Continuous-variable measurement-device-independent quantum key distribution using modulated squeezed states and optical amplifiers

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

*State Key Laboratory of Quantum Optics and Quantum Optics Devices, Institute of Opto-Electronics,
Shanxi University, Taiyuan 030006, People's Republic of China
and Collaborative Innovation Center of Extreme Optics, Shanxi University, Taiyuan 030006, People's Republic of China*

(Received 30 September 2018; revised manuscript received 14 January 2019; published 3 April 2019)

The measurement-device-independent quantum key distribution (MDI-QKD) protocol is immune to imperfect measurement devices. However, its practicality and performance when implemented in continuous-variable (CV) mode are still not satisfactory. We propose a CV-MDI-QKD protocol based on modulated squeezed states, and analyze its security against two-mode Gaussian attack. The results show that the protocol can achieve a higher secret key rate and transmission distance than previous coherent-state and squeezed-state protocols. A method to compensate the imperfection of a practical homodyne detector using phase-sensitive optical amplifiers is also presented. By setting an appropriate optical amplification gain, realistic detectors with ordinary quantum efficiency can be employed. In addition, we discuss the impact of finite-size effects on the secret key rate of the protocol. The methods presented may aid in the practical application of the CV-MDI-QKD protocol.

DOI: 10.1103/PhysRevA.99.042309

I. INTRODUCTION

Quantum key distribution (QKD), one of the most practical areas in quantum information technology, allows two distant parties, Alice and Bob, to establish a common secret key over an insecure quantum channel with the aid of an authenticated classical channel [1–3]. Its security is guaranteed by the basic principles of quantum mechanics, and any eavesdropping behaviors are detectable due to the inevitable perturbation of the quantum states on which the key information is encoded. Continuous-variable (CV) QKD protocols, promising higher secret key rates by using multiphoton quantum states and homodyne (heterodyne) detection at metropolitan distances, have received extensive attention over the past decade [4–20].

Under some ideal assumptions, the CV-QKD protocols can be strictly proved to be unconditionally secure. However, in realistic implementations, the discrepancy between practical devices and their ideal models may lead to some potential security loopholes. The eavesdropper can exploit these loopholes to carry out attacks and acquire secret key information without being noticed. In order to fill the gap between theoretical assumptions and physical implementations, device-independent (DI) QKD [21] and measurement-device-independent (MDI) QKD [22,23] schemes were proposed. The former is still impractical for its low secret key rate and short distance. A more practical solution is the latter, which is immune to all side-channel attacks on measurement devices, the crucial security loophole of QKD implementations. This protocol, in which the measurement is fulfilled by an untrusted relay, has been experimentally demonstrated with discrete variables [24,25]. As a counterpart, based on the principle of CV entanglement swapping [26], the notion of MDI was subsequently extended to CV systems [27–30]. In CV-MDI-QKD protocols, both Alice and Bob send their quantum states to an untrusted third party, Charlie, who performs a CV Bell detection, broadcasts the outcome to the parties, and, in this way, a secret key between the parties is established.

It has been shown that the squeezed-states-based CV-QKD protocol can outperform the coherent-states-based protocol [12,30], but under the conditions of pure and strong squeezing. In order to release these stringent restrictions, the modulated squeezed-states one-way protocol was proposed and demonstrated [31,32]. By combining the advantages of both the squeezed and coherent states, it shows that even mixed squeezed states with moderate squeezing can provide better performance compared with the coherent-states protocol. In this paper, we extend the ideal of a one-way modulated squeezed-states protocol to the MDI framework, and propose a CV-MDI-QKD protocol based on the modulated squeezed states. We prove the security of the protocol against two-mode Gaussian attack, which has been proven to be the optimal attack for CV-MDI protocols [33]. In contrast, only single-mode Gaussian attack was analyzed in previous work [30]. Our results show that both the secret key rate and transmission distance of the proposed protocol are improved compared with the previous coherent- and squeezed-state protocols.

In order to compensate the imperfections of the realistic detectors, which are crucial to the system, two optical phase-sensitive amplifiers are added to the output ports of the quantum channel. It is shown that the inefficiency and dark noise of the practical homodyne detector are dramatically compensated under the condition of realistic optical amplification gain. We also analyze the impact of finite-size effects on the key rate of the proposed protocol.

The rest of this paper is organized as follows. In Sec. II, we present the details of the CV-MDI-QKD protocol with modulated squeezed states and derive the asymptotic secret

[*] yongmin@sxu.edu.cn

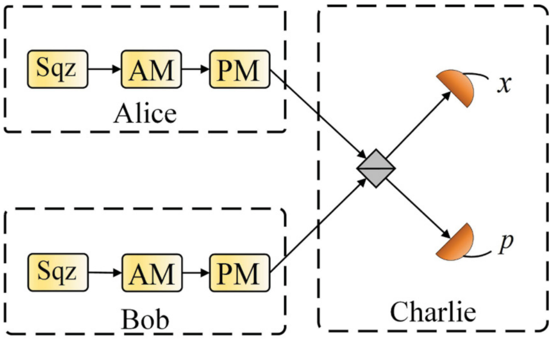

FIG. 1. Prepare-and-measure scheme (PM) of the CV-MDI-QKD protocol with modulated squeezed states. Alice (Bob) generates either an amplitude or a phase quadrature-squeezed vacuum state (Sqz), and modulates the quadrature of the state with a Gaussian modulation using two modulators, the amplitude modulator (AM) and the phase modulator (PM). Then Alice and Bob send their states via a quantum channel to an untrusted third party, Charlie, who performs homodyne detections on the amplitude and phase quadratures of the combined modes and broadcasts the measurement outcomes.

key rate of the protocol. A method for compensating the imperfection of the practical homodyne detectors is described in Sec. III. In Sec. IV, we analyze the impact of finite-size effects on the secret key rate of the protocol. Finally, we draw conclusions in Sec. V.

II. CV-MDI-QKD PROTOCOL WITH MODULATED SQUEEZED STATES

In this section, we first introduce the notion of the CV-MDI-QKD protocol with modulated squeezed states. We then establish an equivalent entanglement-based (EB) scheme of the protocol, and present the security analysis against a two-mode Gaussian attack.

The schematic of the modulated squeezed-states CV-MDI-QKD protocol is illustrated in Fig. 1. Alice and Bob generate x or p quadrature-squeezed vacuum states independently and randomly. To encode the key information, they use amplitude and phase modulators (AM and PM) to displace (independently) the quadratures x and p of their states with a Gaussian modulation. We assume a x quadrature-squeezed state is prepared; the modulation variances V_{AM} and V_{PM} should satisfy $s + V_{\text{AM}} = 1/s + \Delta V_0 + V_{\text{PM}}$ to prevent a potential eavesdropper from obtaining any information on Alice's choice of encoded quadrature, where s and $1/s + \Delta V_0$ denote the squeezing and antisqueezing variances of the states, respectively, and ΔV_0 is the excess noise of the antisqueezing. The resulting states are sent to an untrusted quantum relay, Charlie, via two unsecure lossy and noisy quantum channels, respectively. On Charlie's station, the two input modes are interfered at a 50:50 beam-splitter (BS). The output states are subsequently detected by using two realistic homodyne detectors: One detects the amplitude quadrature and the other detects the phase quadrature, and the final measurement results are revealed.

