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

A. S. Naumchik,[1,*] Roman K. Goncharov,[1,†] and Alexei D. Kiselev[2,3,‡]

[1] *ITMO University, Kronverksky Pr. 49, Saint Petersburg 197101, Russia*
[2] *Laboratory of Quantum Processes and Measurements, ITMO University, Kadetskaya Line 3b, Saint Petersburg 199034, Russia*
[3] *Leading Research Center "National Center for Quantum Internet", ITMO University, Birzhevaya Line 16, Saint Petersburg 199034, Russia*

(Dated: November 16, 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 is detrimental in this case. Moreover, we found that the double homodyne POVM is not uniquely defined, because the squeezing parameter, which governs the POVM, is constrained within an interval determined by the asymmetry parameters of the measurement scheme. Consequently, the Holevo information, which depends on this POVM, also varies with the squeezing parameter within this range.

I. INTRODUCTION

Homodyne detection is a fundamental technique in quantum optics for measuring quadrature components (amplitude and phase) 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 photocurrent yields information about the signal quadratures [8, 9].

Most theoretical treatments assume the strong-local-oscillator (LO) approximation, where the LO is much more intense than the signal [10]. This simplification improves analytical tractability and measurement precision but may also amplify classical LO noise and mask subtle quantum effects such as squeezing. In the weak-LO regime, where the LO and signal amplitudes are comparable, phase-sensitive quantum effects become more visible [11]; however, operation in this regime requires 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 using a single unbalanced beam splitter, are useful when the 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 employed 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 limitations in photon-number resolution, although detector arrays have been proposed to mitigate these drawbacks [14–16].

Another important approach is double-homodyne (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 the classical and quantum regimes; in the weak-LO limit, it reduces to photon-number measurements [18]. In the context of CV-QKD protocols, this method also facilitates 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 compromises CV-QKD security [13, 20–25].

Although the ideal POVMs for projections onto quadrature or coherent states are well known [10, 17], a comprehensive quantum-optical treatment of detector asymmetry – explicitly incorporating the beam-splitter imbalance and detector-efficiency mismatch into the measurement operators – has not yet been developed [15, 16]. Existing complementary studies, such as Ref. [26], have investigated the practical influence of detection imbalance on phase-reference estimation and key-rate performance in CV-QKD systems and illustrated its impact experimentally using Wigner-function reconstructions. However, these analyses remain semi-classical and do not address the modification of the measurement process itself within the quantum-optical formalism. In this

* Email address: naumchik95@gmail.com
† Email address: toloroloe@gmail.com
‡ Email address: alexei.d.kiselev@gmail.com

work, we focus on these imperfections at the level of the quantum measurement and refer to them collectively as asymmetry effects.

In practice, these imperfections are often modeled as additive technical noise (electronic noise, dark counts, finite bandwidth), but asymmetry introduces structured excess noise that must be accounted for to produce reliable security estimates [24–27]. Such 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, 28–31]. Explicitly accounting for measurement asymmetry is therefore an essential part of this defensive toolbox.

Our analysis focuses on an asymmetrical detection scenario: an unbalanced beam splitter combined with unequal (and non-unity) quantum efficiencies of the photodetectors, in contrast to the conventional symmetrical case of a balanced beam splitter and identical detector efficiencies. To derive tractable expressions, we model the photocount statistics by approximating Poisson distributions with Gaussian ones (the Gaussian approximation) and further simplify using the strong-LO approximation. From these approximations, we construct the corresponding POVMs and numerically assess the accuracy of the resulting expressions.

We then apply the developed formalism to a homodyne-based two-quadrature scheme (double homodyne, often referred to as heterodyne in the QKD literature [5, 6, 32]) 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. We then use the obtained asymmetrical POVMs to compute the CV-QKD asymptotic secret fraction, thereby quantifying the impact of measurement asymmetry on protocol security.

The paper is organized as follows. In Sec. II, we derive the statistical distribution of difference photon counts in the Gaussian approximation, from which we obtain the respective POVM. In Sec. III, we analyze the double-homodyne scheme analogously to the previous section and show 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 the GG02 CV-QKD protocol. Finally, in Sec. VI, we summarize the main results and outline directions for future research.

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 spitter is unbalanced and its scattering matrix is chosen to be a real-valued rotation

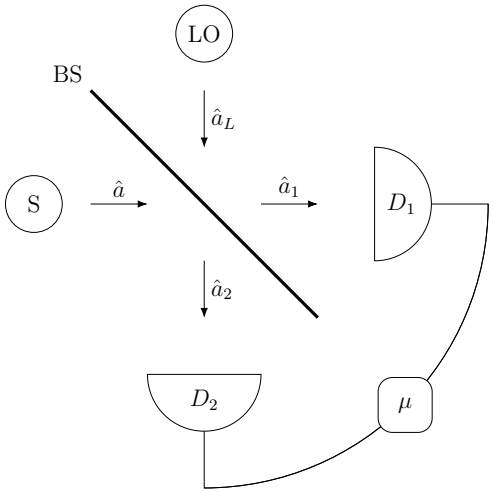


Figure 1: Scheme of a homodyne receiver: S is the source of the signal mode with the annihilation operator $\hat{a}$, LO is the source of the reference mode (local oscillator) with the annihilation operator $\hat{a}_L$, and BS is the beam splitter with the amplitude transmission and reflection coefficients $t = \cos\theta$ and $r = \sin\theta$, respectively; photodetectors D_1 and D_2 have quantum efficiencies η_1 and η_2, and $\mu \equiv m_1 - m_2$ is the photon count difference.

matrix with the transmission and reflection amplitudes, t and r, given by

$$t = \cos\theta \equiv C, \quad r = \sin\theta \equiv S. \tag{1}$$

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

$$|\alpha, \alpha_L\rangle \mapsto |\alpha_1, \alpha_2\rangle, \tag{2}$$
$$\alpha_1 = C\alpha + S\alpha_L, \quad \alpha_2 = -S\alpha + C\alpha_L, \tag{3}$$

so that the joint probability of m_1 and m_2 photon counts for the photodetectors D_1 and D_2 can be computed from the well-known Kelley-Kleiner formula [9] (see also Ref. [8]):

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

where $: \ldots :$ 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, η_l is the quantum efficiency of the detector D_l.

We can now introduce the photon count difference

$$\mu = m_1 - m_2 \tag{5}$$

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

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

It is well known that, by performing summation over m_2, the probabilty $\mathsf{P}(\mu)$ reduces to the Skellam distribution given by [33]

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

where $I_k(z)$ is the modified Bessel function of the first kind [34].

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

$$\int G(x_1 - x_2; \sigma_1) G(x_2; \sigma_2) \mathrm{d}x_2 = G(x_1; \sigma_1 + \sigma_2), \quad (8)$$

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

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

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

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

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

where

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

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

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

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 σ_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 σ_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 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 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

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

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

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

$$\hat{\Pi}_G = \frac{1}{(\eta_1+\eta_2)CS|\alpha_L|} \times \int \mathrm{d}x' G(x-x';\sigma_N)|x',\phi\rangle\langle x',\phi|. \tag{25}$$

Note that the variance σ_N describes the excess noise that takes into account asymmetry effects. In the limiting case of perfect homodyne, we have

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

where $\delta(x)$ is the Dirac δ-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.

From Eq. (15) we are also able to construct POVM's (25) covariance matrix:

$$\Sigma^{\mathrm{H}} = \lim_{z\to 0} R_\phi^{\mathrm{T}} \left[\mathrm{diag}(z,z^{-1}) + \sigma_N \mathbb{I}\right] R_\phi \equiv \Sigma_0^{\mathrm{H}} + \Sigma_N^{\mathrm{H}}, \tag{27}$$

where Σ_0^{H} and Σ_N^{H} denote the covariance matrices of the ideal measurement and the associated excess noise, respectively, $\mathbb{I} = \mathrm{diag}(1,1)$, and R_ϕ is the rotation matrix by angle ϕ.

