Continuous-variable measurement-device-independent quantum key distribution with source-intensity errors

Pu Wang,[1] Xuyang Wang,[1,2] and Yongmin Li[1,2,*]

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

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

(Received 1 January 2020; revised 22 July 2020; accepted 24 July 2020; published 10 August 2020)

Continuous-variable measurement-device-independent quantum key distribution (CV-MDI-QKD) is immune to all detector side channel attacks, however its security requires trusted sources. We investigate the effects of source intensity errors, the most crucial source error, on the security of CV-MDI-QKD protocol with Gaussian-modulated coherent states. We establish a general source intensity errors model and derive the secret key rate based on different assumptions on the abilities of legal parties Alice and Bob. To avoid the adverse effects of the sources' intensity errors on CV-MDI-QKD, we present different data-processing schemes. We also assess the security of the protocol against collective Gaussian attacks in the finite-size scenario with composable security. Taking source intensity errors into consideration, we achieve improved security compared to previous demonstrations. Our results will provide a useful reference for practical implementations of CV-MDI-QKD.

DOI: 10.1103/PhysRevA.102.022609

I. INTRODUCTION

Quantum key distribution (QKD) [1,2] allows two remote and legal parties, Alice and Bob, to distill a common secret key, despite the presence of a potential eavesdropper, Eve. Its security is guaranteed by the fundamental laws of quantum physics [3–7]. Three differing categories of QKD protocols have been proposed and demonstrated: discrete-variable (DV), continuous-variable (CV), and distributed phase reference. In CV-QKD [5–8], the key information is encoded in quadratures of the quantized electromagnetic field, such as those of coherent states [9,10]. Combined with high-efficiency homodyne (heterodyne) measurements, high secret key rates at metropolitan distances can be achieved. Moreover, it can also be conveniently integrated into current passive optical networks. The potential advantages have received extensive attention, and CV-QKD has witnessed rapid development. A number of CV-QKD protocols have been studied and experimentally demonstrated [11–31] over the past two decades. Recently, CV quantum repeaters have been designed, and it is shown that the fundamental rate-distance limit of direct-transmission CV-QKD can be broken, and a secure key can be generated over thousands of kilometers [32,33].

Despite the current rapid progress, there are still some challenges for the real applications of CV-QKD, one of which is its practical security. Theoretically, the CV-QKD protocols have been proven to be unconditionally secure [8,34–36]. In practical implementation, due to the fact that some ideal assumptions of the devices cannot be fully satisfied, some potential security loopholes may be opened, which can be exploited by the eavesdropper to carry out attacks and acquire secret key information without being noticed. To close these loopholes, a device-independent QKD (DI-QKD) [37,38] protocol was proposed to remove all assumptions of the internal working of QKD. However, it is still impractical due to its low secret key rate and short transmission distance. Later on, a measurement-device-independent QKD (MDI-QKD) [39,40] protocol was invented to remove all potential security loopholes in the detection side, the most vulnerable part in practical implementation of a QKD system. It has favorable performance and is feasible at a long distance. As a counterpart, the notion of MDI was subsequently extended to the CV framework [41–45]. In CV-MDI-QKD protocols, both Alice and Bob prepare quantum states and send them to an untrusted third party, Charlie, who performs CV Bell state detection on each received quantum state pair and announces his measurement outcome in a public channel. After data postprocessing, the correlation between Alice's and Bob's data is established and a secret key can be distilled. Note that the one-sided device-independent (1sDI) CV-QKD protocol has been proposed recently [46,47].

The security of the CV-MDI-QKD protocol with Gaussian-modulated coherent states has been firmly established in the finite-size regime [48,49] and composable framework [50]. Although CV-MDI-QKD is intrinsically immune to all detector side-channel attacks, the sources are assumed to be perfectly stable. Even though one can control the source pretty well in practice, there are inevitably some errors. The source errors may occur due to the intensity fluctuation of optical pulses, imprecise alignments of optical modulators and attenuators, unavoidable disturbance from external environments, etc. If the source error is not properly handled, Alice and Bob may overestimate their secret key rate without knowing it and pose a security risk. To address imperfections of state preparation in one-way CV-QKD, several models have

[*] yongmin@sxu.edu.cn

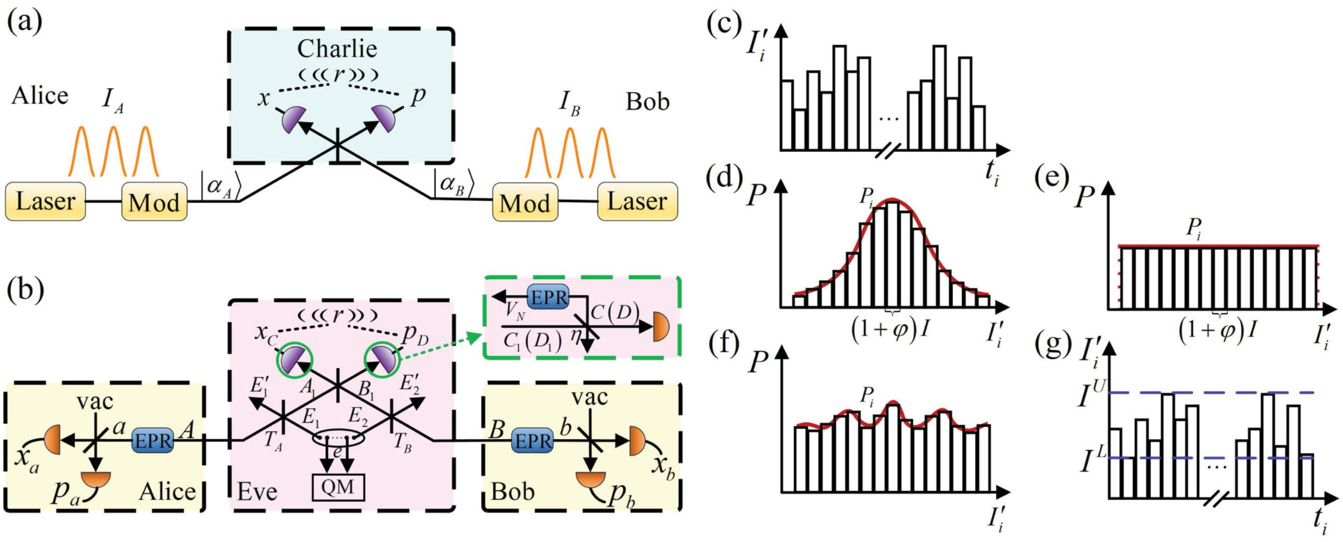

FIG. 1. (a) Prepare-and-measure (PM) scheme of CV-MDI-QKD protocol with Gaussian-modulated coherent states. (b) The equivalent entanglement-based (EB) scheme. (c) The signal pulse intensity changes with time t_i. (d) The signal pulse intensity follows a Gaussian distribution with a mean value of $(1+\varphi)I$. (e) The signal pulse intensity follows a uniform distribution centered in $(1+\varphi)I$. (f) The statistical distribution of the signal pulse intensity is unknown. (g) The upper and lower boundaries of the intensity errors.

been proposed [51–56]. Recently, the imperfection of state preparation was extended to CV-MDI-QKD [57], where the security analysis is based on the single-mode Gaussian attack in the asymptotic limit.

The source intensity fluctuation is the main source imperfection commonly existing in various QKD systems. Analysis of its effect on the security of the QKD protocols is essential. A series of studies have been done on enhancing the security of DV-QKD and DV-MDI-QKD by carefully examining the source intensity errors in practical implementations [58–65]. In contrast to the extensive study of source intensity errors in a DV field, the relevant research in the CV field lags behind. Recently, the effect of the intensity fluctuating source on the one-way CV-QKD protocol was reported [66]. However, the influence of the source intensity errors on the security analysis of CV-MDI-QKD is still an open question.

In this paper, we establish a general source intensity error model for CV-MDI-QKD, in which not only the intensity fluctuations but also the intensity deviations are involved. In practice, the imprecise alignments of source devices (modulators or attenuators) may lead to the intensity deviation [67], which drifts slowly and can be treated as a constant within each QKD transmission round. Based on different assumptions on the abilities of Alice and Bob (we do not place any restriction on Eve, and consider the worst case that she knows exactly the intensity side information of each pulse), we propose different data processing schemes and derive rigorously the secret key rate of the CV-MDI-QKD protocol with Gaussian-modulated coherent states against two-mode Gaussian attack. We also present a finite-key security analysis against collective Gaussian attacks in the composable security framework for the CV-MDI-QKD protocol with source intensity errors.

The rest of this paper is organized as follows. In Sec. II, we provide a short review of the CV-MDI-QKD protocol with Gaussian-modulated coherent states. In Sec. III, we present a general model of the CV-MDI-QKD protocol with source intensity errors, and we show the details of how to calculate the secure key rate based on the two different assumptions about the abilities of Alice and Bob. In Sec. IV, without assumption of any specific distribution, we derive the secret key rate of the protocol in the asymptotic regime and the finite-size regime with composable security, respectively. Our conclusions are drawn in Sec. V.

II. CV-MDI-QKD PROTOCOL WITH GAUSSIAN-MODULATED COHERENT STATES

In this section, we review briefly the Gaussian-modulated coherent states CV-MDI-QKD protocol. The general process of this protocol is described as follows [Fig. 1(a)].

Alice (Bob) uses signal pulses with intensity I_A (I_B) to prepare a series of Gaussian-modulated coherent states $|\alpha_A\rangle$ ($|\alpha_B\rangle$). In the phase space, they can be expressed as

$$\begin{aligned} |\alpha_A\rangle &= ||\alpha_A|e^{i\theta_A}\rangle = |x_A + ip_A\rangle, \\ |\alpha_B\rangle &= ||\alpha_B|e^{i\theta_B}\rangle = |x_B + ip_B\rangle, \end{aligned} \tag{1}$$

where $|\alpha_A|$ ($|\alpha_B|$) is the complex amplitude of the coherent state and $I_A \propto |\alpha_A|^2$ ($I_B \propto |\alpha_B|^2$); θ_A and θ_B indicate the phase of the coherent states; x_A and p_A (x_B and p_B) represent two independent field quadratures with zero mean and identical variance V_A (V_B) in shot-noise units (SNUs). Then both Alice and Bob send their coherent states to Charlie through two different quantum channels. On Charlie's station, the received two signal states are interfered at a beam splitter (BS) with a transmittance of 50%, which produces correlated output states. The output states are subsequently detected by using two homodyne detectors: one detects the amplitude quadrature and the other detects the phase quadrature, and the final measurement results are publicly announced by Charlie. With this announced information, either Alice or Bob can modify the data at hand and generate correlated data with the other.

For convenience of security analysis, we consider the equivalent entanglement-based (EB) scheme [Fig. 1(b)]. Alice starts with an Einstein-Podolsky-Rosen (EPR) state ρ_{aA} with variance $V_A + 1$ and performs heterodyne detection on the retained mode a, which projects mode A onto coherent states. The mode A is sent to an untrusted quantum relay, Charlie, via a quantum channel with length L_{AC}, which is assumed to be controlled by a potential eavesdropper, Eve, and characterized by the transmission T_A and excess noise ε_A. Likewise, Bob does the same. On Charlie's station, the realistic homodyne detector is modeled by assuming that the signal is further attenuated by a BS transformation with transmission efficiency η and mixed with some thermal noise V_N that simulates the electronic noise υ_{el} of the detector. Then the x quadrature of mode C and the p quadrature of mode D are measured by perfect homodyne detectors, and Charlie publicly announces a complex variable $r = (x_C + ip_D)/\sqrt{2}$ to Alice and Bob through a classical channel. After that, Alice and Bob can infer each other's data, and with classical data postprocessing, namely parameter estimation, information reconciliation, and privacy amplification, the secret keys can be extracted.

