

# Asymmetry effects in homodyne-like measurements: Positive operator-valued measures and quantum key distribution

A. S. Naumchik,<sup>1,\*</sup> Roman K. Goncharov,<sup>1,†</sup> and Alexei D. Kiselev<sup>2,3,‡</sup>

<sup>1</sup>*ITMO University, Kronverksky Pr. 49, Saint Petersburg 197101, Russia*

<sup>2</sup>*Laboratory of Quantum Processes and Measurements,*

*ITMO University, Kadetskaya Line 3b, Saint Petersburg 199034, Russia*

<sup>3</sup>*Leading Research Center "National Center for Quantum Internet",*

*ITMO University, Birzhevaya Line 16, Saint Petersburg 199034, Russia*

(Dated: October 23, 2025)

We study applicability of the Gaussian approximation describing photon count statistics for both the homodyne and the double homodyne measurements in the presence of asymmetry effects when the beam splitters are unbalanced and the quantum efficiencies of the photodetectors are not identical. We also use the Gaussian approximation to construct the positive operator-valued measure (POVM) that takes into account the asymmetry effects. The results are applied to calculate the secure key rate of the GG02 protocol under an untrusted noise model. It is found that asymmetry maximizes security key rate over the balanced case.

## I. INTRODUCTION

Homodyne detection is a fundamental technique in quantum optics for measuring quadrature (amplitude and phase) components of light fields and plays a central role in continuous-variable quantum key distribution (CV-QKD) systems [1–7]. In a typical setup a weak quantum signal is combined with a classical local oscillator (LO) at a beam splitter and the two outputs are detected by photodiodes; the difference photocount yields information about the signal quadratures [8, 9].

Most theoretical treatments assume the strong-LO approximation, where the LO is much more intense than the signal [10]. This simplifies analysis and improves precision but may also amplify classical LO noise, masking subtle quantum effects such as squeezing. In the weak-LO regime, where LO and signal amplitudes are comparable, phase-sensitive quantum effects become more visible [11]; however, operation in this regime demands highly efficient and temporally stable detectors to compensate for low optical power [11, 12]. Various measurement schemes, including homodyne intensity correlations with two beam splitters and detectors or cross-correlation with a single unbalanced beam splitter, are useful when overall detection efficiency is limited [11].

Approaches such as unbalanced homodyne detection, where only one output port of the beam splitter is measured, have been used for quantum-state reconstruction based on positive operator-valued measures (POVMs) associated with  $s$ -parametrized quasiprobability distributions ( $s < 1$ ) [13]. These schemes suffer from high noise sensitivity and current limits in photon-number resolution, though detector arrays have been proposed to mitigate these drawbacks [14–16].

Another important approach is double homodyne detection (or eight-port detection), which yields simultaneous outcomes for both conjugate quadratures and allows direct reconstruction of the Husimi  $Q$ -function [14, 17]. At finite LO intensities, this scheme bridges classical and quantum regimes, with the weak LO limit reducing to photon-number measurements [18]. In the context of CV-QKD protocols, this method also enables the symmetrization procedure, since the measurement retains complete information about both quadratures [19].

Practical implementations are affected by nonideal components and asymmetries that must be modeled explicitly. Imperfections such as unbalanced beam splitters, unequal detector efficiencies, finite photon-number resolution, and detector dead times introduce excess noise that degrades measurement fidelity and undermines CV-QKD security [13, 20–25]. Although the ideal POVMs for projections onto quadrature or coherent states are well known [10, 17], an explicit treatment of asymmetry effects (beam-splitter imbalance and detector-efficiency mismatch) has not been carried out in detail in the literature [15, 16]. In this work we therefore focus on these two imperfections and refer to them collectively as *asymmetry effects*.

In practice, such imperfections are commonly modeled as additive technical noise (electronic noise, dark counts, finite bandwidth), but asymmetry introduces structured excess noise that must be accounted for to obtain reliable security estimates [24–26]. These imperfections may also open side channels exploitable by an adversary (e.g., wavelength-dependent or detector-blinding attacks), so countermeasures such as spectral filtering, detector balancing, and careful calibration are essential [25, 27–30]. Accounting explicitly for measurement asymmetry is an important part of this defensive toolbox.

Our analysis focuses on the asymmetrical detection case: an unbalanced beam splitter combined with unequal (and non-unity) quantum efficiencies of the photodetectors, in contrast to the conventional symmetrical

\* Email address: naumchik95@gmail.com

† Email address: toloroloe@gmail.com

‡ Email address: alexei.d.kiselev@gmail.com

case of a balanced beam splitter and identical detector efficiencies. To derive tractable expressions we model photocount statistics by approximating Poisson distributions with Gaussian ones (the *Gaussian approximation*) and further simplify using the local-oscillator (LO) approximation. From these approximations we construct the corresponding POVMs and numerically assess the quality of the approximations.

We then apply the developed formalism to a homodyne-based two-quadrature scheme (double homodyne, often called heterodyne in the QKD literature [5, 6, 31]) to demonstrate applicability beyond single-quadrature detection. We find that the asymmetrical double-homodyne POVM requires an extension to the set of squeezed coherent states. The asymmetrical POVMs obtained are then used to compute the CV-QKD asymptotic secret fraction, thereby quantifying the impact of measurement asymmetry on protocol security.

We also show that the commonly used Skellam-distribution approximation based on the asymptotic expansion of the modified Bessel function of the first kind is not valid in the asymmetrical regime.

The paper is organized as follows. In Sec. II, we obtain the statistical distribution of difference photon counts in Gaussian approximation, from which we obtain the respective POVM. In Sec. III, we conduct the analysis of the double homodyne scheme analogously to the previous section, finding out that the resulting POVM is not well defined for all asymmetry parameters, requiring generalization. In Sec. IV, we generalize the double homodyne POVM to the set of squeezed coherent states. In Sec. V, we apply our results for homodyne and double homodyne detection to calculate the asymptotic secret fraction for an ideal CV-QKD system. Finally, in Sec. VI, we conclude the paper with a brief summary of the results and suggestions for future development.

## II. HOMODYNE DETECTION

We begin with brief discussion of the homodyne measurement setup schematically depicted in Fig. 1. To this end, we assume that the beam splitter is unbalanced and its scattering matrix is chosen to be a real-valued rotation matrix with the transmission and reflection amplitudes,  $t$  and  $r$ , given by

$$t = \cos \theta \equiv C, \quad r = \sin \theta \equiv S. \quad (1)$$

Then the input coherent states of the signal mode and the local oscillator are transformed into the output coherent states as follows

$$|\alpha, \alpha_L\rangle \mapsto |\alpha_1, \alpha_2\rangle, \quad (2)$$

$$\alpha_1 = C\alpha + S\alpha_L, \quad \alpha_2 = -S\alpha + C\alpha_L, \quad (3)$$

so that the joint probability of  $m_1$  and  $m_2$  photon counts for the photodetectors  $D_1$  and  $D_2$  can be computed

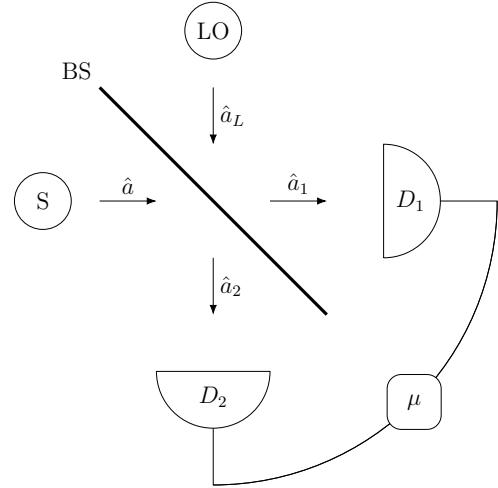


Figure 1: Scheme of a homodyne receiver: S is the source of the signal mode with the annihilation operator  $\hat{a}$ , LO is the source of the reference mode (local oscillator) with the annihilation operator  $\hat{a}_L$ , and BS is the beam splitter with the amplitude transmission and reflection coefficients  $t = \cos \theta$  and  $r = \sin \theta$ , respectively; photodetectors  $D_1$  and  $D_2$  have quantum efficiencies  $\eta_1$  and  $\eta_2$ , and  $\mu \equiv m_1 - m_2$  is the photon count difference.

from the well-known Kelley-Kleiner formula [9] (see also Ref. [8]):

$$\begin{aligned} P(m_1, m_2) &= \langle \alpha_1, \alpha_2 | : \prod_{l=1}^2 \frac{(\eta_l \hat{n}_l)^{m_l} e^{-\eta_l \hat{n}_l}}{m_l!} : | \alpha_1, \alpha_2 \rangle \\ &= \prod_{l=1}^2 \frac{(\eta_l |\alpha_l|^2)^{m_l}}{m_l!} e^{-\eta_l |\alpha_l|^2} \end{aligned} \quad (4)$$

where  $: \dots :$  stands for normal ordering, index  $l \in \{1, 2\}$  labels output ports of the beam splitter,  $\hat{n}_l = \hat{a}_l^\dagger \hat{a}_l$  is the photon number operator,  $m_l$  is the number of photon counts,  $\eta_l$  is the quantum efficiency of the detector  $D_l$ .

We can now introduce the photon count difference

$$\mu = m_1 - m_2 \quad (5)$$

so that its statistical distribution can be written in the form of a product of the two Poisson distributions as follows

$$\begin{aligned} P(\mu) &= \sum_{m_2=\max(0, -\mu)}^{\infty} \frac{(\eta_1 |\alpha_1|^2)^{\mu+m_2}}{(\mu + m_2)!} e^{-\eta_1 |\alpha_1|^2} \\ &\times \frac{(\eta_2 |\alpha_2|^2)^{m_2}}{m_2!} e^{-\eta_2 |\alpha_2|^2}. \end{aligned} \quad (6)$$

It is well known that, by performing summation over  $m_2$ , the probability  $P(\mu)$  reduces to the Skellam distribution

given by [32]

$$\begin{aligned} \mathsf{P}(\mu) &= e^{-\eta_1|\alpha_1|^2} e^{-\eta_2|\alpha_2|^2} \left( \frac{\eta_1|\alpha_1|^2}{\eta_2|\alpha_2|^2} \right)^{\mu/2} \\ &\times I_\mu \left( 2\sqrt{\eta_1\eta_2|\alpha_1|^2|\alpha_2|^2} \right), \end{aligned} \quad (7)$$

where  $I_k(z)$  is the modified Bessel function of the first kind [33].

An important point is that, at sufficiently large  $|\alpha_1|$  and  $|\alpha_2|$ , Poisson distributions that enter Eq. (4) can be approximated using the probability density functions of the normal distributions with mean and variance both equal to the mean of the corresponding Poisson distribution,  $\lambda_i = \eta_i|\alpha_i|^2$ . Then, in the continuum limit where summation in Eq. (6) is replaced with integration, the Skellam distribution (7) can be approximated assuming that the amplitude of the local oscillator,  $|\alpha_L|$ , is large (the strong-LO approximation) and we can apply the convolution formula for Gaussian probability densities

$$\int G(x_1 - x_2; \sigma_1) G(x_2; \sigma_2) dx_2 = G(x_1; \sigma_1 + \sigma_2), \quad (8)$$

$$G(x; \sigma) \equiv \frac{1}{\sqrt{2\pi}\sigma} \exp\left(-\frac{x^2}{2\sigma^2}\right). \quad (9)$$

The above procedure immediately leads to the Gaussian approximation of the form:

$$\mathsf{P}_G(\mu) = G(\mu - \mu_G; \sigma_G), \quad (10)$$

$$\sigma_G = \eta_1|\alpha_1|^2 + \eta_2|\alpha_2|^2 \approx (\eta_1 S^2 + \eta_2 C^2)|\alpha_L|^2, \quad (11)$$

$$\begin{aligned} \mu_G &= \eta_1|\alpha_1|^2 - \eta_2|\alpha_2|^2 \approx (\eta_1 S^2 - \eta_2 C^2)|\alpha_L|^2 \\ &+ CS(\eta_1 + \eta_2)|\alpha_L|\langle \hat{x}_\phi \rangle \end{aligned} \quad (12)$$

where

$$\langle \hat{x}_\phi \rangle \equiv \langle \alpha | \hat{x}_\phi | \alpha \rangle = 2 \operatorname{Re} \alpha e^{-i\phi}, \quad \phi = \arg \alpha_L \quad (13)$$

is the average of the phase-rotated quadrature operator of the signal mode given by

$$\hat{x}_\phi = \hat{a}e^{-i\phi} + \hat{a}^\dagger e^{i\phi}. \quad (14)$$

Alternatively, the probability (10) can be rewritten in the form

$$\mathsf{P}_G(x) = \frac{1}{\sqrt{2\pi}\sigma_G} \exp\left\{-\frac{(x - \langle \hat{x}_\phi \rangle)^2}{2\sigma_x^2}\right\}, \quad (15)$$

where  $x$  is the quadrature variable given by

$$x \equiv \frac{\mu}{(\eta_1 + \eta_2)CS|\alpha_L|} - \frac{\eta_1 S^2 - \eta_2 C^2}{(\eta_1 + \eta_2)CS} |\alpha_L| \quad (16)$$

and  $\sigma_x$  is the quadrature variance

$$\sigma_x \equiv \frac{\eta_1 S^2 + \eta_2 C^2}{[(\eta_1 + \eta_2)CS]^2}. \quad (17)$$

Note that it is rather straightforward to minimize the variance (17) with respect to the transmittance,  $C^2$ , and deduce inequality

$$\sigma_x \geq \sigma_x^{(\min)} = \left( \frac{\sqrt{\eta_1} + \sqrt{\eta_2}}{\eta_1 + \eta_2} \right)^2 \geq 1, \quad (18)$$

where  $\sigma_x$  reaches its minimum value  $\sigma_x^{(\min)}$  at the beam splitter transmittance:  $C^2 = \cos^2 \theta_{\min} = \sqrt{\eta_1}/(\sqrt{\eta_1} + \sqrt{\eta_2})$ .