For convenience of security analysis, the equivalent entanglement-based (EB) scheme of the CV-MDI-QKD protocol with modulated squeezed states is established (Fig. 2). Alice starts with an Einstein-Podolsky-Rosen (EPR) state ρ_{A_0A} with variance V_A and applies a BS transformation with transmission efficiency $1/2$ onto modes A_0 and I, where I is one mode of the EPR state ρ_{I_0I} with variance W_I. Then, she performs homodyne detection on the output mode a, which projects mode A onto modulated squeezed states (see Appendix A for further details). 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 is characterized by the transmission T_A and excess noise ε_A. Likewise, Bob does the same. On Charlie's station, a CV Bell measurement is performed. To this end, the two received modes A' and B' are interfered at a 50:50 BS, and the output two modes C and D are transformed further into the modes C_2 and D_2 to model the realistic homodyne detector with efficiency η and electronic noise v_{el}. Then, both the x quadrature of mode C_2 and p quadrature of mode D_2 are measured by Charlie through perfect homodyne detection and the outcomes are combined into a complex variable $r := (x_{C_2} + ip_{D_2})/\sqrt{2}$, which is publicly announced to Alice and Bob over an authenticated classical channel. Here, knowledge of r enables each party (Alice or Bob) to infer the measurement results of the other party by data postprocessing [27]. As a result, the correlation between Alice and Bob is established and results in mutual information $I_{ab|r} > 0$. Finally, by implementing parameter estimation, information reconciliation, and privacy amplification procedures, the secret keys can be extracted.

Next, we derive the secret key rate of the protocol. Since the protocol is symmetric, for convenience, we assume that Alice is the encoder of information and Bob is the decoder. After communication of Charlie's outcome r, the asymptotical secret key rate against collective attacks is given by [27]

$$K^{\infty} = \beta I_{ab|r} - \chi_{aE|r}, \tag{1}$$

where β is the reconciliation efficiency, $I_{ab|r}$ the Shannon mutual information between Alice and Bob, and $\chi_{aE|r}$ the Holevo bound between Alice and Eve, representing the maximum information of Eve has stolen.

In this paper, we consider a joint two-mode Gaussian attack (see Appendix B for more details), which is the most general eavesdropping strategy for the CV-MDI protocol [33,34]. As shown in Fig. 2, Eve mixes her two ancillary modes E_1 and E_2 with the two incoming modes A and B, respectively, by using two BSs with transmittance T_A (T_B). The optimal correlated attack has proven to be the "negative EPR attack" [27].

Without loss of generality, we assume that the x quadrature is measured by the trusted parties, Alice and Bob. Then the Shannon mutual information between the trusted parties is given by

$$I_{ab|r} = \frac{1}{2}\log_2 \frac{V_{b|r}}{V_{b|r}^{x_a}}, \tag{2}$$

where $V_{b|r}$ and $V_{b|r}^{x_a}$ are the variances of the covariance matrices (CMs), $\gamma_{b|r}$ and $\gamma_{b|r}^{x_a}$ for the amplitude quadrature, respectively. These CMs are given in Appendix B.

The Holevo bound $\chi_{aE|r}$ is given by

$$\chi_{aE|r} = S(\rho_{E|r}) - S\left(\rho_{E|r}^{x_a}\right), \tag{3}$$

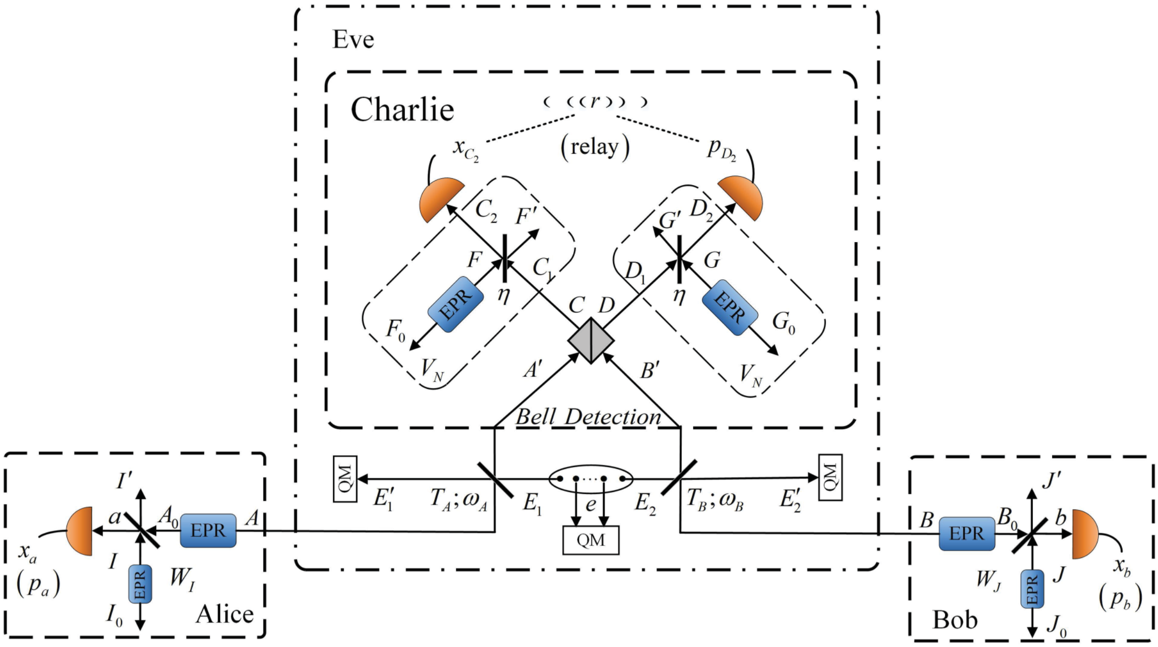

FIG. 2. Entanglement-based scheme of CV-MDI-QKD protocol with modulated squeezed states. Both Alice and Bob prepare a modulated entangled state, then each performs a homodyne detection on one mode of the entangled state and sends the other mode to an untrusted third party, Charlie, through quantum channels with length L_{AC} (L_{BC}), respectively. On Charlie's station, the realistic homodyne detector is modeled by a BS transformation with transmission efficiency η and the thermal state V_N that simulates the electronic noise v_{el} of the detector.

where $S(\rho)$ is the von Neumann entropy of the quantum state ρ. First, we use the fact that Eve is able to purify the system $A_0A'B_0B'$ and, after Charlie's Bell measurement with outcome r, the system A_0B_0E is pure, so that $S(\rho_{E|r}) = S(\rho_{A_0B_0|r})$. Second, after Alice's projective measurement resulting in x_a, the system $B_0I_0I'E$ is pure and we have $S(\rho^{x_a}_{E|r}) = S(\rho^{x_a}_{B_0I_0I'|r})$. Thus, Eq. (3) becomes

$$\chi_{aE|r} = S(\rho_{A_0B_0|r}) - S\left(\rho^{x_a}_{B_0I_0I'|r}\right). \tag{4}$$

The first part can be calculated from the symplectic eigenvalues $\lambda_{1,2}$ of the CM $\gamma_{A_0B_0|r}$, and the second part is determined from $\lambda_{3,4,5}$ of the CM $\gamma^{x_a}_{B_0I_0I'|r}$ (Appendix B). Then, we have

$$\chi_{aE|r} = \sum_{i=1}^{2} g\left(\frac{\lambda_i - 1}{2}\right) - \sum_{i=3}^{5} g\left(\frac{\lambda_i - 1}{2}\right), \tag{5}$$