Here we consider a joint two-mode Gaussian attack [Fig. 1(b)] [41,68], where Eve's two ancillary modes E_1 and E_2 are extracted from a reservoir of entangled states $\{E_1, E_2, e\}$ and mixed with two incoming modes A and B. They have the covariance matrix of the form [41]

$$\gamma_{E_1E_2} = \begin{bmatrix} \omega_A \mathrm{I} & G \\ G & \omega_B \mathrm{I} \end{bmatrix}, \; G = \begin{bmatrix} g & 0 \\ 0 & g_1 \end{bmatrix}, \tag{2}$$

where ω_A and ω_B are the variances of the thermal noise introduced by E_1 and E_2, respectively. g and g_1 represent the quantum correlations between the two modes and must satisfy the physical constraints imposed by the Heisenberg uncertainty principle.

When Alice is the encoder of information, after communication of Charlie's outcome r, the asymptotical secret key rate against collective attacks is expressed as [41]

$$K^{\infty} = \beta I_{ab|r} - \chi_{aE|r}, \tag{3}$$

where β is the reconciliation efficiency, $I_{ab|r}$ is the Shannon mutual information between Alice and Bob, and $\chi_{aE|r}$ is the Holevo bound between Alice and Eve, which puts an upper limit on the information available to Eve on Alice's key. Details for calculation of the key rate can be found in Appendix A.

The result above is based on one assumption that all states are prepared perfectly. However, in practical implementation, there are inevitably some preparation errors, such as source intensity errors [Fig. 1(c)]. In this case, the initial states sent from the sources are different from the target states that Alice and Bob want to prepare. In the following sections, we consider the effects of such source errors on the security of the CV-MDI-QKD protocol. We first discuss two types of statistical distributions of the intensity errors: Gaussian distribution [Fig. 1(d)] and uniform distribution [Fig. 1(e)], and we derive the formulas of the secret key rate under two-mode Gaussian attack. Then we remove the assumption of any specific distribution [Fig. 1(f)], and we derive the secure secret key rate given that Alice and Bob only know the upper and lower boundary values of the intensity errors [Fig. 1(g)].

III. CV-MDI-QKD WITH SOURCE INTENSITY ERRORS

Suppose the sender wants to prepare her signal pulse with intensity I; however, at each time t_i she actually prepares a state with the intensity of $I_i' = I(1+\varphi)(1+\delta_i)$, where φ is the intensity deviation caused by the imprecise alignments of source devices (modulators or attenuators), which can be treated as a constant, because its drift is quite slow within each QKD transmission round, and δ_i is the intensity fluctuation arising from the imprecise intensity control of the source pulse with zero mean and variance of V_f. Since $I \propto |\alpha|^2$, the actual encoded Gaussian random variables of Alice and Bob are

$$\begin{aligned} x_A' &= \sqrt{(1+\varphi_A)(1+\delta_{Ai})}x_A, \\ p_A' &= \sqrt{(1+\varphi_A)(1+\delta_{Ai})}p_A, \\ x_B' &= \sqrt{(1+\varphi_B)(1+\delta_{Bi})}x_B, \\ p_B' &= \sqrt{(1+\varphi_B)(1+\delta_{Bi})}p_B. \end{aligned} \tag{4}$$

After the prepared states transmit through the quantum channel, Charlie performs a CV Bell state detection and obtains

$$\begin{aligned} x_C' &= \frac{1}{\sqrt{2}}(\sqrt{t_B}x_B' - \sqrt{t_A}x_A') + x_N, \\ p_D' &= \frac{1}{\sqrt{2}}(\sqrt{t_B}p_B' + \sqrt{t_A}p_A') + p_N, \end{aligned} \tag{5}$$

where $t_{A/B} = \eta T_{A/B}$, x_N and p_N are noise terms, and their variances are given by

$$\begin{aligned} \sigma_{x_N}^2 &= \frac{\eta}{2}(l - 2\sqrt{1-T_A}\sqrt{1-T_B}g) + \eta\chi_{\text{hom}}, \\ \sigma_{p_N}^2 &= \frac{\eta}{2}(l + 2\sqrt{1-T_A}\sqrt{1-T_B}g_1) + \eta\chi_{\text{hom}}, \end{aligned} \tag{6}$$

where

$$l = \varepsilon_A T_A + \varepsilon_B T_B + 2. \tag{7}$$

Next, based on different assumptions on the abilities of Alice and Bob to characterize the source errors, we investigate the effects of source intensity errors on the security of the CV-MDI-QKD protocol.

A. Alice and Bob have the intensity side information of each individual pulse

Let us first make an assumption that Alice and Bob know the intensity side information of each individual pulse. In this case, Alice and Bob are able to correct the errors of each individual pulse pretty well in principle, such as making real-time feedback control to the optical source. However, this will increase the complexity and cost of the system. It is possible to estimate a security key rate without any hardware adjustment. More precisely, Alice and Bob can revise their data from $x_{A/B}$, $p_{A/B}$ to $x_{A/B}'$, $p_{A/B}'$. In this case, the channel parameters can be correctly estimated, and the final secret key rate is calculated as

$$K_{\text{final}}^{\infty} = \iint_{-\infty}^{+\infty} f(\delta_{A_i}) f(\delta_{B_i}) K^{\infty}(V_{A_i}, V_{B_i}) d\delta_{A_i} d\delta_{B_i}, \tag{8}$$

where $f(\delta_{A_i})$ and $f(\delta_{B_i})$ represent the probability density function of δ_{A_i} and δ_{B_i}, respectively, and $V_{A_i} =$

$(1+\varphi_A)(1+\delta_{A_i})V_A$, $V_{B_i}=(1+\varphi_B)(1+\delta_{B_i})V_B$. By numerical simulation, we find that the final secret key generation rate is basically the same as that without the source errors.

Concretely, we notice that

$$
\begin{aligned}
V(x'_{A/B}) &= V\big(\sqrt{(1+\varphi_{A/B})(1+\delta_{A_i/B_i})}x_{A/B}\big)\\
&= (1+\varphi_{A/B})\big\langle\big(\sqrt{(1+\delta_{A_i/B_i})}x_{A/B}\big)^2\big\rangle\\
&= (1+\varphi_{A/B})V_{A/B}, \qquad (9)
\end{aligned}
$$

and $V(p'_{A/B})=V(x'_{A/B})=(1+\varphi_{A/B})V_{A/B}$. This means that Alice and Bob actually prepare the Gaussian or non-Gaussian modulation coherent states with variances $(1+\varphi_A)V_A$ and $(1+\varphi_B)V_B$. Considering that Alice and Bob choose optimal modulation variances V_A and V_B to encode their information, according to the optimality of Gaussian modulation, the final secret key rate of protocol will slightly decrease, in contrast to the ideal protocol.

B. Alice and Bob only know the statistical distribution of the pulse intensity

In some cases, Alice and Bob only know the statistical distribution rather than the intensity side information of each individual pulse. For instance, φ and δ_i are evaluated before the QKD run. Here, we mainly discuss two types of distributions of δ_i, namely Gaussian distribution and uniform distribution.

To estimate the secret key rate, the channel parameters T_A, ε_A, T_B, ε_B should be known. If Alice and Bob use the recorded data $x_{A/B}$ and $p_{A/B}$ for the parameter estimation, we can obtain (see Appendix B for more details)

$$
\begin{aligned}
T'_A &= (1+\varphi_A)T_{f_A}T_A,\\
T'_B &= (1+\varphi_B)T_{f_B}T_B,\\
\varepsilon'_A &\approx \varepsilon_A/(1+\varphi_A)T_{f_A}+\tfrac{1}{4}V_AV_{f_A},\\
\varepsilon'_B &\approx \varepsilon_B/(1+\varphi_B)T_{f_B}+\tfrac{1}{4}V_BV_{f_B},
\end{aligned}
\qquad (10)
$$

where $T_{f_{A/B}}=(1-V_{f_{A/B}}/8)^2$, and $V_{f_{A/B}}$ is the variance of δ_{A_i/B_i}. In addition,

$$
g'=\frac{\sqrt{1-T_A}\sqrt{1-T_B}}{\sqrt{1-T'_A}\sqrt{1-T'_B}}g,\quad g'_1=\frac{\sqrt{1-T_A}\sqrt{1-T_B}}{\sqrt{1-T'_A}\sqrt{1-T'_B}}g_1. \qquad (11)
$$

When there is a minus intensity deviation, which means $\varphi<0$, we can see that the channel loss and excess noise are always overestimated. However, when there is a positive intensity deviation ($\varphi>0$), the channel loss and excess noise are not always overestimated and may be underestimated. For instance, we assume the parameters have the concrete values of $\varphi_A=\varphi_B=0.1$, $V_{f_A}=V_{f_B}=10^{-4}$, $V_M=20$, and $\varepsilon_A=\varepsilon_B=0.05$. Since Eve has the intensity side information, she can perform a partial intercept-resend (PIR) attack [69,70] and hide the excess noise introduced by her PIR attack according to φ, so that the estimated total excess noise is equal to or even smaller than the original excess noise. Therefore, if Alice and Bob use the recorded data $x_{A/B}$ and $p_{A/B}$ for the parameter estimation, they will overestimate the secret key rate without knowing it, and this opens a security loophole.

To overcome this loophole, we propose to revise the recorded data of Alice and Bob from $x_{A/B}$, $p_{A/B}$ to $\sqrt{(1+\varphi_{A/B})}x_{A/B}$, $\sqrt{(1+\varphi_{A/B})}p_{A/B}$ and use the corrected data for the parameter estimation. In this case, we have (Appendix B)

$$
\begin{aligned}
T'_A &= T_{f_A}T_A,\\
T'_B &= T_{f_B}T_B,\\
\varepsilon'_A &\approx \varepsilon_A/T_{f_A}+\tfrac{1}{4}(1+\varphi_A)V_AV_{f_A},\\
\varepsilon'_B &\approx \varepsilon_B/T_{f_B}+\tfrac{1}{4}(1+\varphi_B)V_BV_{f_B},
\end{aligned}
\qquad (12)
$$

and

$$
g'=\frac{\sqrt{1-T_A}\sqrt{1-T_B}}{\sqrt{1-T'_A}\sqrt{1-T'_B}}g,\quad g'_1=\frac{\sqrt{1-T_A}\sqrt{1-T_B}}{\sqrt{1-T'_A}\sqrt{1-T'_B}}g_1. \qquad (13)
$$

We can find from Eq. (12) that the channel loss and excess noise are overestimated and the potential loophole mentioned above can be closed. Then, Alice and Bob can use the corrected data $\sqrt{(1+\varphi_{A/B})}x_{A/B}$, $\sqrt{(1+\varphi_{A/B})}p_{A/B}$ to obtain the final secret key rate. However, this is still not the best choice, since the key rate can be further improved by enlarging the data, as shown below.