Our next step is to construct the positive operator-valued measure (POVM) based on the Gaussian approximation  $\mathsf{P}_G$ . To this end, note that the probability (15) is the expectation value of the POVM in the coherent state given by

$$\mathsf{P}_G = \langle \alpha | \hat{\Pi}_G | \alpha \rangle. \quad (19)$$

In the case of the perfectly symmetric homodyne measurement with  $\eta_1 = \eta_2 = 1$  and  $C = S = 1/\sqrt{2}$ , the average (19) takes the form

$$\mathsf{P}_G^{(0)} = \frac{1}{|\alpha_L|} Q_{x,\phi}(\alpha), \quad (20)$$

where  $x = \mu/|\alpha_L|$  and  $Q_{x,\phi}(\alpha)$  is the Husimi  $Q$  distribution for the eigenstate of the phase-rotated quadrature operator (14),  $|x, \phi\rangle$ , given by (see, e.g., the textbook[10])

$$Q_{x,\phi}(\alpha) = |\langle \alpha | x, \phi \rangle|^2 = G(x - \langle \hat{x} \rangle_\phi; 1). \quad (21)$$

Thus, we are led to the well-known result that POVM describing sharp homodyne measurements in the Gaussian approximation is proportional to a projector onto  $|x, \phi\rangle$ :

$$\hat{\Pi}_G^{(0)} = \frac{1}{|\alpha_L|} |x, \phi\rangle \langle x, \phi|, \quad (22)$$

In a more general asymmetric case with  $\eta_1 \neq \eta_2$  and  $C \neq S$ , the Gaussian-shaped probability  $\mathsf{P}_G$  can be represented as a Gaussian superposition written as a convolution of  $P_G^{(0)}$  and a Gaussian function  $G(x, \sigma_N)$ . By using the convolution identity (8), we have

$$\mathsf{P}_G(x) = \sqrt{\frac{\sigma_x}{\sigma_G}} \int G(x - x'; \sigma_N) \mathsf{P}_G^{(0)}(x') dx', \quad (23)$$

$$\sigma_N = \sigma_x - 1 \geq 0, \quad (24)$$

where non-negativity of the variance  $\sigma_N$  stems from Eq. (18). This result immediately gives a general formula for the Gaussian approximation POVM

$$\begin{aligned} \hat{\Pi}_G &= \frac{1}{(\eta_1 + \eta_2)CS|\alpha_L|} \\ &\times \int dx' G(x - x'; \sigma_N) |x', \phi\rangle \langle x', \phi|. \end{aligned} \quad (25)$$

Note that the variance  $\sigma_N$  describes the excess noise that takes into account asymmetry effects.

In the limiting case of perfect homodyne, we have

$$\lim_{\sigma_x \rightarrow 1} G(x; \sigma_N) = \lim_{\sigma_N \rightarrow 0} G(x; \sigma_N) = \delta(x), \quad (26)$$

where  $\delta(x)$  is the Dirac  $\delta$ -function, which is the expected behavior for Eq. (23) to hold. Therefore, the constructed POVM (25) is well-defined for all possible parameters of the homodyne scheme.

The exact and approximate analytical results for photon count difference statistical distributions, given by Eq. (7) and Eq. (10) respectively, are valid for the case where the LO and signal modes are both in the coherent states. In the more general case when the quantum state of the signal mode is  $|\psi\rangle$ , the probability distributions can be evaluated using the relations

$$\begin{aligned} P(\mu; |\psi\rangle) &= \int P_{|\psi\rangle}(\alpha) P(\mu; \alpha) d^2\alpha, \\ P_G(x; |\psi\rangle) &= \langle \psi | \hat{\Pi}_G | \psi \rangle, \end{aligned} \quad (27)$$

where  $P_{|\psi\rangle}(\alpha)$  is the Glauber  $P$  function of the quantum state  $|\psi\rangle$ . In Figs. 2 and 14, we show the results computed for the single-photon Fock states obtained utilizing the well-known expression for the  $P$ -function of Fock states  $|\psi\rangle = |n\rangle$  given by

$$P_{|n\rangle}(\alpha) = \frac{e^{|\alpha|^2}}{n!} \left( \frac{\partial^2}{\partial \alpha \partial \alpha^*} \right)^n \delta^2(\alpha), \quad (28)$$

where  $\delta^2(\alpha) = \delta(\operatorname{Re} \alpha) \delta(\operatorname{Im} \alpha)$ .

Figure 2 displays the photocount difference probabilities computed from the exact and Gaussian probability distributions for the balanced beam splitter at different photodetector efficiencies and signal mode input states. Fig. 2a shows that, in agreement with Eq. (12), asymmetry in photodetection results in the shift of the probability maximum. Note that, at  $\delta\theta = 0$ , the photocount variance (11),  $\sigma_G = (\eta_1 + \eta_2)|\alpha_L|^2/2$ , and the quadrature variance (17),  $\sigma_x = 2/(\eta_1 + \eta_2)$ , are both invariant under transposition of the photodetectors:  $\eta_1 \leftrightarrow \eta_2$ .

The distributions for the single-photon states are depicted in Fig. 2b and, similar to the coherent state, demonstrate the effect of asymmetry-induced shift. Another noticeable effect is that the probability minima between the central and side peaks become less pronounced.

**From Fig. 2 it becomes apparent that performance of Gaussian approximation worsens in presence of asymmetry, which we will quantify in Appendix A.**

Our concluding remark concerns an alternative method to approximate Eq. (7) with a Gaussian-shaped distribution which is based on the asymptotic expansions of the modified Bessel functions. In Appendix B we show that, for the asymmetric homodyne scheme, this method generally leads to ill-posed POVMs because the corresponding quadrature variance appears to be too small leading to negative contribution of the excess noise.

### III. DOUBLE HOMODYNE DETECTION

In the section, we consider the eight-port double homodyne scheme depicted in Fig. 3 (see, e.g., Refs. [10, 34]). This measurement scheme is known to allow reconstructing the Husimi  $Q$  function of the signal state [17] providing complete information about the signal state that may be used in CV-QKD protocols. It should be noted that restoration of the complex amplitude of the state completely serves as the basis for composable security proofs [2, 19].

Figure 3 shows two homodyne setups with elements such as beam splitters  $BS_i$  and photodetectors  $D_{1,2}^{(i)}$  labeled by the index  $i \in \{1, 2\}$ . Referring to Fig. 3, the LO and signal modes are transmitted through the beam splitters  $BS_L$  and  $BS_S$ , respectively. Similar to the analysis performed in the previous section, we assume that the modes are in the coherent states,  $|\alpha\rangle$  and  $|\alpha_L\rangle$ . So, we have the amplitudes

$$\begin{aligned} \alpha^{(1)} &= C_S \alpha, & \alpha^{(2)} &= S_S \alpha, \\ \alpha_L^{(1)} &= C_L \alpha_L, & \alpha_L^{(2)} &= -i S_L \alpha_L, \end{aligned} \quad (29)$$

where  $\alpha^{(i)}$  ( $\alpha_L^{(i)}$ ) stands for the amplitude describing the input coherent state of the signal (LO) mode of the homodyne labeled by the upper index  $i \in \{1, 2\}$ . Note that the phase factor  $-i = e^{-i\pi/2}$  in the expression for  $\alpha_L^{(2)}$  is introduced by a suitably chosen phase shifter placed before the corresponding input port of the beam splitter  $BS_2$ .

Direct calculation shows that the joint statistics of the difference photocount events is determined by the product of the Skellam distributions given by

$$P(\mu_1, \mu_2) = P_1(\mu_1) P_2(\mu_2), \quad \mu_i = m_1^{(i)} - m_2^{(i)}, \quad (30)$$

$$\begin{aligned} P_i(\mu_i) &= e^{-\eta_1^{(i)} |\alpha_1^{(i)}|^2} e^{-\eta_2^{(i)} |\alpha_2^{(i)}|^2} \left( \frac{\eta_1^{(i)} |\alpha_1^{(i)}|^2}{\eta_2^{(i)} |\alpha_2^{(i)}|^2} \right)^{\mu_i/2} \\ &\times I_{\mu_i} (2\sqrt{\eta_1^{(i)} \eta_2^{(i)} |\alpha_1^{(i)}|^2 |\alpha_2^{(i)}|^2}), \end{aligned} \quad (31)$$

where, similar to the homodyne scheme, the amplitudes of the coherent states at the output ports of the beam splitter  $BS_i$

$$\alpha_1^{(i)} = C_i \alpha^{(i)} + S_i \alpha_L^{(i)}, \quad \alpha_2^{(i)} = -S_i \alpha^{(i)} + C_i \alpha_L^{(i)} \quad (32)$$

are expressed in terms of the transmission and reflection amplitudes,  $C_i = \cos \theta_i$  and  $S_i = \sin \theta_i$ .

We can now apply Eqs. (10)–(12) to approximate each Skellam distribution on the right hand side of Eq. (30) and derive the Gaussian approximation for the double homodyne scheme in the form:

$$P_G(\mu_1, \mu_2) = G(\mu_1 - \mu_G^{(1)}; \sigma_G^{(1)}) G(\mu_2 - \mu_G^{(2)}; \sigma_G^{(2)}), \quad (33)$$

$$\sigma_G^{(i)} = (\eta_1^{(i)} S_i^2 + \eta_2^{(i)} C_i^2) |\alpha_L^{(i)}|^2, \quad (34)$$

$$\begin{aligned} \mu_G^{(i)} &= (\eta_1^{(i)} S_i^2 - \eta_2^{(i)} C_i^2) |\alpha_L^{(i)}|^2 + C_i S_i (\eta_1^{(i)} + \eta_2^{(i)}) |\alpha_L^{(i)}| \\ &\times 2 \operatorname{Re} \alpha^{(i)} e^{-i\phi}, \quad \phi = \arg \alpha_L. \end{aligned} \quad (35)$$

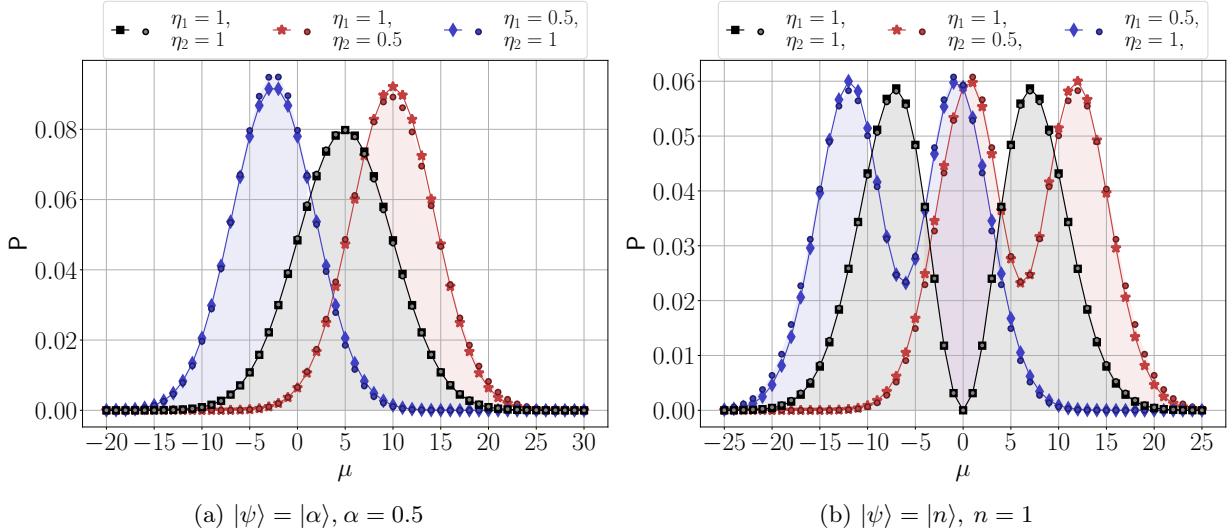


Figure 2: Exact (circle dots) and approximate (solid lines with markers) statistical distributions of photon count difference for the signal mode prepared in (a) the coherent state and in (b) the single photon Fock state computed for different efficiencies at  $|\alpha_L| = 5$  and  $\delta\theta = 0$ .

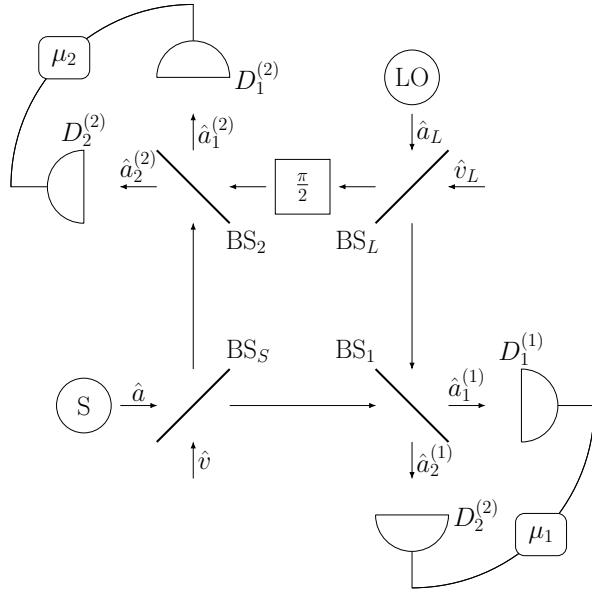


Figure 3: Scheme of an eight port double homodyne receiver.  $S$  is the source of the signal mode  $\hat{a}$ ;  $LO$  is the source of the reference mode  $\hat{a}_L$ ;  $BS_S$  ( $BS_L$ ) is the signal mode (local oscillator) beam splitter;  $\frac{\pi}{2}$  is the quarter wave phase shifter;  $BS_i$  is the beam splitter of  $i$ th homodyne;  $D_{1,2}^{(i)}$  are the photodetectors of the  $i$ th homodyne; and  $\mu_i = m_1^{(i)} - m_2^{(i)}$  is the photon count difference registered by the detectors of  $i$ th homodyne.

