Continuous variable Gaussian and non-Gaussian states: Estimation, nonlocality and quantum key distribution

CHANDAN KUMAR

A thesis submitted for the partial fulfillment of

the degree of Doctor of Philosophy

Department of Physical Sciences
Indian Institute of Science Education & Research Mohali
Knowledge city, Sector 81, SAS Nagar, Manauli PO, Mohali 140306, Punjab, India.

December 2020

Declaration

The work presented in this thesis has been carried out by me under the guidance of Prof. Arvind at the Indian Institute of Science Education and Research Mohali.

This work has not been submitted in part or in full for a degree, diploma or a fellowship to any other University or Institute. Whenever contributions of others are involved, every effort has been made to indicate this clearly, with due acknowledgment of collaborative research and discussions. This thesis is a bonafide record of original work done by me and all sources listed within have been detailed in the bibliography.

Chandan Kumar

Place :
Date :

In my capacity as the supervisor of the candidate's PhD thesis work, I certify that the above statements by the candidate are true to the best of my knowledge.

Dr. Arvind
Professor of Physics
Department of Physical Sciences
IISER Mohali

Place :
Date :

Dedicated to my Guru

Prof. Arvind

Acknowledgments

I heartily thank Prof. Arvind for accepting me as PhD student. I am impressed by his ability to answer my nontrivial questions. I thank doctoral committee members Prof. Kavita Dorai and Dr. Sandeep Goyal. I thank Shikhar Arora for reading a major portion of the thesis. I also thank Sarbani Chatterjee, Rishabh, Raman, Dr. Ritabrata Sengupta, and Dr. Paramdeep Singh Chandi for reading the thesis. I thank Prof. N. Sathyamurthy for his constant academic guidance. I also thank Suguna Madam for her constant encouragement during the last many years. I thank my teachers, Prof. Ramandeep Singh Johal, Dr. K. P. Singh, Prof. Sudeshna Sinha, and Prof. Jasjeet Singh Bagla. I thank past and current members of QCQI group. I acknowledge IISER Mohali for various facilities, especially the Library, and funding during the PhD tenure.

Chandan Kumar

Abstract

Continuous variable (CV) quantum information processing is a well-established area of research today. We consider the quantized electromagnetic field as our system, where the quadrature operators of the electric field are the relevant degrees of freedom. This thesis focuses on quantum state tomography and quantum process tomography, nonlocality, and quantum key distribution (QKD) in the context of CV systems. We first explore the relative performance of various Gaussian measurement schemes in the estimation of single mode Gaussian states. We then discuss an optimal scheme for the characterization of n-mode Gaussian states using photon number measurements. Thereafter, we provide an optimal scheme for the characterization of n-mode Gaussian channels. In a different direction, we explore nonlocality in four mode Gaussian and non-Gaussian states of CV systems using multiphoton Bell-type inequality. We then move on to QKD, where two parties wish to establish a shared secret key. Here we show that photon subtracted two mode squeezed coherent (PSTMSC) states can enhance the performance of continuous variable measurement device independent quantum key distribution (CV-MDI-QKD) protocols. Finally, we examine the possibility of carrying out QKD using coherent states prepared on superconducting rings with a mesoscopic Josephson junction.
The thesis contains seven chapters, and the chapter-wise abstract is as follows.

Chapter 1

We introduce the subject of the thesis and present an overview of the current status of the research and open questions in the field. We then discuss the theoretical framework of CV systems and their description in the phase space. We also discuss different Gaussian operations and measurement schemes. We conclude with the motivations and the goals behind the work carried out in the thesis.

Chapter 2

We estimate single mode Gaussian states using four different measurement schemes: i) homodyne measurement, ii) sequential measurement, iii) Arthurs-Kelly scheme, and iv) heterodyne measurement, and compare their relative performance. We show that the optimal performance of the Arthurs-Kelly scheme and the sequential measurement is equal to the heterodyne measurement. Further, the heterodyne measurement outperforms the homodyne measurement in the mean estimation for squeezed state ensemble,

while the homodyne measurement outperforms the heterodyne measurement for variance estimation for squeezed state ensemble up to a certain range of squeezing parameter. We then proceed to a modified Hamiltonian in the Arthurs-Kelly scheme, where the two meters can be correlated. The optimal performance in this case corresponds to uncorrelated meters.