It is clear that the signal pulse that has a higher intensity than what Alice and Bob plan to send is insecure [66,67]. Thus they can only use the signal pulses with lower intensity than expected to extract the secret keys. To obtain greater numbers of signal pulses for key extraction, Alice and Bob need to enlarge their data. Suppose Alice and Bob revise their data from $\sqrt{(1+\varphi_{A/B})}x_{A/B}$, $\sqrt{(1+\varphi_{A/B})}p_{A/B}$ to $\sqrt{(1+\varphi_{A/B})d_{A/B}}x_{A/B}$, $\sqrt{(1+\varphi_{A/B})d_{A/B}}p_{A/B}$, where $d_{A/B}\geqslant 1$. Then the probabilities of Alice and Bob sending low-intensity signal pulses are

$$
P_A=\int_{-\infty}^{d_A-1} f\big(\delta_{A_i}\big)d\delta_{A_i},\quad P_B=\int_{-\infty}^{d_B-1} f\big(\delta_{B_i}\big)d\delta_{B_i}. \qquad (14)
$$

Here we set $d_{A/B}\leqslant d^U_{A/B}$ (the upper boundary of the distribution interval) for the uniform distributed intensity fluctuation and $d_{A/B}\leqslant 1+3\sqrt{V_{f_{A/B}}}$ (considering the confidence interval with three standard deviations) for Gaussian distributed intensity fluctuation.

If Alice and Bob use the revised data for parameter estimation, they have (Appendix B)

$$
\begin{aligned}
T'_A &= T_{f_A}T_A/d_A,\\
T'_B &= T_{f_B}T_B/d_B,\\
\varepsilon'_A &\approx \varepsilon_Ad_A/T_{f_A}+\tfrac{1}{4}(1+\varphi_A)d_AV_AV_{f_A},\\
\varepsilon'_B &\approx \varepsilon_Bd_B/T_{f_B}+\tfrac{1}{4}(1+\varphi_B)d_BV_BV_{f_B},
\end{aligned}
\qquad (15)
$$

and

$$
g'=\frac{\sqrt{1-T_A}\sqrt{1-T_B}}{\sqrt{1-T'_A}\sqrt{1-T'_B}}g,\quad g'_1=\frac{\sqrt{1-T_A}\sqrt{1-T_B}}{\sqrt{1-T'_A}\sqrt{1-T'_B}}g_1. \qquad (16)
$$

Because there are two optical sources in CV-MDI-QKD, the secret keys can only be extracted when they both send low-intensity pulses; the corresponding probability is $P=P_AP_B$.

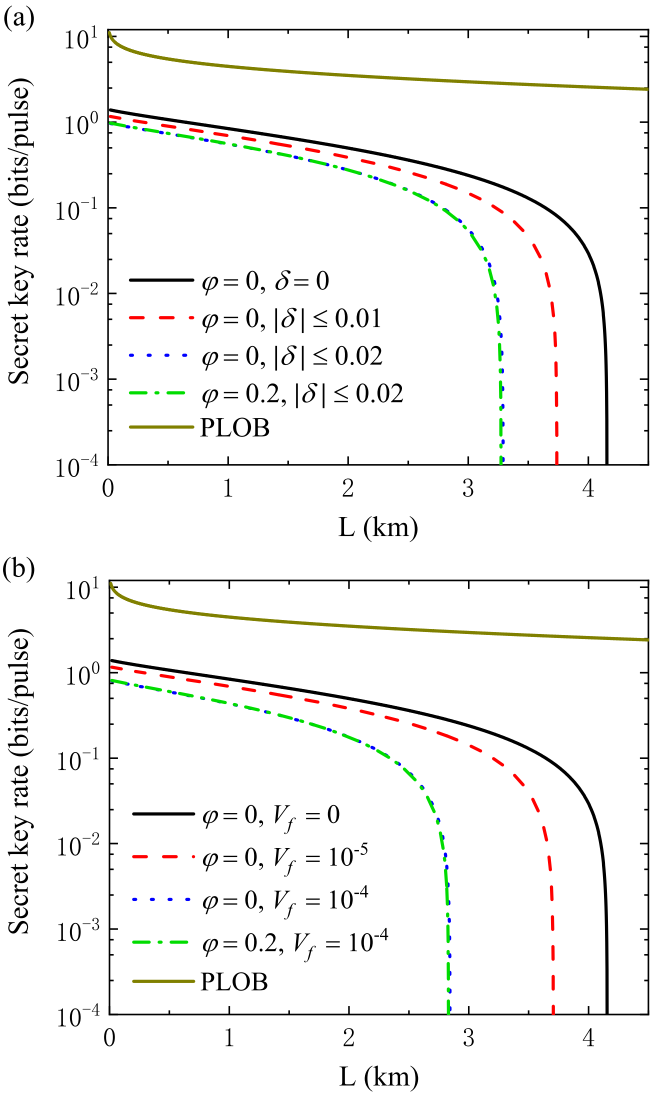

FIG. 2. Secret key rate vs the transmission distance in the symmetric case with different source intensity deviations and fluctuations. (a) Uniform distributed intensity fluctuation; (b) Gaussian distributed intensity fluctuation. Here, we set the reconciliation efficiency $\beta = 0.97$, modulation variance $V_M = 60$, excess noise $\varepsilon_A = \varepsilon_B = 0.002$ SNUs, detection efficiency $\eta = 0.97$, and electrical noise $\upsilon_{\text{el}} = 0.01$.

The final secret key rate is then given by [66]

$$K_{\text{final}}^{\infty} = \beta I_{ab|r} - (1-P)[H(a_x|r) + H(a_p|r)] - P\chi_{aE|r}, \tag{17}$$

where $(1-P)H(a_x|r)$ and $(1-P)H(a_p|r)$ are the information entropy that cannot be used to extract the secure secret keys on the amplitude and phase quadratures of Alice (assuming Alice is the encoder side), respectively. Obviously, larger $d_{A/B}$ indicates that more signal pulses are used for key extraction, but the cost is that the estimated channel loss and excess noise will be higher. Therefore, there is a tradeoff to choose the optimal $d_{A/B}$.

First, we consider the symmetric CV-MDI-QKD protocol in which the untrusted third party, Charlie, is in the middle of Alice and Bob, $L_{AC} = L_{BC}$. Figure 2 shows the secret key rate $K_{\text{final}}^{\infty}$ as a function of the transmission distance $L = L_{AC} + L_{BC}$ for different intensity deviations and fluctuations, where Figs. 2(a) and 2(b) present the results for the uniform distributed intensity fluctuation and the Gaussian distributed intensity fluctuation, respectively. The black solid curve depicts the secret key rate without intensity error, and the upper (dark yellow) solid curve is the Pirandola-Laurenza-Ottaviani-Banchi (PLOB) bound [71], which represents the maximum secret key rate achievable in a repeater-less and lossy channel system. Here, we set $\varphi_A = \varphi_B = \varphi$, $\delta_A = \delta_B = \delta$, $V_{f_A} = V_{f_B} = V_f$, $\eta = 0.97$, and $\upsilon_{\text{el}} = 0.01$. We can see that both the secret key rate and transmission distance decrease with the increases of fluctuation strength. Notice that even with a large deviation of $\varphi = 0.2$, the secret key rate is almost unaffected. This is mainly due to the fact that after the data are corrected, the intensity deviation, as expected, has a negligible impact on the parameter estimation of the protocol.

In CV-MDI-QKD protocols, it has been proved that the performance of the asymmetric case ($L_{AC} \neq L_{BC}$) is superior to the symmetric case ($L_{AC} = L_{BC}$) [41,42,45]. When Alice is the encoder of information, the total transmission distance $L = L_{AC} + L_{BC}$ increases significantly as L_{AC} decreases. If the distance between Charlie and Alice is 0 ($L_{AC} = 0$), the total transmission distance will reach its maximal value. In this case (the most asymmetric case), the two-mode Gaussian attack degenerates into two independent Gaussian attacks [68], which means $g = g_1 = 0$. For different intensity fluctuations, the secret key rates versus the transmission distance in the most asymmetric case are plotted in Fig. 3, where (a) and (b) denote the results for the uniform distributed and Gaussian distributed intensity fluctuations, respectively. The results show that the intensity fluctuation of Alice's source has a greater negative impact on the performance of the protocol compared with that of Bob's source, because Alice is the encoder. Therefore, if the two sources have different intensity fluctuations, the relatively stable source should be placed at the encoder side.

IV. NO ASSUMPTION OF ANY SPECIFIC DISTRIBUTION OF INTENSITY ERRORS

Up to now, we have discussed two types of statistical distributions of the intensity errors: Gaussian distribution and uniform distribution. In this section, we remove the assumption of any specific distribution, and we derive the secure secret key rate given that Alice and Bob only know the upper and lower bound values of intensity errors. Furthermore, we extend the security of the protocol into a finite-size scenario with composable security.

We assume that the intensity of Alice's (Bob's) signal pulse is bounded by $[I_A^L, I_A^U]$ ($[I_B^L, I_B^U]$), where $I_A^{L(U)}$ ($I_B^{L(U)}$) represents the lower (upper) bound values of the intensity errors of Alice's (Bob's) source, and $I_A^{L(U)} = k_A^{L(U)} I_A$ ($I_B^{L(U)} = k_B^{L(U)} I_B$). We also consider the worst-case scenario in which the eavesdropper knows exactly the intensity side information of each individual pulse. Because the intensity probability distribution is unknown, we cannot assess the information acquired by Eve. But fortunately, the key is secure when the signal pulses sent by Alice and Bob have lower intensity than expected. Thus, in order to ensure secure communication, we only need to adjust the data retained by Alice and Bob from

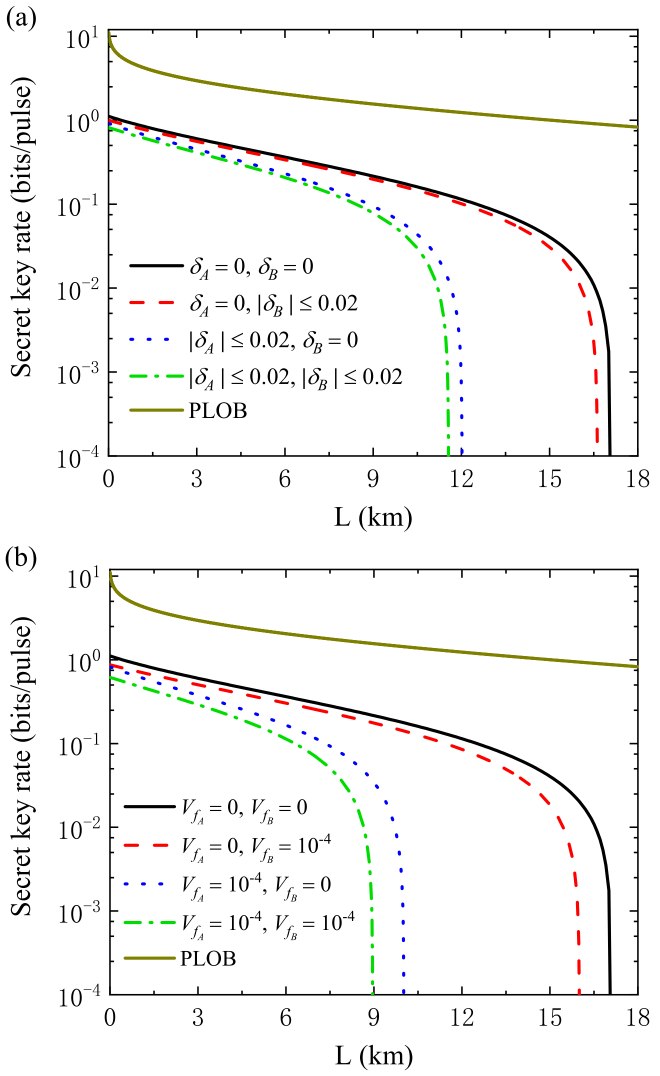

FIG. 3. Achievable secret key rate vs the transmission distance in the most asymmetric case for different intensity fluctuations. Part (a) denotes the results for the uniform distributed intensity fluctuation, and (b) denotes the results for the Gaussian distributed intensity fluctuation. The green dotted-dashed curve is plotted with an intensity deviation of $\delta_A = \delta_B = 0.01$, and there is no intensity deviation for other curves. $d_{A/B}$ is optimal, and other parameters are set to $\beta = 0.97$, $V_M = 19$, $\varepsilon_A = \varepsilon_B = 0.002$, $\eta = 0.97$, $v_{\text{el}} = 0.01$.