Similar to Eq. (15), it is useful to put the probability (33) into the following quadrature form:

$$\begin{aligned} P_G(x_1, x_2) = & \frac{1}{2\pi\sqrt{\sigma_G^{(1)}\sigma_G^{(2)}}} \exp\left\{-\frac{(x_1 - \text{Re } \alpha e^{-i\phi})^2}{\sigma_1}\right. \\ & \left.- \frac{(x_2 - \text{Im } \alpha e^{-i\phi})^2}{\sigma_2}\right\} \end{aligned} \quad (36)$$

where  $x_i$  are the quadrature variables given by

$$\begin{aligned} x_1 = & \frac{1}{2(\eta_1^{(1)} + \eta_2^{(1)})C_1S_1C_S} \\ & \times \left\{ \frac{\mu_1}{|\alpha_L^{(1)}|} - (\eta_1^{(1)}S_1^2 - \eta_2^{(1)}C_1^2)|\alpha_L^{(1)}| \right\}, \end{aligned} \quad (37)$$

$$\begin{aligned} x_2 = & \frac{1}{2(\eta_1^{(2)} + \eta_2^{(2)})C_2S_2S_S} \\ & \times \left\{ \frac{\mu_2}{|\alpha_L^{(2)}|} - (\eta_1^{(2)}S_2^2 - \eta_2^{(2)}C_2^2)|\alpha_L^{(2)}| \right\}, \end{aligned} \quad (38)$$

and relations

$$\sigma_1 = \frac{\sigma_x^{(1)}}{2C_S^2}, \quad \sigma_2 = \frac{\sigma_x^{(2)}}{2S_S^2}, \quad (39)$$

$$\sigma_x^{(i)} = \frac{\eta_1^{(i)}S_i^2 + \eta_2^{(i)}C_i^2}{[(\eta_1^{(i)} + \eta_2^{(i)})C_iS_i]^2} \quad (40)$$

give the quadrature variances  $\sigma_1$  and  $\sigma_2$ .

As in Sec. II, formula (36) giving the  $Q$ -symbol of POVM (see Eq. (19)) provides the starting point for reconstruction of the POVM describing the double homodyne measurements. In the ideal case, where all the beam

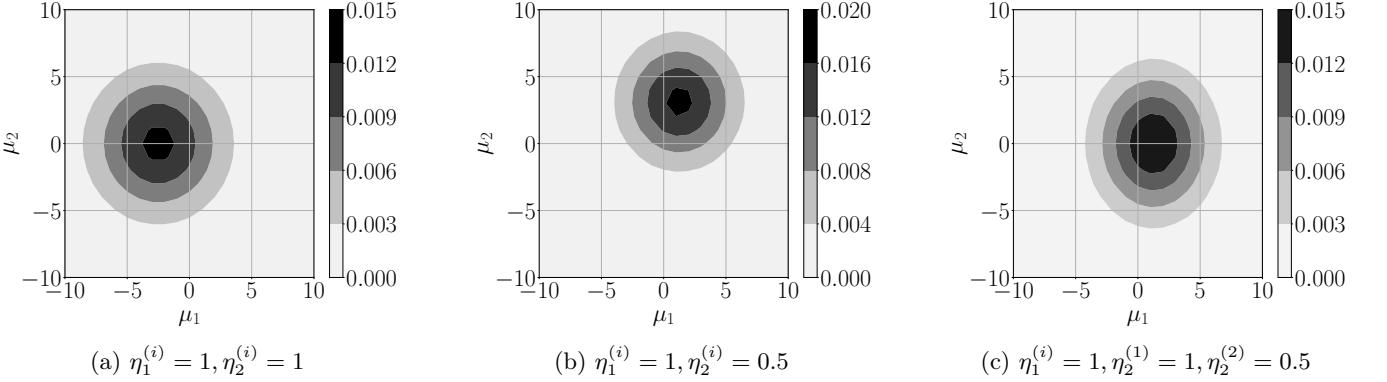


Figure 4: Double homodyne statistical distribution of photocount differences computed from Eq. (30) for various detector efficiencies at  $\alpha = 0.5$  and  $\alpha_L = 5$ . All the beam splitters are taken to be balanced.

splitters are balanced and the photodetection is perfect, we have

$$P_G^{(0)}(x_1, x_2) = \frac{|\langle z|\alpha\rangle|^2}{\pi|\alpha_L|^2}, \quad |\langle z|\alpha\rangle|^2 = e^{-|z-\alpha|^2}, \quad (41)$$

where

$$z = (x_1 + ix_2)e^{i\phi}, \quad x_i = \frac{\mu_i}{|\alpha_L|}. \quad (42)$$

So, the POVM is proportional to a projector onto the coherent state  $|z\rangle \equiv |(x_1 + ix_2)e^{i\phi}\rangle$ :

$$\hat{\Pi}_G^{(0)}(x_1, x_2) = \frac{1}{\pi|\alpha_L|^2}|z\rangle\langle z|. \quad (43)$$

For non-ideal measurements, the probability (36) can be expressed as a Gaussian superposition of the coherent state Husimi functions with the help of the convolution relation (8) as follows

$$\begin{aligned} P_G(x_1, x_2) &= \frac{\sqrt{\sigma_1\sigma_2}}{2\pi\sqrt{\sigma_G^{(1)}\sigma_G^{(2)}}} \int d\beta_1 d\beta_2 G(x_1 - \beta_1; \sigma_N^{(1)}) \\ &\times G(x_2 - \beta_2; \sigma_N^{(2)}) |\langle \beta e^{i\phi} | \alpha \rangle|^2, \quad \beta = \beta_1 + i\beta_2, \end{aligned} \quad (44)$$

where the excess noise variance  $\sigma_N^{(i)}$  is determined by the relation

$$2\sigma_N^{(i)} = \sigma_i - 1. \quad (45)$$

The corresponding expression for the POVM reads

$$\begin{aligned} \hat{\Pi}_G(x_1, x_2) &= \frac{\sqrt{\sigma_1\sigma_2}}{2\pi\sqrt{\sigma_G^{(1)}\sigma_G^{(2)}}} \int d\beta_1 d\beta_2 G(x_1 - \beta_1; \sigma_N^{(1)}) \\ &\times G(x_2 - \beta_2; \sigma_N^{(2)}) |\beta e^{i\phi}\rangle\langle \beta e^{i\phi}|. \end{aligned} \quad (46)$$

An important point is that the results given by Eq. (44) and Eq. (46) are well defined only if  $\sigma_1$  and  $\sigma_2$  are both above unity, so that the excess noise variances (45) are

positive. From Eq. (39), this requires that conditions  $\sigma_x^{(1)} \geq 2C_S^2$  and  $\sigma_x^{(2)} \geq 2S_S^2$  be met.

When the beam splitter  $BS_S$  is balanced  $2C_S^2 = 2S_S^2 = 1$  and inequality (see Eq. (18))

$$\sigma_x^{(i)} \geq \left( \frac{\sqrt{\eta_1^{(i)}} + \sqrt{\eta_2^{(i)}}}{\eta_1^{(i)} + \eta_2^{(i)}} \right)^2 \geq 1 \quad (47)$$

ensures applicability of the expression for the POVM. Otherwise, either  $2C_S^2$  or  $2S_S^2$  will be above unity, and our results are valid only if the value of the corresponding variance  $\sigma_x^{(i)}$  is sufficiently high. For example, at  $\eta_{1,2}^{(i)} = \eta < 1/2$ , the minimal values of  $\sigma_x^{(i)}$  are higher than 2 (see Eq. (47)) and the noise variance will be positive at any disbalance of the signal mode beam splitter because  $\max\{2C_S^2, 2S_S^2\} \leq 2$ . When the noise variance is negative, the POVM reconstruction procedure needs to be generalized. We shall present details on this generalization in the next section. Meanwhile, in the remaining part of this section, we confine ourselves to the cases where  $\sigma_N^{(i)}$  are positive.

The effects of photodetection asymmetry are illustrated in Fig. 4 which presents numerical results for the double homodyne distribution (30) in the photocont difference  $\mu_1-\mu_2$  plane. Referring to Fig. 4, in addition to the shift of the distribution, the asymmetry induced difference of the variances at  $\eta_1^{(1)} + \eta_2^{(1)} \neq \eta_1^{(2)} + \eta_2^{(2)}$  manifests itself as the two dimensional anisotropy of the double homodyne distribution.

#### IV. POSITIVE OPERATOR-VALUED MEASURE AND SQUEEZED STATES

From Eq. (45), the expression for the POVM in the form of incoherent gaussian superposition of coherent states is justified only if both the quadrature variances,  $\sigma_1$  and  $\sigma_2$ , exceed unity. In this section, we show that our procedure employed for derivation of the double homodyne POVM can be suitably generalized by enlarging

a set of the pure states to include the squeezed coherent states

$$|\beta, \zeta\rangle = \hat{D}(\beta)\hat{S}(\zeta)|0\rangle, \quad (48)$$

where  $\hat{D}(\beta)$  ( $\hat{S}(\zeta)$ ) is the displacement (squeezing) operator given by

$$\hat{D}(\beta) = e^{\beta\hat{a}^\dagger - \beta^*\hat{a}}, \quad \hat{S}(\zeta) = e^{\frac{1}{2}(\zeta\hat{a}^{\dagger 2} - \zeta^*\hat{a}^2)}, \quad (49)$$

$\beta$  and  $\zeta$  are the complex-valued amplitude and the squeeze parameter, respectively.

To this end, we consider the case, where the squeeze parameter is given by

$$\zeta = re^{2i\phi}, \quad r \in \mathbb{R} \quad (50)$$

and the non-normalized Husimi distribution for the squeezed state (48) takes the form (see, e.g., the textbook [35])

$$|\langle \beta, re^{2i\phi} | \alpha \rangle|^2 = \frac{1}{\cosh r} \exp \left\{ -\frac{e^{-r}}{\cosh r} \left( \tilde{\beta}_1 e^r - \tilde{\alpha}_1 \right)^2 - \frac{e^r}{\cosh r} \left( \tilde{\beta}_2 e^{-r} - \tilde{\alpha}_2 \right)^2 \right\}, \quad (51)$$

$$\tilde{\beta} = \tilde{\beta}_1 + i\tilde{\beta}_2 = \beta e^{-i\phi}, \quad \tilde{\alpha} = \tilde{\alpha}_1 + i\tilde{\alpha}_2 = \alpha e^{-i\phi}. \quad (52)$$

By using this squeezed state distribution instead of the coherent state one given in Eq. (43), we are led to the expressions for the noise variances modified as follows

$$2\sigma_N^{(1,2)} = \sigma_{1,2} - e^{\pm r} \cosh r. \quad (53)$$

These expressions present the extension of the relations (45) to the case with non-vanishing squeeze parameter. As an immediate consequence of Eq. (53), we find that the conditions for the noise variances to be positive definite can be written in the form of two inequalities

$$4\sigma_N^{(1)} = \delta_1 - e^{2r} \geq 0, \quad 4\sigma_N^{(2)} = \delta_2 - e^{-2r} \geq 0, \quad (54)$$

where the quadrature variance parameters

$$\delta_1 = 2\sigma_1 - 1 = (q+1)\sigma_x^{(1)} - 1 \geq q = \frac{S_S^2}{C_S^2}, \quad (55a)$$

$$\delta_2 = 2\sigma_2 - 1 = (q^{-1}+1)\sigma_x^{(2)} - 1 \geq q^{-1} = \frac{C_S^2}{S_S^2} \quad (55b)$$

are expressed in terms of the disbalance (reflection-to-transmission) ratio of the input beam splitter,  $q$ , and the parameters  $\sigma_x^{(1)}$  and  $\sigma_x^{(2)}$  (see Eq. (40)) that cannot be smaller than unity (see Eq. (47)):  $\sigma_x^{(i)} \geq 1$ .

In our subsequent analysis, we assume without the loss of generality that the reflectance of the input beam splitter  $BS_S$  is larger than its transmittance, so that the disbalance ratio is above unity

$$q = \frac{1 - C_S^2}{C_S^2} = \frac{S_S^2}{C_S^2} \geq 1. \quad (56)$$

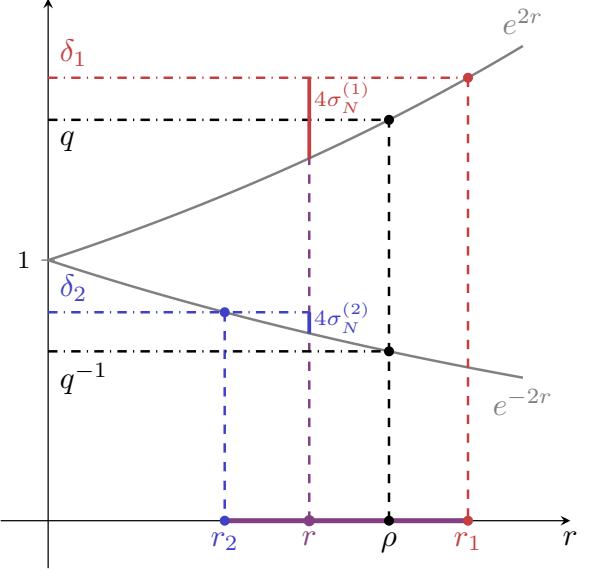


Figure 5: An illustration for the conditions for the noise variances, see Eqs. (54)-(57). Solid grey lines represent the exponents  $e^{\pm 2r}$ . Dashdotted black, red and blue lines are the independent on  $r$  functions  $q$  and  $q^{-1}$ ,  $\delta_1$  and  $\delta_2$  respectively. Solid purple line is the interval of squeezing parameter  $r \in [r_2, r_1]$ ; solid red (blue) line is the magnitude of  $4\sigma_N^{(1)}$  ( $4\sigma_N^{(2)}$ ) at  $r$ .

As is shown in Fig. 5, this implies that the variance  $\delta_1$  is above unity:  $\delta_1 \geq q \geq 1$ , whereas the minimal value of  $\delta_2$  is  $q^{-1} \leq 1$ . It is illustrated that the noise variances are positive provided the squeeze parameter  $r$  is ranged between the endpoints of the interval given by

$$r \in [r_2, r_1], \quad r_1 = \ln^{1/2} \delta_1^{-1/2}, \quad r_2 = \max\{\ln \delta_2^{-1/2}, 0\}. \quad (57)$$

An important point is that the value of the squeeze parameter is not uniquely determined by the conditions (54). We have a unique value of the squeeze parameter only in the limiting case of perfect homodyne measurements with  $\sigma_x^{(1)} = \sigma_x^{(2)} = 1$  and  $\delta_1 = \delta_2^{-1} = q$ . In this case, the squeeze parameter is unambiguously defined

$$r_1 = r_2 = \rho = \frac{1}{2} \ln q = \ln \sqrt{\frac{1 - C_S^2}{C_S^2}} \quad (58)$$

and the probability (36) expressed in terms of the distribution (51)

$$P_G^{(1)}(x_1, x_2) = \frac{\cosh \rho}{2\pi |\alpha_L^{(1)} \alpha_L^{(2)}|} |\langle \beta e^{i\phi}, \rho e^{2i\phi} | \alpha \rangle|^2, \quad (59)$$

$$\beta = e^{-\rho} x_1 + i e^{\rho} x_2 \quad (60)$$

yields the POVM

$$\hat{\Pi}_G^{(1)}(x_1, x_2) = \frac{\cosh \rho}{2\pi |\alpha_L^{(1)} \alpha_L^{(2)}|} \times |\beta e^{i\phi}, \rho e^{2i\phi} \rangle \langle \beta e^{i\phi}, \rho e^{2i\phi}|, \quad (61)$$

which is proportional to the pure squeezed state  $|\beta e^{i\phi}, \rho e^{2i\phi}\rangle$ . The result (58) was reported in Ref. [36].