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

$$\mathsf{P}(\mu;|\psi\rangle) = \int P_{|\psi\rangle}(\alpha)\mathsf{P}(\mu;\alpha)\mathrm{d}^2\alpha,$$
$$\mathsf{P}_G(x;|\psi\rangle) = \langle\psi|\hat{\Pi}_G|\psi\rangle, \tag{28}$$

where $P_{|\psi\rangle}(\alpha)$ is the Glauber P function of the quantum state $|\psi\rangle$. In Fig. 2, 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

$$P_{|n\rangle}(\alpha) = \frac{e^{|\alpha|^2}}{n!}\Big(\frac{\partial^2}{\partial\alpha\partial\alpha^*}\Big)^n \delta^2(\alpha), \tag{29}$$

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

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 perfomance 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

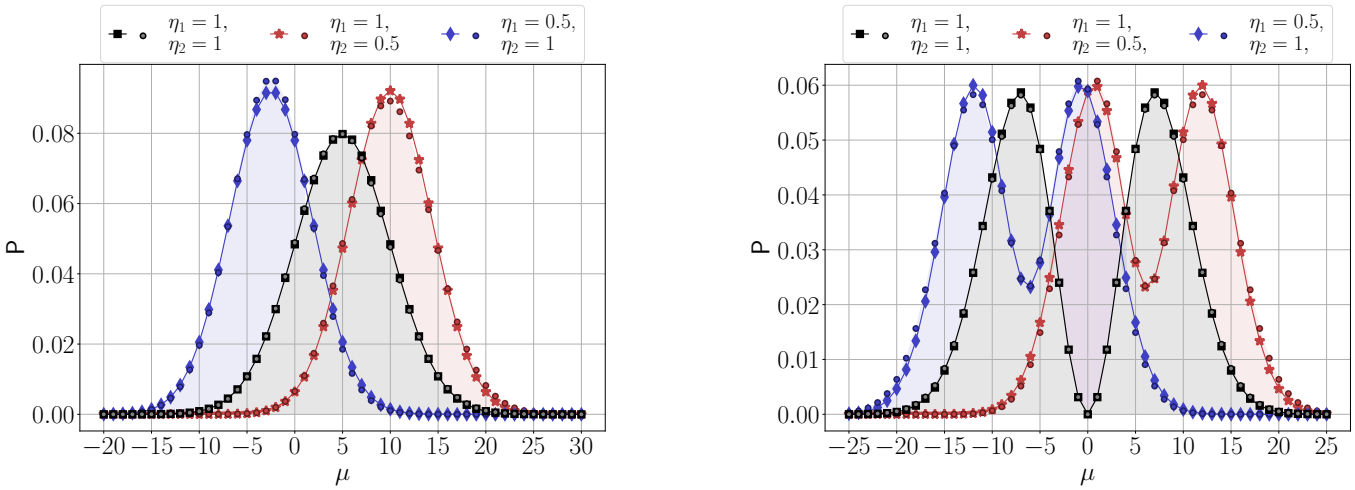
In the section, we consider the eight-port double homodyne scheme depicted in Fig. 3 (see, e.g., Refs. [10, 35]). This measurement scheme is known to allow reconstructing the Husimi Q function of the signal state [17] providing complete information about the signal state that may be used in CV-QKD protocols. 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

$$\alpha^{(1)} = C_S\alpha, \quad \alpha^{(2)} = S_S\alpha,$$
$$\alpha_L^{(1)} = C_L\alpha_L, \quad \alpha_L^{(2)} = -iS_L\alpha_L, \tag{30}$$

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 prod-



(a) $|\psi\rangle = |\alpha\rangle$, $\alpha = 0.5$ (b) $|\psi\rangle = |n\rangle$, $n = 1$

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 for different efficiencies at $|\alpha_L| = 5$ and balanced beamspliiter.

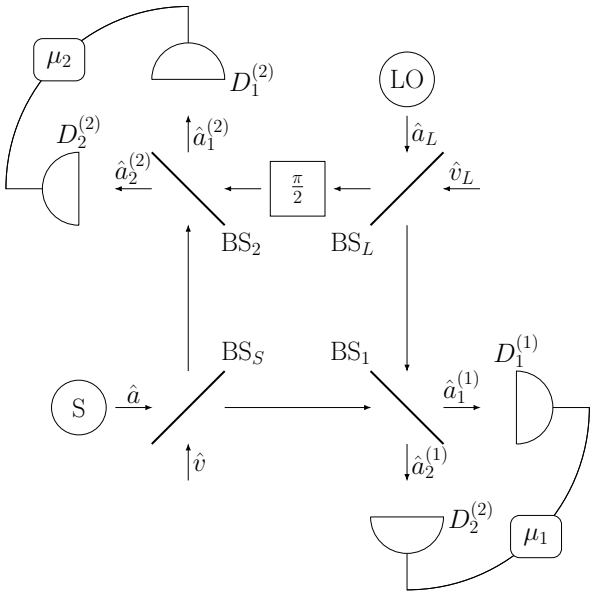


Figure 3: Scheme of an eight port double homodyne receiver. S is the source of the signal mode $\hat{a}$; LO is the source of the reference mode $\hat{a}_L$; BS_S (BS_L) is the signal mode (local oscillator) beam splitter; $\frac{\pi}{2}$ is the quarter wave phase shifter; BS_i is the beam splitter of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

uct of the Skellam distributions given by

$$\mathsf{P}(\mu_1, \mu_2) = \mathsf{P}_1(\mu_1)\mathsf{P}_2(\mu_2), \quad \mu_i = m_1^{(i)} - m_2^{(i)}, \tag{31}$$

$$\mathsf{P}_i(\mu_i) = e^{-\eta_1^{(i)}|\alpha_1^{(i)}|^2} e^{-\eta_2^{(i)}|\alpha_2^{(i)}|^2} \left(\frac{\eta_1^{(i)}|\alpha_1^{(i)}|^2}{\eta_2^{(i)}|\alpha_2^{(i)}|^2}\right)^{\mu_i/2}$$
$$\times I_{\mu_i}\big(2\sqrt{\eta_1^{(i)}\eta_2^{(i)}|\alpha_1^{(i)}|^2|\alpha_2^{(i)}|^2}\big), \tag{32}$$

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

$$\alpha_1^{(i)} = C_i\alpha^{(i)} + S_i\alpha_L^{(i)}, \quad \alpha_2^{(i)} = -S_i\alpha^{(i)} + C_i\alpha_L^{(i)} \tag{33}$$

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. (31) and derive the Gaussian approximation for the double homodyne scheme in the form:

$$\mathsf{P}_G(\mu_1, \mu_2) = G(\mu_1 - \mu_G^{(1)}; \sigma_G^{(1)})G(\mu_2 - \mu_G^{(2)}; \sigma_G^{(2)}), \tag{34}$$

$$\sigma_G^{(i)} = (\eta_1^{(i)}S_i^2 + \eta_2^{(i)}C_i^2)|\alpha_L^{(i)}|^2, \tag{35}$$

$$\mu_G^{(i)} = (\eta_1^{(i)}S_i^2 - \eta_2^{(i)}C_i^2)|\alpha_L^{(i)}|^2 + C_iS_i(\eta_1^{(i)} + \eta_2^{(i)})|\alpha_L^{(i)}|$$
$$\times 2\,\mathrm{Re}\,\alpha^{(i)}e^{-i\phi}, \quad \phi = \arg\alpha_L. \tag{36}$$

Similar to Eq. (15), it is useful to put the probability (34) into the folowing quadrature form:

$$\mathsf{P}_G(x_1, x_2) = \frac{1}{2\pi\sqrt{\sigma_G^{(1)}\sigma_G^{(2)}}} \exp\Big\{-\frac{(x_1 - \mathrm{Re}\,\alpha e^{-i\phi})^2}{\sigma_1}$$
$$- \frac{(x_2 - \mathrm{Im}\,\alpha e^{-i\phi})^2}{\sigma_2}\Big\} \tag{37}$$

where x_i are the quadrature variables given by

$$x_1 = \frac{1}{2(\eta_1^{(1)}+\eta_2^{(1)})C_1S_1C_S} \times\Big\{\frac{\mu_1}{|\alpha_L^{(1)}|}-(\eta_1^{(1)}S_1^2-\eta_2^{(1)}C_1^2)|\alpha_L^{(1)}|\Big\}, \quad (38)$$

$$x_2 = \frac{1}{2(\eta_1^{(2)}+\eta_2^{(2)})C_2S_2S_S} \times\Big\{\frac{\mu_2}{|\alpha_L^{(2)}|}-(\eta_1^{(2)}S_2^2-\eta_2^{(2)}C_2^2)|\alpha_L^{(2)}|\Big\}, \quad (39)$$

and relations

$$\sigma_1 = \frac{\sigma_x^{(1)}}{2C_S^2}, \quad \sigma_2 = \frac{\sigma_x^{(2)}}{2S_S^2}, \quad (40)$$

$$\sigma_x^{(i)} = \frac{\eta_1^{(i)}S_i^2+\eta_2^{(i)}C_i^2}{\Big[(\eta_1^{(i)}+\eta_2^{(i)})C_iS_i\Big]^2} \quad (41)$$

give the quadrature variances σ_1 and σ_2.