$x_{A/B}$, $p_{A/B}$ to $\sqrt{k^U_{A/B}}x_{A/B}$, $\sqrt{k^U_{A/B}}p_{A/B}$, and use them to perform the parameter estimation and key extraction tasks.

Referring to Appendix C 1, when Alice and Bob use the revised data $\sqrt{k^U_{A/B}}x_{A/B}$ and $\sqrt{k^U_{A/B}}p_{A/B}$ for parameter estimation, we have

$$\begin{aligned}
T'_A &= T_{k_A} T_A / k^U_A,\\
T'_B &= T_{k_B} T_B / k^U_B,\\
\varepsilon'_A &\approx \varepsilon_A k^U_A / T_{k_A} + \frac{V_{k_A}}{4m^2_{k_A}} k^U_A V_A,\\
\varepsilon'_B &\approx \varepsilon_B k^U_B / T_{k_B} + \frac{V_{k_B}}{4m^2_{k_B}} k^U_B V_B,
\end{aligned} \tag{18}$$

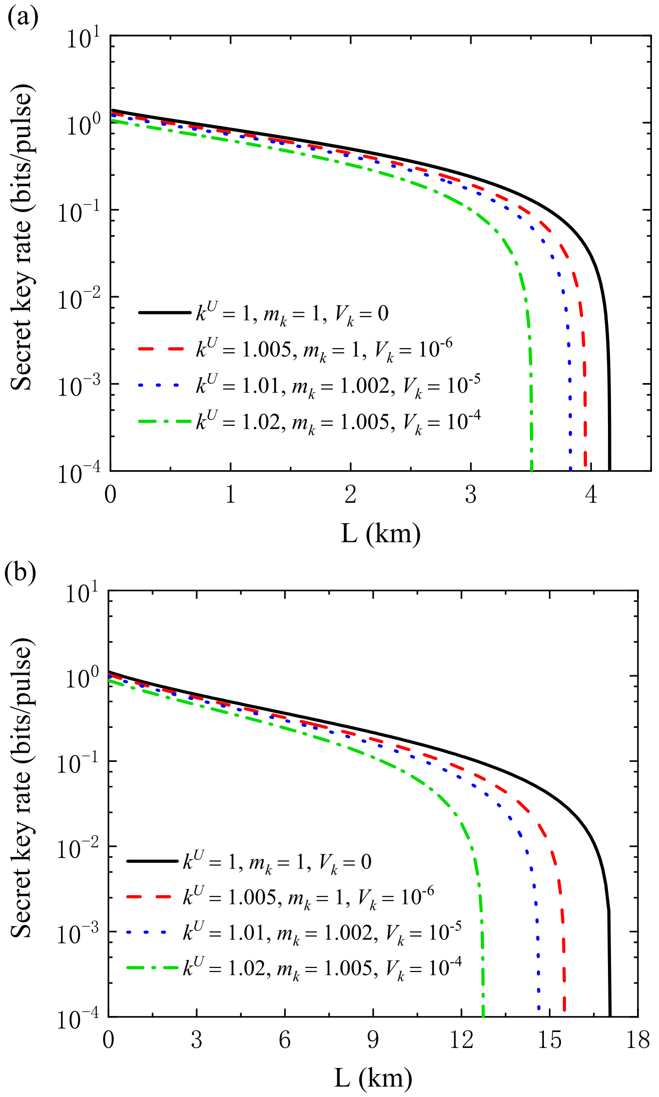

FIG. 4. The secret key rate vs the transmission distance when the statistical distributions of the intensity errors are unknown. Part (a) represents the symmetric case with $V_M = 60$, and (b) represents the most asymmetric case with $V_M = 19$. Other parameters are set to $\beta = 0.97$, $\varepsilon_A = \varepsilon_B = 0.002$, $\eta = 0.97$, and $v_{\text{el}} = 0.01$.

and

$$g' = \frac{\sqrt{1-T_A}\sqrt{1-T_B}}{\sqrt{1-T'_A}\sqrt{1-T'_B}}g, \quad g'_1 = \frac{\sqrt{1-T_A}\sqrt{1-T_B}}{\sqrt{1-T'_A}\sqrt{1-T'_B}}g_1. \tag{19}$$

where m_{k_A} and V_{k_A} (m_{k_B} and V_{k_B}) represent the mean and variance of k_A (k_B), and $T_{k_{A/B}} = m_{k_{A/B}}(1 - V_{k_{A/B}}/8m^2_{k_{A/B}})^2$.

Then the final secret key rate can be given by

$$\begin{aligned}
K^{\infty}_{\text{final}} = {}& \beta I_{ab|r}(V'_A, V'_B, T'_A, \varepsilon'_A, T'_B, \varepsilon'_B, g', g'_1)\\
& - \chi_{aE|r}(V'_A, V'_B, T'_A, \varepsilon'_A, T'_B, \varepsilon'_B, g', g'_1),
\end{aligned} \tag{20}$$

where $V'_A = k^U_A V_A$, $V'_B = k^U_B V_B$.

Figure 4 shows the secret key rate versus the transmission distance in the symmetric (a) and most asymmetric (b) cases with different intensity errors. Here different mean values and variances for k_A (k_B) are used to analyze the performance of the protocol. For simplicity, we set $k_A^U = k_B^U = k^U$, $m_{k_A} = m_{k_B} = m_k$, $V_{k_A} = V_{k_B} = V_k$. The results show that the secret key rate of the most asymmetric case looks more sensitive to source intensity errors than that in the symmetric case. Larger source error means shorter achievable distance.

In a practical implementation of any protocol, the total number of signals exchanged between Alice and Bob is always finite. Therefore, we should consider the finite-size effect. One of the most crucial parts in the finite-size regime is parameter estimation. Different from the asymptotic case, we have to consider the largest possible difference between the expected values and the real observed values due to statistical fluctuations. Here, we exploit the technique of Ref. [49], where the authors have shown that the parameter estimation in CV-MDI-QKD can be performed with almost no public communication. This means that Alice and Bob can use all their raw data for both parameter estimation and secret-key extraction. Then the tradeoff between secret key rate and accuracy of the parameter estimation in the finite-size regime can be removed. Based on this technique, a tight finite-size analysis with composable security for the CV-MDI-QKD protocol has been presented [50]. Here, we extend this work to the case with intensity fluctuations.

The lower bound of the secret key rate against collective Gaussian attacks provided by composable security can be expressed as [50]

$$K_{\rm com}^{s'} = R^L - \frac{1}{\sqrt{n}}\Delta_{\rm AEP} + \frac{1}{n}\log_2\left(p - \frac{2}{3}ps_{\rm SM}\right) + \frac{2}{n}\log_2(2s), \qquad (21)$$

where s' is the overall security parameter and $s' = s + s_{\rm SM} + s_{\rm EC} + s_{\rm PE}$. s comes from the leftover hash lemma; $s_{\rm SM}$ is the smoothing parameter entering the smooth conditional min-entropy; $s_{\rm EC}$ is the error in the error-correction routine; and $s_{\rm PE}$ is the probability of error related to the parameter estimation procedure. n denotes the total number of signals exchanged between Alice and Bob. p is the probability of successful error correction. $\Delta_{\rm AEP} = 4(d+1)\sqrt{\log_2(9/2p^2s_{\rm SM}^2)}$, where d is the number of bits on which each measurement result is encoded. And

$$R^L = \beta I_{ab}\left(\Omega_a^{\max}, \Omega_b^{\max}, \Omega_c^{\min}\right) - \chi_{aE}\left(\Omega_a^{\max}, \Omega_b^{\max}, \Omega_c^{\min}\right), \qquad (22)$$

where $\Omega_a^{\max}$, $\Omega_b^{\max}$, and $\Omega_c^{\min}$ are the boundary values on covariance matrix elements with statistic fluctuations. These values give a lower bound on the secret key rate and ensure the security of the CV-MDI-QKD protocol in the finite-size, composable setting. Detailed derivations can be found in Appendix C 2.

Figure 5 shows the lower bound of the secret key rate as a function of total exchanged signals n in the symmetric (a) and most asymmetric (b) cases considering both the source errors and composable security. Here, we consider a fixed source error: $k^U = 1.01$, $m_k = 1.002$, and $V_k = 10^{-5}$. The key rate is obtained by optimizing modulation variance. We can find that the finite size obviously limits the secret key rate of the protocol. For each transmission distance, there is a minimal n corresponding to a positive key rate. However, with the increase of the number of exchanged signals, the key rate increases rapidly and almost reaches that of the asymptotic case.

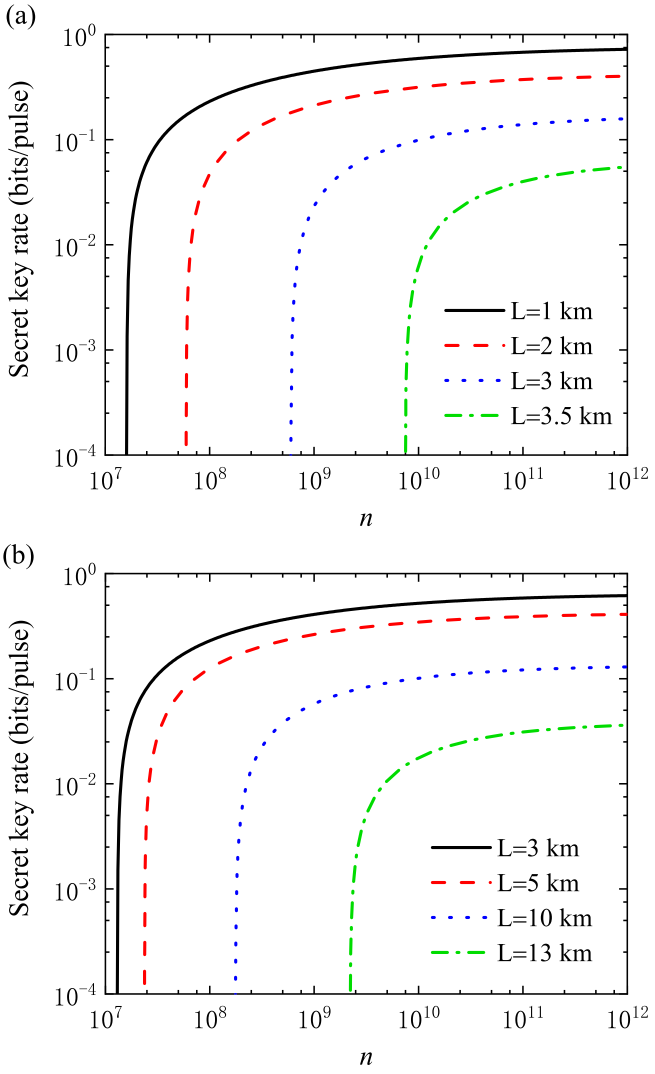

FIG. 5. Lower bound of the secret key rate vs the number of exchanged signals n with different transmission distances. Part (a) represents the symmetric case, and (b) represents the most asymmetric case. The plots are obtained by setting $p = 0.99$, $s = s_{\rm SM} = s_{\rm EC} = s_{\rm PE} = 10^{-21}$, and $d = 5$. Other parameters are set to $\beta = 0.97$, $\varepsilon_A = \varepsilon_B = 0.002$, $\eta = 0.97$, and $v_{\rm el} = 0.01$.