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

We first consider the performance of the protocol in the symmetric case, which means $L_{\mathrm{AC}} = L_{\mathrm{BC}}$. The secret key rates K^{∞} as a function of the transmission distance $L = L_{\mathrm{AC}} + L_{\mathrm{BC}}$ (a channel loss of 0.2 dB per km is assumed hereafter) for different CV-MDI-QKD protocols are shown in Fig. 3. To simulate the performance of the 5.2-dB ($s = 3$) modulated squeezed-state protocol (red dotted-dashed line), a realistic antisqueezing excess noise of $\Delta V_0 = 3.2$ is used. In comparison with the coherent-state protocol with optimal modulation variance (black solid line), the squeezed-state protocol with pure 5.2-dB (blue dashed line) and 7-dB squeezing (blue short-dashed line, equivalent to 10-dB two-mode squeezing analyzed in Ref. [30]), both the secret key rate and transmission distance are improved with a total maximal transmission distance increase of 4.2, 3.2, and 1.5 km, respectively. Notably, the performance of the protocol almost reaches that of the squeezed-state protocol with a pure 10-dB squeezing

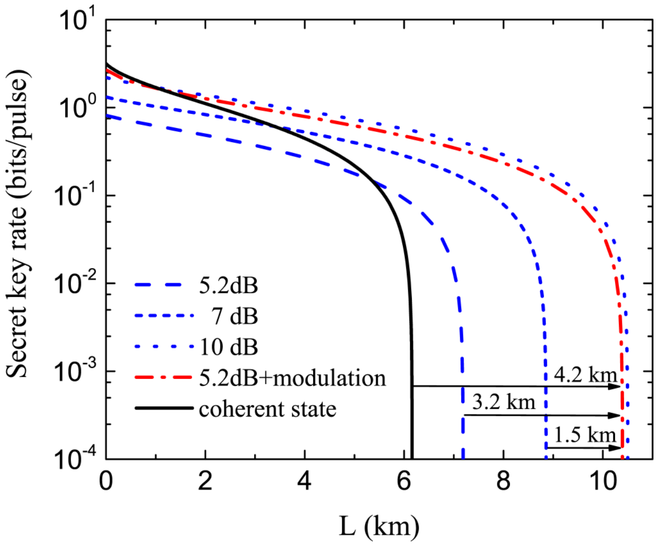

FIG. 3. Secret key rate vs transmission distance in symmetric case for different CV-MDI-QKD protocols: coherent state with optimal modulation variance (solid line), squeezed states with a pure 5.2-dB squeezing (dashed line), squeezed states with a pure 7-dB squeezing (short-dashed line), squeezed states with a pure 10-dB squeezing (dotted line), and modulated squeezed states with optimal modulation variance (dotted-dashed line). Here, we set the reconciliation efficiency β= 0.99 [35], excess noise $\varepsilon_A = \varepsilon_B = 0.002$ shot noise units (SNUs), and ideal detection $\eta = 1$, $v_{\mathrm{el}} = 0$.

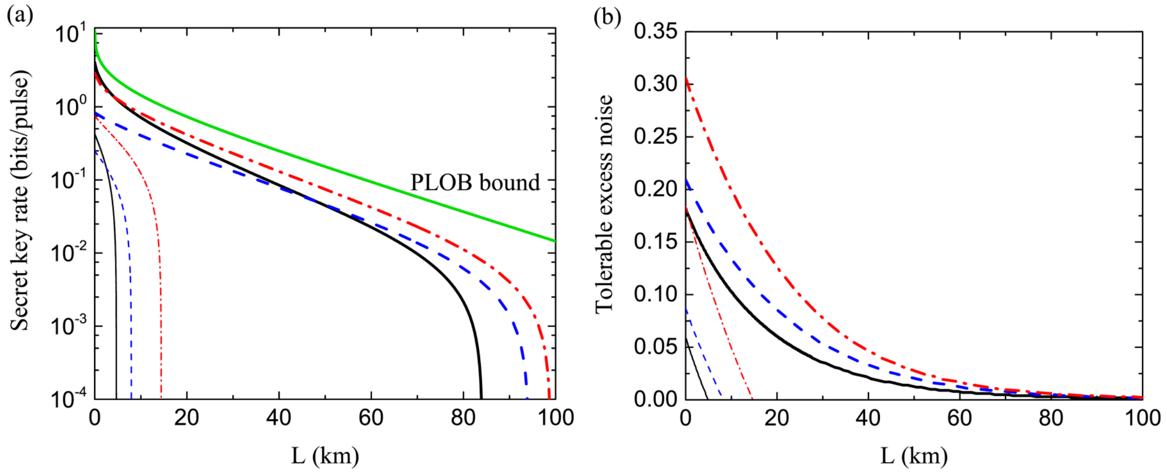

FIG. 4. Comparison between three different protocols in the most asymmetric case: coherent states (solid line), squeezed states with 5.2-dB squeezing (dashed line), and modulated squeezed states with 5.2-dB squeezing (dotted-dashed line). Bold lines and light lines represent two situations using ideal homodyne detectors with $\eta = 1,\ v_{\mathrm{el}} = 0$ and imperfect detectors with $\eta = 0.9,\ v_{\mathrm{el}} = 0.01$, respectively. (a) Secret key rate vs transmission distance, where green (upper) solid line is PLOB bound. Excess noise is $\varepsilon_A = \varepsilon_B = 0.002$. (b) Tolerable excess noise vs transmission distance. In (a,b), reconciliation efficiency is set to $\beta= 0.99$.

(blue dotted line). These results reveal the advantages of the modulated squeezed-state protocol.

For CV-MDI-QKD protocols, it has been proved that the performance of the asymmetric case ($L_{\mathrm{AC}} \neq L_{\mathrm{BC}}$) is superior to the symmetric case ($L_{\mathrm{AC}} = L_{\mathrm{BC}}$) [27]. When Alice is the encoder of information, the transmission distance L_{BC} increases significantly as L_{AC} decreases. If Charlie's location is close to Alice, the total transmission distance L will increase to its maximal value with the same parameters. Next, we investigate the performance of the protocol in the most asymmetric case ($L_{\mathrm{AC}} = 0$), in which the two-mode Gaussian attack degenerates into two independent Gaussian attacks [36]. In Fig. 4(a), the secret key rates K^{∞} as a function of transmission distance L for different CV-MDI-QKD protocols are shown. The Pirandola-Laurenza-Ottaviani-Banchi (PLOB) bound [37], representing the maximum secret key rate achievable in the repeaterless and lossy channel system, is also plotted for comparison. We find that the secret key rate of the modulated squeezed-state protocol is closest to the PLOB bound, which manifests the superior performance of our protocol. The total maximal transmission distances can reach up to approximately 100 and 15 km under ideal homodyne detection ($\eta = 1,\ v_{\mathrm{el}} = 0$) and imperfect detection ($\eta = 0.9,\ v_{\mathrm{el}} = 0.01$) conditions, respectively. Figure 4(b) shows the relationship between the maximum tolerable excess noise $\varepsilon = \varepsilon_A = \varepsilon_B$ and the transmission distance L. It is clear that our protocol improves resistance to the excess noise; therefore, a higher secret key rate and transmission distance can be achieved. In the above comparisons, we have optimized the modulation variances for both the coherent-state and modulated squeezed-state protocols.