As in Sec. II, formula (37) 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 splitters are balanced and the photodetection is perfect, we have

$$\mathsf{P}_G^{(0)}(x_1,x_2) = \frac{|\langle z|\alpha\rangle|^2}{\pi|\alpha_L|^2}, \quad |\langle z|\alpha\rangle|^2 = e^{-|z-\alpha|^2}, \quad (42)$$

where

$$z = (x_1+ix_2)e^{i\phi}, \quad x_i = \frac{\mu_i}{|\alpha_L|}. \quad (43)$$

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

$$\hat{\Pi}_G^{(0)}(x_1,x_2) = \frac{1}{\pi|\alpha_L|^2}|z\rangle\langle z|. \quad (44)$$

For non-ideal measurements, the probability (37) can be expressed as a Gaussian superposition of the coherent state Husimi functions with the help of the convolution relation (8) as follows

$$\mathsf{P}_G(x_1,x_2) = \frac{\sqrt{\sigma_1\sigma_2}}{2\pi\sqrt{\sigma_G^{(1)}\sigma_G^{(2)}}}\int \mathrm{d}\beta_1\mathrm{d}\beta_2 G(x_1-\beta_1;\sigma_N^{(1)}) \times G(x_2-\beta_2;\sigma_N^{(2)})|\langle\beta e^{i\phi}|\alpha\rangle|^2, \quad \beta=\beta_1+i\beta_2, \quad (45)$$

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

$$2\sigma_N^{(i)} = \sigma_i - 1. \quad (46)$$

The corresponding expression for the POVM reads

$$\hat{\Pi}_G(x_1,x_2) = \frac{\sqrt{\sigma_1\sigma_2}}{2\pi\sqrt{\sigma_G^{(1)}\sigma_G^{(2)}}}\int \mathrm{d}\beta_1\mathrm{d}\beta_2 G(x_1-\beta_1;\sigma_N^{(1)}) \times G(x_2-\beta_2;\sigma_N^{(2)})|\beta e^{i\phi}\rangle\langle\beta e^{i\phi}|. \quad (47)$$

An important point is that the results given by Eq. (45) and Eq. (47) are well defined only if σ_1 and σ_2 are both above unity, so that the excess noise variances (46) are positive. From Eq. (40), 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))

$$\sigma_x^{(i)} \geq \left(\frac{\sqrt{\eta_1^{(i)}}+\sqrt{\eta_2^{(i)}}}{\eta_1^{(i)}+\eta_2^{(i)}}\right)^2 \geq 1 \quad (48)$$

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. (48)) 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 (31) in the photocont difference μ_1-μ_2 plane. Referring to Fig. 4, in addition to the shift of the distribution, the asymmetry induced difference of the variances at $\eta_1^{(1)}+\eta_2^{(1)} \neq \eta_1^{(2)}+\eta_1^{(2)}$ manifests itself as the two dimensional anisotropy of the double homodyne distribution.

IV. POSITIVE OPERATOR-VALUED MEASURE AND SQUEEZED STATES

From Eq. (46), the expression for the POVM in the form of incoherent gaussian superposition of coherent states is justified only if both the quadrature variances, σ_1 and σ_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

$$|\beta,\zeta\rangle = \hat{D}(\beta)\hat{S}(\zeta)|0\rangle, \quad (49)$$

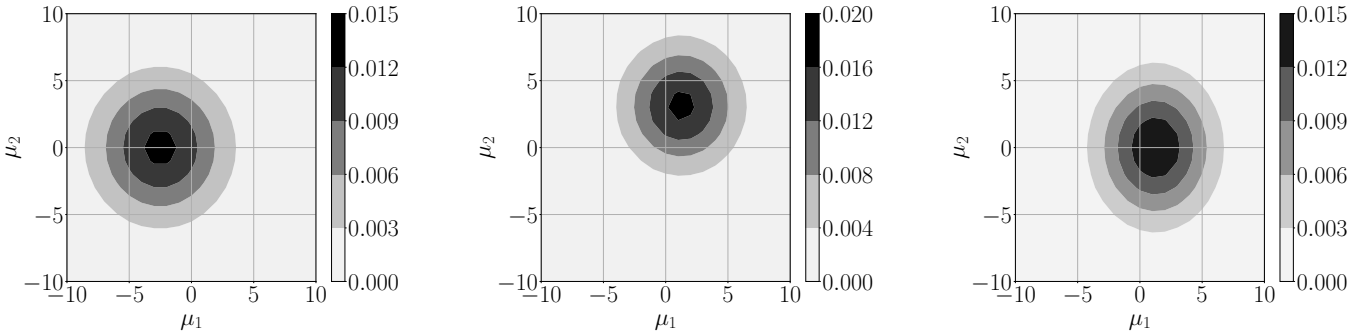
where $\hat{D}(\beta)$ ($\hat{S}(\zeta)$) is the displacement (squeezing) operator given by

$$\hat{D}(\beta) = e^{\beta\hat{a}^\dagger-\beta^*\hat{a}}, \quad \hat{S}(\zeta) = e^{\frac{1}{2}\left(\zeta\hat{a}^{\dagger 2}-\zeta^*\hat{a}^2\right)}, \quad (50)$$

β and ζ are the complex-valued amplitude and the squeeze parameter, respectively.

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

$$\zeta = re^{2i\phi}, \quad r\in\mathbb{R} \quad (51)$$



(a) $\eta_1^{(i)} = 1, \eta_2^{(i)} = 1$ (b) $\eta_1^{(i)} = 1, \eta_2^{(i)} = 0.5$ (c) $\eta_1^{(i)} = 1, \eta_2^{(1)} = 1, \eta_2^{(2)} = 0.5$

Figure 4: Double homodyne statistical distribution of photocount differences computed from Eq. (31) for various detector efficiencies at $\alpha = 0.5$ and $\alpha_L = 5$. All the beam splitters are taken to be balanced.

and the non-normalized Husimi distribution for the squeezed state (49) takes the form (see, e.g., the textbook [36])

$$|\langle\beta, re^{2i\phi}|\alpha\rangle|^2 = \frac{1}{\cosh r}\exp\Big\{-\frac{e^{-r}}{\cosh r}\left(\tilde{\beta}_1 e^r - \tilde{\alpha}_1\right)^2 - \frac{e^r}{\cosh r}\left(\tilde{\beta}_2 e^{-r} - \tilde{\alpha}_2\right)^2\Big\}, \tag{52}$$

$$\tilde{\beta} = \tilde{\beta}_1 + i\tilde{\beta}_2 = \beta e^{-i\phi}, \quad \tilde{\alpha} = \tilde{\alpha}_1 + i\tilde{\alpha}_2 = \alpha e^{-i\phi}. \tag{53}$$

By using this squeezed state distribution instead of the coherent state one given in Eq. (44), we are led to the expressions for the noise variances modified as follows

$$2\sigma_N^{(1,2)} = \sigma_{1,2} - e^{\pm r}\cosh r. \tag{54}$$

These expressions present the extension of the relations (46) to the case with non-vanishing squeeze parameter. As an immediate consequence of Eq. (54), we find that the conditions for the noise variances to be positive definite can be written in the form of two inequalities

$$4\sigma_N^{(1)} = \delta_1 - e^{2r} \geq 0, \quad 4\sigma_N^{(2)} = \delta_2 - e^{-2r} \geq 0, \tag{55}$$

where the quadrature variance parameters

$$\delta_1 = 2\sigma_1 - 1 = (q+1)\sigma_x^{(1)} - 1 \geq q = \frac{S_S^2}{C_S^2}, \tag{56a}$$

$$\delta_2 = 2\sigma_2 - 1 = (q^{-1}+1)\sigma_x^{(2)} - 1 \geq q^{-1} = \frac{C_S^2}{S_S^2} \tag{56b}$$

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. (41)) that cannot be smaller than unity (see Eq. (48)): $\sigma_x^{(i)} \geq 1$.