To further study the effect of intensity fluctuations, in Fig. 6 we simulate the secret key rate versus transmission distance with different intensity fluctuations for $n = 10^8$. It is clear that intensity fluctuations degrade the performance of the protocol. We also see that it is possible in principle to obtain a high secret key rate for a practical block size of $n = 10^8$. Therefore, our results indicate that the CV-MDI-QKD protocol with source intensity errors is still feasible when considering the finite-size effects with composable security, although the secret key rate is decreased to some extent compared with that of the ideal source.

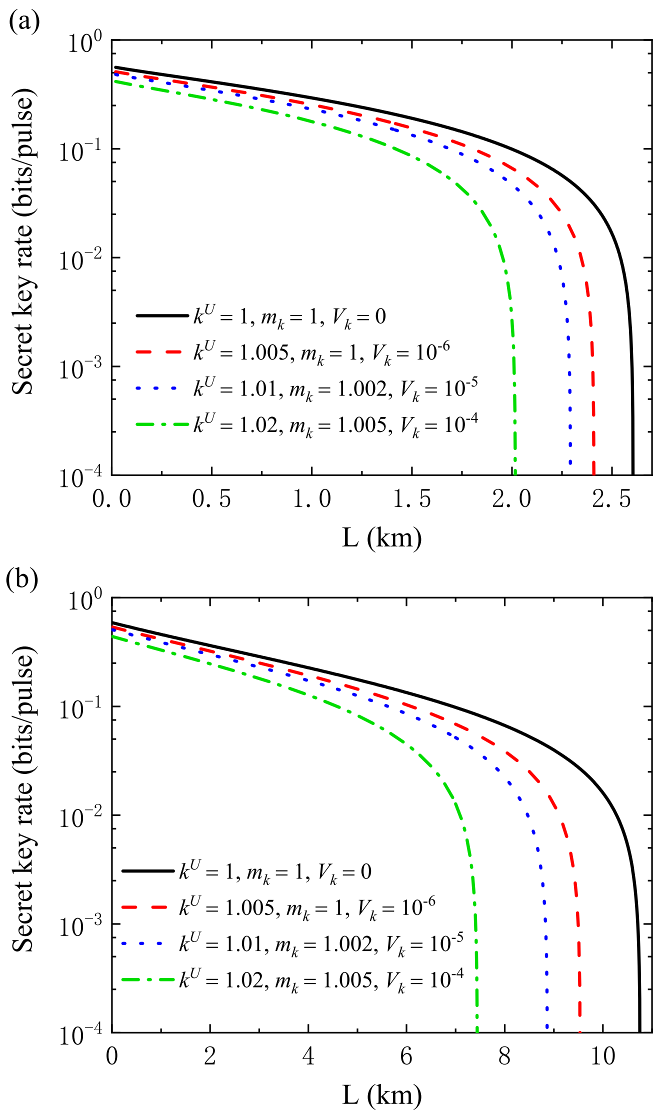

FIG. 6. Lower bound of the secret key rate vs the transmission distance for $n = 10^8$ with different intensity fluctuations. Part (a) represents the symmetric case, and (b) represents the most asymmetric case. Other parameters are the same as in Fig. 5.

V. CONCLUSIONS

We have presented a security analysis for CV-MDI-QKD with source intensity errors. Specifically, we have established a general intensity error model and derived the secure key rate of the CV-MDI-QKD protocol under two-mode Gaussian attack based on different assumptions on the abilities of Alice and Bob. A data-processing scheme was proposed to improve the security due to the intensity deviations of the source. In addition, we found that the intensity fluctuation on the encoder's side has a greater negative impact on the performance of the protocol compared with that on the nonencoder's side. Therefore, for two sources with different intensity fluctuation, the relatively stable source should be placed at the encoder's side to optimize the protocol. Furthermore, we have assessed the security of the protocol against collective Gaussian attacks in the finite-size scenario with composable security. The most general class of coherent attacks can immediately be obtained by exploiting the Gaussian–de Finetti reduction [36,50].

In conclusion, our work verifies the feasibility of the CV-MDI-QKD protocol with source intensity errors, and it constitutes an important step toward the practical security of the CV-MDI-QKD protocol. It is interesting to further investigate other practical security issues of CV-MDI-QKD in the future.

ACKNOWLEDGMENTS

This work is supported by the National Key R&D Program of China (Grant No. 2016YFA0301403); the National Natural Science Foundation of China (NSFC) (Grants No. 11774209 and No. 61378010); key Research and Development Projects of Shanxi Province (Project No. 201803D121065); and Shanxi 1331KSC.

APPENDIX A: CALCULATION OF THE SECRET KEY RATE

Based on Charlie's outcome r, the covariance matrix $\gamma_{ab|r}$ is given by

$$\gamma_{ab|r} = \begin{bmatrix} V\mathbb{I} & 0 \\ 0 & V\mathbb{I} \end{bmatrix} - (V^2 - 1) \times \begin{bmatrix} \frac{T_A}{\theta} & 0 & -\frac{\sqrt{T_A T_B}}{\theta} & 0 \\ 0 & \frac{T_A}{\theta'} & 0 & \frac{\sqrt{T_A T_B}}{\theta'} \\ -\frac{\sqrt{T_A T_B}}{\theta} & 0 & \frac{T_B}{\theta} & 0 \\ 0 & \frac{\sqrt{T_A T_B}}{\theta'} & 0 & \frac{T_B}{\theta'} \end{bmatrix}, \tag{A1}$$

where we have set $V = V_M + 1$, $V_M = V_A = V_B$, and

$$\begin{aligned} \theta &= (T_A + T_B)V_M + \varepsilon_A T_A + \varepsilon_B T_B + 2 \\ &\quad - 2\sqrt{1 - T_A}\sqrt{1 - T_B} g + 2\chi_{\text{hom}}, \\ \theta' &= (T_A + T_B)V_M + \varepsilon_A T_A + \varepsilon_B T_B + 2 \\ &\quad + 2\sqrt{1 - T_A}\sqrt{1 - T_B} g_1 + 2\chi_{\text{hom}}. \end{aligned} \tag{A2}$$

Here, $\chi_{\text{hom}} = (1 - \eta)/\eta + v_{el}/\eta$ is the total noise introduced by the realistic homodyne detector, referred to its input.

The covariance matrix of the state $\rho_{b|ra}$, conditioned on Alice's heterodyne measurement results x_a, p_a, is given by

$$\gamma_{b|ra} = \gamma_{b|r} - \sigma_{ab|r}(\gamma_{a|r} + 1)^{\text{MP}} \sigma_{ab|r}^T, \tag{A3}$$

where $\gamma_{b|r}$, $\sigma_{ab|r}$, and $\gamma_{a|r}$ are the submatrices of the covariance matrix $\gamma_{ab|r}$; MP denotes the Moore-Penrose inverse of a matrix. The conditional matrix is thus given by

$$\gamma_{b|ra} = \begin{bmatrix} V - \frac{(V^2-1)T_B}{\theta - V_M T_A} & 0 \\ 0 & V - \frac{(V^2-1)T_B}{\theta' - V_M T_A} \end{bmatrix}. \tag{A4}$$

Then, the Shannon mutual information between Alice and Bob can be calculated by

$$I_{ab|r} = \frac{1}{2}\log_2 \frac{V_{b|r}^x + 1}{V_{b|ra}^x + 1} + \frac{1}{2}\log_2 \frac{V_{b|r}^p + 1}{V_{b|ra}^p + 1} = \frac{1}{2}\log_2 \frac{\xi_1}{\xi_2}, \tag{A5}$$

where

$$\begin{aligned} \xi_1 &= (\theta - V_M T_A)(\theta' - V_M T_A)(\theta - V_M T_B)(\theta' - V_M T_B), \\ \xi_2 &= \theta\theta'(\theta - V_M T_A - V_M T_B)(\theta' - V_M T_A - V_M T_B). \end{aligned} \tag{A6}$$

Because Eve's system purifies ab, the Holevo bound $\chi_{aE|r}$ can be written as

$$\begin{aligned}\chi_{aE|r} &= S(\rho_{E|r}) - S(\rho_{E|ra})\\ &= S(\rho_{ab|r}) - S(\rho_{b|ra}).\end{aligned}\tag{A7}$$

$S(\rho_{ab|r})$ is the von Neumann entropy of the quantum state $\rho_{ab|r}$ and can be calculated from the symplectic eigenvalues $\lambda_{1,2}$ of the covariance matrix $\gamma_{ab|r}$,

$$\lambda_{1,2} = \sqrt{\frac{1}{2}(A \pm \sqrt{A^2 - 4B})},\tag{A8}$$

where $A = 2V^2 + [\xi_3^2 - V(\theta+\theta')\xi_4]/\theta\theta'$, $B = V^2(\xi_4 - V\theta)(\xi_4 - V\theta')/\theta\theta'$, $\xi_3 = (V^2-1)T_A - (V^2-1)T_B$, and $\xi_4 = (V^2-1)T_A + (V^2-1)T_B$.

$S(\rho_{b|ra})$ can be calculated from the symplectic eigenvalues λ_3 of the covariance matrix $\gamma_{b|ra}$, and $\lambda_3 = \sqrt{\det \gamma_{b|ra}}$.

Then,

$$\chi_{aE|r} = G\left(\frac{\lambda_1 - 1}{2}\right) + G\left(\frac{\lambda_2 - 1}{2}\right) - G\left(\frac{\lambda_3 - 1}{2}\right),\tag{A9}$$

where $G(x) = (x+1)\log_2(x+1) - x\log_2 x$.

Finally, the secure secret key rate is calculated using Eqs. (3), (A5), and (A9). Note that it has been proven that the optimal correlated attack that Eve can perform is the "negative EPR attack" in which [41]

$$\begin{aligned}g_1 &= -g = \phi,\\ \phi &= \min\{\sqrt{(\omega_A - 1)(\omega_B + 1)}, \sqrt{(\omega_A + 1)(\omega_B - 1)}\},\end{aligned}\tag{A10}$$

and the key rate meets the minimum value.