Chapter 3

We describe optimal schemes for the characterization of Gaussian states and Gaussian channels using photon-number-resolving detectors. A total of $2n^2 + 3n$ parameters are required for the complete description of an n-mode Gaussian state. Our scheme is able to tomograph an n-mode Gaussian state using $2n^2 + 3n$ distinct photon number measurements and is therefore optimal. Further, we propose an optimal scheme to characterize Gaussian channels using coherent state probes and photon number measurements.

Chapter 4

We study nonlocality in four-mode CV systems using a multiphoton Bell-type inequality, which is based on the Clauser-Horne 1974 Bell test inequality. The inequality is able to detect nonlocality in states with finite as well as arbitrary number of photons. We apply the inequality to two-photon states and four mode Gaussian states including pure and mixed state. We also consider leakage in the system modeled by beam splitters, and show that the inequality is able to detect the nonlocality of noisy Gaussian states as well. Finally, we examine nonlocality in pair-coherent states and entangled coherent states, which are prominent examples of nonclassical non-Gaussian states.

Chapter 5

We consider PSTMSC state as a resource state for CV-MDI-QKD protocols, and show that it enhances the transmission distances remarkably. We identify coherence, defined as the amount of displacement of the vacuum state, along with non-Gaussianity as advantageous resources, which can significantly enhance the performance of prevalent CV-MDI-QKD protocols. In the process, we also compute the covariance matrix of the PSTMSC state in the phase space formalism.

Chapter 6

We propose a QKD scheme based on long lived coherent states prepared on superconducting rings with a mesoscopic Josephson junction. These coherent states can be

stored for long durations in a no dissipation condition before actually performing the key distribution. We present two variants of the protocol, one requiring time stamping of the states and offering a higher key rate and the other without time stamping and a lower key rate. This work is a step towards having non-photon based QKD protocols, which will be eventually desirable as photon states cannot be stored for long, and therefore the key distribution has to be implemented immediately after photon exchange has occurred.

Chapter 7

We provide a summary of the research carried out for this thesis, and discuss possible future directions.

Contents

List of Publications

Out of this Thesis

1. **Chandan Kumar**, Jaskaran Singh, Soumyakanti Bose and Arvind. *Coherence assisted non-Gaussian measurement device independent quantum key distribution* Phys. Rev. A **100**, 052329, (2019).

2. **Chandan Kumar**, Ritabrata Sengupta and Arvind. *Optimal characterization of Gaussian channels using photon-number-resolving detector* Phys. Rev. A **102**, 012616, (2020).

3. **Chandan Kumar**, Jaskaran Singh and Arvind. *On-demand quantum key distribution using superconducting rings with a mesoscopic Josephson junction* arXiv:1808.06471 [quant-ph] (Submitted in journal).

4. **Chandan Kumar**, Gaurav Saxena and Arvind. *Multiphoton Bell's inequalities: a tool to unearth nonlocality of continuous variable states* arXiv:2008.08426v1 [quant-ph] (Submitted in journal)

5. **Chandan Kumar** and Arvind. *Estimation of Wigner distribution of Gaussian states* (Manuscript in preparation).

Other publications

1. Arghadip Koner, **Chandan Kumar** and N. Sathyamurthy. *Heat capacity of endohedral fullerenes Rg@C_{60} (Rg=He, Ne, Ar, Kr)*, Molecular Physics **116**, 19-20, 2728-2735, (2018).

2. Arghadip Koner, **Chandan Kumar**, Pradeep Kumar and N. Sathyamurthy. *Heat capacity of endohedral carbon nanotube Rg@CNT (Rg=He, Ne, Ar, Kr)*, Chemical Physics Letters **745**, 137251, (2020).

Expository articles

1. **Chandan Kumar** *Bound States of Spherically Symmetric Potentials: Heat Capacity Calculations*, Resonance: Journal of Science Education **25**, 11, (2020).

2. **Chandan Kumar** *Scattering and Bound States in One-Dimensional Potential*, (Accepted in Resonance: Journal of Science Education).