When the homodyne measurements are not perfect due to unbalanced beam splitters and nonideal photodetectors, the squeeze parameter is no longer uniquely defined. So, in the interval (57), we have the decomposition of the probability (36)

$$\begin{aligned} P_G(x_1, x_2) = & \frac{\sqrt{\sigma_1 \sigma_2}}{2\pi \sqrt{\sigma_G^{(1)} \sigma_G^{(2)}}} \\ & \times \int d\beta_1 d\beta_2 G(x_1 e^{-r} - \beta_1; \sigma_N^{(1)}(r) e^{-2r}) \\ & \times G(x_2 e^r - \beta_2; \sigma_N^{(2)}(r) e^{2r}) |\langle \beta e^{i\phi}, r e^{2i\phi} | \alpha \rangle|^2 \end{aligned} \quad (62)$$

that varies with the squeeze parameter  $r$ . Similarly, the corresponding POVM

$$\begin{aligned} \hat{\Pi}_G(x_1, x_2) = & \frac{\sqrt{\sigma_1 \sigma_2}}{2\pi \sqrt{\sigma_G^{(1)} \sigma_G^{(2)}}} \\ & \times \int d\beta_1 d\beta_2 G(x_1 e^{-r} - \beta_1; \sigma_N^{(1)}(r) e^{-2r}) \\ & \times G(x_2 e^r - \beta_2; \sigma_N^{(2)}(r) e^{2r}) \\ & \times |\beta e^{i\phi}, r e^{2i\phi} \rangle \langle \beta e^{i\phi}, r e^{2i\phi}| \end{aligned} \quad (63)$$

decomposed into the Gaussian incoherent superposition of the pure squeezed states explicitly depends on the value of  $r$ . Our analysis suggests that the ambiguity (non-uniqueness) of the Gaussian representation (63) for the double-homodyne POVM is a universal feature coming into play in the presence of imperfections. Even when  $\delta_2 \geq 1$  and the coherent-state representation (46) for the POVM is well-defined, the photocount statistics can be reproduced using the squeezed-state representation (63) with  $0 < r \leq r_1$ . One of the way to make the Gaussian POVM decomposition unique is to place additional constraints on the noise variances that would fix the value of the squeeze parameter. For example, the squeeze parameter would take the minimal (maximal) value:  $r = \min\{r_1, r_2\}$  ( $r = \max\{r_1, r_2\}$ ) provided the constraint requires minimization of the noise variance  $\sigma_N^{(2)}$  ( $\sigma_N^{(1)}$ ).

## V. INCORPORATING MEASUREMENT IMPERFECTIONS INTO THE GG02 CV-QKD PROTOCOL

In this section, we apply our results on asymmetric measurements to analyze the Gaussian-modulated coherent state (GMCS, or GG02 [1]) CV-QKD protocol. We compute the mutual information, Holevo information, and asymptotic secret fraction (secure key rate per symbol) under both trusted and untrusted noise scenario, to assess the impact of measurement asymmetry on the protocol's security.

In the GG02 protocol the mutual information between Alice and Bob when Bob performs homodyne detection is given by

$$I_{AB}^H = \frac{1}{2} \log \left[ 1 + \frac{4TV_A}{\sigma_x + 2\xi} \right], \quad (64)$$

where  $T$  is the channel transmission,  $\xi$  is the channel noise variance,  $V_A$  is Alice's modulation variance, and  $\sigma_x$  is given by Eq. (17). If Bob used double homodyne detection, mutual information takes the form

$$I_{AB}^{DH} = \frac{1}{2} \sum_i \log \left[ 1 + \frac{2TV_A}{\sigma_i + \xi} \right], \quad (65)$$

where  $\sigma_i$  are defined by Eq. (40). The details of these derivations are given in Appendix C.

**First, we will calculate Holevo information in the trusted noise scenario. [add desc]** We will use the fact that prepare-and-measure (PM) and entanglement-based (EB) protocols are equivalent (see App. C), allowing us to calculate Holevo information from the two mode squeezed vacuum state covariance matrix. After transmitting through noisy channel (see Ref. [37]) covariance matrix reads

$$\begin{aligned} \Sigma_{AB}^{EB} = & \begin{pmatrix} V\mathbb{I} & \sqrt{T(V^2-1)}\sigma_Z \\ \sqrt{T(V^2-1)}\sigma_Z & [T(V-1)+1+2\xi]\mathbb{I} \end{pmatrix} \\ \equiv & \begin{pmatrix} a\mathbb{I} & c\sigma_Z \\ c\sigma_Z & V_B\mathbb{I} \end{pmatrix}, \end{aligned} \quad (66)$$

where  $\mathbb{I} = \text{diag}(1, 1)$ ,  $\sigma_Z = \text{diag}(1, -1)$ , and

$$V = 1 + 4V_A. \quad (67)$$

Eve's entropy,  $S_E = S_{AB}$ , is calculated from the symplectic eigenvalues of  $\Sigma_{AB}^{EB}$  as [38]

$$\begin{aligned} \nu_{1,2} = & \frac{1}{2} (z \pm [V_B - a]), \\ z = & \sqrt{(a + V_B)^2 - 4c^2}. \end{aligned} \quad (68)$$

If covariance matrix of system  $AB$  is in the form

$$\sigma_{AB} = \begin{pmatrix} A & C \\ C^T & B \end{pmatrix}, \quad (69)$$

noisy Gaussian measurement of system  $B$  transforms  $A$  mode as follows [39],

$$\sigma_{A|B}^{(m)} = A - C(B + \sigma_{\Pi}^{(m)})^{-1}C^T, \quad m \in \{H, DH\} \quad (70)$$

where  $\sigma_{\Pi}^{(m)}$  is the POVM covariance matrix, deduced from Eq. (15) and Eq. (36) for homodyne and double homodyne respectively as

$$\sigma_{\Pi}^H = \mathbb{I} + \sigma_N \Pi_{qp}, \quad (71)$$

$$\sigma_{\Pi}^{DH} = \begin{pmatrix} 2\sigma_1 - 1 & 0 \\ 0 & 2\sigma_2 - 1 \end{pmatrix}, \quad (72)$$

where  $\Pi_q = \text{diag}(1, 0)$  and  $\Pi_p = \text{diag}(0, 1)$ . If Bob uses homodyne detection, we arrive at conditional matrix with symplectic eigenvalue

$$\Sigma_{A|B}^H = a\mathbb{I} - \frac{c^2}{V_B + \sigma_N}\Pi_{q,p}, \quad (73)$$

$$\nu_3^H = \sqrt{a\left(a - \frac{c^2}{V_B + \sigma_N}\right)}. \quad (74)$$

If Bob uses double homodyne measurement, we have

$$\Sigma_{A|B}^{\text{DH}} = \begin{pmatrix} a - \frac{c^2}{V_B + 2\sigma_1 - 1} & 0 \\ 0 & a - \frac{c^2}{V_B + 2\sigma_2 - 1} \end{pmatrix}, \quad (75)$$

$$\nu_3^{\text{DH}} = a\sqrt{\frac{(V_B + 2\sigma_1 - 1 - \frac{c^2}{a})(V_B + 2\sigma_2 - 1 - \frac{c^2}{a})}{(V_B + 2\sigma_1 - 1)(V_B + 2\sigma_2 - 1)}} \quad (76)$$

Note that in this scenario generalization to double homodyne POVM in the form of projectors onto squeezed coherent states Eq. (63) from projectors onto coherent states Eq. (46) is not required as it is not necessary to separate noise part of covariance matrix.

The Holevo information is calculated as

$$\begin{aligned} \chi_{EB} &\equiv S_E - S_{E|B} = S_{AB} - S_{A|B} \\ &= \sum_{i=1,2} g(\nu_i) - g(\nu_3), \end{aligned} \quad (77)$$

where

$$g(\nu) = \frac{\nu+1}{2} \log \frac{\nu+1}{2} - \frac{\nu-1}{2} \log \frac{\nu-1}{2}, \quad (78)$$

with appropriate substitution of  $\nu_i$  depending on the measurement scheme, and the asymptotic secret fraction is then calculated as

$$R = \beta I_{AB} - \chi_{EB}, \quad (79)$$

where  $\beta$  is the reconciliation efficiency.

The effects of detection asymmetry on mutual information, Holevo information, and the asymptotic secure key rate are illustrated in Fig. 6 for homodyne detection and Fig. 7 for double homodyne detection. Our numerical results for the homodyne case are inconsistent with Ref. [24]: the dependence of the asymptotic secret fraction on the beam splitter transmittance deviation is maximal for the symmetric case, but our results suggest otherwise. This is due our attribution of asymmetry noise to  $S_{A|B}$ , while in Ref. [24] it is attributed to Eve, modifying  $S_{AB}$ .

The dependence of the asymptotic secure key rate on channel length in the presence of asymmetrical detection is shown in Fig. 8. These results indicate that in the untrusted noise scenario, asymmetric homodyne detection offers slight advantage at large distance over ideal, symmetric detection, which maximizes the Holevo information. In contrast, double homodyne detection consistently yields better performance. Yet, due to the way

$\nu_3^{\text{DH}}$  is dependent on noise variances, at large distances asymmetry results in lesser secure key rate. At smaller distances, where  $T \approx 1$ , asymmetry reduces the secure key rate of both homodyne and double homodyne detection. **LITERATURE WILL BE HERE**

Now we will move on to untrusted noise scenario [add desc]. Conditional entropy is calculated from symplectic eigenvalues

$$\mu_3^H = \sqrt{a\left(a - \frac{c^2}{V_B}\right)}, \quad (80)$$

$$\mu_3^{\text{DH}} = a - \frac{c^2}{V_B + 1}. \quad (81)$$

Joint entropy will be calculated from symplectic eigenvalues of the matrix

$$\Sigma_{AB}^{\text{EB}'} \begin{pmatrix} a\mathbb{I} & c\sigma_Z \\ c\sigma_Z & V_B\mathbb{I} + \sigma_\eta^{(m)} \end{pmatrix}, \quad (82)$$

where  $\sigma_\eta^{(m)}$  is the noise part of  $\sigma_\Pi^{(m)}$ . Explicitly, per Eq. (71) and (72),

$$\sigma_\eta^H = \sigma_N \Pi_{qp}, \quad (83)$$

$$\sigma_\eta^{\text{DH}} = \begin{pmatrix} 2\sigma_1 - 1 - e^{2r} & 0 \\ 0 & 2\sigma_2 - 1 - e^{-2r} \end{pmatrix}. \quad (84)$$

Note that Holevo information for double homodyne detection is explicitly dependent on squeezing parameter  $r$  that lies in the interval (57). For calculations, we will numerically find  $r$  that maximizes Holevo information. **Describing 9, 10, 11.**

## VI. CONCLUSION AND DISCUSSION

In this paper, we have studied the effects of asymmetry introduced by unbalanced beam splitters and different efficiencies of the photodetectors in photocount statistics of homodyne and double homodyne detection. We have performed numerical analysis to explore the applicability range for the Gaussian approximation derived by approximating the Poisson distributions using the probability density functions of normally distributed random variables.

By using the Gaussian approximation, we have developed the method for constructing POVMs of homodyne-based schematics. This method is applied to deduce the expression for the POVM that generalizes the well-known results to the case of the asymmetric homodyne detection. This POVM is found to be well defined across all parameter settings of the scheme with the excess noise variance modified by the asymmetry and incorporates the effect of asymmetry-induced shift of the mean value (these effects are illustrated in Fig. 2).

We have used the total variational distance (A5),  $D_P$ , to quantify the statistical distance between the Skellam and Gaussian distributions and evaluate the accuracy of

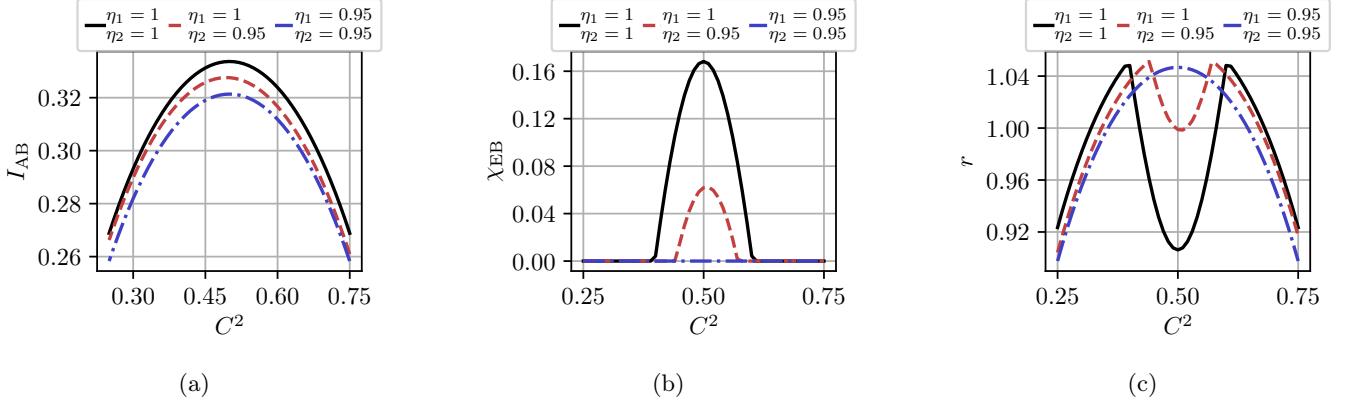


Figure 6: (a) Mutual information, (b) Holevo information, and (c) asymptotic secret fraction using homodyne measurement as functions of the beam splitter transmission, for various detector efficiencies at  $V_A = 1, T = 0.95, \xi = 0.5 \cdot 10^{-3}, \beta = 0.95$

