. Bai, S.-Y. Wang, W.-S. Bao, and G.-H. Zeng, Phys. Rev. A **97**, 042329 (2018).
[40] Q. Liao, Y. Wang, D. Huang, and Y. Guo, Opt. Express **26**, 19907 (2018).
[41] D. Bai, P. Huang, H. Ma, T. Wang, and G. Zeng, J. Phys. B **52**, 135502 (2019).
[42] Y. Wang, X. Wang, J. Li, D. Huang, L. Zhang, and Y. Guo, Phys. Lett. A **382**, 1149 (2018).
[43] H.-L. Yan, W. Zhu, and Y. Fu, Sci. Rep. **9**, 49 (2019).
[44] D. B. S. Soh, C. Brif, P. J. Coles, N. Lütkenhaus, R. M. Camacho, J. Urayama, and M. Sarovar, Phys. Rev. X **5**, 041010 (2015).
[45] B. Qi, Phys. Rev. A **94**, 042340 (2016).
[46] A. Marie and R. Alléaume, Phys. Rev. A **95**, 012316 (2017).
[47] T. Wang, P. Huang, Y. Zhou, W. Liu, and G. Zeng, Phys. Rev. A **97**, 012310 (2018).
[48] S. Pirandola, New J. Phys. **15**, 113046 (2013).
[49] A. S. Holevo, Probl. Inf. Transm. **9**, 177 (1973).