APPENDIX B: ESTIMATION OF CHANNEL PARAMETERS

After Charlie's detection, we have

$$\begin{aligned}x'_C &= \frac{1}{\sqrt{2}}(\sqrt{t_B}x'_B - \sqrt{t_A}x'_A) + x_N,\\ p'_D &= \frac{1}{\sqrt{2}}(\sqrt{t_B}p'_B + \sqrt{t_A}p'_A) + p_N,\end{aligned}\tag{B1}$$

where

$$\begin{aligned}x'_{A/B} &= \sqrt{(1+\varphi_{A/B})\big(1+\delta_{A_i/B_i}\big)}x_{A/B},\\ p'_{A/B} &= \sqrt{(1+\varphi_{A/B})\big(1+\delta_{A_i/B_i}\big)}p_{A/B}.\end{aligned}\tag{B2}$$

Thus,

$$\begin{aligned}V(x'_C) &= \frac{\eta}{2}(u + l - 2\sqrt{1-T_A}\sqrt{1-T_B}g) + \eta\chi_{\text{hom}},\\ V(p'_D) &= \frac{\eta}{2}(u + l + 2\sqrt{1-T_A}\sqrt{1-T_B}g_1) + \eta\chi_{\text{hom}},\end{aligned}\tag{B3}$$

where

$$u = T_B(1+\varphi_B)V_B + T_A(1+\varphi_A)V_A.\tag{B4}$$

If Alice and Bob use the recorded data $x_{A/B}$ and $p_{A/B}$ for parameter estimation, then

$$\begin{aligned}\sqrt{t'_{Ax}} &= -\sqrt{2}\frac{\langle x_A x'_C\rangle}{\langle x_A^2\rangle} = \frac{\langle x_A\sqrt{t_A}x'_A\rangle}{\langle x_A^2\rangle}\\ &= \sqrt{(1+\varphi_A)t_A}\Big\langle\sqrt{\big(1+\delta_{A_i}\big)}\Big\rangle,\\ \sqrt{t'_{Ap}} &= \sqrt{2}\frac{\langle p_A p'_D\rangle}{\langle p_A^2\rangle} = \frac{\langle p_A\sqrt{t_A}p'_A\rangle}{\langle p_A^2\rangle}\\ &= \sqrt{(1+\varphi_A)t_A}\Big\langle\sqrt{\big(1+\delta_{A_i}\big)}\Big\rangle.\end{aligned}\tag{B5}$$

Making a Taylor expansion around $\delta_{Ai} = 0$, we obtain

$$\Big\langle\sqrt{\big(1+\delta_{A_i}\big)}\Big\rangle \approx 1 - \tfrac{1}{8}V_{f_A},\tag{B6}$$

hence $t'_A = (1+\varphi_A)(1 - V_{f_A}/8)^2 t_A$.

By defining $T_{f_A} := (1 - V_{f_A}/8)^2$, we have

$$T'_A = t'_A/\eta = (1+\varphi_A)T_{f_A}t_A/\eta = (1+\varphi_A)T_{f_A}T_A.\tag{B7}$$

Similarly, $T'_B = (1+\varphi_B)T_{f_B}T_B$.

To find explicitly the expression of the excess noises, we assume that the coherent states are perfectly prepared and transmit through the quantum channels with transmission (T'_A, T'_B) and excess noise (ε'_A, ε'_B). In this case, Charlie's detection results x'_C, p'_D can be rewritten as

$$\begin{aligned}x'_C &= \frac{1}{\sqrt{2}}(\sqrt{t'_B}x_B - \sqrt{t'_A}x_A) + x'_N,\\ p'_D &= \frac{1}{\sqrt{2}}(\sqrt{t'_B}p_B + \sqrt{t'_A}p_A) + p'_N,\end{aligned}\tag{B8}$$

and

$$\begin{aligned}V(x'_C) &= \frac{\eta}{2}(u' + l' - 2\sqrt{1-T'_A}\sqrt{1-T'_B}g') + \eta\chi_{\text{hom}},\\ V(p'_D) &= \frac{\eta}{2}(u' + l' + 2\sqrt{1-T'_A}\sqrt{1-T'_B}g'_1) + \eta\chi_{\text{hom}},\end{aligned}\tag{B9}$$

where

$$u' = T'_B V_B + T'_A V_A, \quad l' = \varepsilon'_A T'_A + \varepsilon'_B T'_B + 2.\tag{B10}$$

Comparing Eq. (B3) with Eq. (B9), we have

$$\begin{aligned}T'_A V_A + \varepsilon'_A T'_A &= T_A(1+\varphi_A)V_A + \varepsilon_A T_A,\\ T'_B V_B + \varepsilon'_B T'_B &= T_B(1+\varphi_B)V_B + \varepsilon_B T_B,\\ \sqrt{1-T'_A}\sqrt{1-T'_B}g' &= \sqrt{1-T_A}\sqrt{1-T_B}g,\\ \sqrt{1-T'_A}\sqrt{1-T'_B}g'_1 &= \sqrt{1-T_A}\sqrt{1-T_B}g_1.\end{aligned}\tag{B11}$$

Simple algebra leads to

$$\begin{aligned}\varepsilon'_A &\approx \varepsilon_A/(1+\varphi_A)T_{f_A} + \frac{1}{4}V_A V_{f_A},\\ \varepsilon'_B &\approx \varepsilon_B/(1+\varphi_B)T_{f_B} + \frac{1}{4}V_B V_{f_B},\\ g' &= \frac{\sqrt{1-T_A}\sqrt{1-T_B}}{\sqrt{1-T'_A}\sqrt{1-T'_B}}g,\end{aligned}$$

$$g_1' = \frac{\sqrt{1-T_A}\sqrt{1-T_B}}{\sqrt{1-T_A'}\sqrt{1-T_B'}}g_1. \tag{B12}$$

If Alice and Bob use the revised data $\sqrt{(1+\varphi_{A/B})}x_{A/B}$ and $\sqrt{(1+\varphi_{A/B})}p_{A/B}$ for parameter estimation, we have

$$\begin{aligned}\sqrt{t_{Ax}'} &= -\sqrt{2}\frac{\langle\sqrt{(1+\varphi_A)}x_A x_C'\rangle}{\langle(\sqrt{(1+\varphi_A)}x_A)^2\rangle} = \frac{\langle x_A\sqrt{t_A}x_A'\rangle}{\sqrt{(1+\varphi_A)}\langle x_A^2\rangle}\\ &= \langle\sqrt{(1+\delta_{A_i})}\rangle\sqrt{t_A},\\ \sqrt{t_{Ap}'} &= \sqrt{2}\frac{\langle\sqrt{(1+\varphi_A)}p_A p_D'\rangle}{\langle(\sqrt{(1+\varphi_A)}p_A)^2\rangle} = \frac{\langle p_A\sqrt{t_A}p_A'\rangle}{\sqrt{(1+\varphi_A)}\langle p_A^2\rangle}\\ &= \langle\sqrt{(1+\delta_{A_i})}\rangle\sqrt{t_A}.\end{aligned} \tag{B13}$$

Hence $t_A' = \langle\sqrt{(1+\delta_{A_i})}\rangle^2 t_A = T_{f_A}t_A$ and $T_A' = t_A'/\eta = T_{f_A}T_A$. Similarly, $T_B' = T_{f_B}T_B$. Then,

$$\begin{aligned}\varepsilon_A' &\approx \varepsilon_A/T_{f_A} + \frac{1}{4}(1+\varphi_A)V_A V_{f_A},\\ \varepsilon_B' &\approx \varepsilon_B/T_{f_B} + \frac{1}{4}(1+\varphi_B)V_B V_{f_B},\\ g' &= \frac{\sqrt{1-T_A}\sqrt{1-T_B}}{\sqrt{1-T_A'}\sqrt{1-T_B'}}g,\\ g_1' &= \frac{\sqrt{1-T_A}\sqrt{1-T_B}}{\sqrt{1-T_A'}\sqrt{1-T_B'}}g_1.\end{aligned} \tag{B14}$$

If Alice and Bob use the revised data $\sqrt{(1+\varphi_{A/B})d_{A/B}}x_{A/B}$ and $\sqrt{(1+\varphi_{A/B})d_{A/B}}p_{A/B}$ for parameter estimation, we have

$$\begin{aligned}\sqrt{t_{Ax}'} &= -\sqrt{2}\frac{\langle\sqrt{(1+\varphi_A)d_A}x_A x_C'\rangle}{\langle(\sqrt{(1+\varphi_A)d_A}x_A)^2\rangle}\\ &= \frac{\sqrt{t_A}}{\sqrt{d_A}}\langle\sqrt{(1+\delta_{A_i})}\rangle,\\ \sqrt{t_{Ap}'} &= \sqrt{2}\frac{\langle\sqrt{(1+\varphi_A)d_A}p_A p_D'\rangle}{\langle(\sqrt{(1+\varphi_A)d_A}p_A)^2\rangle}\\ &= \frac{\sqrt{t_A}}{\sqrt{d_A}}\langle\sqrt{(1+\delta_{A_i})}\rangle.\end{aligned} \tag{B15}$$

Hence $T_A' = t_A'/\eta = T_{f_A}t_A/d_A\eta = T_{f_A}T_A/d_A$. Similarly, $T_B' = T_{f_B}T_B/d_B$. Then,

$$\begin{aligned}\varepsilon_A' &\approx \varepsilon_A d_A/T_{f_A} + \frac{1}{4}(1+\varphi_A)d_A V_A V_{f_A},\\ \varepsilon_B' &\approx \varepsilon_B d_B/T_{f_B} + \frac{1}{4}(1+\varphi_B)d_B V_B V_{f_B},\\ g' &= \frac{\sqrt{1-T_A}\sqrt{1-T_B}}{\sqrt{1-T_A'}\sqrt{1-T_B'}}g,\\ g_1' &= \frac{\sqrt{1-T_A}\sqrt{1-T_B}}{\sqrt{1-T_A'}\sqrt{1-T_B'}}g_1.\end{aligned} \tag{B16}$$

APPENDIX C: PARAMETER ESTIMATION IN SEC. IV

1. Parameter estimation in the asymptotical case

For intensity errors $k_A I_A$ and $k_B I_B$ of Alice and Bob, Charlie's measurement results are

$$\begin{aligned}x_C' &= \frac{1}{\sqrt{2}}(\sqrt{t_B}\sqrt{k_B}x_B - \sqrt{t_A}\sqrt{k_A}x_A) + x_N,\\ p_D' &= \frac{1}{\sqrt{2}}(\sqrt{t_B}\sqrt{k_B}p_B + \sqrt{t_A}\sqrt{k_A}p_A) + p_N.\end{aligned} \tag{C1}$$

Thus,

$$\begin{aligned}V(x_C') &= \frac{\eta}{2}(u'' + l - 2\sqrt{1-T_A}\sqrt{1-T_B}g) + \eta\chi_{\text{hom}},\\ V(p_D') &= \frac{\eta}{2}(u'' + l + 2\sqrt{1-T_A}\sqrt{1-T_B}g_1) + \eta\chi_{\text{hom}},\end{aligned} \tag{C2}$$

where

$$u'' = T_B\langle k_B\rangle V_B + T_A\langle k_A\rangle V_A. \tag{C3}$$

If Alice and Bob use the revised data $\sqrt{k_{A/B}^U}x_{A/B}$ and $\sqrt{k_{A/B}^U}p_{A/B}$ for parameter estimation, we have

$$\begin{aligned}\sqrt{t_{Ax}'} &= -\sqrt{2}\frac{\langle\sqrt{k_A^U}x_A x_C'\rangle}{\langle(\sqrt{k_A^U}x_A)^2\rangle} = \frac{\sqrt{t_A}}{\sqrt{k_A^U}}\langle\sqrt{k_A}\rangle,\\ \sqrt{t_{Ap}'} &= \sqrt{2}\frac{\langle\sqrt{k_A^U}p_A p_D'\rangle}{\langle(\sqrt{k_A^U}p_A)^2\rangle} = \frac{\sqrt{t_A}}{\sqrt{k_A^U}}\langle\sqrt{k_A}\rangle.\end{aligned} \tag{C4}$$