List of Figures

List of Tables

LIST OF TABLES

Abbreviations used in the Thesis

BS	:	Beam Splitter
CHSH	:	Clauser-Horne-Shimony-Holt
CV	:	Continuous Variable
dc	:	direct current
DV	:	Discrete Variable
EB	:	Entanglement Based
EPR	:	Einstein-Podolsky-Rosen
FT	:	Fourier Transform
MDI	:	Measurement Device Independent
PA	:	Photon Addition
PC	:	Photon Catalysis
PS	:	Photon Subtraction
PNRD	:	Photon Number Resolving Detector
POVM	:	Positive Operator Valued Measure
QIP	:	Quantum Information Processing
QKD	:	Quantum Key Distribution
QPT	:	Quantum Process Tomography
QSE	:	Quantum State Estimation
QST	:	Quantum State Tomography
RR	:	Reverse Reconciliation
SNR	:	Signal-to-Noise Ratio
SQUID	:	Superconducting Quantum Interference Device
TMSV	:	Two Mode Squeezed Vacuum
TMSC	:	Two Mode Squeezed Coherent

Chapter 1

Introduction

Quantum mechanics is a fundamental theory in physics that describes how nature acts at the smallest level. It introduces several ideas which are strikingly different from classical mechanics, and forces us to look at the world in a fundamentally new way. For example, observables such as energy, momentum and angular momentum of a bound system can only take discrete values. The act of measurement in quantum mechanics has a very different connotation as compared to that in classical physics. The result of a measurement is in general probabilistic and the act of measurement invariably disturbs the quantum system. Heisenberg uncertainty principle provides a lower bound for the product of noise in a position measurement and the momentum disturbance caused by that measurement [1]. Later, Kennard and Weyl provided a lower bound on the product of uncertainties of ideal measurements of position and momentum, where each of the measurements is performed on a different sub-ensemble of identically prepared systems [2, 3]. Therefore, quantum systems have inherent noise. Quantum mechanics allows a system to be in a superposition of different states. The measurement of an observable on a quantum system results in the collapse of the initial state, which can be expressed as a superposition of the eigenstates of the observable, to the eigenstate corresponding to the observed value. The fundamentally probabilistic nature of quantum mechanics advocated by the Copenhagen school has been contested by several researchers, and several different interpretations of quantum mechanics have been put forward [4, 5, 6, 7]. The problem of how the collapse occurs or more generally to describe the mechanism of measurement in quantum mechanics is an important problem known as the measurement problem and is still an open problem today. A famous paper by Einstein, Podolsky, and Rosen based on the analysis of joint quantum systems, conservation laws and the principle of locality, claimed that quantum mechanics is an incomplete theory. This is known as the EPR paradox [8], and the concepts of entanglement, steering and nonlocality originated as a direct consequence of the EPR

paradox [9, 10, 11].

A new field was born in the 1980s, known as quantum information, which combines ideas from quantum mechanics and information science and has several practical applications. Many of the non-intuitive ideas of quantum mechanics have been utilized to perform tasks which are not possible in the domain of classical information processing paradigm. For instance, the working principle of quantum computers is based on quantum phenomena, such as, superposition principle and quantum entanglement [12], while the no-cloning theorem forms the basis of quantum key distribution (QKD) protocols that allows unconditionally secure distribution of secret keys for cryptography [13].

Two different kinds of quantum systems, namely, discrete variable (DV) and continuous variable (CV) systems, can be used for encoding, manipulating, and decoding information in quantum information processing (QIP). If the system observables used for encoding information have discrete eigenvalues, the corresponding system is termed as a DV system. Quantum bit or Qubit, a system with two distinguishable states, is the simplest example of a DV system. There are many examples of such systems, including electron spin, photon polarization, superconducting qubits, and nucleus spin. In general, an n-level DV quantum system in this context is called a qudit. If the system observables used for encoding information have continuous eigenvalues, the corresponding system is termed as a CV system. There are many examples of such systems, including vibrational modes of solids, atomic ensembles, quantized electromagnetic field, and Josephson junctions. Different systems are suitable for different quantum tasks, for instance, atomic or solid-state based CV systems are promising candidates for quantum computation. Similarly, in the case of quantum communication, electromagnetic field in the optical frequencies is a feasible option. In the quantum optical context the states of the optical field, which go beyond the single photon level are expected to play a very important role.