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

$$q = \frac{1 - C_S^2}{C_S^2} = \frac{S_S^2}{C_S^2} \geq 1. \tag{57}$$

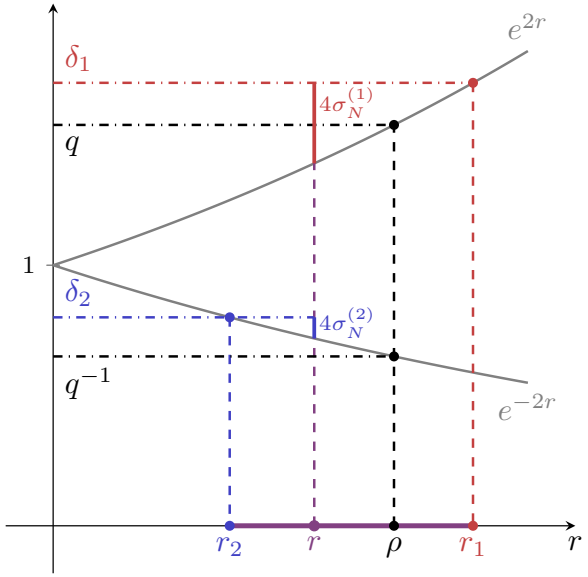


Figure 5: An illustration for the conditions for the noise variances, see Eqs. (55)-(58). Solid grey lines represent the exponents $e^{\pm 2r}$. Dashdotted black, red and blue lines are the independent on r functions q and q^{-1}, δ_1 and δ_2 respectively. Solid purple line is the interval of squeezing 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 δ_1 is above unity: $\delta_1 \geq q \geq 1$, whereas the minimal value of δ_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

$$r \in [r_2, r_1], \; r_1 = \ln \delta_1^{1/2}, \; r_2 = \ln \delta_2^{-1/2} \tag{58}$$

An important point is that the value of the squeeze parameter is not uniquely determined by the conditions (55). 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

$$r_1 = r_2 = \rho = \frac{1}{2}\ln q = \ln\sqrt{\frac{1-C_S^2}{C_S^2}} \tag{59}$$

and the probability (37) expressed in terms of the distribution (52)

$$\mathsf{P}_G^{(1)}(x_1,x_2) = \frac{\cosh\rho}{2\pi|\alpha_L^{(1)}\alpha_L^{(2)}|}|\langle\beta e^{i\phi},\rho e^{2i\phi}|\alpha\rangle|^2, \tag{60}$$

$$\beta = e^{-\rho}x_1 + ie^{\rho}x_2 \tag{61}$$

yields the POVM

$$\hat{\Pi}_G^{(1)}(x_1,x_2) = \frac{\cosh\rho}{2\pi|\alpha_L^{(1)}\alpha_L^{(2)}|} \times |\beta e^{i\phi},\rho e^{2i\phi}\rangle\langle\beta e^{i\phi},\rho e^{2i\phi}|, \tag{62}$$

which is propotional to the pure squeezed state $|\beta e^{i\phi},\rho e^{2i\phi}\rangle$. The result (59) was reported in Ref. [37].

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 (58), we have the decomposition of the probability (37)

$$\begin{aligned}\mathsf{P}_G(x_1,x_2) &= \frac{\sqrt{\sigma_1\sigma_2}}{2\pi\sqrt{\sigma_G^{(1)}\sigma_G^{(2)}}} \\ &\times \int \mathrm{d}\beta_1\mathrm{d}\beta_2 G(x_1e^{-r}-\beta_1;\sigma_N^{(1)}(r)e^{-2r}) \\ &\times G(x_2e^{r}-\beta_2;\sigma_N^{(2)}(r)e^{2r})|\langle\beta e^{i\phi},re^{2i\phi}|\alpha\rangle|^2\end{aligned} \tag{63}$$

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

$$\begin{aligned}\hat{\Pi}_G(x_1,x_2) &= \frac{\sqrt{\sigma_1\sigma_2}}{2\pi\sqrt{\sigma_G^{(1)}\sigma_G^{(2)}}} \\ &\times \int \mathrm{d}\beta_1\mathrm{d}\beta_2 G(x_1e^{-r}-\beta_1;\sigma_N^{(1)}(r)e^{-2r}) \\ &\times G(x_2e^{r}-\beta_2;\sigma_N^{(2)}(r)e^{2r}) \\ &\times |\beta e^{i\phi},re^{2i\phi}\rangle\langle\beta e^{i\phi},re^{2i\phi}|\end{aligned} \tag{64}$$

decomposed into the Gaussian incoherent superposition of the pure squeezed states explicitly depends on the value of r.

Constructing POVM's (64) covariance matrix from Eq. (63) yields

$$\begin{aligned}\Sigma^{\mathrm{DH}} &= \begin{pmatrix} e^{2r} & 0 \\ 0 & e^{-2r}\end{pmatrix} + \begin{pmatrix} \delta_1 - e^{2r} & 0 \\ 0 & \delta_2 - e^{-2r}\end{pmatrix} \\ &\equiv \Sigma_0^{\mathrm{DH}} + \Sigma_N^{\mathrm{DH}},\end{aligned} \tag{65}$$

where, similarly to Eq. (27), we defined matrices of perfect measurement Σ_0^{DH} and excess noise Σ_N^{DH}. Note that the condition (55) is equivalent to the requirement of Σ_N^{DH} being positive.

Our analysis suggests that the ambiguity (nonuniqueness) of the Gaussian represention (64) 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 represention (47) for the POVM is well-defined, the photocount statistics can be reproduced using the squeezed-state representation (64) 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 "amount" of noise, i.e. the product of variances $\sigma_N^{(i)}$, is maximized by the midpoint of the interval $\frac{r_1+r_2}{2}$.

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

In this section, we apply the developed formalism for asymmetric measurements to analyze the Gaussian-modulated coherent-state (GMCS, or GG02 [1]) CV-QKD protocol. We evaluate the mutual information, Holevo information, and asymptotic secret fraction (secure key rate per symbol) under the untrusted-noise scenario to quantify how measurement asymmetry affects protocol security.

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

$$I_{\mathrm{AB}}^{\mathrm{H}} = \frac{1}{2}\log\left[1 + \frac{4TV_{\mathrm{A}}}{\sigma_x + 2\xi}\right], \tag{66}$$

where T is the channel transmission, ξ is the channel noise variance, V_{A} is Alice's modulation variance, and σ_x is given by Eq. (17). If Bob uses double-homodyne detection, mutual information takes the form

$$I_{\mathrm{AB}}^{\mathrm{DH}} = \frac{1}{2}\sum_i \log\left[1 + \frac{2TV_{\mathrm{A}}}{\sigma_i + \xi}\right], \tag{67}$$

where σ_i are given by Eq. (41). The details of these derivations are given in Appendix C.

Next, we compute the Holevo information in the untrusted-noise scenario, in which detection imperfections are modeled as additional noise accessible to the eavesdropper (Eve). We assume that Eve controls a Gaussian channel that modifies only the covariance matrix, leaving the mean unchanged, while Bob's measurements are considered ideal. Using the equivalence between the prepare-and-measure (PM) and entanglement-based (EB) pictures (see App. C), the Holevo information can be derived from the covariance matrix of the two mode squeezed vacuum (TMSV) state $\Sigma_{\mathrm{AB}}^{\mathrm{EB}}$. After transmitting through noisy channel (see Ref. [38]), TMSV co-

variance matrix reads

$$\Sigma_{\mathrm{AB}}^{\mathrm{EB}} = \begin{pmatrix} V\mathbb{I} & \sqrt{T\left(V^2-1\right)}\sigma_Z \\ \sqrt{T\left(V^2-1\right)}\sigma_Z & [T(V-1)+1+2\xi]\,\mathbb{I} \end{pmatrix} \equiv \begin{pmatrix} V\mathbb{I} & c\sigma_Z \\ c\sigma_Z & V_{\mathrm{B}}\mathbb{I} \end{pmatrix}, \tag{68}$$

where $\sigma_Z = \mathrm{diag}(1,-1)$, and

$$V = 1 + 4V_{\mathrm{A}}. \tag{69}$$

In the paradigm described previosly, Eve's entropy, $S_{\mathrm{E}} = S_{\mathrm{AB}}$ will be calculated from symplectic eigenvalues of the following covariance matrix:

$$\Sigma_{\mathrm{AB}}^{(m)} = \begin{pmatrix} V\mathbb{I} & c\sigma_z \\ c\sigma_z & V_{\mathrm{B}}\mathbb{I} + \Sigma_N^{(\mathrm{m})} \end{pmatrix}, \quad m \in \{\mathrm{H}, \mathrm{DH}\} \tag{70}$$

where Σ_N^{H} (Σ_N^{DH}) is given by Eq. (27) (Eq. (65)).

The conditional entropy $S_{\mathrm{E|B}} = S_{\mathrm{A|B}}$ is found via partial measurement formula [39], written for $\Sigma_{\mathrm{AB}}^{(m)}$ as follows:

$$\Sigma_{\mathrm{A|B}}^{(m)} = V\mathbb{I} - c^2\sigma_z(V_{\mathrm{B}}\mathbb{I} + \Sigma^{(m)})^{-1}\sigma_z, \quad m \in \{\mathrm{H}, \mathrm{DH}\}. \tag{71}$$

For homodyne detection, calculating symplectic eigenvalue of conditional covariance matrix as square root of the determinant yields:

$$\nu_3^{\mathrm{H}} = \sqrt{V\left(V - \frac{c^2}{V_{\mathrm{B}} + \sigma_N}\right)}. \tag{72}$$

The same calculation for double homodyne results in:

$$\nu_3^{\mathrm{DH}} = V\sqrt{\frac{\left(V_{\mathrm{B}} + \delta_1 - \frac{c^2}{V}\right)\left(V_{\mathrm{B}} + \delta_2 - \frac{c^2}{V}\right)}{\left(V_{\mathrm{B}} + \delta_1\right)\left(V_{\mathrm{B}} + \delta_2\right)}}. \tag{73}$$

The Holevo information is thus

$$\chi_{\mathrm{EB}} \equiv S_{\mathrm{E}} - S_{\mathrm{E|B}} = S_{\mathrm{AB}} - S_{\mathrm{A|B}} = \sum_{i=1,2} g(\nu_i) - g(\nu_3), \tag{74}$$

where

$$g(\nu) = \frac{\nu+1}{2}\log\frac{\nu+1}{2} - \frac{\nu-1}{2}\log\frac{\nu-1}{2}, \tag{75}$$

with appropriate substitution of ν_i depending on the measurement scheme.