Hence $t_A' = \langle\sqrt{k_A}\rangle^2 t_A/k_A^U$. We define $m_{k_A} := \langle k_A\rangle$, $V_{k_A} := \text{var}(k_A)$, and $k_A' := k_A/m_{k_A}$. Then

$$\text{E}(k_A') = 1, \quad \text{var}(k_A') = V_{k_A}/m_{k_A}^2. \tag{C5}$$

Making a Taylor expansion around $k_A' - 1$, we can obtain

$$\langle\sqrt{k_A'}\rangle \approx 1 - V_{k_A}/8m_{k_A}^2. \tag{C6}$$

Using this, we have

$$\begin{aligned}\langle\sqrt{k_A}\rangle^2 &= \langle\sqrt{m_{k_A}k_A'}\rangle^2\\ &= m_{k_A}(1 - V_{k_A}/8m_{k_A}^2)^2 := T_{k_A}.\end{aligned} \tag{C7}$$

Hence $T_A' = t_A'/\eta = T_{k_A}T_A/k_A^U$. Likewise, $T_B' = T_{k_B}T_B/k_B^U$. Similar to the procedure used before, we finally obtain

$$\begin{aligned}\varepsilon_A' &\approx \varepsilon_A k_A^U/T_{k_A} + \frac{V_{k_A}}{4m_{k_A}^2}k_A^U V_A,\\ \varepsilon_B' &\approx \varepsilon_B k_B^U/T_{k_B} + \frac{V_{k_B}}{4m_{k_B}^2}k_B^U V_B,\\ g' &= \frac{\sqrt{1-T_A}\sqrt{1-T_B}}{\sqrt{1-T_A'}\sqrt{1-T_B'}}g,\\ g_1' &= \frac{\sqrt{1-T_A}\sqrt{1-T_B}}{\sqrt{1-T_A'}\sqrt{1-T_B'}}g_1.\end{aligned} \tag{C8}$$

2. Parameter estimation in the finite-size scenario

In practical applications of CV-MDI-QKD, in order to extract the secret key using the local data, Alice and Bob need to displace their raw data as follows [49]:

$$\begin{aligned} x_{dA} &= x'_A - g_{x'_A}(r), \quad p_{dA} = p'_A - g_{p'_A}(r), \\ x_{dB} &= x'_B - g_{x'_B}(r), \quad p_{dB} = p'_B - g_{p'_B}(r), \end{aligned} \tag{C9}$$

where x'_A, p'_A and x'_B, p'_B represent the raw data of Alice and Bob, respectively. $g_*(r)$, $* = x'_A, p'_A, x'_B, p'_B$, is an affine function of r and is defined as

$$g_*(r) = u_* x'_C + \nu_* p'_D, \tag{C10}$$

where the parameters u_* and ν_* are chosen to satisfy

$$\begin{aligned} \langle x_{dA}x'_C\rangle = \langle p_{dA}x'_C\rangle = \langle x_{dA}p'_D\rangle = \langle p_{dA}p'_D\rangle = 0, \\ \langle x_{dB}x'_C\rangle = \langle p_{dB}x'_C\rangle = \langle x_{dB}p'_D\rangle = \langle p_{dB}p'_D\rangle = 0. \end{aligned} \tag{C11}$$

This implies

$$\begin{aligned} u_* &= \frac{\langle *x'_C\rangle\langle p'^2_D\rangle - \langle *p'_D\rangle\langle x'_Cp'_D\rangle}{\langle x'^2_C\rangle\langle p'^2_D\rangle - \langle x'_Cp'_D\rangle^2}, \\ \nu_* &= \frac{\langle *p'_D\rangle\langle x'^2_C\rangle - \langle *x'_C\rangle\langle x'_Cp'_D\rangle}{\langle x'^2_C\rangle\langle p'^2_D\rangle - \langle x'_Cp'_D\rangle^2}. \end{aligned} \tag{C12}$$

Then the covariance matrix of $(x_{dA}, p_{dA}, x_{dB}, p_{dB})$ equals the conditional covariance matrix of (x'_A, p'_A, x'_B, p'_B) conditioned on (x'_C, p'_D), which is sufficient to assess the security of a CV-MDI-QKD (see Appendix A). The covariance matrix of $(x_{dA}, p_{dA}, x_{dB}, p_{dB})$ has the form

$$\gamma_{dAdB} = \begin{bmatrix} \langle x^2_{dA}\rangle & \langle x_{dA}p_{dA}\rangle & \langle x_{dA}x_{dB}\rangle & \langle x_{dA}p_{dB}\rangle \\ \langle x_{dA}p_{dA}\rangle & \langle p^2_{dA}\rangle & \langle p_{dA}x_{dB}\rangle & \langle p_{dA}p_{dB}\rangle \\ \langle x_{dA}x_{dB}\rangle & \langle p_{dA}x_{dB}\rangle & \langle x^2_{dB}\rangle & \langle x_{dB}p_{dB}\rangle \\ \langle x_{dA}p_{dB}\rangle & \langle p_{dA}p_{dB}\rangle & \langle x_{dB}p_{dB}\rangle & \langle p^2_{dB}\rangle \end{bmatrix}. \tag{C13}$$

By averaging the covariance matrix, we have it in a simple form,

$$\gamma_{dAdB} = \begin{bmatrix} \sum_a \mathbb{I} & \sum_c \sigma_z \\ \sum_c \sigma_z & \sum_b \mathbb{I} \end{bmatrix}, \tag{C14}$$

where

$$\begin{aligned} \sum_a &= \frac{\langle x^2_{dA}\rangle + \langle p^2_{dA}\rangle}{2}, \\ \sum_b &= \frac{\langle x^2_{dB}\rangle + \langle p^2_{dB}\rangle}{2}, \\ \sum_c &= \frac{\langle x_{dA}x_{dB}\rangle - \langle p_{dA}p_{dB}\rangle}{2}. \end{aligned} \tag{C15}$$

To obtain the covariance matrix γ_{dAdB}, the unknown parameters $\sum_a$, $\sum_b$, and $\sum_c$ need to be estimated. If Alice and Bob locally prepare $2n$ coherent states, then the real estimated values are defined as

$$\hat{\sum_a} = \sum_{j=1}^{n} \frac{x^2_{dA_j} + p^2_{dA_j}}{2n}, \quad \hat{\sum_b} = \sum_{j=1}^{n} \frac{x^2_{dB_j} + p^2_{dB_j}}{2n}. \tag{C16}$$

For $\hat{\sum}_c$, one can exploit the relationships between $\langle x_{dA}x_{dB}\rangle$, $\langle p_{dA}p_{dB}\rangle$ and $\langle x'^2_C\rangle$, $\langle p'^2_D\rangle$, $\langle x'_Cp'_D\rangle$, and obtain

$$\begin{aligned} \hat{\sum_c} &= \omega_1 \sum_{j=1}^{n} \frac{x'^2_{C_j}}{n} + \omega_2 \sum_{j=1}^{n} \frac{p'^2_{D_j}}{n} + \omega_3 \sum_{j=1}^{n} \frac{x'_{C_j}p'_{D_j}}{n}, \\ \sum_{j=1}^{n} \frac{x'_{C_j}p'_{D_j}}{n} &= \sum_{j=1}^{n} \frac{\left(x'_{C_j} + p'_{D_j}\right)^2}{4n} - \sum_{j=1}^{n} \frac{\left(x'_{C_j} - p'_{D_j}\right)^2}{4n}, \end{aligned} \tag{C17}$$

where

$$\begin{aligned} \omega_1 &= -\tfrac{1}{2}\left(u_{x'_A}u_{x'_B} + u_{p'_A}u_{p'_B}\right), \\ \omega_2 &= \tfrac{1}{2}\left(\nu_{x'_A}\nu_{x'_B} + \nu_{p'_A}\nu_{p'_B}\right), \\ \omega_3 &= \tfrac{1}{2}\left(u_{x'_A}\nu_{x'_B} + \nu_{x'_A}u_{x'_B} - u_{p'_A}\nu_{p'_B} - \nu_{p'_A}u_{p'_B}\right). \end{aligned} \tag{C18}$$

We can find that all the required parameters can be locally estimated by Alice and Bob, without the need for public communication. Hence, Alice and Bob can exploit all their local data for both parameter estimation and secret key extraction.

Our goal is to give a lower bound on the secret key rate. It is known that this bound can be obtained by computing $\sum_a^{\max}$ (the upper bound of $\hat{\sum}_a$), $\sum_b^{\max}$ (the upper bound of $\hat{\sum}_b$), and $\sum_c^{\min}$ (the lower bound of $\hat{\sum}_c$). By applying the cumulative distribution function of the chi-square distribution, the following bounds hold, except with probability s_{PE} [50]:

$$\begin{aligned} \sum_a^{\max} &= \sum_a/(1-\delta_{\mathrm{PE}}), \\ \sum_b^{\max} &= \sum_b/(1-\delta_{\mathrm{PE}}), \\ \sum_c^{\min} &= \sum_c/(1+\delta_{\mathrm{PE}}), \end{aligned} \tag{C19}$$

where $\delta_{\mathrm{PE}} = \sqrt{n^{-1}8\ln(8/s_{\mathrm{PE}})}$.

In our protocol, we have

$$\begin{aligned} \langle x'_Ax'_C\rangle &= -\sqrt{\frac{t_AT_{k_A}}{2k^U_A}}V'_A, \\ \langle p'_Ap'_D\rangle &= \sqrt{\frac{t_AT_{k_A}}{2k^U_A}}V'_A, \\ \langle x'_Bx'_C\rangle = \langle p'_Bp'_D\rangle &= \sqrt{\frac{t_BT_{k_B}}{2k^U_B}}V'_B, \end{aligned} \tag{C20}$$

where $V'_{A/B} = k^U_{A/B}V_M$, and this yields

$$\begin{aligned} u_{x'_A} &= -\sqrt{\frac{t_AT_{k_A}}{2k^U_A}}\frac{V'_A}{V(x'_C)}, \quad \nu_{p'_A} = \sqrt{\frac{t_AT_{k_A}}{2k^U_A}}\frac{V'_A}{V(p'_D)}, \\ u_{x'_B} &= \sqrt{\frac{t_BT_{k_B}}{2k^U_B}}\frac{V'_B}{V(x'_C)}, \quad \nu_{p'_B} = \sqrt{\frac{t_BT_{k_B}}{2k^U_B}}\frac{V'_B}{V(p'_D)}. \end{aligned} \tag{C21}$$

Then, we obtain

$$\begin{aligned}\sum_{a}^{\max} &= \frac{V_A'}{1-\delta_{\mathrm{PE}}}\left(1-\frac{t_A T_{k_A} V_A' V_{CD}}{4k_A^U}\right),\\ \sum_{b}^{\max} &= \frac{V_B'}{1-\delta_{\mathrm{PE}}}\left(1-\frac{t_B T_{k_B} V_B' V_{CD}}{4k_B^U}\right),\\ \sum_{c}^{\min} &= \sqrt{\frac{t_A t_B T_{k_A} T_{k_B}}{k_A^U k_B^U}}\frac{V_A' V_B' V_{CD}}{4(1+\delta_{\mathrm{PE}})},\end{aligned} \tag{C22}$$

where $V_{CD} = 1/V(x_C') + 1/V(p_D')$.

