Finite-size analysis of continuous-variable measurement-device-independent quantum key distribution

Xueying Zhang,[1] Yichen Zhang,[1,*] Yijia Zhao,[1] Xiangyu Wang,[1] Song Yu,[1,†] and Hong Guo[1,2]

[1]*State Key Laboratory of Information Photonics and Optical Communications, Beijing University of Posts and Telecommunications, Beijing 100876, China*

[2]*State Key Laboratory of Advanced Optical Communication Systems and Networks, School of Electronics Engineering and Computer Science, Center for Quantum Information Technology, Center for Computational Science and Engineering, Peking University, Beijing 100871, China*

We study the impact of the finite-size effect on the continuous-variable measurement-device-independent quantum key distribution (CV-MDI QKD) protocol, mainly considering the finite-size effect on the parameter estimation procedure. The central-limit theorem and maximum likelihood estimation theorem are used to estimate the parameters. We also analyze the relationship between the number of exchanged signals and the optimal modulation variance in the protocol. It is proved that when Charlie's position is close to Bob, the CV-MDI QKD protocol has the farthest transmission distance in the finite-size scenario. Finally, we discuss the impact of finite-size effects related to the practical detection in the CV-MDI QKD protocol. The overall results indicate that the finite-size effect has a great influence on the secret-key rate of the CV-MDI QKD protocol and should not be ignored.

I. INTRODUCTION

Quantum key distribution (QKD) [1–4] is the most mature technology in quantum cryptography, which allows two distant legitimate parties, Alice and Bob, to generate secret keys through an untrusted channel controlled by an eavesdropper, Eve. The coherent-state continuous-variable QKD protocol (CV-QKD) [5,6], based on continuous modulation (Gaussian modulation), was proposed in 2002 [7]. To effectively improve protocol security transmission distance, a continuous-variable two-way quantum key distribution protocol was proposed [8,9]. After that, the CV-QKD protocol has received increasing attention in the past few years due to its high secret-key rate and low-cost advantage [10–15]. In the experiment, Jouguet *et al.* [16] achieved the CV-QKD experiment of all-fiber Gaussian modulation coherent state and homodyne detection of 80 km in the laboratory. The field tests of a CV-QKD system [17] have extended the distribution distance to 50 km over commercial fiber, where the secure key rates are two orders of magnitude higher than previous field test demonstrations.

Although the QKD protocols, including CV protocols [14,15,18], are guaranteed to have unconditional security in theory based on quantum physics, the actual security is related to the performance of the device. Due to the imperfection of the detector in the practical CV-QKD system, Eve can implement quantum hacking attacks for CV detectors, such as the local oscillator calibration attack [19,20], the wavelength attack [21,22], the detector saturation attack [23]. These attacks use the detector's imperfect characteristics to operate the detector results to reduce the additional noise variance, so that Alice and Bob estimate the secret-key rate too high, resulting in security risks. For this reason, continuous-variable measurement-device-independent (CV-MDI) protocol has been proposed

[24,25]. Since the measurement part of the protocol is completely committed by an untrusted third party, the security of the protocol does not depend on the security of the detector. Therefore, this protocol can naturally resist all hacker attacks against detectors.

In most conventional security proofs, the theoretical security analysis relies on the assumption that the two communication parties exchange the infinite number of signals in the asymptotic scheme [4]. Hence, the finite-size effect is the key problem that CV protocol needs to be solved in the practical implementation. In recent years, the attention of researchers has gradually shifted to the practical security of CV-QKD protocol. Scarani and Renner [26] proposed a security bound based on smooth min-entropy in 2008. In 2010, Leverrier *et al.* [27] extended the finite-size analysis framework from discrete-variable (DV) protocol to CV protocol, taking into account the finite-size effect of the parameter estimation process. In 2012, Jouguet *et al.* [28] researched the finite-size effect of the CV-QKD protocol on the secret-key rate in the case of practical detections. So far, the security of the CV-MDI QKD protocol in the asymptotic scenario has been demonstrated [24,25,29–31]. But the feasibility of CV-MDI QKD protocol under finite-size effects has not yet been confirmed.

To solve this problem, we study the influence of the finite-size effect on the CV-MDI QKD protocol under collective attack. Here we only consider the reverse reconciliation protocol and for the direct reconciliation protocol we can use the similar calculation method. The numerical simulations of the protocol are given at block lengths between 10^6 and 10^{10}. When Charlie is placed in Bob (asymmetric case) and considering the optimal modulation variance conditions, the farthest transmission distance can reach 86 km for reconciliation efficiency $\beta = 1$ and 75 km for $\beta = 96.9\%$. Finally, we discuss the impact of the practical detection on the CV-MDI QKD protocol under the finite-size effect.

The rest of this paper is organized as follows: In Sec. II, we first introduce the main idea of the CV-MDI QKD protocol, and

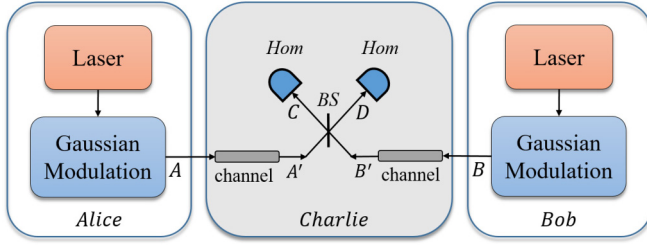*zhangyc@bupt.edu.cn
†yusong@bupt.edu.cn

FIG. 1. A schematic diagram of CV-MDI QKD. BS stands for 50 : 50 beam splitter, Hom stands for homodyne detection.

then study the finite-size analysis of the parameter-estimation process of CV-MDI QKD protocol in detail and introduce the method and formulas that are used in finite-size analysis. In Sec. III, we show the simulation results of the secret-key rate and give the optimal modulation variance and the maximal transmission distance under different conditions. Our conclusions are drawn in Sec. IV.

II. CV-MDI QKD PROTOCOL AND PARAMETER ESTIMATION

The setup of the CV-MDI QKD protocol is illustrated in Fig. 1. The Gaussian modulation coherent-state CV-MDI QKD protocol is mainly described as follows: First, Alice and Bob use lasers to generate light sources, and prepare Gaussian coherent states independently by using the phase modulator and amplitude modulator, respectively. Then, Alice and Bob send the prepared quantum states to an untrusted third party (Charlie) for a continuous-variable Bell measurement. The specific operation is that Charlie receives two quantum states through a 50 : 50 beam splitter, and then uses two homodyne detectors to measure the interference results. Next, Charlie publishes his measurement results. Finally, Alice and Bob use the corrected data for parameter estimation, data postprocessing, data reconciliation, and private-key amplification to get the final security secret key.