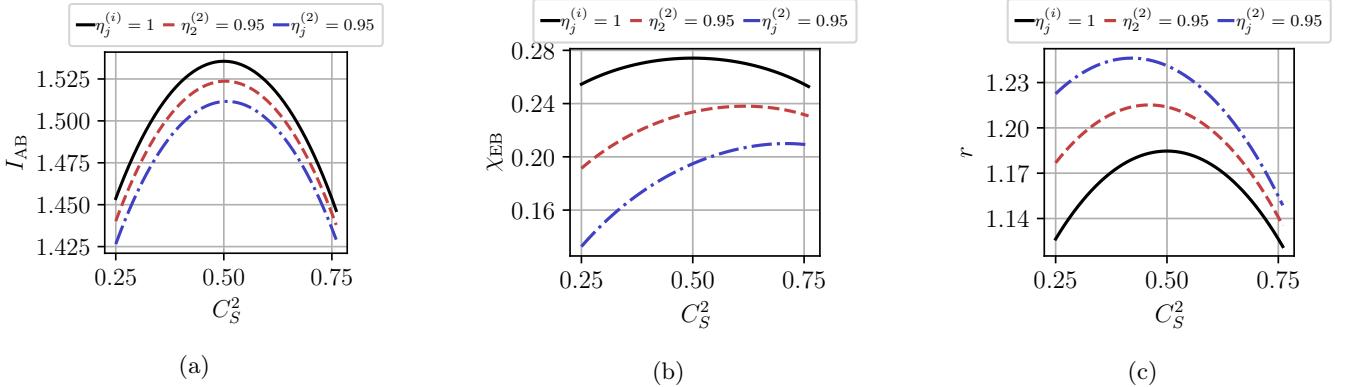


Figure 7: (a) Mutual information, (b) Holevo information, and (c) asymptotic secret fraction using double homodyne detection as functions of the signal beam splitter transmission. All other beam splitters are assumed to be balanced. Results are shown for various detector efficiencies; efficiencies not specified in the legend are taken to be unity. Parameters:  $V_A = 1, T = 0.95, \xi = 0.5 \cdot 10^{-3}, \beta = 0.95$ . (Trusted noise)

the Gaussian approximation across various asymmetry parameters. We find that, for the signal mode prepared in the coherent state  $|\alpha\rangle$ , the distance increases with  $|\alpha|$  (see Fig. 12a) and, in the small-amplitude region with  $|\alpha| \leq 0.1$ , the maximum value of the distance can be estimated at about 0.13 reached when the local oscillator amplitude  $|\alpha_L|$  is in the vicinity of unity. At  $|\alpha_L| > 1$ , the distance rapidly drops with the LO amplitude. For example, at  $|\alpha| = 0.5$ , the distance falls below 0.05 when the ratio  $|\alpha_L|/|\alpha|$  exceeds five (see Fig. 12b).

We have found that (see Figs. 13 and 14) dependence of the distance on the photodetector efficiencies (the imbalance angle of the beam splitter) is sensitive to the imbalance of the beam splitter (photodetector efficiencies). Thus, by varying parameters of BS we may achieve the best approximation for given quantum efficiencies and vice versa. In general, our findings indicate that the quality of the agreement between the exact and approximate photocount distributions varies with the degree of asym-

metry.

Our formalism allows us to easily analyze various homodyne-based schematics. It can be extended to describe more complex measurement systems. We have demonstrated this by performing an analysis for the eight-port asymmetric double homodyne scheme. For this scheme, we have deduced the Gaussian approximation (see Eqs. (33)–(35)) and the corresponding POVM expressed in terms of the projectors onto coherent states (see Eq. (46)). As is shown in Fig. 4, the asymmetry induces effects such as shifts and anisotropy of the distributions in the photocount difference plane.

As shown in the main text, the applicability of double homodyne POVM in the form (46) may be broken provided that the beam splitter for the signal mode is unbalanced. To resolve this, an extension to the set of squeezed coherent states is needed (see Eq. (63)), leading to explicit dependency of POVM on the squeezing parameter, which is not defined unambiguously. This implies

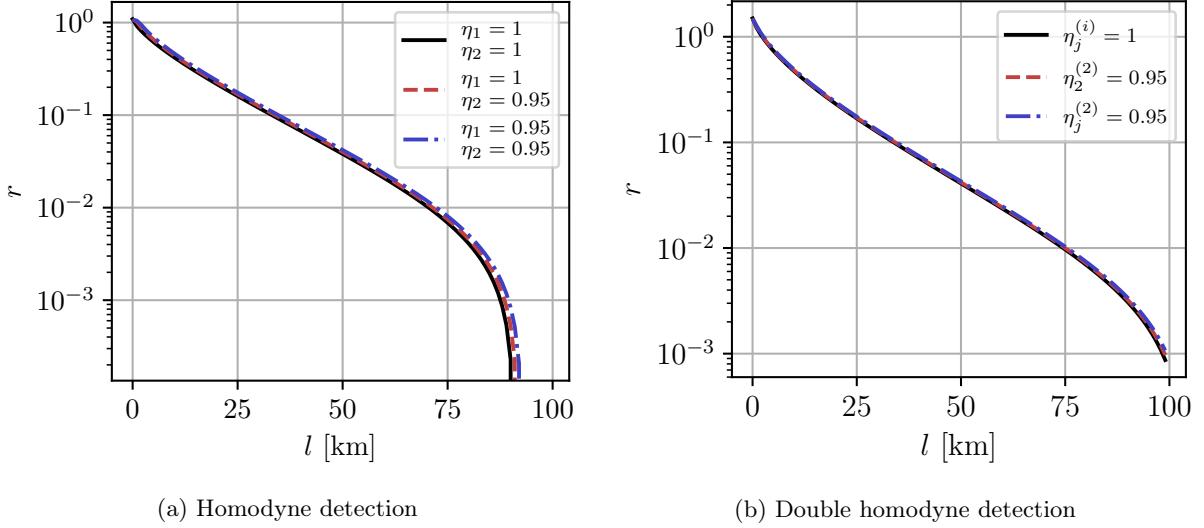


Figure 8: Asymptotic secret fraction as a function of channel length computed for (a) homodyne detection and (b) double homodyne detection, shown for various detector efficiencies. Parameters are  $V_A = 1, T = 0.95, \xi = 0.5 \cdot 10^{-3}, \beta = 0.95$ . The losses are assumed to be 20 dB per 100 km. (Trusted noise)

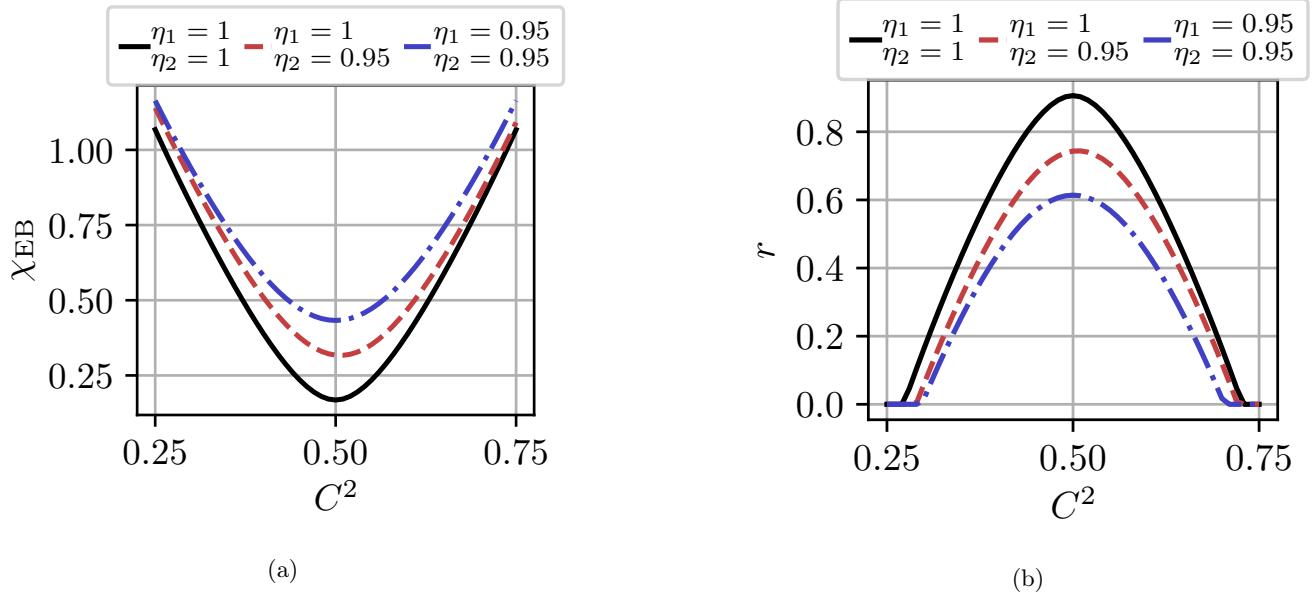


Figure 9: (a) Holevo information and (b) asymptotic secret fraction using homodyne measurement as functions of the beam splitter transmission, for various detector efficiencies at  $V_A = 1, T = 0.95, \xi = 0.5 \cdot 10^{-3}, \beta = 0.95$  (Untrusted noise)

that there are, generally, infinitely many POVMs representing one set of the parameters of double homodyne scheme, and so the squeezing parameter needs additional rule to make the POVM well-defined. Practically, however, ambiguousness of POVM does not matter, as all of their averages represent the same photon count difference statistical distribution (33) or, equivalently, quadrature distribution (36). This is supported by our calculations for mutual information between Alice and Bob in Gaus-

sian modulated coherent states CV-QKD protocol (for a comprehensive review see, e.g., Ref. [37]). As we have shown, choosing any POVM in the form (63) would yield the same result for secret fraction, as it is dependent only on variances of quadrature distribution (36).

Generalization to complex transmission and reflection coefficients for both homodyne and double homodyne is trivial. For homodyne, this would entail changing the definition of  $\phi$  in Eq. (13) to  $\phi' \equiv \phi + \phi_t - \phi_r$ ,

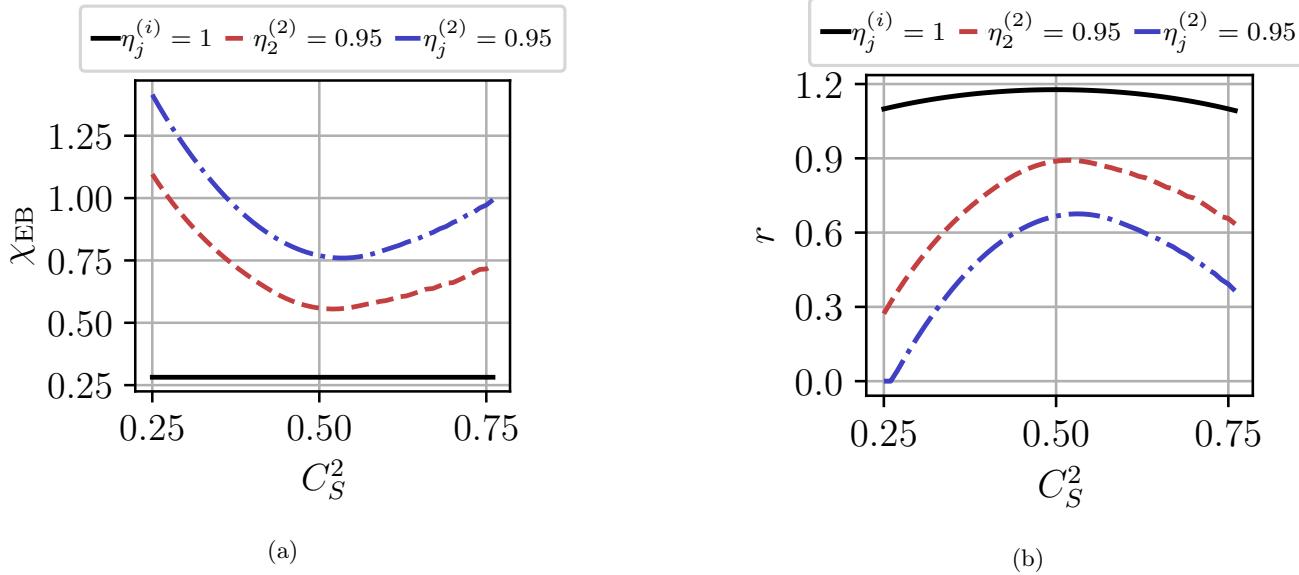


Figure 10: (a) Holevo information and (b) asymptotic secret fraction using double homodyne detection as functions of the signal beam splitter transmission. All other beam splitters are assumed to be balanced. Results are shown for various detector efficiencies; efficiencies not specified in the legend are taken to be unity. Parameters:

$$V_A = 1, T = 0.95, \xi = 0.5 \cdot 10^{-3}, \beta = 0.95. \quad (\text{Untrusted noise})$$

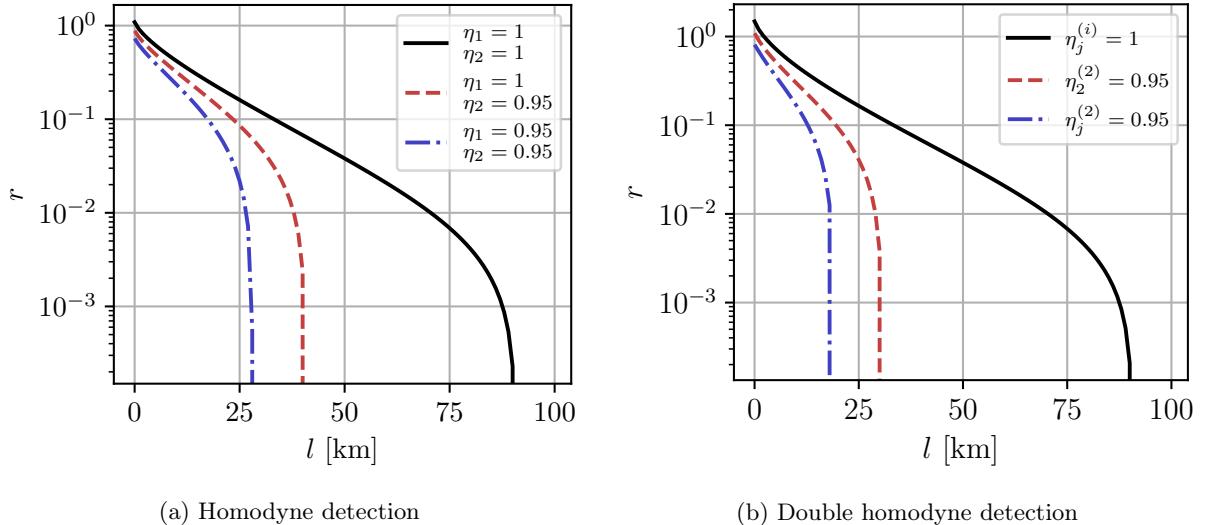


Figure 11: Asymptotic secret fraction as a function of channel length computed for (a) homodyne detection and (b) double homodyne detection, shown for various detector efficiencies. Parameters are  $V_A = 1, T = 0.95, \xi = 0.5 \cdot 10^{-3}, \beta = 0.95$ . The losses are assumed to be 20 dB per 100 km. (**Untrusted noise**)

where  $\phi_t$  and  $\phi_r$  are phases of complex transmission and reflection coefficients, respectively, and the definition of quadrature variable (16) would remain unchanged. For double homodyne, introducing phases as  $\phi_{r,t}^{(j)}, i \in \{1, 2, S, L\}$ , a change of  $\text{Re } \alpha e^{-i\phi} \mapsto \text{Re } \alpha e^{-i(\phi - \phi_t^{(L)} - \phi_t^{(S)})}$  and  $\text{Im } \alpha e^{-i\phi} \mapsto \text{Im } \alpha e^{-i(\phi - \phi_r^{(L)} - \phi_r^{(S)})}$  is needed in Eq. (36), leaving quadrature variables (37), (38) un-

changed if  $\phi_r^{(1)} + \phi_t^{(1)} = \phi_r^{(2)} + \phi_t^{(2)} = 0$ .