Note that in the case of double homodyne detection, joint entropy S_{AB} and thereby Holevo information χ_{EB} are explicitly dependent on squeezing parameter $r \in [r_2, r_1]$ (58), as seen from the expression for covariance matrix (70). Moreover, as illustated by Fig. 6, the choice of r significantly affects the value of χ_{EB}. Regarding Fig. 6, for ideal double homodyne only $r = 0$ is allowed (black dot), yielding respective eigenvalues. When

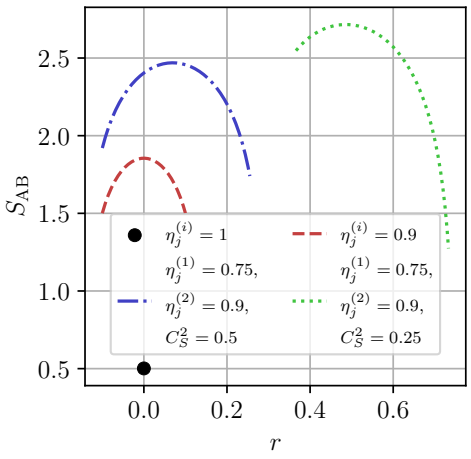


Figure 6: Joint entropy S_{AB} as a function of squeezing parameter r for various detector efficiencies. Unless specified, all beam spliiters are taken to be balanced. Parameters: $V_{\mathrm{A}} = 1, T = 0.95, \xi = 0.5 \cdot 10^{-3}$.

detection efficiencies are unity and $C_S^2 \neq 0.5$, the singular allowed value of r shifts to $r = \rho \neq 0$ (59), as shown at point ρ in Fig. 5. In this case, the value of S_{AB} is independent of ρ and determined solely by modulation variance V_{A} and channel parameters T and ξ. In the symmetrical but non-ideal case (red curve), symmetrical interval $[-r_1, r_1]$ arises, and joint entropy is maximized by the midpoint $r = 0$. In this case, choosing the POVM in the form superposition of coherent states (47) is not only allowed, but optimal. In asymmetrical case, if $C_S^2 = 0.5$ (blue curve), while using $r = 0$, i.e. Eq. (47), is possible, joint entropy is maximized by $r \neq 0$. Finally, in asymmetrical case with $C_S^2 \neq 0.5$ (green curve), usage of $r = 0$ results in one of eigenvalues being less than 1, which is impossible. Therefore, the more general representation given by Eq. (64) must be employed. For calculations, we will optimize r to maximize χ_{EB}.

The asymptotic secret fraction is

$$K = \beta I_{AB} - \chi_{EB}, \tag{76}$$

where β is the reconciliation efficiency.

The effects of detection asymmetry on mutual information, Holevo information, and the asymptotic secure key rate are illustrated in Fig. 7 for homodyne detection and Fig. 8 for double homodyne detection. From Fig. 7, it is evident that while asymmetry in homodyne detection generally degrades performance, the combination of a non-balanced beamsplitter and unequal detector efficiencies can be beneficial, resulting in maxima of the mutual information and secret fraction with given parameters. Correspondingly, the minima of the Holevo information exhibit similar behavior. Our numerical results for the homodyne case are qualitatively consistent with Ref. [24], namely the dependence of the asymptotic secret fraction on the beam splitter transmittance deviation and balanced detector deviation. Similar behavior

can be seen from Fig. 8 for double homodyne. However, while mutual information in double homodyne is generally higher than in homodyne, the significantly greater increase in Holevo information leads to a lower secret key fraction overall. An interesting feature illustrated by the black curves in this figure is that, under ideal detection efficiencies, variations in the beamsplitter transmission cause reduction in the Holevo information. As seen previosly in Fig. 6, this is the case of joint entropy being constant in r and therefore C_S^2 per Eq. (59), so that only dependency of conditional entropy on asymmetry remains. Conditional entropy is reduced by asymmetry, see Eq. (73).

The dependence of the asymptotic secure key rate on channel length in the presence of asymmetrical detection is shown in Fig. 9. These results indicate that in the untrusted noise scenario, asymmetry noise significantly reduces maximal channel length. Consistent with previous results, asymmetrical double homodyne performs worse than asymmetrical homodyne, due to Holevo information being high. The discrepancy in our Holevo information calculations leads to results for the asymptotic secret fraction dependence under double homodyne detection that differ from those in Ref. [26], although both works reach the same conclusion regarding its degraded performance.

VI. DISCUSSION AND CONCLUSION

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.

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.

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. (34)-(36)) and the corresponding POVM expressed in terms of the projectors onto coherent states (see Eq. (47)). 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 (47) 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. (64)), leading to explicit dependency of POVM on the squeezing parameter, which is defined by interval (58), illustrated by Fig. 5. This implies 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. This becomes relevant in untrusted noise security analysis. Namely, while mutual information between Alice and Bob and conditional entropy in Gaussian modulated coherent states CV-QKD protocol are calculated with variances of quadrature distribution (37) (see Appendix C for explicit calculations), joint entropy, and thereby Holevo information, is explicitly dependent on the squeezing parameter (see Fig. 6), due to the need of separating asymmetry noise from perfect measurement. We optimize the squeezing parameter to maximize Holevo information.

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. 9). In trusted-noise CV-QKD [27], 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 [30], 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).

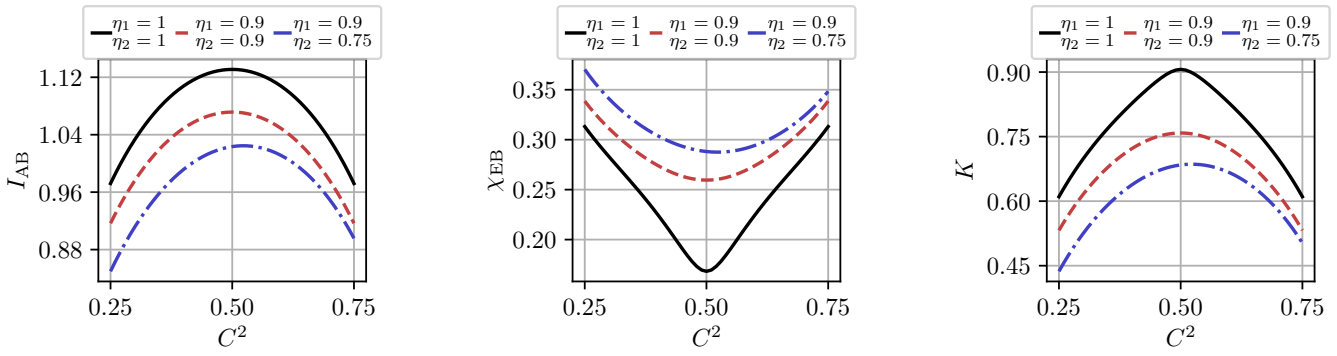
Appendix A: Statistical distance between Gaussian approximation and Skellam distribution

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

$$\mathsf{P}_G(\mu) = G(\mu - \mu_G; \sigma_G), \tag{A1}$$

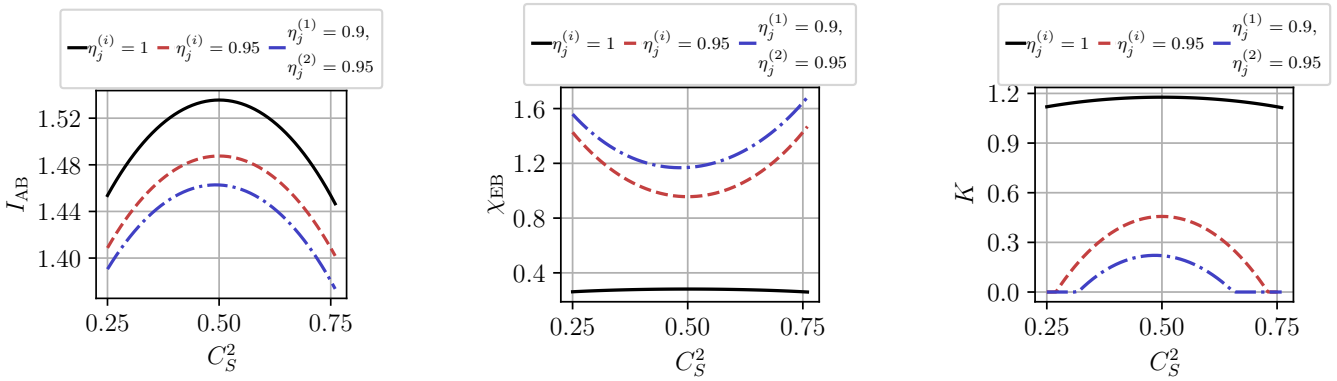
$$\sigma_G = \eta_1|\alpha_1|^2 + \eta_2|\alpha_2|^2 \approx (\eta_1 S^2 + \eta_2 C^2)|\alpha_L|^2, \tag{A2}$$

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



(a) (b) (c)

Figure 7: (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 $V_{\mathrm{A}} = 1, T = 0.95, \xi = 0.5 \cdot 10^{-3}, \beta = 0.95$



(a) (b) (c)

Figure 8: (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: $V_{\mathrm{A}} = 1, T = 0.95, \xi = 0.5 \cdot 10^{-3}, \beta = 0.95$.