The above is the protocol process of the CV-MDI QKD protocol in the prepare-and-measure (PM) scheme. The PM scheme is easy to implement, but it often uses the entanglement-based (EB) scheme in security analysis. The equivalence between the EB scheme of the CV-MDI QKD protocol and the PM scheme has been proven in Ref. [24], and the EB scheme of the CV-MDI QKD protocol is shown in Fig. 2. The equivalence is reflected in two points: On the one hand, the equivalence of the state preparation; that is, the heterodyne detection of one mode of the two-mode squeezed (EPR) state is equivalent to the preparation of a Gaussian modulation coherent state. On the other hand, the data correction process in the PM scheme is equivalent to the displacement operation in the EB scheme. Therefore, only the EB version of the CV-MDI QKD protocol is analyzed in the following security analysis.

To calculate the secret-key rate of the CV-MDI QKD protocol, the researchers proposed two calculation methods [24,25]: One is the secret-key-rate formula based on entanglement swapping. That is, assuming that Bob's EPR state preparation and displacement operations are regarded as manipulated
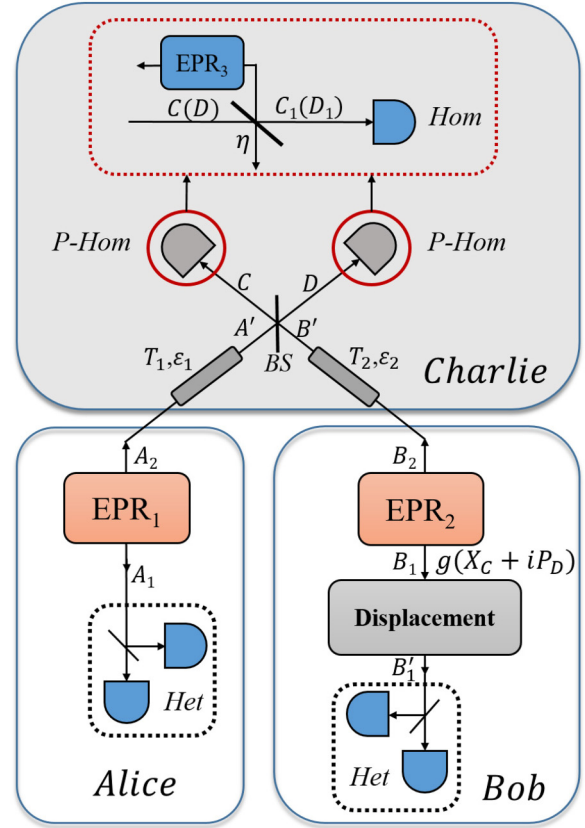

FIG. 2. Entanglement-based scheme of CV-MDI QKD with practical detector. T_1 (T_2) is the channel transmittance for Alice-Charlie (Bob-Charlie), ε_1 (ε_2) is the channel excess noise for Alice-Charlie (Bob-Charlie). η is the efficiency of the detection, v is the variance of the thermal state, v_{el} is the variance of electronic noise. EPR is the two-mode squeezed state, P-Hom is practical homodyne detection, Hom is ideal homodyne detection, Het is heterodyne detection.

by Eve in Fig. 2, then the CV-MDI QKD protocol can be equivalent to a one-way CV-QKD protocol. The other is the secret-key-rate formula based on the subscenario. That is, each subscenario is the same as a one-way CV-QKD protocol, and the final secret-key rate is the mean of the key rate of each subscenario. CV-MDI QKD protocol in the asymptotic regime and collective attack conditions, the secret-key rate of the former is smaller than the latter's secret-key rate. Moreover, in the case of finite size, the two security analysis methods are equivalent to the coherent-state CV-QKD one-way protocol using heterodyne detection. In the following, because the idea of security analysis is more concise and the calculation of the secret-key rate is simpler, we adopt the former secret-key-rate calculation method.

According to the finite-size-effect analysis of the discrete-variable QKD protocol against collective attacks, the expression of the secret-key rate of the one-way CV-QKD protocol against collective attack in the finite-size case is [27]

$$k = \frac{n}{N}\left[\beta I(a:b) - S_{\epsilon_{PE}}(b:E) - \Delta(n)\right], \quad (1)$$

where N is the total number of signals exchanged by Alice and Bob, of which only n signals are used to generate the keys. $\beta \in$

[0,1] is the reconciliation efficiency, and $I(a : b)$ is the mutual information of Alice and Bob. Considering the influence of the finite-size effect on the accuracy of the parameter estimation; that is, under certain failure probability ϵ_{PE}, the true channel parameters are within a certain confidence interval near the estimated parameters, then the conditional entropy of Eve and Bob is expressed as $S_{\epsilon_{PE}}(b : E)$. The most important parameter in the expression, $\Delta(n)$, is related to the security of the private key amplification [27]. Its value is given by

$$\Delta(n) = (2\mathrm{dim}H_X + 3)\sqrt{\frac{\log_2(2/\bar{\epsilon})}{n}} + \frac{2}{n}\log_2(1/\epsilon_{PA}). \quad (2)$$

In Eq. (1), $\Delta(n)$ is the correction term in the formula for the security secret-key rate, which varies with the total length of the exchanged signals. The first term of Eq. (2) is the convergence speed of the smooth minimum entropy of an independent and identically distributed state to the von Neumann entropy, which is the main part to determine $\Delta(n)$. H_X corresponds to the dimension of the *Hilbert* space of the variable x in the raw key, taking dim $H_X = 2$ [27] in the CV protocol. $\bar{\epsilon}$ and ϵ_{PA} are the smoothing parameter and the failure probability of private key amplification processes, respectively, and we take their optimal value as $\bar{\epsilon} = \epsilon_{PA} = 10^{-10}$ [27].