Note that, according to Appendix B, an alternative method based on the Gaussian approximation for the Bessel function that enters the Skellam distribution generally leads to results that are not suitable for dealing with asymmetry-induced effects in homodyne detection.

Our concluding remark is to put our results in the context of CV-QKD security [40]. The asymmetry ef-

fects described in the paper, such as deviations from the ideal 50:50 beam splitter ratio and mismatched detector efficiencies, introduce vulnerabilities into CV-QKD systems. These vulnerabilities can be exploited by adversaries through attack strategies such as the wavelength attack [27, 28] and the homodyne detector blinding [29] and saturation [30]. The wavelength attack leverages the wavelength-dependent coupling ratio of fiber beam splitters and can be countered by using proper spectral filtering. Blinding and saturation attacks exploit the saturation behavior of homodyne detectors, and their effectiveness is amplified by receiver imbalance. If the splitting ratio deviates from ideal one, an injected bright pulse more easily displaces the detector output, facilitating saturation and biasing excess noise estimation.

In the main text, we analyzed how measurement asymmetry impacts the performance of CV-QKD system in the untrusted noise scenario, where asymmetry noise is accessible to Eve. In this case, even relatively small asymmetry significantly reduces maximum channel length (see Fig. 8). In trusted-noise CV-QKD [26], if Alice and Bob are unaware of detector's arms asymmetry, they may misinterpret the increased variance as channel excess noise rather than trusted detector imperfection. This leads to an overestimation of channel excess noise and an underestimation of trusted detector noise. Similar to blinding attacks, this vulnerability can be mitigated by inserting attenuators to balance the detection scheme.

Despite the existence of countermeasures for the attacks described, implementing analytical corrections based on the formalism developed in this paper would be preferable for accurate security assessment and performance optimization.

## ACKNOWLEDGEMENTS

The work was supported by the Russian Science Foundation (project No. 24-11-00398).

## Appendix A: Statistical distance between Gaussian approximation and Skellam distribution

In this Appendix, we study the performance of Gaussian approximation for the statistics of photon count difference (10):

$$P_G(\mu) = G(\mu - \mu_G; \sigma_G), \quad (A1)$$

$$\sigma_G = \eta_1|\alpha_1|^2 + \eta_2|\alpha_2|^2 \approx (\eta_1 S^2 + \eta_2 C^2)|\alpha_L|^2, \quad (A2)$$

$$\begin{aligned} \mu_G &= \eta_1|\alpha_1|^2 - \eta_2|\alpha_2|^2 \approx (\eta_1 S^2 - \eta_2 C^2)|\alpha_L|^2 \\ &+ CS(\eta_1 + \eta_2)|\alpha_L|\langle \hat{x}_\phi \rangle \end{aligned} \quad (A3)$$

by comparing it with the exact statistics of difference events governed by the Skellam distribution (7):

$$\begin{aligned} P(\mu) &= e^{-\eta_1|\alpha_1|^2} e^{-\eta_2|\alpha_2|^2} \left( \frac{\eta_1|\alpha_1|^2}{\eta_2|\alpha_2|^2} \right)^{\mu/2} \\ &\times I_\mu(2\sqrt{\eta_1\eta_2|\alpha_1|^2|\alpha_2|^2}), \end{aligned} \quad (A4)$$

both repeated here for ease. We will limit our numerical results to the coherent signal state only, except in cases where the curves show sufficiently distinct differences.

We evaluate the statistical distance between the probability distributions using the total variational distance that can be computed as half of the  $L^1$  distance

$$D_P \equiv D(P, P_G) \equiv \frac{1}{2} \sum_{\mu=-\infty}^{\infty} |P(\mu) - P_G(\mu)|. \quad (A5)$$

Note that, according to Eq. (A5),  $\mu$  takes integer values and we evaluate the distance between the probability mass functions, whereas the normalization condition for the Gaussian function (A1)

$$\int_{-\infty}^{\infty} P_G(\mu) d\mu = 1 \quad (A6)$$

implies applicability of the continuum limit. For integer  $\mu$ , the integral on the left hand side of Eq. (A6) should be replaced with a sum and we have the relation

$$\sum_{\mu=-\infty}^{\infty} P_G(\mu) = \vartheta_3(\pi\mu_G, e^{-2\pi^2\sigma_G}) \equiv N_G \quad (A7)$$

where  $\vartheta_3$  is the Jacobi elliptic theta function [33].

In the applicability region of the continuum limit, the normalization constant  $N_G$  is close to unity. The numerical analysis shows that  $|N_G - 1| \leq 10^{-4}$  at  $2\sigma_G \geq 1$ . The latter gives the condition for the LO amplitude

$$|\alpha_L| \geq \frac{1}{\sqrt{2(\eta_1 S^2 + \eta_2 C^2)}} \equiv \alpha_N \quad (A8)$$

which ensures both applicability of the continuum limit and proper normalization of the Gaussian approximation. In our calculations, the probability  $P_G$  will be numerically corrected by introducing the factor  $N_G^{-1}$  provided that  $|\alpha_L|$  is below the "renormalization point"  $\alpha_N$ .

The curves presented in Fig. 12 illustrate how the accuracy of the Gaussian approximation is affected by the signal and LO amplitudes,  $|\alpha|$  and  $|\alpha_L|$ . More specifically, in Fig. 12a (Fig. 12b), the statistical distance is numerically evaluated as a function of the amplitude  $|\alpha|$  ( $|\alpha_L|$ ) at different values of the photodetectors efficiencies provided that the value of the other amplitude  $|\alpha_L|$  ( $|\alpha|$ ) is fixed.

Referring to Fig. 12a, the curves behave as expected: given the LO amplitude  $|\alpha_L|$ , the distance monotonically increases with  $|\alpha|$ . It is shown that, at  $|\alpha_L| = 5$  and

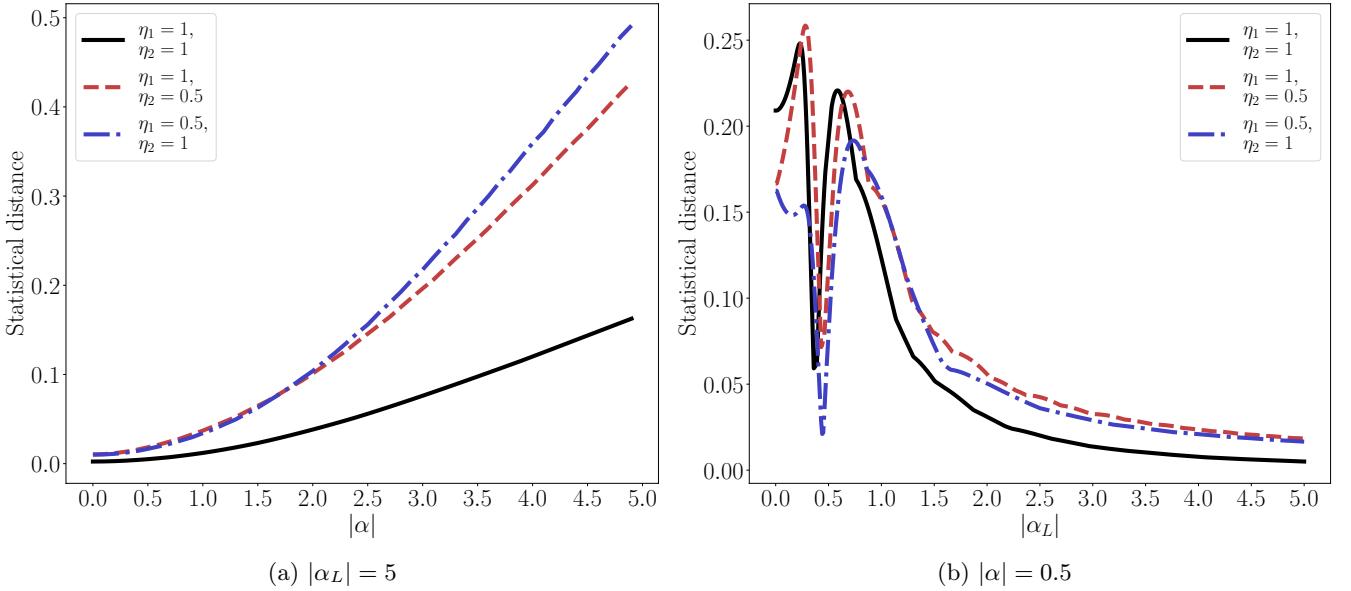


Figure 12: Statistical distance  $D_P = D(P, P_G)$  as a function of (a) signal amplitude and (b) LO amplitude at different detector efficiencies.

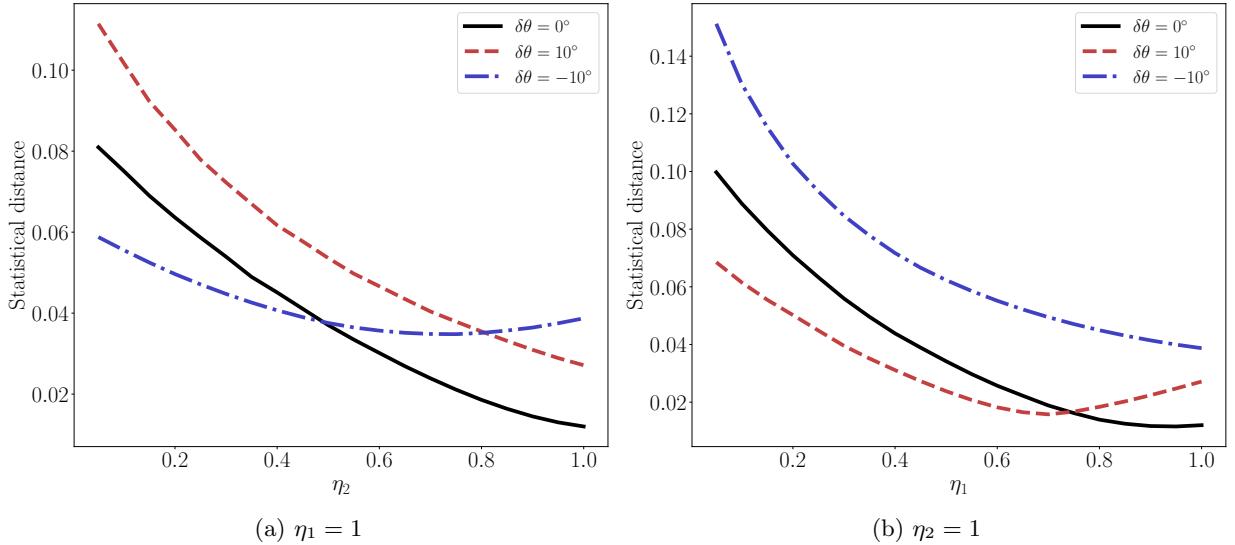


Figure 13: Statistical distance  $D_P = D(P, P_G)$  as a function of photodetector efficiency (a)  $\eta_2$  at  $\eta_1 = 1$  and (b)  $\eta_1$  at  $\eta_2 = 1$  for different values of the beam splitter disbalance angle  $\delta\theta$  (see eq. (A9)). The amplitudes are  $|\alpha| = 1$  and  $|\alpha_L| = 5$ .

$|\alpha| > 1$ , the perfectly symmetric homodyne presents the case with minimal distance,  $D_P$ , while in the presence of asymmetry, the curves exhibit a rapid growth and the quality of the Gaussian approximation rapidly degrades to the point, where  $D_P > 0.1$ , so it is not useful for its intended purpose.

When it comes to dependencies of the statistical distance on the LO oscillator amplitude computed at fixed value of  $|\alpha|$ , the above results suggest that the smaller the amplitude  $|\alpha|$  the better the accuracy of the Gaussian approximation. We can also expect the distance will

be small provided that  $|\alpha_L|$  is large and the strong-LO approximation is applicable.

Referring to Fig. 12b, the curves evaluated at  $|\alpha| = 0.5$  display a non-monotonic behavior with two local maxima in the weak LO range where  $|\alpha_L| < 1$ . By contrast, after the second maximum at  $|\alpha_L| > 1$ , the distance falls with the LO amplitude and it drops below 0.05 at  $|\alpha_L| > 2$ .