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

$$\mathsf{P}(\mu) = e^{-\eta_1|\alpha_1|^2} e^{-\eta_2|\alpha_2|^2} \left(\frac{\eta_1|\alpha_1|^2}{\eta_2|\alpha_2|^2}\right)^{\mu/2} \times I_\mu\left(2\sqrt{\eta_1\eta_2|\alpha_1|^2|\alpha_2|^2}\right), \tag{A4}$$

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

$$D_P \equiv \mathtt{D}\left(\mathsf{P}, \mathsf{P}_G\right) \equiv \frac{1}{2} \sum_{\mu=-\infty}^{\infty} |\mathsf{P}(\mu) - \mathsf{P}_G(\mu)|. \tag{A5}$$

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

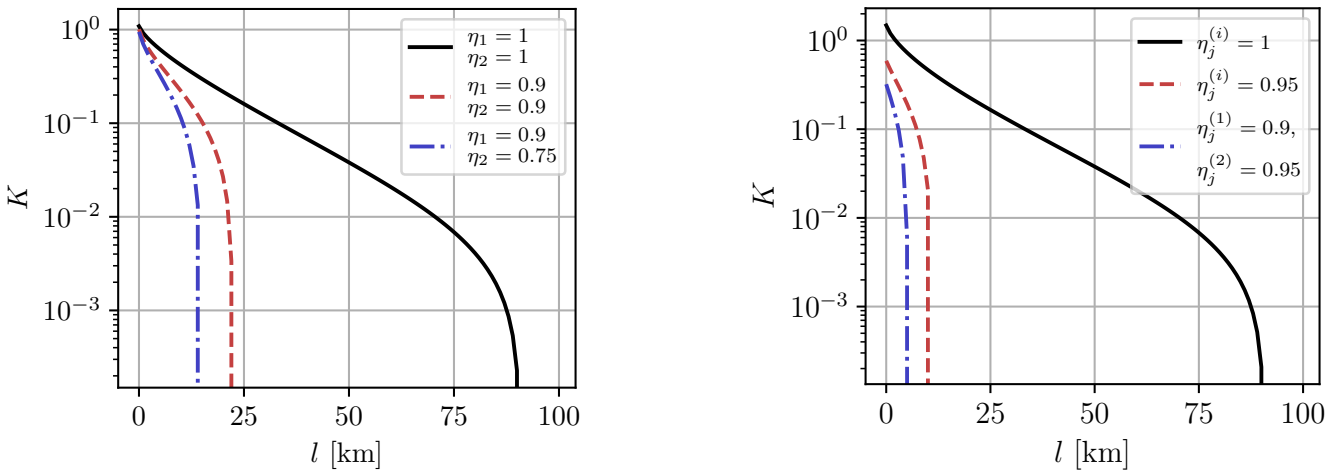
$$\int_{-\infty}^{\infty} \mathsf{P}_G(\mu)\mathrm{d}\mu = 1 \tag{A6}$$

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

$$\sum_{\mu=-\infty}^{\infty} \mathsf{P}_G(\mu) = \vartheta_3(\pi\mu_G, e^{-2\pi^2\sigma_G}) \equiv N_G \tag{A7}$$

where ϑ_3 is the Jacobi elliptic theta function [34].

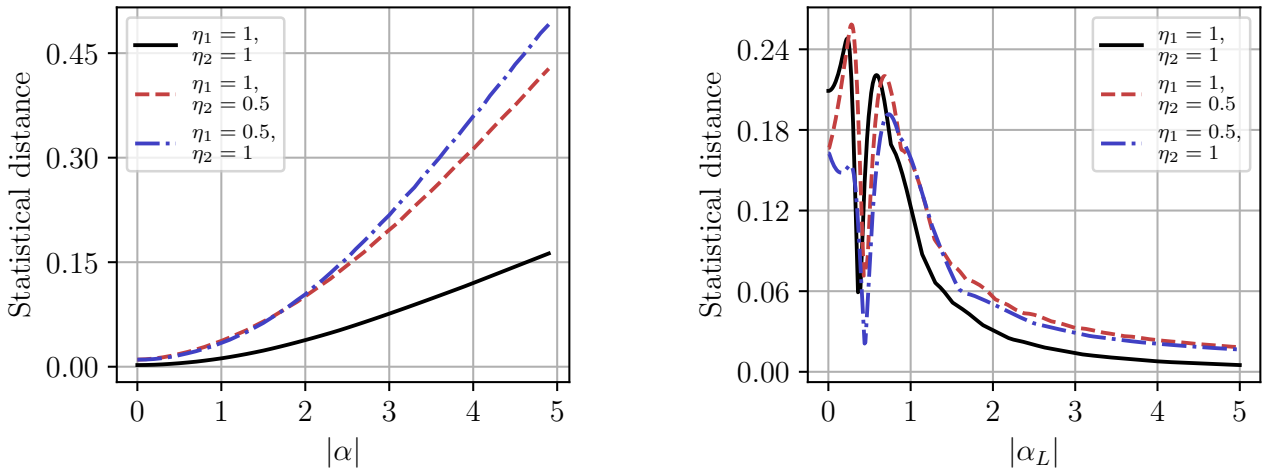
In the applicability region of the continuum limit, the normalization constant N_G is close to unity. The numerical analysis shows that $|N_G - 1| \leq 10^{-4}$ at $2\sigma_G \geq 1$.



(a) Homodyne detection

(b) Double homodyne detection

Figure 9: 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 $V_{\mathrm{A}} = 1, T = 0.95, \xi = 0.5 \cdot 10^{-3}, \beta = 0.95$. The losses are assumed to be 20 dB per 100 km.



(a) $|\alpha_L| = 5$

(b) $|\alpha| = 0.5$

Figure 10: Statistical distance $D_P = \mathtt{D}(\mathsf{P}, \mathsf{P}_G)$ as a function of (a) signal amplitude and (b) LO amplitude at different detector efficiencies.

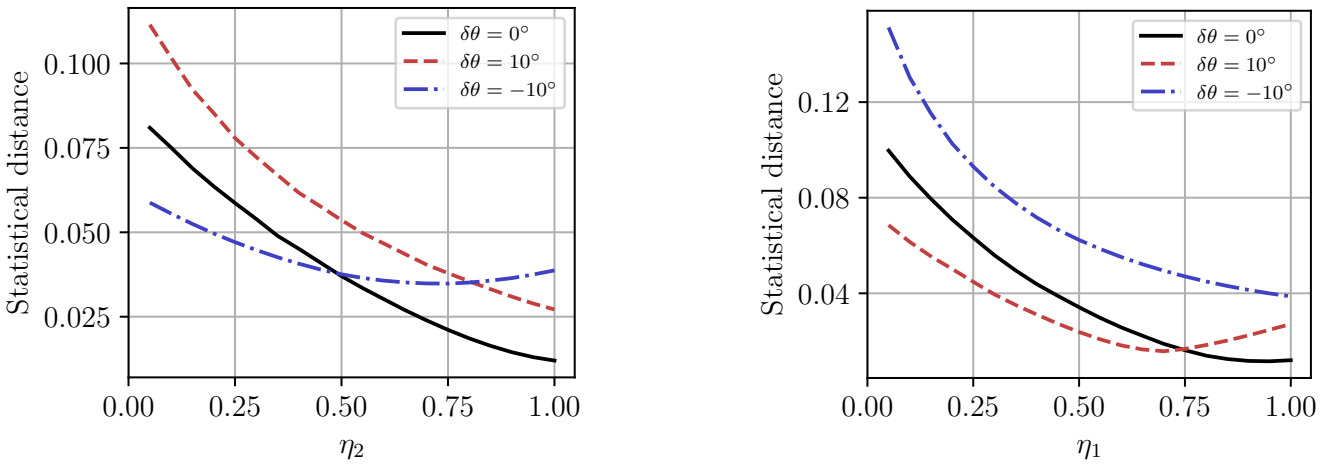
The latter gives the condition for the LO amplitude

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

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" α_N.