Figure 4 reveals that the imperfection of the homodyne detector decreases the maximal transmission distance dramatically. In Fig. 5, we plot the achievable secret key rate vs detection efficiency η and transmission distance L. The protocol requires a minimum of 76% detection efficiency for a positive key rate under the conditions of $L= 0$, $\beta= 1$, $\varepsilon_A = \varepsilon_B = 0.002$, and $v_{\mathrm{el}} = 0$. For a transmission distance of 20 km, the protocol requires a higher detection efficiency (>90%), which is difficult to achieve in current fiber-based optical detection.

III. MODIFIED PROTOCOL WITH OPTICAL AMPLIFIERS

As mentioned above, the imperfection of a practical homodyne detector has a significant impact on the secret key rate and transmission distance of the CV-MDI system. To overcome this limitation, we use the phase-sensitive amplifiers (PSAs) in front of the homodyne detector, as shown in Fig. 6. The PSA [38,39] is a degenerate optical parametric amplifier that permits noiseless amplification of a chosen quadrature (x or p) and squeezing of the orthogonal quadrature. The behaviors of the PSA are described by the transformations

$$\begin{bmatrix} x_{C_1} \\ p_{C_1} \end{bmatrix} = \gamma_{\mathrm{PSA}_1} \begin{bmatrix} x_C \\ p_C \end{bmatrix} = \begin{bmatrix} \sqrt{k} & 0 \\ 0 & 1/\sqrt{k} \end{bmatrix} \begin{bmatrix} x_C \\ p_C \end{bmatrix}, \tag{6}$$

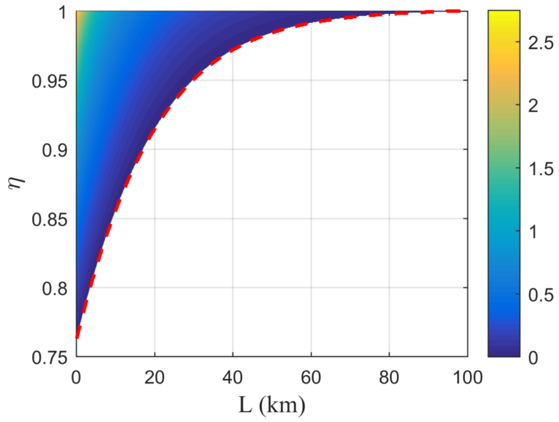

FIG. 5. Secret key rate vs detection efficiency and transmission distance under the most asymmetric case (5.2-dB squeezing). Simulation parameters are reconciliation efficiency $\beta= 1$, modulation variance $V_M = 10^4$, excess noise $\varepsilon_A = \varepsilon_B = 0.002$, and electronic noise $v_{\mathrm{el}} = 0$.

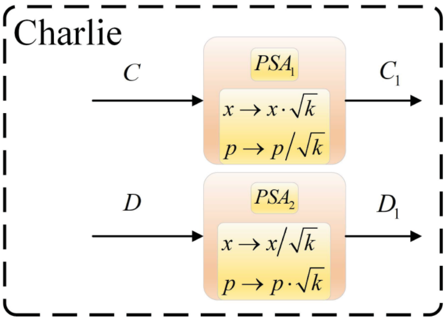

FIG. 6. Model of phase-sensitive amplifiers placed at front of homodyne detectors.

and

$$\begin{bmatrix} x_{D_1} \\ p_{D_1} \end{bmatrix} = \gamma_{\mathrm{PSA}_2} \begin{bmatrix} x_D \\ p_D \end{bmatrix} = \begin{bmatrix} 1/\sqrt{k} & 0 \\ 0 & \sqrt{k} \end{bmatrix} \begin{bmatrix} x_D \\ p_D \end{bmatrix}, \tag{7}$$

where $k \geqslant 1$ denotes the gain of the amplification, and the amplitude quadrature of the mode C and the phase quadrature of the mode D are amplified. Combined with the calculations presented in Sec. II, we find that the usage of the PSAs modifies θ_1 and θ_1' into

$$\begin{aligned} \theta_2 &= u - 2\sqrt{1-T_A}\sqrt{1-T_B}g + 2\chi_{\mathrm{hom}}/k, \\ \theta_2' &= u + 2\sqrt{1-T_A}\sqrt{1-T_B}g' + 2\chi_{\mathrm{hom}}/k, \end{aligned} \tag{8}$$

where

$$u = (T_A + T_B)V + (1-T_A)\omega_A + (1-T_B)\omega_B. \tag{9}$$

In this scenario, the asymptotical secret key rate against collective attacks becomes

$$K_{\mathrm{PSA}}^{\infty} = \beta I_{ab|r} - \chi_{aE|r}. \tag{10}$$

In Fig. 7, we plot the secret key rate K_{PSA}^{∞} as a function of the transmission distance L for different gain factors k under the condition of practical homodyne detectors ($\eta = 0.6,\ \upsilon_{\mathrm{el}} = 0.1$). It is clear that larger amplification gain causes a more pronounced improvement effect. As k increases, the secret key rate of the protocol becomes closer to the PLOB bound. When k tends to infinity, the secret key rate and total maximal transmission distance are the same as those of ideal homodyne detection.

In practice, the usage of PSA would introduce small amounts of excess noises, which could be modeled by an ideal PSA followed by a BS (with nearly perfect transmission efficiency) with a thermal state injecting. From the view of Alice and Bob, the added noises are indistinguishable from the electronic noises that introduced by the practical homodyne detector, both increasing the noises of the detection system. Therefore, we could attribute the added noises to virtual electronic noises of the homodyne detector. The effects of the imperfect PSAs on the secret key rate are shown in Fig. 7 (dashed lines). As predicted, the added noises reduce the secret key rate and transmission distance slightly. However, the usage of practical PSAs still effectively compensates the imperfection of practical homodyne detectors and boosts the performance of the CV-MDI-QKD.

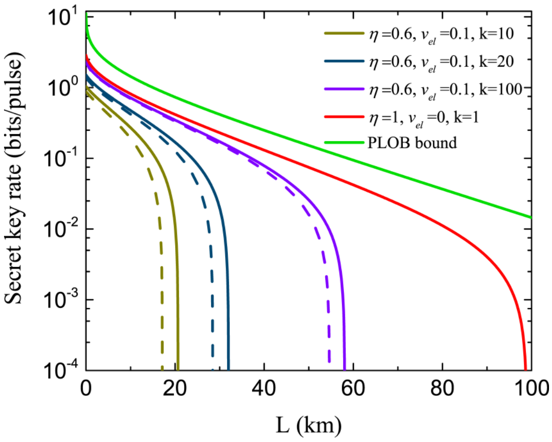

FIG. 7. Secret key rate vs transmission distance for different gains of amplification with the most asymmetric case (5.2-dB squeezing). From left to right, the lines correspond to gain factors of 10, 20, 100, ∞ (equivalent to an ideal homodyne detection case), and PLOB bound [the green (upper) line]. The solid and dashed lines represent perfect PSAs (no excess noise) and realistic PSAs (with excess noise of 0.2 SNU), respectively. The modulation variance has been optimized. Other parameters are set to $\beta = 0.99$, $\varepsilon_A = \varepsilon_B = 0.002$.