In the following, we study the impact of the finite-size effect on the parameter estimation process of the CV-MDI QKD protocol. More precisely, we analyze the influence of finite signal length N on the estimation of channel excess noise ε_1, ε_2. Due to the limited signal length, the statistical fluctuation of the sampling estimation in the parameter estimation process will be worse, which makes the evaluation accuracy of both communication sides on Eve's eavesdropping behavior worse. To ensure the security of the protocol, it is necessary to do the worst estimate of the impact of eavesdropping. That is, one needs to compute the maximum value of the Holevo information between Eve and Bob in the case of statistical fluctuation in the parameter estimation, the maximum value of $S_{\epsilon_{PE}}(b : E)$.

The calculation of $S_{\epsilon_{PE}}(b : E)$ depends on the covariance matrix $\gamma_{A_1 B'_1}$ of shared state $\rho_{A_1 B'_1}$ of Alice and Bob in the EB version of the protocol. In particular, in the CV-MDI QKD protocol, we need to consider the statistical fluctuation of the channel transmittance (T_1, T_2) and the excess noise of the Alice-Charlie channel and the Bob-Charlie channel $(\varepsilon_1, \varepsilon_2)$, the Alice modulation variance V_A, and the Bob modulation variance V_B, respectively.

In the EB version of the CV-MDI QKD protocol, as shown in Fig. 1, before Charlie makes a homodyne detection to the C and D modes respectively, $\gamma_{A_1 CDB_1}$ takes the following form:

$$\gamma_{A_1 CDB_1} = \begin{pmatrix} V_1 I_2 & \sqrt{\frac{1}{2}T_1(V_1^2 - 1)}\sigma_z & \sqrt{\frac{1}{2}T_1(V_1^2 - 1)}\sigma_z & 0I_2 \\ \sqrt{\frac{1}{2}T_1(V_1^2 - 1)}\sigma_z & [\frac{1}{2}T_1(V_1 + \chi_1) + \frac{1}{2}T_2(V_1 + \chi_2)]I_2 & [\frac{1}{2}T_1(V_1 + \chi_1) - \frac{1}{2}T_2(V_1 + \chi_2)]I_2 & \sqrt{\frac{1}{2}T_2(V_2^2 - 1)}\sigma_z \\ \sqrt{\frac{1}{2}T_1(V_1^2 - 1)}\sigma_z & [\frac{1}{2}T_1(V_1 + \chi_1) - \frac{1}{2}T_2(V_1 + \chi_2)]I_2 & [\frac{1}{2}T_1(V_1 + \chi_1) + \frac{1}{2}T_2(V_1 + \chi_2)]I_2 & -\sqrt{\frac{1}{2}T_2(V_2^2 - 1)}\sigma_z \\ 0I_2 & \sqrt{\frac{1}{2}T_2(V_2^2 - 1)}\sigma_z & -\sqrt{\frac{1}{2}T_2(V_2^2 - 1)}\sigma_z & V_2 I_2 \end{pmatrix},$$

$$(3)$$

where I_2 is the 2×2 identity matrix and $\sigma_z = \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}$, so $\gamma_{A_1 CDB_1}$ is obviously an 8×8 covariance matrix. The parameters of the above matrix are given by $V_1 = V_A + 1$, $V_2 = V_B + 1$, where V_A and V_B are the modulation variance of Alice and Bob in the PM protocol. T_1 and T_2 are the transmittance of the Alice-Charlie channel and the Bob-Charlie channel. ε_1 and ε_2 in $\chi_1 = \frac{1}{T_1} - 1 + \varepsilon_1$, $\chi_2 = \frac{1}{T_2} - 1 + \varepsilon_2$ are the excess noise of the corresponding channel. According to the covariance matrix in Eq. (3), we know the modulation variance of Alice and Bob, $\langle x_1^2 \rangle$ and $\langle x_2^2 \rangle$, the variance of Charlie, $\langle y_1^2 \rangle$, $\langle y_2^2 \rangle$, and $\langle y_1 y_2 \rangle$, the covariance of Alice and Charlie, $\langle x_1 y_1 \rangle$, and the covariance of Bob and Charlie, $\langle x_2 y_2 \rangle$. These values and secret-key-rate parameters are related through

$$\langle x_1^2 \rangle = V_1 - 1 = V_A, \quad \langle x_2^2 \rangle = V_2 - 1 = V_B, \quad (4)$$

$$\langle y_1^2 \rangle = \langle y_2^2 \rangle = \frac{1}{2}(T_1 V_A + T_2 V_B) + 1 + \frac{1}{2}(T_1 \varepsilon_1 + T_2 \varepsilon_2), \quad (5)$$

$$\langle x_1 y_1 \rangle = \sqrt{\frac{T_1}{2}}(V_1 - 1) = \sqrt{\frac{T_1}{2}}V_A, \quad \langle x_2 y_2 \rangle = \sqrt{\frac{T_2}{2}}(V_2 - 1) = \sqrt{\frac{T_2}{2}}V_B, \quad (6)$$

$$\langle y_1 y_2 \rangle = \frac{1}{2}(T_1 V_A - T_2 V_B) + \frac{1}{2}(T_1 \varepsilon_1 - T_2 \varepsilon_2). \quad (7)$$

In practical CV-MDI QKD systems, the quantities estimated by Alice and Bob are obtained by the sampling of $m = N - n$ pairs of correlated variables $(x_i, y_i)_{i=1...m}$. Since the Alice-Charlie channel and the Bob-Charlie channel are

linear channels, the variables of Alice, Bob, and Charlie follow a Gaussian distribution. Within this model, we consider that the data before the beam splitter is represented as y'_1, y'_2. So before the beam splitter, Alice and Charlie's and Bob and Charlie's

data are linked through the following relation:

$$
\begin{aligned}
y'_1 &= t'_1 x_1 + z_1, \\
y'_2 &= t'_2 x_2 + z_2,
\end{aligned}
\tag{8}
$$

where $t'_1 = \sqrt{T_1}$, $t'_2 = \sqrt{T_2}$, z_1, z_2 follow a centered normal distribution with unknown variance $\sigma'^2_1 = 1 + T_1 \varepsilon_1$, $\sigma'^2_2 = 1 + T_2 \varepsilon_2$. According to the known parameter relations in the covariance matrix, it can be expressed that the variance of the unknown parameters before the beam splitter:

$$
\begin{aligned}
\langle y'^2_1 \rangle &= \langle y_1^2 \rangle + \langle y_1 y_2 \rangle \\
&= T_1 V_A + 1 + T_1 \varepsilon_1 = t'^2_1 V_A + \sigma'^2_1,
\end{aligned}
\tag{9}
$$

$$
\begin{aligned}
\langle y'^2_2 \rangle &= \langle y_2^2 \rangle - \langle y_1 y_2 \rangle \\
&= T_2 V_B + 1 + T_2 \varepsilon_2 = t'^2_2 V_B + \sigma'^2_2.
\end{aligned}
\tag{10}
$$