QIP based on DV and CV systems are called DV and CV QIP, respectively. The Hilbert spaces associated with CV systems are infinite dimensional. In this thesis, our focus is on the CV systems where for most part we have dealt with the electromagnetic fields and in one chapter we have dealt with superconducting rings. In the electromagnetic fields case, we have considered quadrature amplitudes of the quantized electromagnetic field as the relevant degrees of freedom, which are mathematically equivalent to the position and momentum variables of the harmonic oscillator. The classical electromagnetic field is described as a collection of modes, which are solutions to the Maxwell equations and upon quantization each mode behaves like a harmonic oscillator. Most of the studies in CV systems have revolved around Gaussian states, for instance, coherent states, thermal states, and squeezed states [14, 15]. Similarly, most of the research is based on Gaussian operations, which are described by Hamiltonians

up to second order in the quadrature operators. Examples include displacement operations, phase change operations, single-mode squeezers, and two-mode beam splitters. These Gaussian operations transform a Gaussian state into another Gaussian state. This enhanced interest in the Gaussian states and the Gaussian operations is due to their elegant mathematical framework and ease in experimental implementations. From the mathematical point of view, the effect of Gaussian operations on Gaussian states is particularly easy as Gaussian states are completely specified by the first and second moments of the quadrature operators. Further, Gaussian states are easy to prepare as for any physical system with quadratic Hamiltonian, the ground and thermal states are Gaussian [16].

However, there are certain tasks, where non-Gaussian operations are required such as quantum entanglement distillation [17], quantum error correction [18] and universal quantum computation [19]. Similarly, Gaussian measurements based Bell inequalities can detect nonlocality only in non-Gaussian states [20, 21]. Further, several investigations have found that non-Gaussian operations, like photon addition, photon subtraction, and photon catalysis enhance nonclassicality as well as entanglement content [22, 23, 24, 25, 26, 27, 28, 29]. These non-Gaussian states have been shown to enhance the performance of various quantum protocols including quantum teleportation [24, 30, 31] and QKD [32, 33]. Therefore, the study of non-Gaussian states, which has gained relevance recently is important. Generally homodyne or heterodyne measurement scheme is employed in CV systems; however, the use of photon number resolving detector is required for the implementation of photon addition, subtraction and catalysis operations, and with current experimental advances, their implementation has become possible [34, 35].

In this thesis, we first deal with the estimation of the Wigner distribution of Gaussian states, where we compare the relative performance of various measurement schemes. In the next work, we consider the tomography of Gaussian states based on photon number measurements, which is then employed as a basis for another protocol for the tomography of Gaussian channels. Next, we study the interconversion of quantum optical nonclassicality to quantum nonlocality via passive operations. In the last topic involving electromagnetic fields, we delve into CV-QKD, where two distant parties want to establish a shared secret key. We investigate the advantages of photon subtraction, a non-Gaussian operation, on two mode squeezed coherent state in CV-QKD. In the last work, we explore the possibility of CV-QKD using superconducting rings with a mesoscopic Josephson junction. In this chapter, we summarize the basic notions of quantum mechanics and CV systems, including their phase space representation, which are necessary to read this thesis.

1.1 Basics of quantum mechanics

In this section, we briefly introduce the basic concepts of quantum mechanics.

State of a quantum mechanical system

The state of any quantum mechanical system $\mathcal{S}$ lies in a Hilbert space $\mathcal{H}$ (a vector space with defined inner product). The dimension of the Hilbert space $\mathcal{H}$ depends on the system under consideration and can be either finite or infinite. The state of a quantum system is completely described by a density operator $\hat{\rho}$ satisfying the following property:

$$\hat{\rho} = \hat{\rho}^{\dagger}, \quad \hat{\rho} \geq 0, \quad \mathrm{Tr}\hat{\rho} = 1. \tag{1.1}$$

A pure state is represented by a vector $|\Phi\rangle$ in the Hilbert space $\mathcal{H}$. Any two states in the Hilbert space $\mathcal{H}$, which differ from each other by a phase factor, represent the same state. The density operator corresponding to a pure state $|\Phi\rangle$ takes the form

$$\hat{\rho} = |\Phi\rangle\langle\Phi|. \tag{1.2}$$

The density operator of the most general mixed state can be described in terms of pure state as following:

$$\hat{\rho} = \sum_i p_i |\Phi_i\rangle\langle\Phi_i|, \quad p_i > 0, \quad \sum_i p_i = 1. \tag{1.3}$$

These Φ_i's need not be orthogonal. Further, any density operator can be realized through infinitely different ensembles [12, 36]. Pure and mixed states can be easily distinguished through the following condition:

$$\begin{aligned} &\mathrm{Tr}\left(\hat{\rho}^2\right) = 1, \quad \text{Pure state,} \\ &\mathrm{Tr}\left(\hat{\rho}^2\right) < 1, \quad \text{Mixed state.} \end{aligned} \tag{1.4}$$