IV. SECURITY ANALYSIS IN FINITE-SIZE SCENARIO

In a practical implementation of any protocol, the total number of signals exchanged by Alice and Bob is always finite. Here, we analyze the impact of finite-size effects on the key rate of the proposed CV-MDI protocol. The secret key rate in the finite-size scenario can be written as [40]

$$K_{\mathrm{PSA}}^{\mathrm{finite}} = \frac{n}{N}[\beta I_{ab|r} - \chi_{aE|r} - \Delta(n)], \tag{11}$$

where N is the total number of signals exchanged between Alice and Bob, n is the number of signals used to extract the key, and the remaining $(N-n)$ signals are used for parameter estimation. $\Delta(n)$ is the parameter related to the security of the privacy amplification and is given by [40]

$$\Delta(n) \approx 7\sqrt{\frac{\log_2(2/\bar{\epsilon})}{n}}, \tag{12}$$

where $\bar{\epsilon}$ is the probability of error during privacy amplification.

Here, we exploit the recent results of Ref. [41]. The output variables of the relay (Charlie) are

$$\begin{aligned} x_{C_2} &= \frac{1}{\sqrt{2}}\left(\sqrt{t_B}x_B^M - \sqrt{t_A}x_A^M\right) + x_N, \\ p_{D_2} &= \frac{1}{\sqrt{2}}\left(\sqrt{t_B}p_B^M + \sqrt{t_A}p_A^M\right) + p_N, \end{aligned} \tag{13}$$

where $t_{A/B} = \eta k T_{A/B}, x_{A/B}^M$ $(p_{A/B}^M)$ are the displacement variables used for Gaussian modulation with zero mean and variance V_{AM} (V_{PM}). x_N and p_N are noise terms and their variances are given by

$$\begin{aligned} \sigma_{x_N}^2 &= \frac{\eta k}{2}(l_1 - 2\sqrt{1-T_A}\sqrt{1-T_B}g) + \eta\chi_{\mathrm{hom}}, \\ \sigma_{p_N}^2 &= \frac{\eta k}{2}(l_2 + 2\sqrt{1-T_A}\sqrt{1-T_B}g') + \eta\chi_{\mathrm{hom}}, \end{aligned} \tag{14}$$

where

$$\begin{aligned} l_1 &= (T_A + T_B)s + (1 - T_A)\omega_A + (1 - T_B)\omega_B, \\ l_2 &= (T_A + T_B)(1/s + \Delta V_0) + (1 - T_A)\omega_A + (1 - T_B)\omega_B. \end{aligned} \tag{15}$$

Using Eq. (14), Eq. (8) can be rewritten as

$$\begin{aligned} \theta_2 &= \frac{2}{\eta k}\sigma_{x_N}^2 + (T_A + T_B)V_{\mathrm{AM}}, \\ \theta_2' &= \frac{2}{\eta k}\sigma_{p_N}^2 + (T_A + T_B)V_{\mathrm{PM}}. \end{aligned} \tag{16}$$

From Eq. (16), we find that the secret key rate depends on the unknown parameters T_A, T_B, $\sigma_{x_N}^2$, and $\sigma_{p_N}^2$. By estimating these parameter values, we can obtain the confidence intervals (CIs) (see Appendix C for further details),

$$\begin{aligned} \mathrm{CI}(\hat{T}_A) &= [T_A - z_{\delta_{PE}/2}\sigma_A/\eta k,\ T_A + z_{\delta_{PE}/2}\sigma_A/\eta k], \\ \mathrm{CI}(\hat{T}_B) &= [T_B - z_{\delta_{PE}/2}\sigma_B \eta k,\ T_B + z_{\delta_{PE}/2}\sigma_B/\eta k], \\ \mathrm{CI}(\hat{\sigma}_{x_N}^2) &= [\sigma_{x_N}^2 - z_{\delta_{PE}/2}s_x,\ \sigma_{x_N}^2 + z_{\delta_{PE}/2}s_x], \\ \mathrm{CI}(\hat{\sigma}_{p_N}^2) &= [\sigma_{p_N}^2 - z_{\delta_{PE}/2}s_p,\ \sigma_{p_N}^2 + z_{\delta_{PE}/2}s_p], \end{aligned} \tag{17}$$

where $z_{\delta_{PE}/2} = \sqrt{2}\mathrm{erf}^{-1}(1 - \delta_{PE})$, $1 - \delta_{PE}$ is the confidence level, and $erf^{-1}(x)$ is the inverse function of the error function.

In the following, we calculate the secret key rate in the finite-size scenario for the symmetric and most asymmetric cases. In the symmetric case, the lower bound of the secret key rate is

$$K^{\mathrm{low}} = K_{\mathrm{PSA}}^{\mathrm{finite}}[T_A^{\mathrm{low}},\ T_B^{\mathrm{low}},\ (\sigma_{x_N}^2)^{up},\ (\sigma_{p_N}^2)^{up}]. \tag{18}$$

However, in the most asymmetric case the situation is different. The lowest transmittance T_B^{low} does not mean Eve's strongest attack. In contrast, there is an optimal $T_B = T_B^{\mathrm{max}}$ for Eve's attack. This means that the minimum value of the secret key rate is described by

$$\begin{aligned} K^{\mathrm{low}} &= \frac{n}{N}\{\beta I_{ab|r}[T_A^{\mathrm{low}},\ T_B^{\mathrm{low}},\ (\sigma_{x_N}^2)^{up},\ (\sigma_{p_N}^2)^{up}] \\ &\quad -\chi_{aE|r}[T_A^{\mathrm{low}},\ T_B^{up},\ (\sigma_{x_N}^2)^{up},\ (\sigma_{p_N}^2)^{up}] - \Delta(n)\}, \\ &\quad (T_B < T_B^{\mathrm{max}}), \\ K^{\mathrm{low}} &= K_{\mathrm{PSA}}^{\mathrm{finite}}[T_A^{\mathrm{low}},\ T_B^{\mathrm{low}},\ (\sigma_{x_N}^2)^{up},\ (\sigma_{p_N}^2)^{up}], \\ &\quad (T_B > T_B^{\mathrm{max}}). \end{aligned} \tag{19}$$

Figure 8 shows the secret key rate K^{low} as a function of transmission distance L in the symmetric and most asymmetric cases considering the finite-size effect. The modulation variance is optimal for each distance. In addition, we optimize the ratio n/N to obtain the largest secret key rate with N total samples. Results show that the influence of the finite-size effect cannot be neglected. The fewer signals exchanged, the more pronounced this effect. As the number of exchanged signals increases, more signals can be used for parameter estimation and key extraction, and the secret key rate approximates to the asymptotic scenario. When the number of exchanged signals is 10^{10}, the performance of the protocol almost reaches that of the asymptotic scenario, and total maximal transmission distances up to approximately 10 and 56 km can be achieved for practical homodyne detections in the symmetric and most asymmetric cases, respectively. Obviously, if a higher k value is used, the performance can be improved further.