Maximum-likelihood estimators $\hat{t}'_1$, $\hat{t}'_2$, $\hat{\sigma}'^2_1$, $\hat{\sigma}'^2_2$, $\hat{V}_A$, and $\hat{V}_B$ are known for the normal linear model [27]:

$$
\hat{t}'_1 = \frac{\sum_{i=1}^{m} x_{1i} y'_{1i}}{\sum_{i=1}^{m} x_{1i}^2}, \quad \hat{t}'_2 = \frac{\sum_{i=1}^{m} x_{2i} y'_{2i}}{\sum_{i=1}^{m} x_{2i}^2},
\tag{11}
$$

$$
\hat{\sigma}'^2_1 = \frac{1}{m} \sum_{i=1}^{m} \left(y'_{1i} - \hat{t}'_1 x_{1i} \right)^2,
$$

$$
\hat{\sigma}'^2_2 = \frac{1}{m} \sum_{i=1}^{m} \left(y'_{2i} - \hat{t}'_2 x_{2i} \right)^2,
\tag{12}
$$

$$
\hat{V}_A = \frac{1}{m} \sum_{i=1}^{m} x_{2i}^2,
$$

$$
\hat{V}_B = \frac{1}{m} \sum_{i=1}^{m} x_{1i}^2.
\tag{13}
$$

The estimators $\hat{t}'_1$, $\hat{t}'_2$, $\hat{\sigma}'^2_1$, $\hat{\sigma}'^2_2$, $\hat{V}_A$, and $\hat{V}_B$ are independent estimators with the following distributions:

$$
\hat{t}'_1 \sim \mathrm{N}\left(t'_1, \frac{\sigma'^2_1}{\sum_{i=1}^{m} x_{1i}^2} \right), \quad \hat{t}'_2 \sim \mathrm{N}\left(t'_2, \frac{\sigma'^2_2}{\sum_{i=1}^{m} x_{2i}^2} \right),
\tag{14}
$$

$$
\frac{m \hat{\sigma}'^2_1}{\sigma'^2_1}, \frac{m \hat{\sigma}'^2_2}{\sigma'^2_2}, \frac{m \hat{V}_A}{V_A}, \frac{m \hat{V}_B}{V_B} \sim \chi^2(m-1),
\tag{15}
$$

where t'_1, t'_2, σ'^2_1, σ'^2_2, V_A, and V_B are the true values of the parameters. Due to the limit of length m, we can estimate the confidence interval for these parameters when the confidence probability is $\epsilon_{PE/2}$:

$$
\begin{aligned}
t'_1 &\in [\hat{t}'_1 - \Delta t'_1, \hat{t}'_1 + \Delta t'_1], \\
t'_2 &\in [\hat{t}'_2 - \Delta t'_2, \hat{t}'_2 + \Delta t'_2],
\end{aligned}
\tag{16}
$$

$$
\begin{aligned}
\sigma'^2_1 &\in \left[\hat{\sigma}'^2_1 - \Delta \sigma'^2_1, \hat{\sigma}'^2_1 + \Delta \sigma'^2_1 \right], \\
\sigma'^2_2 &\in \left[\hat{\sigma}'^2_2 - \Delta \sigma'^2_2, \hat{\sigma}'^2_2 + \Delta \sigma'^2_2 \right],
\end{aligned}
\tag{17}
$$

$$
\begin{aligned}
V_A &\in [\hat{V}_A - \Delta V_A, \hat{V}_A + \Delta V_A], \\
V_B &\in [\hat{V}_B - \Delta V_B, \hat{V}_B + \Delta V_B],
\end{aligned}
\tag{18}
$$

where

$$
\Delta t'_1 = z_{\epsilon_{PE}/2} \sqrt{\frac{\hat{\sigma}'^2_1}{m V_A}}, \quad \Delta t'_2 = z_{\epsilon_{PE}/2} \sqrt{\frac{\hat{\sigma}'^2_2}{m V_A}},
$$

$$
\Delta \sigma'^2_1 = z_{\epsilon_{PE}/2} \frac{\hat{\sigma}'^2_1 \sqrt{2}}{\sqrt{m}}, \quad \Delta V_A = z_{\epsilon_{PE}/2} \frac{\hat{V}_A \sqrt{2}}{\sqrt{m}},
$$

$$
\Delta \sigma'^2_2 = z_{\epsilon_{PE}/2} \frac{\hat{\sigma}'^2_2 \sqrt{2}}{\sqrt{m}}, \quad \Delta V_B = z_{\epsilon_{PE}/2} \frac{\hat{V}_B \sqrt{2}}{\sqrt{m}},
$$

and $z_{\epsilon_{PE}/2}$ satisfies $1 - \mathrm{erf}(z_{\epsilon_{PE}/2}/\sqrt{2})/2 = \epsilon_{PE}/2$. ϵ_{PE} is the failure probability of the parameter estimation process, which generally takes 10^{-10}. $\mathrm{erf}(x)$ is the error function, which is defined as

$$
\mathrm{erf}(x) = \frac{2}{\sqrt{\pi}} \int_0^x e^{-t^2} dt.
\tag{19}
$$

We can estimate $T_1 = \hat{t}^2_1$, $T_2 = \hat{t}^2_2$ and $\varepsilon_1 = \frac{\hat{\sigma}'^2_1 - 1}{\hat{t}^2_1}$, $\varepsilon_2 = \frac{\hat{\sigma}'^2_2 - 1}{\hat{t}^2_2}$ by previous estimators and confidence intervals. Next, Charlie uses two homodyne detectors to measure the C and D modes, and Bob performs displacement operations based on Charlie's measurements. Indeed, the CV-MDI QKD protocol is equivalent to a one-way CV-QKD protocol when Bob's EPR state preparations and displacement operations are also untrusted. Then the covariance matrix $\gamma_{A_1 B'_1}$ of the state $\rho_{A_1 B'_1}$ shared by Alice and Bob is

$$
\gamma_{A_1 B'_1} = \begin{pmatrix} V_1 I_2 & \sqrt{T(V_1^2 - 1)} \sigma_z \\ \sqrt{T(V_1^2 - 1)} \sigma_z & [T(V_1 - 1) + 1 + T\varepsilon'] I_2 \end{pmatrix},
\tag{20}
$$

where

$$
T = \frac{T_1}{2} g^2,
$$

$$
\begin{aligned}
\varepsilon' &= 1 + \frac{1}{T_1} [2 + T_2(\varepsilon_2 - 2) + T_1(\varepsilon_2 - 1)] \\
&\quad + \frac{1}{T_1} \left(\frac{\sqrt{2}}{g} \sqrt{V_B} - \sqrt{T_2} \sqrt{V_B + 2} \right)^2.
\end{aligned}
$$