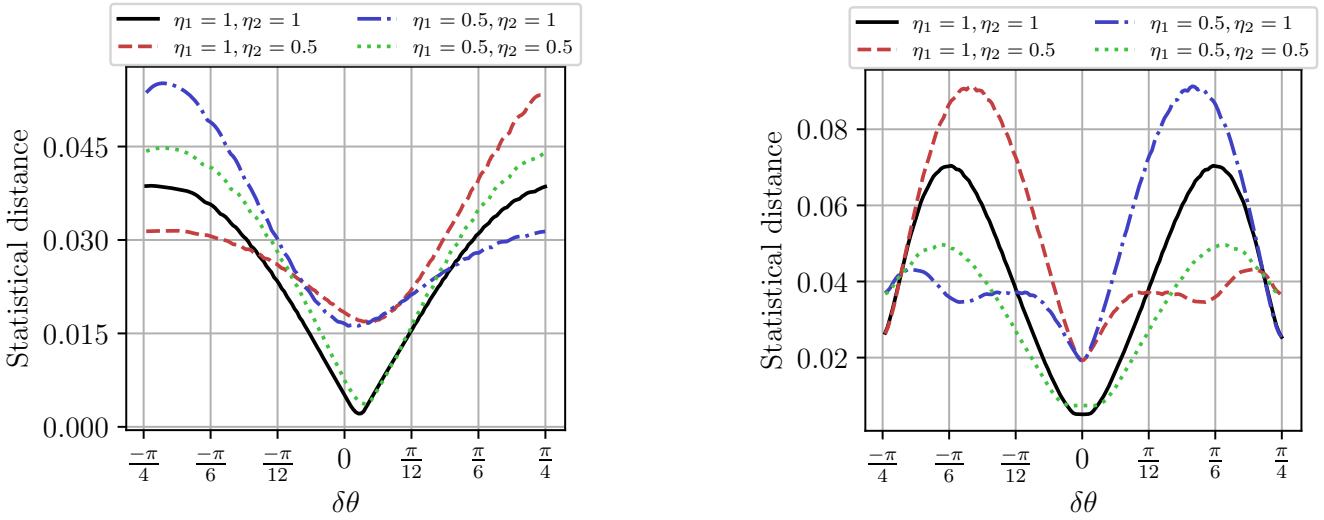
The curves presented in Fig. 10 illustrate how the accuracy of the Gaussian approximation is affected by the signal and LO amplitudes, $|\alpha|$ and $|\alpha_L|$. More specifically, in Fig. 10a (Fig. 10b), the statistical distance is numerically evaluated as a function of the amplitude $|\alpha|$ ($|\alpha_L|$) at different values of the photodetectors efficiencies provided that the value of the other amplitude $|\alpha_L|$ ($|\alpha|$) is fixed.

Referring to Fig. 10a, 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 $|\alpha| > 1$, 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



(a) $\eta_1 = 1$ (b) $\eta_2 = 1$

Figure 11: Statistical distance $D_P = \mathtt{D}(\mathsf{P}, \mathsf{P}_G)$ as a function of photodetector efficiency (a) η_2 at $\eta_1 = 1$ and (b) η_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 $|\alpha_L| = 5$.



(a) $|\psi\rangle = |\alpha\rangle$, $\alpha = 0.5$ (b) $|\psi\rangle = |n\rangle$, $n = 1$

Figure 12: Statistical distance $D_P = \mathtt{D}(\mathsf{P}, \mathsf{P}_G)$ 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 $|\alpha_L| = 5$.

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. 10b, 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) 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, $\lim_{|\alpha_L|\to 0} \mathsf{P}_G(\mu) = \delta(\mu)$.

From Fig. 10b, 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 η_1 and η_2. The curves plotted in Fig. 10 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

$$\delta\theta \equiv \frac{\pi}{4}-\theta. \tag{A9}$$

In Figure 11 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. 12 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-motonic 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:

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

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:

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

This formula can be deduced by performing a saddle-point analysis for the integral representation of the Bessel functions [40].

Heuristically, it can also be obtained from from the lowest order asymptotic expansion for the Bessel function [34]: $I_\mu(z)\approx e^z(1-(4\mu^2-1)/(8z))/\sqrt{2\pi z}$ assuming that, for small values of x, $1-x$ can be replaced with e^{-x} (the factors independent of μ are not essential because they can be incorporated into the normalization factor of the Gaussian approximation).

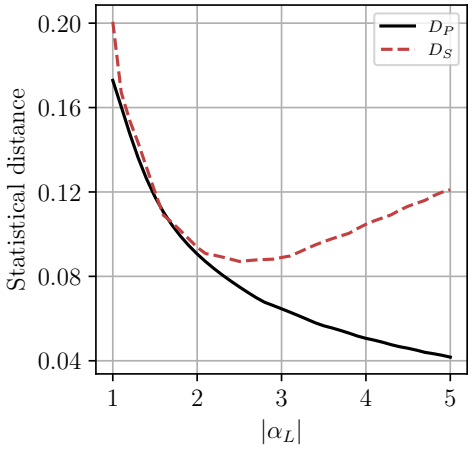


Figure 13: Distances, $D_P=D(\mathsf{P},\mathsf{P}_G)$ and $D_S=D(P,\mathsf{P}_G^{(s)})$, between the Skellam distribution, P, and two Gaussian approximations, P_G (see Eq. (10)) and $\mathsf{P}_G^{(s)}$ (see Eq. (B5)), as a function of $|\alpha_L|$ the beam splitter disbalance angle at $\delta\theta=15^\circ$ $\alpha=1$, and $\eta_1=\eta_2=1$.

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

$$z=2\sqrt{\eta_1\eta_2}|\alpha_1||\alpha_2|\approx 2CS\sqrt{\eta_1\eta_2}|\alpha_L|^2, \tag{B3}$$

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

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

$$\mathsf{P}_G^{(s)}(\mu)=G(\mu-\tilde{\mu}_G;\tilde{\sigma}_G), \tag{B5}$$

$$\tilde{\mu}_G=\sqrt{\eta_1\eta_2}\Big[CS|\alpha_L|^2\ln\frac{\eta_1 S^2}{\eta_2 C^2}+|\alpha_L|\langle\hat{x}_\phi\rangle\Big], \tag{B6}$$

$$\tilde{\sigma}_G=2CS\sqrt{\eta_1\eta_2}|\alpha_L|^2. \tag{B7}$$

Similar to Eq. (15), we cast the probabilty (B5) into

the following quadrature form:

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

$$\tilde{x} = \frac{\mu}{\sqrt{\eta_1\eta_2}|\alpha_L|} - CS|\alpha_L| \ln\frac{\eta_1 S^2}{\eta_2 C^2}, \tag{B9}$$

$$\tilde{\sigma}_x = \frac{2CS}{\sqrt{\eta_1\eta_2}}, \tag{B10}$$

so that we may follow the line of reasoning presented in Sec. II to deduce the POVM

$$\hat{\Pi}_G^{(s)} = \frac{1}{\sqrt{\eta_1\eta_2}|\alpha_L|} \times \int \mathrm{d}x' G(x-x';\tilde{\sigma}_N)|x',\phi\rangle\langle x',\phi| \tag{B11}$$

with the noise variance

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

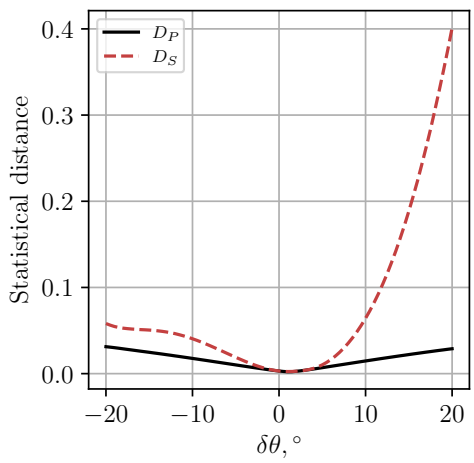


Figure 14: Distances, $D_P = D(\mathsf{P}, \mathsf{P}_G)$ and $D_S = D(\mathsf{P}, \mathsf{P}_G^{(s)})$, between the Skellam distribution, P, and two Gaussian approximations, P_G (see Eq. (10)) and $\mathsf{P}_G^{(s)}$ (see Eq. (B5)), as a function of the beam splitter disbalance angle $\delta\theta$ 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 13 demonstrates that, at $\delta\theta \neq 0$, by contrast to the distance between P and P_G, $D_P = \mathtt{D}(\mathsf{P}, \mathsf{P}_G)$ which is a monotonically decreasing function of $|\alpha_L|$, the distance between the Skellam distribution and the approximate distribution (B5), $D_S = \mathtt{D}(\mathsf{P}, \mathsf{P}_G^{(s)})$, reveals non-monotonic behaviour and increases with $|\alpha_L|$ at sufficiently large LO amplitudes. Referring to Fig. 14, 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 $2CS \le \sqrt{\eta_1\eta_2}$. 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 this appendix, we provide detailed derivations of mutual information between Alice and Bob in the GG02 protocol used in the main text. We also show the equivalency between Prepare-and-Measure (PM) and Entanglement-Based (EB) schemes.