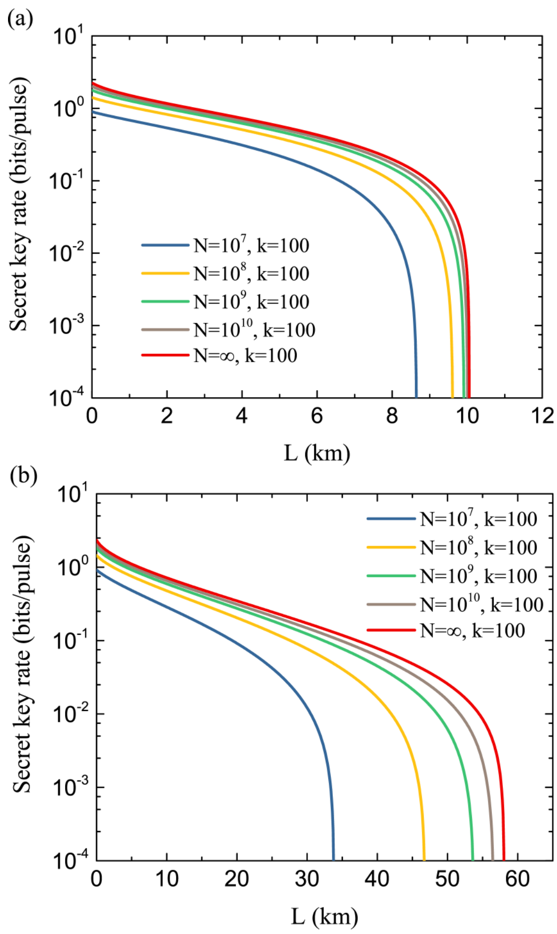

FIG. 8. Secret key rate vs transmission distance with finite-size effect in (a) symmetric and (b) the most asymmetric cases (5.2-dB squeezing). From left to right, the block length N is equal to 10^7, 10^8, 10^9, 10^{10}, and ∞. Modulation variance is optimal, and other parameters are set to $\delta_{PE} = \bar{\epsilon} = 10^{-10}$, $\varepsilon_A = \varepsilon_B = 0.002$, $\beta = 0.99$, $\eta = 0.6$, and $v_{\mathrm{el}} = 0.1$.

V. CONCLUSIONS

In summary, we have proposed a CV-MDI-QKD scheme using modulated squeezed states and investigated its security under a two-mode Gaussian attack. The results show that the proposed protocol outperforms the coherent- and squeezed-state protocols in terms of the secret key rate and maximal transmission distance. It was found that the imperfection of a practical homodyne detector has a significant impact on the performance of the protocol. To overcome this limitation, we applied the PSA technology to the proposed protocol. Furthermore, we analyzed the security of the protocol in the finite-size scenario. Further theoretical studies including the composable security analysis [42–46] and Gaussian postselection [47] are expected. For the experimental realization, even though the experimental preparation of squeezed states is more complex than that of coherent states, the technology of generating squeezed states has become relatively mature. For instance, the technology of generating a mixed 5.2-dB squeezed state is now readily available. In addition, 15-dB squeezing has been observed in experiment [48]. On the other hand, optical phase-sensitive amplifiers have been demonstrated in various experiments. Therefore, the proposed protocol is feasible in principle.

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 (201803D121065), and Shanxi 1331KSC.

APPENDIX A: EQUIVALENT EB SCHEME OF MODULATED SQUEEZED-STATES PROTOCOL

In this Appendix, we establish an equivalent EB schem-e of the modulated squeezed-states protocol. In Fig. 9, Alice (Bob) starts with an EPR state ρ_{A_0A} with variance V_A and applies a BS transformation with transmission efficiency $1/2$ onto modes A_0 and I. The output mode a is detected by a homodyne detector, and the mode A of the EPR state is sent to Charlie via a quantum channel.

To establish the equivalence of the PM and the EB schemes, the following conditions should be satisfied:

$$V_A = s{+}V_{\mathrm{AM}},\quad V_{A|a} = s. \tag{A1}$$

To meet the second condition, two additional modes, I_0 and I, are introduced. The covariance matrix γ_{I_0I} describing the EPR state with variance W_I is given by

$$\gamma_{I_0I} = \begin{bmatrix} W_I\mathrm{I} & \sqrt{W_I^2-1}\sigma_z \\ \sqrt{W_I^2-1}\sigma_z & W_I\mathrm{I} \end{bmatrix}. \tag{A2}$$

Using the relation $a = (A_0 + I)/\sqrt{2}$, we have

$$\begin{aligned} C_{Aa} &= \langle x_A x_a\rangle = \frac{1}{\sqrt{2}}\langle x_A x_{A_0}\rangle = \frac{1}{\sqrt{2}}\sqrt{V_A^2-1}, \\ V_a &= \langle x_a^2\rangle = \frac{1}{2}\left(\langle x_{A_0}^2\rangle + \langle x_I^2\rangle\right) = \frac{1}{2}(V_A + W_I). \end{aligned} \tag{A3}$$

The conditional variance is therefore given by

$$V_{A|a} = V_A - \frac{C_{Aa}^2}{V_a} = \frac{V_A W_I + 1}{V_A + W_I}. \tag{A4}$$

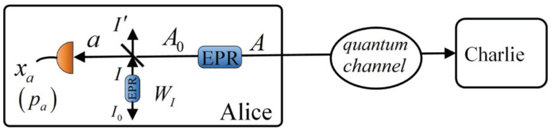

FIG. 9. Equivalent EB scheme of the modulated squeezed-states protocol. The preparation of the modulated squeezed states is replaced by an EPR source combined with a homodyne detection.

Then, applying Eq. (A1), we finally obtain

$$W_I = \frac{V_A s - 1}{V_A - s}. \tag{A5}$$

APPENDIX B: CALCULATION OF THE SECRET KEY RATE

We consider a joint two-mode Gaussian attack. Eve mixes her two ancillary modes together with the incoming modes. Here, the two ancillary modes are extracted from a reservoir of entangled ancillas, $\{E_1, E_2, e\}$, and have the covariance matrix of the form [33]

$$\gamma_{E_1E_2} = \begin{bmatrix} \omega_A\mathrm{I} & G \\ G & \omega_B\mathrm{I} \end{bmatrix},\quad G = \begin{bmatrix} g & 0 \\ 0 & g' \end{bmatrix}, \tag{B1}$$

where ω_A and ω_B are the variances of the thermal noise introduced by E_1 and E_2, respectively. g and g' represent the quantum correlations between the two modes and must satisfy the physical constraints imposed by the Heisenberg uncertainty principle. In addition, the optimal correlated attack has proven to be the "negative EPR attack," in which Eve injects EPR entanglement into the channels to destroy the Bell detection [27]:

$$\begin{aligned} &g' = -g = \phi, \\ &\phi = \min\{\sqrt{(\omega_A-1)(\omega_B+1)}, \sqrt{(\omega_A+1)(\omega_B-1)}\}. \end{aligned} \tag{B2}$$

We assume that $V_A = V_B = V$ and $W_I = W_J$. Then, the resulting covariance matrix $\gamma_{ab|r}$ is

$$\begin{aligned} \gamma_{ab|r} = &\frac{1}{2}\begin{bmatrix} (V+W_I)I & 0 \\ 0 & (V+W_I)\mathrm{I} \end{bmatrix} \\ &- \frac{(V^2-1)}{2}\begin{bmatrix} \frac{T_A}{\theta_1} & 0 & -\frac{\sqrt{T_AT_B}}{\theta_1} & 0 \\ 0 & \frac{T_A}{\theta_1'} & 0 & \frac{\sqrt{T_AT_B}}{\theta_1'} \\ -\frac{\sqrt{T_AT_B}}{\theta_1} & 0 & \frac{T_B}{\theta_1} & 0 \\ 0 & \frac{\sqrt{T_AT_B}}{\theta_1'} & 0 & \frac{T_B}{\theta_1'} \end{bmatrix}, \end{aligned} \tag{B3}$$

where

$$\begin{aligned} \theta_1 &= (T_A+T_B)V + (1-T_A)\omega_A + (1-T_B)\omega_B \\ &\quad - 2\sqrt{1-T_A}\sqrt{1-T_B}g + 2\chi_{\mathrm{hom}}, \\ \theta_1' &= (T_A+T_B)V + (1-T_A)\omega_A + (1-T_B)\omega_B \\ &\quad + 2\sqrt{1-T_A}\sqrt{1-T_B}g' + 2\chi_{\mathrm{hom}}. \end{aligned} \tag{B4}$$

Here, $\chi_{\mathrm{hom}} = (1-\eta)/\eta + v_{\mathrm{el}}/\eta$ is the total noise introduced by the realistic homodyne detector relative to the signal's input (C_1 or D_1).