Observables and expectation values

Any observable $\hat{A}$ in quantum mechanics is represented by a Hermitian operator, which can be expressed as

$$\hat{A} = \sum_k \lambda_k |\Psi_k\rangle\langle\Psi_k|, \quad \sum_k |\Psi_k\rangle\langle\Psi_k| = \mathbb{1}. \tag{1.5}$$

Here $|\Psi_k\rangle$'s are the eigenfunctions of the operator $\hat{A}$ and λ_k is the eigenvalue corresponding to the eigenfunction $|\Psi_k\rangle$. For a pure state $|\Psi\rangle$ and a mixed state $\hat{\rho}$, the expectation value of operator $\hat{A}$ is given by

$$\langle\hat{A}\rangle = \langle\Psi|\hat{A}|\Psi\rangle \quad \text{and} \quad \langle\hat{A}\rangle = \mathrm{Tr}(\hat{\rho}\hat{A}). \tag{1.6}$$

Unitary evolution

The evolution of a closed quantum system is unitary and may be written as [36]

$$\hat{U}(\alpha) = \exp\left[-i\int_{\alpha_i}^{\alpha_f} \frac{d\alpha\, \hat{G}(\alpha)}{\hbar}\right], \tag{1.7}$$

where $\hat{G}(\alpha)$ is the generator of the evolution or transformation, and α is the parameter characterizing the transformation. For the special case of time evolution caused by a time independent Hamiltonian $\hat{H}$, the unitary operator can be written as

$$\hat{U}(t) = e^{-it\hat{H}/\hbar}. \tag{1.8}$$

The time evolution of the density operator under the action of a unitary operator $\hat{U}(t)$ can be written as

$$\hat{\rho} \xrightarrow{\hat{U}(t)} \hat{U}(t)\hat{\rho}\hat{U}(t)^\dagger. \tag{1.9}$$

Quantum measurement

Quantum measurement is described by a set of operators $\{\hat{E}_i\}$, where the index i denotes the measurement outcome of an experiment. The measurement operators $\{\hat{E}_i\}$ satisfy the completeness relation $\sum_i \hat{E}_i^\dagger \hat{E}_i = \mathbb{1}$. If the initial state of the system before the measurement is given by pure state $|\psi\rangle$ or mixed state $\hat{\rho}$, the probability of i^{th} outcome is given by

$$p_i = \langle\psi|\hat{E}_i^\dagger \hat{E}_i|\psi\rangle \quad \text{or} \quad P_i = \text{Tr}(\hat{\rho}\hat{E}_i^\dagger \hat{E}_i), \tag{1.10}$$

and the post measurement state is given by

$$|\psi\rangle \to p_i^{-1/2}\hat{E}_i|\psi\rangle \quad \text{or} \quad \hat{\rho} \to P_i^{-1}(\hat{E}_i\rho\hat{E}_i^\dagger). \tag{1.11}$$

If we are only interested in the probabilities of various outcomes, we can define alternative set of positive operators $\hat{\Pi}_i = \hat{E}_i^\dagger \hat{E}_i$ describing the measurement. The set $\{\hat{\Pi}_i\}$ of operators satisfying the completeness relation $\sum_i \hat{\Pi}_i = \mathbb{1}$ is called positive operator valued measures (POVM). A special case of these measurements is called projective measurements and is represented by operators $\hat{P}_i$ satisfying

$$\hat{P}_i = \hat{P}_i^\dagger, \quad \hat{P}_i\hat{P}_j = \delta_{ij}\hat{P}_i, \quad \sum_i \hat{P}_i = \mathbb{1}. \tag{1.12}$$

Bipartite system

Consider a bipartite system composed of two subsystems A and B. Let $\mathcal{H}_A$ and $\mathcal{H}_B$ represent the Hilbert space of the subsystems A and B of dimensions m and n, respectively. The Hilbert space of the bipartite system is described by the tensor product of the individual subsystem

$$\mathcal{H}_S = \mathcal{H}_A \otimes \mathcal{H}_B, \tag{1.13}$$

and is of dimension $N = m \times n$. Let $\{|\psi_i\rangle\}$ and $\{|\phi_j\rangle\}$ form an orthonormal basis for the Hilbert spaces $\mathcal{H}_A$ and $\mathcal{H}_B$, respectively. A pure state of the combined system can be expressed as

$$|\Psi\rangle = \sum_{i,j} c_{ij} |\psi_i\rangle \otimes |\phi_j\rangle. \tag{1.14}$$