Note, that, when  $|\alpha| < 0.1$  and the signal mode state is close to the vacuum state, the two local maxima of  $D_P$  can be estimated to be slightly above 0.08 and 0.1, respectively. So, in this case, the distribution (10)

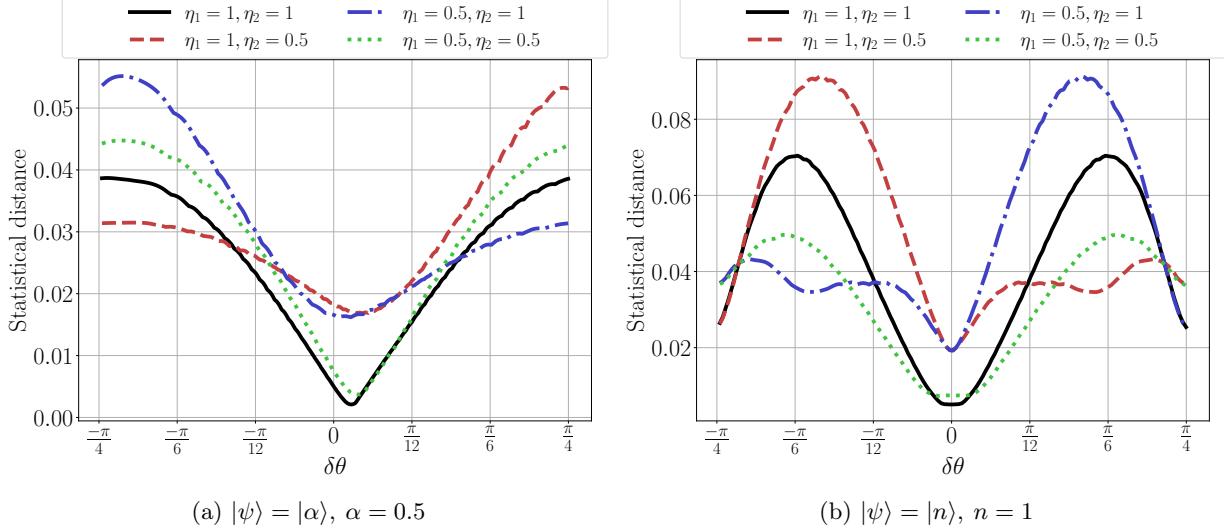


Figure 14: Statistical distance  $D_P = D(\mathbf{P}, \mathbf{P}_G)$  as a function of the beam splitter disbalance angle,  $\delta\theta$ , for the signal mode prepared in (a) the coherent state and in (b) the single photon Fock state at different efficiencies with  $|\alpha_L| = 5$ .

might be regarded as a reasonable approximation even in the weak LO range where the probability  $P_G$  approaches the close neighborhood of the singular limit,  $\lim_{|\alpha_L| \rightarrow 0} P_G(\mu) = \delta(\mu)$ .

From Fig. 12b, it can also be seen that the distance vs LO amplitude dependence that can be used as a tool to characterize the applicability region of the strong-LO approximation is nearly insensitive to asymmetry. In other words, the latter does not produce noticeable effects on the accuracy of the approximation.

The parameters describing the photodetection asymmetry are the efficiencies  $\eta_1$  and  $\eta_2$ . The curves plotted in Fig. 12 are computed at different values of the efficiencies.

To quantify deviation of the beam splitter transmission and reflection amplitudes from the balanced 50 : 50 values  $t = \cos \theta = r = \sin \theta = 1/\sqrt{2}$  at the angle  $\theta = \pi/4$ , we introduce the beam splitter *disbalance angle* given by

$$\delta\theta \equiv \frac{\pi}{4} - \theta. \quad (\text{A9})$$

In Figure 13 we plot the distance against the efficiency of the photodetector assuming that the other photodetector is perfect. The curves are evaluated at different values of the disbalance angle (A9).

In Fig. 14 the statistical distance vs disbalance angle curves are presented for coherent and one-photon signal states. These curves illustrate how the beam splitter disbalance and the photodetector efficiencies influence the accuracy of the Gaussian approximation. The distance is shown to be minimal in the vicinity of the balanced beam splitter point with a vanishing disbalance angle,  $\delta\theta = 0$ . The efficiency dependence of the distance is shown to decrease monotonically at  $\delta\theta = 0$ . In contrast, for disbalanced beam splitter, this dependence can reveal non-monotonic behavior.

## Appendix B: Gaussian approximation from Skellam distribution

The derivation procedure for the Gaussian approximation outlined in Sec. II transforms the photocount difference probability (6) into the form of a convolution of the normal distributions by approximating the Poisson distributions. In this Appendix, we discuss an alternative method where the starting point is the Skellam distribution (7). For convenience, we shall reproduce the expression for this distribution here:

$$P(\mu) = e^{-\eta_1|\alpha_1|^2} e^{-\eta_2|\alpha_2|^2} \left( \frac{\eta_1|\alpha_1|^2}{\eta_2|\alpha_2|^2} \right)^{\frac{\mu}{2}} \times I_\mu \left( 2\sqrt{\eta_1\eta_2|\alpha_1|^2|\alpha_2|^2} \right), \quad (\text{B1})$$

where  $I_k(z)$  is the modified Bessel function of the first kind and the amplitudes  $|\alpha_{1,2}|$  are given by Eq. (3).

The method under consideration (see, e.g. the textbook [10]) assumes that, in the strong LO limit, the argument of the modified Bessel function is large and  $I_\mu(z)$  can be approximated using its asymptotic expansion taken in the Gaussian form:

$$I_\mu(z) \approx \frac{1}{\sqrt{2\pi z}} \exp \left[ z - \frac{\mu^2}{2z} \right]. \quad (\text{B2})$$

This formula can be deduced by performing a saddle-point analysis for the integral representation of the Bessel functions [41].

Heuristically, it can also be obtained from the lowest order asymptotic expansion for the Bessel function [33]:  $I_\mu(z) \approx e^z (1 - (4\mu^2 - 1)/(8z))/\sqrt{2\pi z}$  assuming that, for small values of  $x$ ,  $1 - x$  can be replaced with  $e^{-x}$  (the factors independent of  $\mu$  are not essential be-

cause they can be incorporated into the normalization factor of the Gaussian approximation).

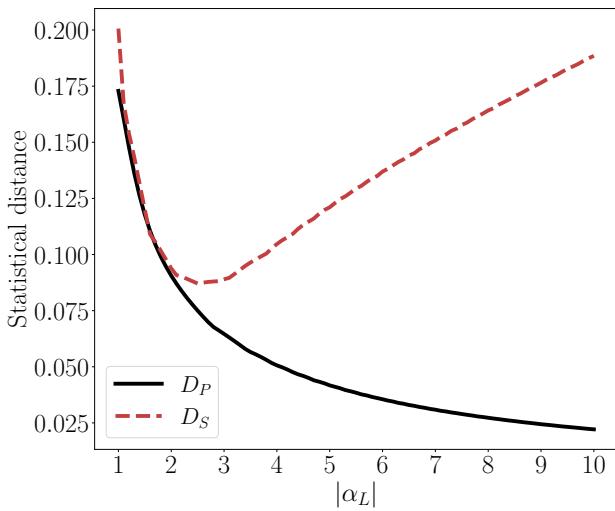


Figure 15: Distances,  $D_P = D(P, P_G)$  and  $D_S = D(P, P_G^{(s)})$ , between the Skellam distribution,  $P$ , and two Gaussian approximations,  $P_G$  (see Eq. (10)) and  $P_G^{(s)}$  (see Eq. (B5)), as a function of  $|\alpha_L|$  the beam splitter disbalance angle at  $\delta\theta = 15^\circ$   $\alpha = 1$ , and  $\eta_1 = \eta_2 = 1$ .

Assuming that  $CS \neq 0$  and  $|\alpha_L|$  is sufficiently large, we can use the approximate relations

$$z = 2\sqrt{\eta_1\eta_2}|\alpha_1||\alpha_2| \approx 2CS\sqrt{\eta_1\eta_2}|\alpha_L|^2, \quad (\text{B3})$$

$$\ln\left(\frac{\eta_1|\alpha_1|^2}{\eta_2|\alpha_2|^2}\right)^{\frac{\mu}{2}} \approx \frac{\mu}{2}\left(\ln\frac{\eta_1S^2}{\eta_2C^2} + \frac{\langle\hat{x}_\phi\rangle}{CS|\alpha_L|}\right) \quad (\text{B4})$$

to obtain the Gaussian approximation for the Skellam distribution (B1) given by

$$P_G^{(s)}(\mu) = G(\mu - \tilde{\mu}_G; \tilde{\sigma}_G), \quad (\text{B5})$$

$$\tilde{\mu}_G = \sqrt{\eta_1\eta_2}\left[CS|\alpha_L|^2 \ln\frac{\eta_1S^2}{\eta_2C^2} + |\alpha_L|\langle\hat{x}_\phi\rangle\right], \quad (\text{B6})$$

$$\tilde{\sigma}_G = 2CS\sqrt{\eta_1\eta_2}|\alpha_L|^2. \quad (\text{B7})$$

Similar to Eq. (15), we cast the probability (B5) into the following quadrature form:

$$P_G^{(s)}(\tilde{x}) = \frac{1}{\sqrt{2\pi\tilde{\sigma}_G}} \exp\left\{-\frac{(\tilde{x} - \langle\hat{x}_\phi\rangle)^2}{2\tilde{\sigma}_x^2}\right\}, \quad (\text{B8})$$

$$\tilde{x} = \frac{\mu}{\sqrt{\eta_1\eta_2}|\alpha_L|} - CS|\alpha_L| \ln\frac{\eta_1S^2}{\eta_2C^2}, \quad (\text{B9})$$

$$\tilde{\sigma}_x = \frac{2CS}{\sqrt{\eta_1\eta_2}}, \quad (\text{B10})$$

so that we may follow the line of reasoning presented in

Sec. II to deduce the POVM

$$\begin{aligned} \hat{\Pi}_G^{(s)} &= \frac{1}{\sqrt{\eta_1\eta_2}|\alpha_L|} \\ &\times \int dx' G(x - x'; \tilde{\sigma}_N)|x', \phi\rangle\langle x', \phi| \end{aligned} \quad (\text{B11})$$

with the noise variance

$$\tilde{\sigma}_N = \tilde{\sigma}_x - 1, \quad 0 \leq \tilde{\sigma}_x \leq \tilde{\sigma}_x^{(\max)} = 1/\sqrt{\eta_1\eta_2}. \quad (\text{B12})$$

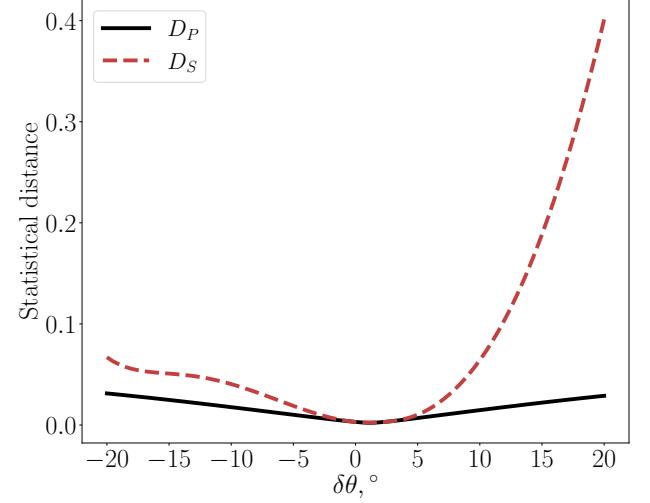


Figure 16: Distances,  $D_P = D(P, P_G)$  and  $D_S = D(P, P_G^{(s)})$ , between the Skellam distribution,  $P$ , and two Gaussian approximations,  $P_G$  (see Eq. (10)) and  $P_G^{(s)}$  (see Eq. (B5)), as a function of the beam splitter disbalance angle  $\delta\theta$  at  $\alpha = 1$ ,  $\alpha_L = 10$  and  $\eta_1 = \eta_2 = 1$ .

Note that, in the symmetric case with  $C = S$  and  $\eta_1 = \eta_2$ , the Gaussian distributions given by Eqs. (10) and (B5) are equivalent. This is no longer the case in the presence of asymmetry effects.

Figure 15 demonstrates that, at  $\delta\theta \neq 0$ , by contrast to the distance between  $P$  and  $P_G$ ,  $D_P = D(P, P_G)$  which is a monotonically decreasing function of  $|\alpha_L|$ , the distance between the Skellam distribution and the approximate distribution (B5),  $D_S = D(P, P_G^{(s)})$ , reveals non-monotonic behaviour and increases with  $|\alpha_L|$  at sufficiently large LO amplitudes. Referring to Fig. 16, disbalance of the beam splitter has strong detrimental effect on the accuracy of the approximation (B5).

What is more important is that, by contrast the noise excess variance (24) which is always positive, the variance (B12) becomes negative when  $2CS \leq \sqrt{\eta_1\eta_2}$ . The latter breaks applicability of Eq. (B11) giving an ill-posed POVM.

### Appendix C: Mutual Information in GG02 protocol and equivalence between Prepare-and-Measure and Entanglement-based schemes

In the GG02 protocol, Alice prepares an ensemble of coherent states  $|\alpha = q + ip\rangle$  with probabilities  $p_A(\alpha)$  distributed according to Gaussian law,

$$p_A(\alpha) = \frac{1}{\pi V_A} \exp \left[ -\frac{|\alpha|^2}{2V_A} \right], \quad (\text{C1})$$

$$\rho_A = \int d^2\alpha p_A(\alpha) |\alpha\rangle\langle\alpha|. \quad (\text{C2})$$

After transmission through a Gaussian channel, which attenuates the coherent amplitude by a factor of  $\sqrt{T}$ , where  $T$  is the channel transmission, the state is transformed as  $|\alpha\rangle \mapsto |\sqrt{T}\alpha\rangle \equiv |\tilde{\alpha} = \tilde{q} + i\tilde{p}\rangle$ . If independent channel noise is present, the ensemble reads

$$\tilde{p}_A = \frac{1}{\pi\xi T} \int d^2\tilde{\alpha} p_A(\tilde{\alpha}) \int d^2\alpha' \exp \left[ -\frac{|\alpha'|^2}{\xi} \right] \times |\tilde{\alpha} - \alpha'\rangle\langle\tilde{\alpha} - \alpha'|, \quad (\text{C3})$$

where  $\xi$  is the channel noise variance. Note that variance of  $p_A(\tilde{\alpha})$  is  $TV_A$ .

Then, Bob performs a measurement described by POVM  $\{\hat{\Pi}_x\}$ , where the index  $x$  corresponds to the measurement outcomes (e.g., quadrature values  $q$  and  $p$  in homodyne detection). The probability that Bob obtains measurement outcome  $x$  is given by the Born rule:

$$p_B(x, \tilde{\alpha}) \sim p_A(\tilde{\alpha}) \int d^2\alpha' \exp \left[ -\frac{|\alpha'|^2}{\xi} \right] Q_x(\tilde{\alpha} - \alpha'), \quad (\text{C4})$$

where  $Q_x(\tilde{\alpha})$  is the  $Q$ -function of POVM used.