Here one selects $g = \sqrt{2/T_2} \sqrt{V_B/(V_B + 2)}$ [24] so that the equivalent excess noise ε' is minimal. So there is

$$
\varepsilon' = \varepsilon_1 + \frac{1}{T_1} [T_2(\varepsilon_2 - 2) + 2].
\tag{21}
$$

Accordingly, the mutual information between Alice and Bob has the following form:

$$
I_{AB} = \log_2 \left[\frac{T(V + \chi) + 1}{T(1 + \chi) + 1} \right],
\tag{22}
$$

where $\chi = \frac{1}{T} - 1 + \varepsilon'$.

In the equivalent one-way-protocol model, the analysis method of the finite-size effect on the parameter estimation is consistent with the CV-QKD protocol. Within this model,

Alice and Bob's data respectively satisfies the Gaussian distribution and their data are linked through the following relation:

$$y = tx + z, \qquad (23)$$

where $t = \sqrt{T}$ and z follows a centered normal distribution with unknown variance $\sigma^2 = 1 + T\epsilon'$. For any value of the modulation variance V_A, $S(b:E)$ and the variables t, σ^2 are related as follows:

$$\left.\frac{\partial S(b:E)}{\partial t}\right|_{\sigma^2} < 0, \quad \left.\frac{\partial S(b:E)}{\partial \sigma^2}\right|_{t} > 0. \qquad (24)$$

This means that, under $1 - \epsilon_{PE}$ probability, there is a covariance matrix that minimizes the secret-key rate:

$$\gamma_{A_1 B_1'} = \begin{pmatrix} (V_A + 1)I_2 & t_{\min}Z\sigma_z \\ t_{\min}Z\sigma_z & (t_{\min}^2 V_A + \sigma_{\max}^2)I_2 \end{pmatrix}, \qquad (25)$$

where V_A is the modulation variance of Alice. And for Gaussian modulation, the parameter $Z = (V_A^2 + 2V_A)^{1/2}$. To analyze the impact of the statistical fluctuation of each parameter on the covariance matrix, the parameters to be estimated are substituted into the above matrix. The covariance matrix is changed into

$$\gamma_{A_1 B_1'} = \begin{pmatrix} (V_A + 1)I_2 & \frac{t_1'}{t_2'}\sqrt{\frac{V_B}{V_B+2}}Z\sigma_z \\ \frac{t_1'}{t_2'}\sqrt{\frac{V_B}{V_B+2}}Z\sigma_z & \left[\frac{t_1'^2}{t_2'^2}\frac{V_B}{V_B+2}V_A + 1 + \frac{V_B}{V_B+2}\left(\frac{\sigma_1'^2+\sigma_2'^2-2t_2'^2}{t_2'^2}\right)\right]I_2 \end{pmatrix}. \qquad (26)$$

When the estimated parameters are determined, we can calculate the maximum value of $S_{\epsilon_{PE}}(b:E)$. In consequence, the secret-key rate of the CV-MDI QKD protocol against collective attack with the finite-size effect can be calculated according to Eqs. (1) and (2).

III. SIMULATION RESULTS AND DISCUSSION

In this section, we give and discuss the numerical simulation results of the CV-MDI QKD protocol in the ideal detection case with the finite-size effect. See the appendix for the impact of the practical detection on the CV-MDI QKD protocol. To consider the characteristics of CV-MDI QKD protocol, we first perform numerical simulations of the secret-key rate in the ideal reconciliation efficiency. In the following figures, the dark red solid lines, dark blue dot-dashed lines, dark black dotted lines, light yellow solid lines, light pink dot-dashed lines, and light green dotted lines correspond to the block lengths of 10^6, 10^7,
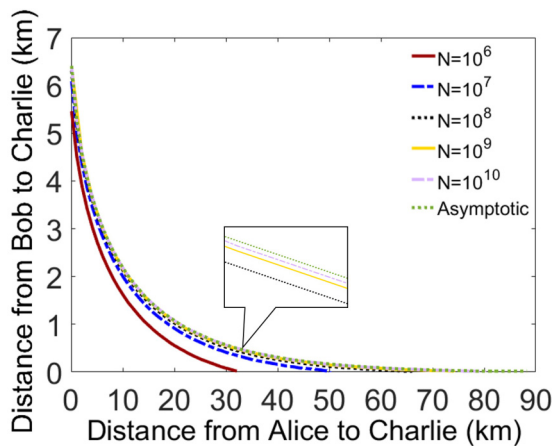

FIG. 3. Comparison between the maximal transmission distance for the CV-MDI QKD protocol under the finite-size effect. The CV-MDI QKD protocol with ideal reconciliation efficiency $\beta = 1$, where the secret-key rate k is positive. The block lengths from left to right curves correspond to $N = 10^6$, 10^7, 10^8, 10^9, 10^{10}. Here we use the ideal modulation variance $V_A = V_B = 10^5$ and excess noises $\varepsilon_1 = \varepsilon_2 = 0.002$ [16].

10^8, 10^9, 10^{10}, and asymptotic curves, respectively. Figure 3 shows the relationship between transmission distance from Alice to Charlie (L_{AC}) and from Bob to Charlie (L_{BC}) of the CV-MDI QKD protocol under the finite-size effect. It can be seen that, under different block lengths, when Bob is placed in the untrusted third party ($L_{BC} = 0$), the asymmetric structure L_{AC} has the farthest transmission distance; more than 85 km. When L_{BC} increases, L_{AC} decreases rapidly and the sum of the two is also reduced. For $N = 10^{10}$ (light green dashed line), even if L_{AC} is reduced to 0, the farthest L_{BC} cannot exceed 7 km.