The covariance matrix of the state, conditioned on Alice's measurement result (x_a), can be written as

$$\gamma_{b|r}^{x_a} = \gamma_{b|r} - \sigma_{ab|r}(X\gamma_{a|r}X)^{\mathrm{MP}}\sigma_{ab|r}^T, \tag{B5}$$

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, and $X = \mathrm{diag}(1, 0)$. After some simple algebra, we obtain the explicit form of $\gamma_{b|r}^{x_a}$,

$$\gamma_{b|r}^{x_a} = \begin{bmatrix} \xi_1 & 0 \\ 0 & \varphi_1 \end{bmatrix}, \tag{B6}$$

where

$$\begin{aligned} \xi_1 &= (V + W_I)[\xi + (V^2 - 1)T_B]/2\xi, \\ \xi &= -(V + W_I)\theta_1 + (V^2 - 1)T_A, \\ \varphi_1 &= [V + W_I - (V^2 - 1)T_B/\theta_1']/2. \end{aligned}$$

The Shannon mutual information between the trusted parties can be calculated by the first diagonal elements of the matrices $\gamma_{b|r}$ and $\gamma_{b|r}^{x_a}$:

$$I_{ab|r} = \frac{1}{2}\log_2\frac{V_{b|r}}{V_{b|r}^{x_a}} = \frac{1}{2}\log_2\frac{\varphi_2}{\xi_1}, \tag{B7}$$

where $\varphi_2 = [V + W_I - (V^2 - 1)T_B/\theta_1]/2$.

The Holevo bound $\chi_{aE|r}$ is given by

$$\chi_{aE|r} = S(\rho_{A_0B_0|r}) - S(\rho_{B_0I_0I'|r}^{x_a}), \tag{B8}$$

where the entropy $S(\rho_{A_0B_0|r})$ can be calculated from the symplectic eigenvalues $\lambda_{1,2}$ of the covariance matrix $\gamma_{A_0B_0|r}$,

$$\begin{aligned} \gamma_{A_0B_0|r} = &\begin{bmatrix} V\mathrm{I} & 0 \\ 0 & V\mathrm{I} \end{bmatrix} \\ &- (V^2 - 1)\begin{bmatrix} \frac{T_A}{\theta_1} & 0 & -\frac{\sqrt{T_AT_B}}{\theta_1} & 0 \\ 0 & \frac{T_A}{\theta_1'} & 0 & \frac{\sqrt{T_AT_B}}{\theta_1'} \\ -\frac{\sqrt{T_AT_B}}{\theta_1} & 0 & \frac{T_B}{\theta_1} & 0 \\ 0 & \frac{\sqrt{T_AT_B}}{\theta_1'} & 0 & \frac{T_B}{\theta_1'} \end{bmatrix}. \end{aligned} \tag{B9}$$

The symplectic eigenvalues are given by

$$\lambda_{1,2}^2 = \tfrac{1}{2}(A \pm \sqrt{A^2 - 4B}), \tag{B10}$$

where $A = 2V^2 + [\xi_2^2 - V(\theta_1 + \theta_1')\xi_3]/\theta_1\theta_1'$, $B = V^2(\xi_3 - V\theta_1)(\xi_3 - V\theta_1')/\theta_1\theta_1'$, $\xi_2 = (V^2 - 1)T_A - (V^2 - 1)T_B$, and $\xi_3 = (V^2 - 1)T_A + (V^2 - 1)T_B$.

Similarly, the entropy $S(\rho_{B_0I_0I'|r}^{x_a})$ is determined from the symplectic eigenvalues $\lambda_{3,4,5}$ of the covariance matrix $\gamma_{B_0I_0I'|r}^{x_a}$,

$$\gamma_{B_0I_0I'|r}^{x_a} = \begin{bmatrix} V - \frac{\phi_1}{\tau} & 0 & -\frac{\sqrt{2}W_I\phi_2}{\tau} & 0 & -\frac{\phi_2\phi_5}{\tau} & 0 \\ 0 & V - \frac{(V^2-1)T_B}{\theta_1'} & 0 & \frac{\phi_2}{\sqrt{2}\theta_1'} & 0 & 0 \\ -\frac{\sqrt{2}W_I\phi_2}{\tau} & 0 & \frac{2W_I\phi_3}{\tau} & 0 & \frac{\sqrt{2}\phi_3\phi_5}{\tau} & 0 \\ 0 & \frac{\phi_2}{\sqrt{2}\theta_1'} & 0 & \frac{\phi_4}{2} & 0 & -\frac{\phi_5}{\sqrt{2}} \\ -\frac{\phi_2\phi_5}{\tau} & 0 & \frac{\sqrt{2}\phi_3\phi_5}{\tau} & 0 & W_I - \frac{\phi_5^2\theta_1}{\tau} & 0 \\ 0 & 0 & 0 & -\frac{\phi_5}{\sqrt{2}} & 0 & W_I \end{bmatrix}, \tag{B11}$$

where

$$\begin{aligned} \phi_1 &= (V + W_I)(V^2 - 1)T_B, \\ \phi_2 &= (V^2 - 1)\sqrt{T_AT_B},\ \phi_3 = V\theta_1 - (V^2 - 1)T_A, \\ \phi_4 &= V + W_I - (V^2 - 1)T_A/\theta_1', \quad \phi_5 = \sqrt{W_I^2 - 1}, \\ \tau &= (V + W_I)\theta_1 - (V^2 - 1)T_A. \end{aligned} \tag{B12}$$

The symplectic eigenvalues $\lambda_{3,4,5}$ can be calculated by finding the (standard) eigenvalues of the matrix $i\Omega\gamma_{B_0I_0I'|r}^{x_a}$, where

$$\Omega = \bigoplus_{k=1}^{n=3}\begin{bmatrix} 0 & 1 \\ -1 & 0 \end{bmatrix}. \tag{B13}$$

At this stage, the Holevo quantities $\chi_{aE|r}$ are given by

$$\begin{aligned} \chi_{aE|r} &= S(\rho_{A_0B_0|r}) - S(\rho_{B_0I_0I'|r}^{x_a}) \\ &= \sum_{i=1}^{2} g\left(\frac{\lambda_i - 1}{2}\right) - \sum_{i=3}^{5} g\left(\frac{\lambda_i - 1}{2}\right). \end{aligned} \tag{B14}$$

APPENDIX C: PARAMETER ESTIMATION IN FINITE-SIZE SCENARIO

We assume that $m = N - n$ number of signals are used for parameter estimation. Then, we can write the estimator of the transmissivity t_A as follows:

$$\hat{t}_{Ax} = 2\left[\frac{\sum_{i=1}^{m} x_{A,i}^{M} x_{C_2,i}}{\sum_{i=1}^{m}\left(x_{A,i}^{M}\right)^2}\right]^2, \quad \hat{t}_{Ap} = 2\left[\frac{\sum_{i=1}^{m} p_{A,i}^{M} p_{D_2,i}}{\sum_{i=1}^{m}\left(p_{A,i}^{M}\right)^2}\right]^2. \tag{C1}$$