For homodyne detection, Eq. (C4) takes the form given by Eq. (15)

$$p_B^H(x, \tilde{\alpha}) \sim \exp \left[ -\frac{(x - 2\tilde{q})^2}{2(\sigma_x + 2\xi)} - \frac{\tilde{q}^2}{2TV_A} \right]. \quad (\text{C5})$$

Rewriting exponential's power in Eq.(C5) in quadratic form results in

$$\begin{aligned} & -\frac{1}{2} (\tilde{q} \ x) \begin{pmatrix} TV_A & 2TV_A \\ 2TV_A & 4TV_A + \sigma_x + 2\xi \end{pmatrix}^{-1} \begin{pmatrix} \tilde{q} \\ x \end{pmatrix} \\ & \equiv -\frac{1}{2} (\tilde{q} \ x) \Sigma^{H^{-1}} \begin{pmatrix} \tilde{q} \\ x \end{pmatrix}, \end{aligned} \quad (\text{C6})$$

and with covariance matrix  $\Sigma^H$ , mutual information between Alice and Bob can be calculated as follows [42]

$$I_{AB}^H = \frac{1}{2} \log \frac{\Sigma_{11}^H \Sigma_{22}^H}{\det \Sigma^H} = \frac{1}{2} \log \left[ 1 + \frac{4TV_A}{\sigma_x + 2\xi} \right], \quad (\text{C7})$$

where  $\Sigma_{ii}^H$  are diagonal elements of  $\Sigma^H$ , and all logarithms are base 2.

If double homodyne detection is used, from Eq. (C4) we have (see Eq. (36)):

$$p_B^{DH}(x, \tilde{\alpha}) \sim \exp \left[ -\frac{(x_1 - \tilde{q})^2}{2\left(\frac{\sigma_1}{2} + \frac{\xi}{2}\right)} - \frac{\tilde{q}^2}{2TV_A} - \frac{(x_2 - \tilde{p})^2}{2\left(\frac{\sigma_2}{2} + \frac{\xi}{2}\right)} - \frac{\tilde{p}^2}{2TV_A} \right]. \quad (\text{C8})$$

Analogously to Eq. (C6), we obtain covariance matrices as follows:

$$\Sigma^{DH^{(i)}} = \begin{pmatrix} TV_A & TV_A \\ TV_A & TV_A + \frac{\sigma_i}{2} + \frac{\xi}{2} \end{pmatrix}, \quad i = 1, 2, \quad (\text{C9})$$

from which we obtain mutual information as

$$\begin{aligned} I_{AB}^{DH} &= \frac{1}{2} \sum_{i=1,2} \log \frac{\Sigma_{11}^{DH^{(i)}} \Sigma_{22}^{DH^{(i)}}}{\det \Sigma^{DH^{(i)}}} = \\ & \frac{1}{2} \sum_i \log \left[ 1 + \frac{2TV_A}{\sigma_i + \xi} \right]. \end{aligned} \quad (\text{C10})$$

Consider two mode squeezed vacuum state (TMSVS), in ket notation written as [38]

$$|\Psi\rangle_{AB} = \sqrt{1 - \lambda^2} \sum_{n=0}^{\infty} \lambda^n |n, n\rangle_{AB}, \quad (\text{C11})$$

where  $\lambda = \tanh r$ ,  $r$  is the squeezing parameter. Let Alice hold the state  $\varsigma_{AB} = |\Psi\rangle_{AB}\langle\Psi|_{AB}$ . In the entanglement-based (EB) protocol, Alice measures one mode using a double measurement, which corresponds to a POVM of coherent state projectors  $\{\hat{\Pi}_\beta = \frac{|\beta\rangle\langle\beta|}{\pi}\}$ , and sends the second mode to Bob. The probability that Alice observes double homodyne outcome  $\beta$  is given by the Born rule:

$$p_A^{EB}(\beta) = \text{Tr} \hat{\Pi}_\beta \varsigma_A, \quad (\text{C12})$$

where

$$\varsigma_A = \text{Tr}_B \varsigma_{AB} = (1 - \lambda^2) \sum_n \lambda^{2n} |n\rangle\langle n|. \quad (\text{C13})$$

is the reduced density matrix of Alice's mode. Substituting Eq. (C13) into Eq. (C12) yields

$$p_A^{EB}(\beta) = \frac{(1 - \lambda^2)}{\pi} \exp [(\lambda^2 - 1) |\beta|^2]. \quad (\text{C14})$$

After Alice obtains outcome  $\beta$ , second mode before channel transmission reads

$$\varsigma_B^\beta = |-\lambda\beta^*\rangle\langle-\lambda\beta^*| \quad (\text{C15})$$

and the ensemble reads

$$\varsigma_B = \int d^2\beta p_A^{EB}(\beta) |-\lambda\beta^*\rangle\langle-\lambda\beta^*|, \quad (\text{C16})$$

exactly the same as Eq. (C2) after substituting

$$\alpha = -\lambda\beta^*, \quad \frac{1 - \lambda^2}{\lambda^2} = \frac{1}{2V_A}. \quad (\text{C17})$$

It follows that covariance matrix of TMSVS can be used to calculate Holevo information in the PM protocol.

- 
- [1] F. Grosshans and P. Grangier, Continuous variable quantum cryptography using coherent states, *Phys. Rev. Lett.* **88**, 057902 (2002).
- [2] C. Weedbrook, A. M. Lance, W. P. Bowen, T. Symul, T. C. Ralph, and P. K. Lam, Quantum cryptography without switching, *Phys. Rev. Lett.* **93**, 170504 (2004).
- [3] C. Weedbrook, S. Pirandola, R. García-Patrón, N. J. Cerf, T. C. Ralph, J. H. Shapiro, and S. Lloyd, Gaussian quantum information, *Rev. Mod. Phys.* **84**, 621 (2012).
- [4] E. Diamanti and A. Leverrier, Distributing secret keys with quantum continuous variables: Principle, security and implementations, *Entropy* **17**, 6072 (2015).
- [5] R. Goncharov, I. Vorontsova, D. Kirichenko, I. Filipov, I. Adam, V. Chistiakov, S. Smirnov, B. Nasedkin, B. Pervushin, D. Kargina, E. Samsonov, and V. Egorov, The rationale for the optimal continuous-variable quantum key distribution protocol, *Optics* **3**, 338 (2022).
- [6] Y. Zhang, Y. Bian, Z. Li, S. Yu, and H. Guo, Continuous-variable quantum key distribution system: Past, present, and future, *Applied Physics Reviews* **11**, 011318 (2024).
- [7] A. Gaidash, A. D. Kiselev, G. Miroshnichenko, and A. Kozubov, Intermodulation-induced dynamics of continuous-variable quantum-key-distribution observables, *Phys. Rev. A* **109**, 062615 (2024).
- [8] W. Vogel and J. Grabow, Statistics of difference events in homodyne detection, *Phys. Rev. A* **47**, 4227 (1993).
- [9] P. L. Kelley and W. H. Kleiner, Theory of electromagnetic field measurement and photoelectron counting, *Phys. Rev.* **136**, A316 (1964).
- [10] W. Vogel and D.-G. Welsch, *Quantum Optics*, 3rd ed. (Wiley-VCH, Berlin, 2006) p. 508.
- [11] W. Vogel, Homodyne correlation measurements with weak local oscillators, *Phys. Rev. A* **51**, 4160 (1995).
- [12] B. L. Schumaker, Noise in homodyne detection, *Opt. Lett.* **9**, 189 (1984).
- [13] S. Wallentowitz and W. Vogel, Unbalanced homodyning for quantum state measurements, *Phys. Rev. A* **53**, 4528 (1996).
- [14] G. S. Thekkadath, D. S. Phillips, J. F. F. Bulmer, W. R. Clements, A. Eckstein, B. A. Bell, J. Lugani, T. A. W. Wolterink, A. Lita, S. W. Nam, T. Gerrits, C. G. Wade, and I. A. Walmsley, Tuning between photon-number and quadrature measurements with weak-field homodyne detection, *Phys. Rev. A* **101**, 031801 (2020).
- [15] J. Sperling, W. Vogel, and G. S. Agarwal, True photocounting statistics of multiple on-off detectors, *Phys. Rev. A* **85**, 023820 (2012).
- [16] T. Lipfert, J. Sperling, and W. Vogel, Homodyne detection with on-off detector systems, *Phys. Rev. A* **92**, 053835 (2015).
- [17] T. Richter, Double homodyne detection and quantum state determination, in *European Quantum Electronics Conference* (Optica Publishing Group, 1998) p. QTUG38.
- [18] A. Cives-Esclop, A. Luis, and L. L. Sánchez-Soto, An eight-port detector with a local oscillator of finite intensity, *Journal of Optics B: Quantum and Semiclassical Optics* **2**, 526 (2000).
- [19] A. Leverrier, Security of continuous-variable quantum key distribution via a gaussian de finetti reduction, *Phys. Rev. Lett.* **118**, 200501 (2017).
- [20] V. Y. Len, M. Byelova, V. Uzunova, and A. Semenov, Realistic photon-number resolution in generalized hong-ou-mandel experiment, *Physica Scripta* **97**, 105102 (2022).
- [21] I. Yeremenko, M. Dmytryuk, and A. Semenov, Realistic photon-number resolution in gaussian boson sampling, *Physical Review A* **110**, 043715 (2024).
- [22] A. Reutov and D. Sych, Photon counting statistics with imperfect detectors, in *Journal of Physics: Conference Series*, Vol. 2086 (IOP Publishing, 2021) p. 012096.
- [23] A. A. Hajomer, A. N. Oruganti, I. Derkach, U. L. Andersen, V. C. Usenko, and T. Gehring, Finite-size security of continuous-variable quantum key distribution with imperfect heterodyne measurement, arXiv preprint arXiv:2501.10278 (2025).
- [24] A. Ruiz-Chamorro, D. Cano, A. Garcia-Callejo, and V. Fernandez, Effects of experimental impairments on the security of continuous-variable quantum key distribution, *Heliyon* **9** (2023).
- [25] X.-Y. Wang, X.-B. Guo, Y.-X. Jia, Y. Zhang, Z.-G. Lu, J.-Q. Liu, and Y.-M. Li, Accurate shot-noise-limited calibration of a time-domain balanced homodyne detector for continuous-variable quantum key distribution, *J. Lightwave Technol.* **41**, 5518 (2023).
- [26] V. C. Usenko and R. Filip, Trusted noise in continuous-variable quantum key distribution: a threat and a defense, *Entropy* **18**, 20 (2016).
- [27] J.-Z. Huang, Z.-Q. Yin, S. Wang, H.-W. Li, W. Chen, G.-C. Guo, and Z.-F. Han, Wavelength attack scheme on continuous-variable quantum key distribution system using heterodyne detection protocol, arXiv preprint arXiv:1206.6550 (2012).
- [28] J.-Z. Huang, S. Kunz-Jacques, P. Jouguet, C. Weedbrook, Z.-Q. Yin, S. Wang, W. Chen, G.-C. Guo, and Z.-F. Han, Quantum hacking on quantum key distribution using homodyne detection, *Physical Review A* **89**, 032304 (2014).
- [29] H. Qin, R. Kumar, V. Makarov, and R. Alléaume, Homodyne-detector-blinding attack in continuous-variable quantum key distribution, *Physical Review A* **98**, 012312 (2018).
- [30] H. Qin, R. Kumar, and R. Alléaume, Quantum hacking: Saturation attack on practical continuous-variable quantum key distribution, *Physical Review A* **94**, 012325 (2016).
- [31] S. Pirandola, U. L. Andersen, L. Banchi, M. Berta, D. Bunandar, R. Colbeck, D. Englund, T. Gehring, C. Lupo, C. Ottaviani, J. L. Pereira, M. Razavi, J. S. Shaari, M. Tomamichel, V. C. Usenko, G. Vallone, P. Viloresi, and P. Wallden, Advances in quantum cryptography, *Adv. Opt. Photon.* **12**, 1012 (2020).

- [32] J. G. Skellam, The frequency distribution of the difference between two poisson variates belonging to different populations, *Journal of the Royal Statistical Society Series A: Statistics in Society* **109**, 296 (1946).
- [33] F. W. J. Olver, D. W. Lozier, R. F. Boisvert, and C. W. Clark, eds., *NIST Handbook of Mathematical Functions* (NIST & Cambridge University Press, New York, 2010) p. 951.
- [34] P. Lahti, J.-P. Pellonpää, and J. Schultz, Realistic eight-port homodyne detection and covariant phase space observables, *Journal of Modern Optics* **57**, 1171 (2010).
- [35] C. Gerry and P. Knight, *Introductory Quantum Optics* (Cambridge University Press, NY, 2005) p. 317.
- [36] M. G. Genoni, S. Mancini, and A. Serafini, General-dyne unravelling of a thermal master equation, *Russian Journal of Mathematical Physics* **21**, 329 (2014).
- [37] F. Laudenbach, C. Pacher, C.-H. F. Fung, A. Poppe, M. Peev, B. Schrenk, M. Hentschel, P. Walther, and H. Hübel, Continuous-variable quantum key distribution with gaussian modulation—the theory of practical implementations, *Advanced Quantum Technologies* **1**, 1800011 (2018).
- [38] C. Weedbrook, S. Pirandola, R. García-Patrón, N. J. Cerf, T. C. Ralph, J. H. Shapiro, and S. Lloyd, Gaussian quantum information, *Rev. Mod. Phys.* **84**, 621 (2012).
- [39] A. Serafini, *Quantum Continuous Variables: A Primer of Theoretical Methods* (CRC Press, Taylor & Francis Group, Boca Raton, 2017) p. 350.
- [40] Y. Zhang, Y. Bian, Z. Li, S. Yu, and H. Guo, Continuous-variable quantum key distribution system: Past, present, and future, *Applied Physics Reviews* **11** (2024).
- [41] M. Freyberger, K. Vogel, and W. P. Schleich, From photon counts to quantum phase, *Physics Letters A* **176**, 41 (1993).
- [42] J. Soch *et al.*, Statproofbook/statproofbook.github.io: The book of statistical proofs (version 2023), <https://doi.org/10.5281/zenodo.4305949> (2024), accessed: 2025-07-15.