For the sake of optimizing the performance of the protocol, we also need to consider the optimal modulation variance of the protocol under different block lengths. Figure 4 shows the relationship between the modulation variance and the secret-key rate under the ideal reconciliation efficiency of the CV-MDI QKD protocol with the finite-size effect. We find that, with the improvement of the modulation variance, the secret-key rate gradually converges under the ideal reconciliation efficiency ($\beta = 1$). The optimal modulation variance of the CV-MDI QKD protocol with the finite-size effect in the asymmetric case tends to be infinite. We choose $V_A = V_B = 10^5$ to see the performance of the protocol in the ideal modulation.

Figure 5 displays the impact of the finite-size effect on the CV-MDI QKD protocol under the asymmetric case and ideal modulation variance. As shown in the figure, when the data length is $N = 10^6$ (dark red solid line), the security transmission distance is about 32 km. When the data length is $N = 10^{10}$ (light pink dot-dashed line), the security transmission distance of the protocol is up to 86 km, and the longer the data length, the closer the security transmission distance is to asymptotic regime.

Noteworthily, in Eq. (1), the reconciliation efficiency β can be regarded as the ratio between the actual extracted mutual information and the ideal extracted mutual information [32]. After data reverse reconciliation, the length of the key shared between Alice and Bob becomes $n\beta I(x:y)$. Therefore, under the finite-size effect, imperfect reconciliation efficiency will also affect the security transmission distance of the CV-MDI QKD protocol. Figure 6 shows the optimal modulation variance of the CV-MDI QKD protocol
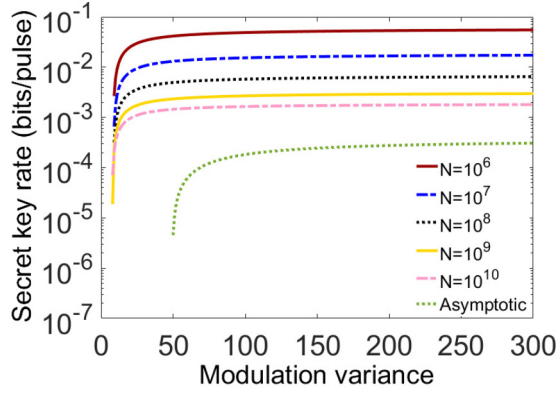
FIG. 4. Optimal modulation variance for the CV-MDI QKD protocol in the asymmetric case with the finite-size effect. CV-MDI QKD protocol with ideal reconciliation efficiency $\beta = 1$. From top to bottom, the block length N is equal to 10^6, 10^7, 10^8, 10^9, and 10^{10}. Here we use the excess noises $\varepsilon_1 = \varepsilon_2 = 0.002$ [16].

FIG. 6. Optimal modulation variance for the CV-MDI QKD protocol in asymmetric case with the finite-size effect. The CV-MDI QKD protocol with imperfect reconciliation efficiency $\beta = 96.9\%$. From top to bottom, the block length N is equal to 10^6, 10^7, 10^8, 10^9, and 10^{10}. Here we use the excess noises $\varepsilon_1 = \varepsilon_2 = 0.002$ [16].

with imperfect reconciliation efficiency $\beta= 96.9\%$ [33,34] in different block lengths. The numbers at the end of the arrow are the values of the optimal modulation variance. The simulation results show that the finite-size effect has an influence on the optimal modulation variance under the imperfect reconciliation efficiency. With the increase of block length, the optimal modulation variance is decreasing.

Similarly, in the imperfect reconciliation efficiency, the asymmetric case of the CV-MDI QKD protocol has the farthest security transmission distance, as shown in Fig. 7. And the selection of the optimal modulation variance increases the final security transmission distance. In Fig. 8, we display the relationship between secret-key rate and transmission distance of the CV-MDI QKD protocol in the asymmetric case with the finite-size effect under imperfect reconciliation efficiency and optimal modulation variance. The simulation results show that the optimal modulation variance improves the security transmission distance while increasing the secret-key rate. And

when the data length is 10^6 (dark red solid line), the security transmission distance is about 23 km.When the data length is 10^{10} (light pink dot-dashed line), the protocol has a far greater security transmission distance, close to 75 km in the case of imperfect reconciliation efficiency ($\beta = 96.9\%$).

IV. CONCLUSION

In this paper, we roughly describe the CV-MDI QKD protocol and propose a finite-size analysis of the CV-MDI QKD protocol under collective attack. This provides a bridge for the theoretical and practicality of the CV-MDI QKD protocol. By using the continuous-variable protocol under the finite-size scenario of the secret-key-rate formula for numerical simulation, we see that the secret-key rate and the
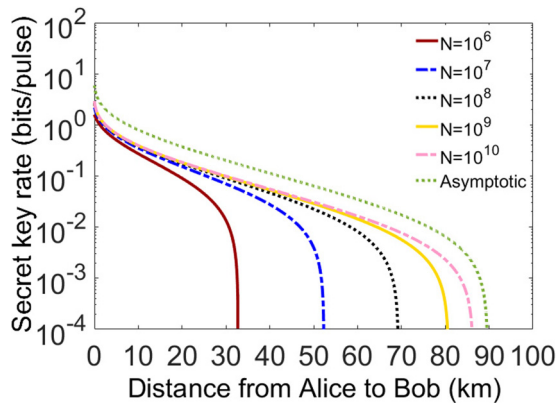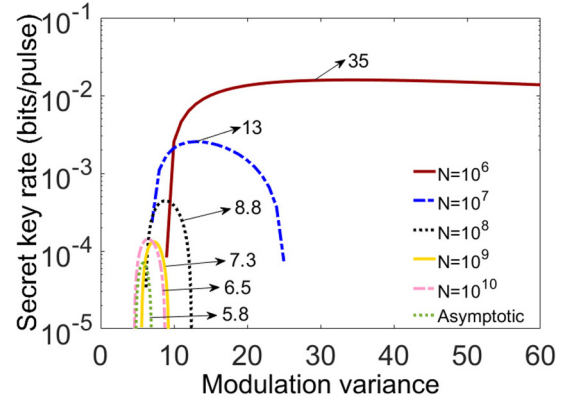