We assume that $\hat{t}_{Ax}$ and $\hat{t}_{Ap}$ have the following normal distribution,

$$\hat{t}_{Ax} \sim \mathcal{N}[\mathrm{E}(\hat{t}_{Ax}), \quad \mathrm{Var}(\hat{t}_{Ax})], \quad \hat{t}_{Ap} \sim \mathcal{N}[\mathrm{E}(\hat{t}_{Ap}), \quad \mathrm{Var}(\hat{t}_{Ap})], \tag{C2}$$

where the mean and variance of $\hat{t}_{Ax}$ and $\hat{t}_{Ap}$ are given, respectively, by [41]

$$\begin{aligned} &\mathrm{E}(\hat{t}_{Ax}) = t_A, \quad \mathrm{E}(\hat{t}_{Ap}) = t_A, \\ &\mathrm{Var}(\hat{t}_{Ax}) = \frac{8t_A}{m}(t_A + t_B/2)\left[1 + \frac{\sigma_{x_N}^2}{(t_A + t_B/2)V_{\mathrm{AM}}}\right], \\ &\mathrm{Var}(\hat{t}_{Ap}) = \frac{8t_A}{m}(t_A + t_B/2)\left[1 + \frac{\sigma_{p_N}^2}{(t_A + t_B/2)V_{\mathrm{PM}}}\right]. \end{aligned} \tag{C3}$$

The optimal estimator of the variance is then given by [49]

$$\mathrm{Var}(\hat{t}_A) = \frac{\mathrm{Var}(\hat{t}_{Ax})\mathrm{Var}(\hat{t}_{Ap})}{\mathrm{Var}(\hat{t}_{Ax}) + \mathrm{Var}(\hat{t}_{Ap})} := \sigma_A^2. \tag{C4}$$

Similarly, we have $\mathrm{Var}(\hat{t}_B) = \sigma_B^2$. In addition, the unbiased estimator of $\sigma_{x_N}^2$ is

$$\hat{\sigma}_{x_N}^2 = \frac{1}{m-2}\sum_{i=1}^{m}\left[x_{C_2,i} - \frac{1}{\sqrt{2}}\left(\sqrt{\hat{t}_B}x_{B,i}^M - \sqrt{\hat{t}_A}x_{A,i}^M\right)\right]^2, \quad \text{(C5)}$$

which has the following distribution:

$$\frac{(m-2)\hat{\sigma}_{x_N}^2}{\sigma_{x_N}^2} \sim \chi^2(m-2). \quad \text{(C6)}$$

Then, the mean and variance of $\hat{\sigma}_{x_N}^2$ are

$$\mathrm{E}\left(\hat{\sigma}_{x_N}^2\right) = \sigma_{x_N}^2, \ \mathrm{Var}\left(\hat{\sigma}_{x_N}^2\right) = \frac{2}{m-2}\left(\sigma_{x_N}^2\right)^2 := s_x^2. \quad \text{(C7)}$$

Similarly, $\mathrm{Var}(\hat{\sigma}_{p_N}^2) = s_p^2$. Furthermore, we have $\hat{T}_{A/B} = \hat{t}_{A/B}/\eta k$. Finally, we obtain the confidence intervals (CIs) with confidence level $1 - \delta_{PE}$,

$$\begin{aligned}
\mathrm{CI}(\hat{T}_A) &= [T_A - z_{\delta_{PE}/2}\sigma_A/\eta k, \ T_A + z_{\delta_{PE}/2}\sigma_A/\eta k],\\
\mathrm{CI}(\hat{T}_B) &= [T_B - z_{\delta_{PE}/2}\sigma_B/\eta k, \ T_B + z_{\delta_{PE}/2}\sigma_B/\eta k],\\
\mathrm{CI}\left(\hat{\sigma}_{x_N}^2\right) &= \left[\sigma_{x_N}^2 - z_{\delta_{PE}/2}s_x, \ \sigma_{x_N}^2 + z_{\delta_{PE}/2}s_x\right],\\
\mathrm{CI}\left(\hat{\sigma}_{p_N}^2\right) &= \left[\sigma_{p_N}^2 - z_{\delta_{PE}/2}s_p, \ \sigma_{p_N}^2 + z_{\delta_{PE}/2}s_p\right]. \quad \text{(C8)}
\end{aligned}$$

[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. Photonics **8**, 595 (2014).

[4] C. Silberhorn, T. C. Ralph, N. Lütkenhaus, and G. Leuchs, Phys. Rev. Lett. **89**, 167901 (2002).

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

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

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

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

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

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

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

[12] R. García-Patrón and N. J. Cerf, Phys. Rev. Lett. **102**, 130501 (2009).

[13] 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).

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

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

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

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

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

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

[20] 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 Photonics Technol. Lett. **30**, 650 (2018).

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

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

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

[24] Z. Tang, Z. Liao, F. Xu, B. Qi, L. Qian, and H.-K. Lo, Phys. Rev. Lett. **112**, 190503 (2014).

[25] H.-L. Yin, T.-Y. Chen, Z.-W. Yu, H. Liu, L.-X. You, Y.-H. Zhou, S.-J. Chen, Y. Mao, M.-Q. Huang, W.-J. Zhang *et al.*, Phys. Rev. Lett. **117**, 190501 (2016).

[26] S. L. Braunstein and H. J. Kimble, Phys. Rev. Lett. **80**, 869 (1998).

[27] S. Pirandola, C. Ottaviani, G. Spedalieri, C. Weedbrook, S. L. Braunstein, S. Lloyd, T. Gehring, C. S. Jacobsen, and U. L. Andersen, Nat. Photonics **9**, 397 (2015).

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

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

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

[31] V. C. Usenko and R. Filip, New J. Phys. **13**, 113007 (2011).

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

[33] C. Ottaviani, G. Spedalieri, S. L. Braunstein, and S. Pirandola, Phys. Rev. A **91**, 022320 (2015).

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

[35] M. Milicevic, C. Feng, L. M. Zhang, and P. G. Gulak, npj Quantum Inf. **4**, 21 (2018).

[36] Y.-J. Zhao, Y.-C. Zhang, B.-J. Xu, S. Yu, and H. Guo, Phys. Rev. A **97**, 042328 (2018).

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

[38] S. Fossier, E. Diamanti, T. Debuisschert, R. Tualle-Brouri, and P. Grangier, J. Phys. B: At., Mol. Opt. Phys. **42**, 114014 (2009).

[39] H. Zhang, J. Fang, and G.-Q. He, Phys. Rev. A **86**, 022338 (2012).

[40] A. Leverrier, F. Grosshans, and P. Grangier, Phys. Rev. A **81**, 062343 (2010).

[41] P. Papanastasiou, C. Ottaviani, and S. Pirandola, Phys. Rev. A **96**, 042332 (2017).

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

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

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

[45] Z.-Y. Chen, Y.-C. Zhang, G. Wang, Z.-Y. Li, and H. Guo, Phys. Rev. A **98**, 012314 (2018).

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

[47] N. Walk, T. C. Ralph, T. Symul, and P. K. Lam, Phys. Rev. A **87**, 020303(R) (2013).

[48] H. Vahlbruch, M. Mehmet, K. Danzmann, and R. Schnabel, Phys. Rev. Lett. **117**, 110801 (2016).

[49] L. Ruppert, V. C. Usenko, and R. Filip, Phys. Rev. A **90**, 062310 (2014).