Further, considering the equivalence between the PM scheme and the EB scheme of the CV-MDI-QKD protocol, the covariance matrix $\gamma_{ab|r}$ of Appendix A can be rewritten as

$$\gamma_{ab|r} = \gamma_{ab}' = \begin{bmatrix} \Omega_a^{\max}\mathbb{I} & \Omega_c^{\min}\sigma_z \\ \Omega_c^{\min}\sigma_z & \Omega_b^{\max}\mathbb{I} \end{bmatrix} \tag{C23}$$

and

$$\begin{aligned}\Omega_a^{\max} &= \frac{1}{1-\delta_{\mathrm{PE}}}\left(V_a-\frac{t_A T_{k_A}\left(V_a^2-1\right)V_{CD}}{4k_A^U}\right),\\ \Omega_b^{\max} &= \frac{1}{1-\delta_{\mathrm{PE}}}\left(V_b-\frac{t_B T_{k_B}\left(V_b^2-1\right)V_{CD}}{4k_B^U}\right),\\ \Omega_c^{\min} &= \sqrt{\frac{t_A t_B T_{k_A} T_{k_B}}{k_A^U k_B^U}}\frac{\sqrt{\left(V_a^2-1\right)\left(V_b^2-1\right)}V_{CD}}{4(1+\delta_{\mathrm{PE}})},\end{aligned} \tag{C24}$$

where $V_{a/b} = k_{A/B}^U V_M + 1$.

Finally, one can calculate the final secret key rate using the boundary values derived above.

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

[2] V. Scarani, H. Bechmann-Pasquinucci, N. J. Cerf, M. Dušek, N. Lütkenhaus, and M. Peev, Rev. Mod. Phys. **81**, 1301 (2009).

[3] H.-K. Lo, M. Curty, and K. Tamaki, Nat. Photon. **8**, 595 (2014).

[4] E. Diamanti, H.-K. Lo, B. Qi, and Z. Yuan, npj Quantum Inf. **2**, 16025 (2016).

[5] S. L. Braunstein and P. van Loock, Rev. Mod. Phys. **77**, 513 (2005).

[6] X.-B. Wang, T. Hiroshima, A. Tomita, and M. Hayashi, Phys. Rep. **448**, 1 (2007).

[7] 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).

[8] E. Diamanti and A. Leverrier, Entropy **17**, 6072 (2015).

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

[10] F. Grosshans, G. Van Assche, J. Wenger, R. Brouri, N. J. Cerf, and P. Grangier, Nature (London) **421**, 238 (2003).

[11] C. Weedbrook, A. M. Lance, W. P. Bowen, T. Symul, T. C. Ralph, and P. K. Lam, Phys. Rev. Lett. **93**, 170504 (2004).

[12] S. Pirandola, S. Mancini, S. Lloyd, and S. L. Braunstein, Nat. Phys. **4**, 726 (2008).

[13] A. Leverrier and P. Grangier, Phys. Rev. Lett. **102**, 180504 (2009).

[14] L. S. Madsen, V. C. Usenko, M. Lassen, R. Filip, and U. L. Andersen, Nat. Commun. **3**, 1083 (2012).

[15] V. C. Usenko and F. Grosshans, Phys. Rev. A **92**, 062337 (2015).

[16] A. M. Lance, T. Symul, V. Sharma, C. Weedbrook, T. C. Ralph, and P. K. Lam, Phys. Rev. Lett. **95**, 180503 (2005).

[17] J. Lodewyck, M. Bloch, R. Garcia-Patron, S. Fossier, E. Karpov, E. Diamanti, T. Debuisschert, N. J. Cerf, R. Tualle-Brouri, S. W. McLaughlin *et al.*, Phys. Rev. A **76**, 042305 (2007).

[18] B. Qi, L.-L. Huang, L. Qian, and H.-K. Lo, Phys. Rev. A **76**, 052323 (2007).

[19] S. Fossier, E. Diamanti, T. Debuisschert, A. Villing, R. Tualle-Brouri, and P. Grangier, New J. Phys. **11**, 045023 (2009).

[20] Y. Shen, H.-X. Zou, L. Tian, P.-X. Chen, and J.-M. Yuan, Phys. Rev. A **82**, 022317 (2010).

[21] X.-Y. Wang, Z.-L. Bai, S.-F. Wang, Y.-M. Li, and K.-C. Peng, Chin. Phys. Lett. **30**, 010305 (2013).

[22] P. Jouguet, S. Kunz-Jacques, A. Leverrier, P. Grangier, and E. Diamanti, Nat. Photon. **7**, 378 (2013).

[23] R. Blandino, A. Leverrier, M. Barbieri, J. Etesse, P. Grangier, and R. Tualle-Brouri, Phys. Rev. A **86**, 012327 (2012).

[24] J. Fiurášek and N. J. Cerf, Phys. Rev. A **86**, 060302(R) (2012).

[25] H. M. Chrzanowski, N. Walk, S. M. Assad, J. Janousek, S. Hosseini, T. C. Ralph, T. Symul, and P. K. Lam, Nat. Photon. **8**, 333 (2014).

[26] D. Huang, P. Huang, H. S. Li, T. Wang, Y.-M. Zhou, and G.-H. Zeng, Opt. Lett. **41**, 3511 (2016).

[27] Y.-M. Li, X.-Y. Wang, Z.-L. Bai, W.-Y. Liu, S.-S. Yang, and K.-C. Peng, Chin. Phys. B **26**, 040303 (2017).

[28] X.-Y. Wang, W.-Y. Liu, P. Wang, and Y.-M. Li, Phys. Rev. A **95**, 062330 (2017).

[29] N. Wang, S.-N. Du, W.-Y. Liu, X.-Y. Wang, Y.-M. Li, and K.-C. Peng, Phys. Rev. Appl. **10**, 064028 (2018).

[30] F. Karinou, H. H. Brunner, C. F. Fung, L. C. Comandar, S. Bettelli, D. Hillerkuss, M. Kuschnerov, S. Mikroulis, D. Wang, C. Xie *et al.*, IEEE Photon. Technol. Lett. **30**, 650 (2018).

[31] Y.-C. Zhang, Z.-Y. Li, Z.-Y. Chen, C. Weedbrook, Y.-J. Zhao, X.-Y. Wang, Y.-D. Huang, C.-C. Xu, X.-X. Zhang, Z.-Y. Wang *et al.*, Quantum Sci. Technol. **4**, 035006 (2019).

[32] J. Dias and T. C. Ralph, Phys. Rev. A **95**, 022312 (2017).

[33] F. Furrer and W. J. Munro, Phys. Rev. A **98**, 032335 (2018).

[34] F. Furrer, T. Franz, M. Berta, A. Leverrier, V. B. Scholz, M. Tomamichel, and R. F. Werner, Phys. Rev. Lett. **109**, 100502 (2012).

[35] A. Leverrier, Phys. Rev. Lett. **114**, 070501 (2015).

[36] A. Leverrier, Phys. Rev. Lett. **118**, 200501 (2017).

[37] A. Acín, N. Brunner, N. Gisin, S. Massar, S. Pironio, and V. Scarani, Phys. Rev. Lett. **98**, 230501 (2007).

[38] J. Barrett, L. Hardy, and A. Kent, Phys. Rev. Lett. **95**, 010503 (2005).

[39] S. L. Braunstein and S. Pirandola, Phys. Rev. Lett. **108**, 130502 (2012).

[40] H.-K. Lo, M. Curty, and B. Qi, Phys. Rev. Lett. **108**, 130503 (2012).

[41] 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).

[42] Z.-Y. Li, Y.-C. Zhang, F.-H. Xu, X. Peng, and H. Guo, Phys. Rev. A **89**, 052301 (2014).

[43] X.-C. Ma, S.-H. Sun, M.-S. Jiang, M. Gui, and L.-M. Liang, Phys. Rev. A **89**, 042335 (2014).

[44] Y.-C. Zhang, Z.-Y. Li, S. Yu, W.-Y. Gu, X. Peng, and H. Guo, Phys. Rev. A **90**, 052325 (2014).

[45] P. Wang, X.-Y. Wang, and Y.-M. Li, Phys. Rev. A **99**, 042309 (2019).

[46] T. Gehring, V. Händchen, J. Duhme, F. Furrer, T. Franz, C. Pacher, R. F. Werner, and R. Schnabel, Nat. Commun. **6**, 8795 (2015).

[47] N. Walk, S. Hosseini, J. Geng, O. Thearle, J. Y. Haw, S. Armstrong, S. M. Assad, J. Janousek, T. C. Ralph, T. Symul *et al.*, Optica **3**, 634 (2016).

[48] X.-Y. Zhang, Y.-C. Zhang, Y.-J. Zhao, X.-Y. Wang, S. Yu, and H. Guo, Phys. Rev. A **96**, 042334 (2017).

[49] C. Lupo, C. Ottaviani, P. Papanastasiou, and S. Pirandola, Phys. Rev. Lett. **120**, 220505 (2018).

[50] C. Lupo, C. Ottaviani, P. Papanastasiou, and S. Pirandola, Phys. Rev. A **97**, 052327 (2018).

[51] R. Filip, Phys. Rev. A **77**, 022310 (2008).

[52] Y. Shen, J. Yang, and H. Guo, J. Phys. B **42**, 235506 (2009).

[53] V. C. Usenko and R. Filip, Phys. Rev. A **81**, 022318 (2010).

[54] Y.-J. Shen, X. Peng, J. Yang, and H. Guo, Phys. Rev. A **83**, 052304 (2011).

[55] P. Jouguet, S. Kunz-Jacques, E. Diamanti, and A. Leverrier, Phys. Rev. A **86**, 032309 (2012).

[56] W.-Y. Liu, X.-Y. Wang, N. Wang, S.-N. Du, and Y.-M. Li, Phys. Rev. A **96**, 042312 (2017).

[57] H.-X. Ma, P. Huang, T. Wang, S.-Y. Wang, W.-S. Bao, and G.-H. Zeng, Phys. Lett. A **383**, 126005 (2019).

[58] X.-B. Wang, C.-Z. Peng, J. Zhang, L. Yang, and J.-W. Pan, Phys. Rev. A **77**, 042311 (2008).

[59] X.-B. Wang, L. Yang, C.-Z. Peng, and J.-W. Pan, New J. Phys. **11**, 075006 (2009).

[60] J.-Z. Hu and X.-B. Wang, Phys. Rev. A **82**, 012331 (2010).

[61] H.-H. Chi, Z.-W. Yu, and X.-B. Wang, Phys. Rev. A **86**, 042307 (2012).

[62] C. Jiang, Z.-W. Yu, and X.-B. Wang, Phys. Rev. A **94**, 062323 (2016).

[63] C. Jiang, Z.-W. Yu, and X.-B. Wang, Phys. Rev. A **95**, 032325 (2017).

[64] L. Liu, F.-Z. Guo, and Q.-Y. Wen, Sci. Rep. **7**, 11370 (2017).

[65] C. Jiang, Z.-W. Yu, and X.-B. Wang, Phys. Rev. A **97**, 042331 (2018).

[66] C.-Y. Li, L. Qian, and H.-K. Lo, arXiv:1908.11423.

[67] Y. Zheng, P. Huang, A.-Q. Huang, J.-Y. Peng, and G.-H. Zeng, Phys. Rev. A **100**, 012313 (2019).

[68] S. Pirandola, New J. Phys. **15**, 113046 (2013).

[69] P. Jouguet, S. Kunz-Jacques, and E. Diamanti, Phys. Rev. A **87**, 062313 (2013).

[70] J. Lodewyck, T. Debuisschert, R. García-Patrón, R. Tualle-Brouri, N. J. Cerf, and P. Grangier, Phys. Rev. Lett. **98**, 030503 (2007).

[71] S. Pirandola, R. Laurenza, C. Ottaviani, and L. Banchi, Nat. Commun. **8**, 15043 (2017).