FIG. 5. Secret-key rate for the CV-MDI QKD protocol in the asymmetric case with the finite-size effect. The CV-MDI QKD protocol with ideal reconciliation efficiency $\beta = 1$. The block lengths from left to right curves correspond to $N = 10^6$, 10^7, 10^8, 10^9, 10^{10} and the asymptotic regime. Here we use the ideal modulation variance $V_A = V_B = 10^5$, and excess noises $\varepsilon_1 = \varepsilon_2 = 0.002$ [16].
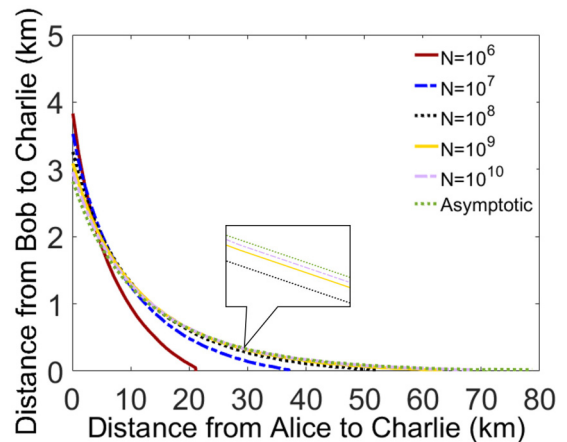

FIG. 7. Comparison among the maximal transmission distance for the CV-MDI QKD protocol under the finite-size effect. The CV-MDI QKD protocol with imperfect reconciliation efficiency $\beta = 96.9\%$, within which the secret-key rate k is positive. The block lengths from left to right curves correspond to $N = 10^6$, 10^7, 10^8, 10^9, 10^{10}. Here we use the optimal modulation variance and excess noises $\varepsilon_1 = \varepsilon_2 = 0.002$ [16].
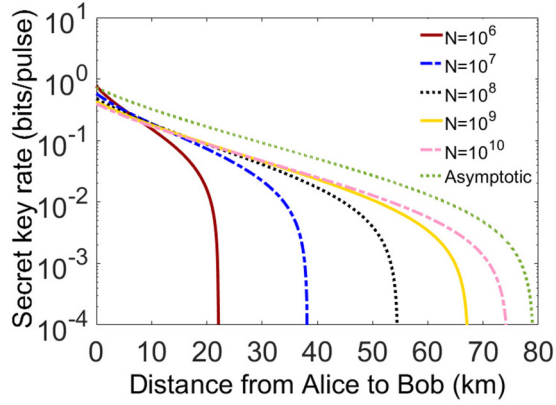
FIG. 8. Secret-key rate for the CV-MDI QKD protocol in the asymmetric case with the finite-size effect. The CV-MDI QKD protocol with imperfect reconciliation efficiency $\beta = 96.9\%$. The block lengths from left to right curves correspond to $N = 10^6$, 10^7, 10^8, 10^9, 10^{10}, and the asymptotic regime. Here we use the optimal modulation variance and excess noises $\varepsilon_1 = \varepsilon_2 = 0.002$ [16].

security transmission distance are affected when considering the finite-size effect.

The results demonstrate that the finite-size effect also influences the optimal modulation variance. With the increase of the block length, the optimal modulation variance is decreasing. And at various block lengths between 10^6 and 10^{10}, when Bob is placed in an untrusted third party; that is, under the asymmetric case, the CV-MDI QKD protocol has the farthest security transmission distance. The CV-MDI QKD protocol of the asymmetric structure with the finite-size effect can safely transmit about 86 km under the ideal reconciliation efficiency and optimal modulation variance conditions at 10^{10} block size. When the reconciliation efficiency is 96.9%, under the above conditions, the maximum transmission distance of the protocol is about 75 km.

It can be seen that, as with the CV-QKD one-way protocol, in the CV-MDI QKD protocol, the fewer signals exchanged, the more obvious is the finite-size effect, and the faster the secret-key rate and security transmission distance drop. The overall results show that the practical implementation of CV-MDI QKD should not neglect the influence of the finite-size effect.

Note that we mainly focus on the impact of the finite-size effect on the CV-MDI QKD protocol under arbitrary collective attack. Recently, the composable security of the CV-MDI QKD protocol against coherent attacks in a practical finite-size scenario has been proved rigorously [35,36].

Note added. An independent work [37] has been posted on arXiv. This work also studies the impact of the finite-size effect of the CV-MDI QKD protocol.

ACKNOWLEDGMENTS

APPENDIX DISCUSSION OF PRACTICAL DETECTION

We now consider the finite-size effect related to the detection setup. Since the third party Charlie uses two homodyne detectors to measure the quantum state for the Bell measurement in the practical system, the impact of the practical detectors on the CV-MDI QKD protocol should be considered. Although the security of the CV-MDI QKD protocol is not limited by the detector, its performance is constrained by the performance of the detector. To research the effect of the practical detection on the protocol in the case of the finite-size effect, we mainly consider the ideal coordination efficiency ($\beta = 1$) situation. Now, the EB version of the CV-MDI QKD protocol in a practical detection scheme is shown in Fig. 2. An imperfect homodyne detection is represented by a beam splitter and thermal noise, wherein the transmittance of the beam splitter is the detection efficiency η, the relationship between the variance of the thermal state v and detector electronic noise variance v_{el} is $v = 1 + v_{el}/(1 - \eta)$. For the CV-MDI QKD protocol considering the practical detector, it is also necessary to estimate the covariance matrix between Alice and Bob. The estimated parameters are the variance of Alice, Bob, Charlie, Alice and Charlie's covariance, and Bob and Charlie's covariance:

$$\langle x_1^2 \rangle = V_1 - 1 = V_A, \quad \langle x_2^2 \rangle = V_2 - 1 = V_B, \quad \text{(A1)}$$

$$\begin{aligned}
\langle y_1^2 \rangle = \langle y_2^2 \rangle &= \eta\left[\tfrac{1}{2}T_1(V_1 + \chi_1) + \tfrac{1}{2}T_2(V_2 + \chi_2)\right] \\
&\quad + 1 - \eta + v_{el} = \tfrac{1}{2}\eta(T_1 V_A + T_2 V_B) \\
&\quad + \tfrac{1}{2}\eta(T_1\varepsilon_1 + T_2\varepsilon_2) + 1 + v_{el},
\end{aligned} \quad \text{(A2)}$$