Alice prepares an ensemble of coherent states $|\alpha = q + ip\rangle$ with probabilities $p_{\mathrm{A}}(\alpha)$ distributed according to Gaussian law,

$$p_{\mathrm{A}}(\alpha) = \frac{1}{\pi V_{\mathrm{A}}} \exp\left[-\frac{|\alpha|^2}{2V_{\mathrm{A}}}\right], \tag{C1}$$

$$\rho_{\mathrm{A}} = \int \mathrm{d}^2\alpha\, p_{\mathrm{A}}(\alpha)|\alpha\rangle\langle\alpha|. \tag{C2}$$

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

$$\tilde{\rho}_{\mathrm{A}} = \frac{1}{\pi\xi T}\int \mathrm{d}^2\tilde{\alpha}\, p_{\mathrm{A}}(\tilde{\alpha}) \int \mathrm{d}^2\alpha' \exp\left[-\frac{|\alpha'|^2}{\xi}\right] \times |\tilde{\alpha}-\alpha'\rangle\langle\tilde{\alpha}-\alpha'|, \tag{C3}$$

where ξ is the channel noise variance. Note that variance of $p_{\mathrm{A}}(\tilde{\alpha})$ 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:

$$p_{\mathrm{B}}(x,\tilde{\alpha}) \sim p_{\mathrm{A}}(\tilde{\alpha}) \int \mathrm{d}^2\alpha' \exp\left[-\frac{|\alpha'|^2}{\xi}\right] Q_x(\tilde{\alpha}-\alpha'), \tag{C4}$$

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

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

$$p_{\mathrm{B}}^{\mathrm{H}}(x,\tilde{\alpha}) \sim \exp\left[-\frac{(x-2\tilde{q})^2}{2\,(\sigma_x+2\xi)} - \frac{\tilde{q}^2}{2TV_{\mathrm{A}}}\right]. \tag{C5}$$

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

$$-\frac{1}{2}\begin{pmatrix}\tilde{q} & x\end{pmatrix}\begin{pmatrix}TV_{\mathrm{A}} & 2TV_{\mathrm{A}}\\ 2TV_{\mathrm{A}} & 4TV_{\mathrm{A}}+\sigma_x+2\xi\end{pmatrix}^{-1}\begin{pmatrix}\tilde{q}\\ x\end{pmatrix}$$
$$\equiv -\frac{1}{2}\begin{pmatrix}\tilde{q} & x\end{pmatrix}\Sigma^{\mathrm{H}^{-1}}\begin{pmatrix}\tilde{q}\\ x\end{pmatrix}, \tag{C6}$$

and with covariance matrix Σ^{H}, mutual information between Alice and Bob can be calculated as follows [41]

$$I_{\mathrm{AB}}^{\mathrm{H}}=\frac{1}{2}\log\frac{\Sigma_{11}^{\mathrm{H}}\Sigma_{22}^{\mathrm{H}}}{\det\Sigma^{\mathrm{H}}}=\frac{1}{2}\log\left[1+\frac{4TV_{\mathrm{A}}}{\sigma_x+2\xi}\right], \tag{C7}$$

where Σ_{ii}^{H} are diagonal elements of Σ^{H}, and all logarithms are base 2.

If double homodyne detection is used, from Eq. (C4) we have (see Eq. (37)):

$$p_{\mathrm{B}}^{\mathrm{DH}}(x,\tilde{\alpha})\sim$$
$$\exp\left[-\frac{(x_1-\tilde{q})^2}{2\left(\frac{\sigma_1}{2}+\frac{\xi}{2}\right)}-\frac{\tilde{q}^2}{2TV_{\mathrm{A}}}-\frac{(x_2-\tilde{p})^2}{2\left(\frac{\sigma_2}{2}+\frac{\xi}{2}\right)}-\frac{\tilde{p}^2}{2TV_{\mathrm{A}}}\right]. \tag{C8}$$

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

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

from which we obtain mutual information as

$$I_{\mathrm{AB}}^{\mathrm{DH}}=\frac{1}{2}\sum_{i=1,2}\log\frac{\Sigma_{11}^{\mathrm{DH}^{(i)}}\Sigma_{22}^{\mathrm{DH}^{(i)}}}{\det\Sigma^{\mathrm{DH}^{(i)}}}=$$
$$\frac{1}{2}\sum_i\log\left[1+\frac{2TV_{\mathrm{A}}}{\sigma_i+\xi}\right]. \tag{C10}$$

Now we move on to the equivalency between PM and EB schemes. Consider two mode squeezed vacuum state (TMSVS), in ket notation written as [42]

$$|\Psi\rangle_{\mathrm{AB}}=\sqrt{1-\lambda^2}\sum_{n=0}^{\infty}\lambda^n|n,n\rangle_{\mathrm{AB}}, \tag{C11}$$

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

$$p_{\mathrm{A}}^{\mathrm{EB}}(\beta)=\mathrm{Tr}\,\hat{\Pi}_\beta\varsigma_{\mathrm{A}}, \tag{C12}$$

where

$$\varsigma_{\mathrm{A}}=\mathrm{Tr}_{\mathrm{B}}\,\varsigma_{\mathrm{AB}}=\left(1-\lambda^2\right)\sum_n\lambda^{2n}|n\rangle\langle n|. \tag{C13}$$

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

$$p_{\mathrm{A}}^{\mathrm{EB}}(\beta)=\frac{\left(1-\lambda^2\right)}{\pi}\exp\left[\left(\lambda^2-1\right)|\beta|^2\right]. \tag{C14}$$

After Alice obtains outcome β, second mode before channel transmission reads

$$\varsigma_{\mathrm{B}}^{\beta}=|-\lambda\beta^*\rangle\langle-\lambda\beta^*| \tag{C15}$$

and the ensemble reads

$$\varsigma_{\mathrm{B}}=\int\mathrm{d}^2\beta\,p_{\mathrm{A}}^{\mathrm{EB}}(\beta)|-\lambda\beta^*\rangle\langle-\lambda\beta^*|, \tag{C16}$$

exactly the same as Eq. (C2) after substituting

$$\alpha=-\lambda\beta^*,\quad \frac{1-\lambda^2}{\lambda^2}=\frac{1}{2V_{\mathrm{A}}}. \tag{C17}$$

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, Intermode-interaction-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-oumandel experiment, Physica Scripta **97**, 105102 (2022).

[21] I. Yeremenko, M. Dmytruk, 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] J. O. Bartlett, A. J. M. Wilson, C. J. Chunnilall, and R. Kumar, Detector asymmetry in continuous variable quantum key distribution (2025).

[27] V. C. Usenko and R. Filip, Trusted noise in continuous-variable quantum key distribution: a threat and a defense, Entropy **18**, 20 (2016).

[28] 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).

[29] 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).

[30] 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).

[31] H. Qin, R. Kumar, and R. Alléaume, Quantum hacking: Saturation attack on practical continuous-variable quantum key distribution, Physical Review A **94**, 012325 (2016).

[32] 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. Villoresi, and P. Wallden, Advances in quantum cryptography, Adv. Opt. Photon. **12**, 1012 (2020).

[33] 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).

[34] 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.

[35] 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).

[36] C. Gerry and P. Knight, *Introductory Quantum Optics* (Cambridge University Press, NY, 2005) p. 317.

[37] M. G. Genoni, S. Mancini, and A. Serafini, General-dyne unravelling of a thermal master equation, Russian Journal of Mathematical Physics **21**, 329 (2014).

[38] 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).

[39] A. Serafini, *Quantum Continuous Variables: A Primer of Theoretical Methods* (CRC Press, Taylor & Francis Group, Boca Raton, 2017) p. 350.

[40] M. Freyberger, K. Vogel, and W. P. Schleich, From photon counts to quantum phase, Physics Letters A **176**, 41 (1993).

[41] 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.

[42] 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).