$$\begin{aligned}
\langle x_1 y_1 \rangle &= \sqrt{\eta}\sqrt{\frac{T_1}{2}}(V_1 - 1) = \sqrt{\frac{\eta T_1}{2}}V_A, \\
\langle x_2 y_2 \rangle &= \sqrt{\eta}\sqrt{\frac{T_2}{2}}(V_2 - 1) = \sqrt{\frac{\eta T_2}{2}}V_B,
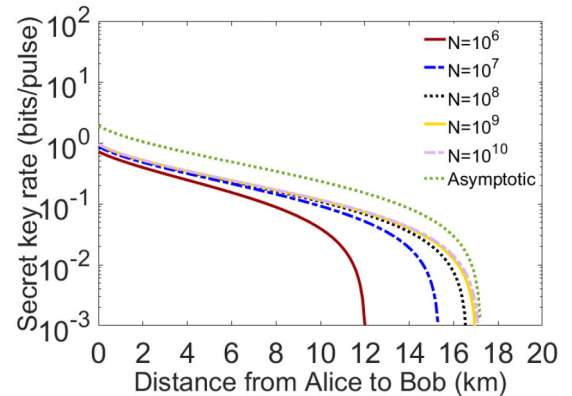\end{aligned} \quad \text{(A3)}$$

FIG. 9. Secret-key rate for CV-MDI QKD protocol in asymmetric case with finite-size effect. The CV-MDI QKD protocol with perfect reconciliation efficiency $\beta = 1$ and imperfect homodyne detectors $\eta = 96\%$, $v_{el} = 0.015$. The block lengths from left to right curves correspond to $N = 10^6$, 10^7, 10^8, 10^9, 10^{10}, and the asymptotic regime. Here we use the ideal modulation variance $V_A = V_B = 10^5$, and excess noises $\varepsilon_1 = \varepsilon_2 = 0.002$ [16].

$$\langle y_1 y_2 \rangle = \eta \left[\tfrac{1}{2} T_1 (V_1 + \chi_1) - \tfrac{1}{2} T_2 (V_2 + \chi_2) \right]$$
$$= \tfrac{1}{2} \eta (T_1 V_A - T_2 V_B) + \tfrac{1}{2} \eta (T_1 \varepsilon_1 - T_2 \varepsilon_2). \quad \text{(A4)}$$

The parameter estimations below are calculated in the same way as the calculation without considering the detections, but the statistical fluctuations of η and v_{el} are taken into account. Correspondingly, the equivalent excess noise is written as [24]

$$\varepsilon' = 1 + \frac{T_1 \chi_1 + T_2 \chi_2 - T_2}{T_1} + \frac{2 \chi_3}{T_1}, \quad \text{(A5)}$$

where $\chi_3 = \frac{1-\eta}{\eta} + \frac{v_{el}}{\eta}$, and the optimized displacement operation amplification coefficient is $g = \sqrt{2/(\eta T_2)} \sqrt{V_B/(V_B + 2)}$.

Figure 9 gives the impact of the finite-size effect on the CV-MDI QKD protocol considering the practical detection. Compared with the results of Fig. 5, we found that imperfect detectors have a significant effect on the secret-key rate and the security transmission distance. For instance, when the block length is 10^{10}, the security transmission distance is the farthest, only 17 km. Conceivably, the results will be even more pessimistic in terms of practical reconciliation efficiency.

[1] C. Bennett and G. Brassard, Lecture Notes in Computer Science **196**, 475 (1984).

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

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

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

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

[6] C. Weedbrook, S. Pirandola, R. Garcia-Patron, N. J. Cerf, T. C. Ralph, J. H. Shapiro, and S. Lloyd, Rev. Mod. Phys. **84**, 621 (2012).

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

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

[9] C. Ottaviani, S. Mancini, and S. Pirandola, Phys. Rev. A **92**, 062323 (2015).

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

[11] F. Grosshans, Phys. Rev. Lett. **94**, 020504 (2005).

[12] M. Navascues and A. Acin, Phys. Rev. Lett. **94**, 020505 (2005).

[13] M. M. Wolf, G. Giedke, and J. I. Cirac, Phys. Rev. Lett. **96**, 080502 (2006).

[14] M. Navascues, F. Grosshans, and A. Acin, Phys. Rev. Lett. **97**, 190502 (2006).

[15] R. Garcia-Patron and N. J. Cerf, Phys. Rev. Lett. **97**, 190503 (2006).

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

[17] Y. Zhang, Z. Li, Z. Chen, C. Weedbrook, Y. Zhao, X. Wang, C. Xu, X. Zhang, Z. Wang, M. Li, X. Zhang, Z. Zheng, B. Chu, X. Gao, N. Meng, W. Cai, Z. Wang, G. Wang, S. Yu, and H. Guo, arXiv:1709.04618.

[18] J. Muller-Quade and R. Renner, New J. Phys. **11**, 085006 (2009).

[19] X. C. Ma, S. H. Sun, M. S. Jiang, and L. M. Liang, Phys. Rev. A **88**, 022339 (2013).

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

[21] J. Z. Huang, C. Weedbrook, Z. Q. Yin, S. Wang, H. W. Li, W. Chen, G. C. Guo, and Z. F. Han, Phys. Rev. A **87**, 062329 (2013).

[22] X. C. Ma, S. H. Sun, M. S. Jiang, and L. M. Liang, Phys. Rev. A **87**, 052309 (2013).

[23] H. Qin, R. Kumar, and R. Alleaume, Phys. Rev. A **94**, 012325 (2016).

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

[25] 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).

[26] V. Scarani and R. Renner, Phys. Rev. Lett. **100**, 200501 (2008).

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

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

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

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

[31] Y. Zhang, Z. Li, C. Weedbrook, K. Marshall, S. Pirandola, S. Yu, and H. Guo, Entropy **17**, 4547 (2015).

[32] A. Leverrier, R. Alleaume, J. Boutros, G. Zemor, and P. Grangier, Phys. Rev. A **77**, 042325 (2008).

[33] P. Jouguet, S. Kunz-Jacques, and A. Leverrier, Phys. Rev. A **84**, 062317 (2011).

[34] X. Wang, Y. Zhang, S. Li, B. Xu, S. Yu, and H. Guo, Quantum Inf. Comput. **17**, 1123 (2017).

[35] C. Lupo, C. Ottaviani, P. Papanastasiou, and S. Pirandola, arXiv:1704.07924.

[36] Y. Zhang, Z. Li, S. Yu, and H. Guo, Frontiers in Optics (FiO 2017), JW4A.33 (2017).

[37] P. Papanastasiou, C. Ottaviani, and S. Pirandola, arXiv:1707.04599.