Let $|\psi\rangle$ and $|\phi\rangle$ represent pure states in Hilbert space $\mathcal{H}_A$ and $\mathcal{H}_B$, respectively. Then, any state of the combined system $|\Psi\rangle$ in Hilbert space $\mathcal{H}_S$, which can not be expressed in the tensor product form as

$$|\Psi\rangle \neq |\psi\rangle \otimes |\phi\rangle, \tag{1.15}$$

is termed entangled. A mixed state $\hat{\rho}_{AB}$ is said to be entangled if it can not be written as a convex sum of product states [37, 38]:

$$\hat{\rho}_{AB} \neq \sum_i p_i \hat{\rho}_{Ai} \otimes \hat{\rho}_{Bi}, \quad p_i > 0, \quad \sum_i p_i = 1, \tag{1.16}$$

where $\hat{\rho}_{Ai}$ and $\hat{\rho}_{Bi}$ are density matrices in $\mathcal{H}_A$ and $\mathcal{H}_B$, respectively.

Partial trace

Now we define the notion of partial trace which is helpful in obtaining the state of the subsystems from the state of the combined system. Suppose we are interested in evaluating the expectation value of operator $\hat{O}_A$ acting on the Hilbert space $\mathcal{H}_A$. Let $\hat{\rho}_{AB}$ be the density operator representing the state of the bipartite system, then the expectation value of the observable $\hat{O}_A \otimes \hat{\mathbb{1}}_B$ acting on the Hilbert space $\mathcal{H}_A \otimes \mathcal{H}_B$ can be calculated as

$$\langle \hat{O}_A \rangle = \text{Tr}(\hat{\rho}_{AB} \hat{O}_A \otimes \hat{\mathbb{1}}_B) = \text{Tr}_A(\hat{O}_A \text{Tr}_B(\hat{\rho}_{AB})). \tag{1.17}$$

The operation Tr_A or Tr_B is called partial trace and represents tracing of system A or B, respectively. We wish to know the equivalent density operator $\hat{\rho}_A$ of subsystem A that allows us to directly compute the expectation value of the operator $\hat{O}_A$ on the subsystem A as

$$\langle \hat{O}_A \rangle = \text{Tr}(\hat{\rho}_A \hat{O}_A). \tag{1.18}$$

On comparing Eqs. (1.17) and (1.18), we find that $\hat{\rho}_A = \mathrm{Tr}_B(\hat{\rho}_{AB})$, which is called reduced density operator of the subsystem A and is obtained by partial tracing of subsystem B from the bipartite density operator $\hat{\rho}_{AB}$. Thus, we can use the reduced density operator $\hat{\rho}_A$ to calculate the expectation value of any operator acting on the subsystem A without referring to the bipartite system.

1.2 Continuous variable systems

An n-mode CV system is equivalent to n quantized radiation modes of the electromagnetic field or n quantum harmonic oscillators. We represent an n-mode quantum system using n pairs of Hermitian operator $\hat{q}_i, \hat{p}_i$ $(i = 1, \ldots, n)$ known as quadrature operators [14, 15, 39, 40, 41, 42]. These quadrature operators can be grouped together in a column vector as

$$\hat{\xi} = (\hat{\xi}_i) = (\hat{q}_1, \hat{p}_1 \ldots, \hat{q}_n, \hat{p}_n)^T, \quad i = 1, 2, \ldots, 2n. \tag{1.19}$$

This allows us to write the canonical commutation relations for the quadrature operators in a compact form as ($\hbar$=1)

$$[\hat{\xi}_i, \hat{\xi}_j] = i\Omega_{ij}, \quad (i, j = 1, 2, ..., 2n), \tag{1.20}$$

where Ω is the $2n \times 2n$ matrix given by

$$\Omega = \bigoplus_{k=1}^{n} \omega = \begin{pmatrix} \omega & & \\ & \ddots & \\ & & \omega \end{pmatrix}, \quad \omega = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}. \tag{1.21}$$

The quadrature operators $\hat{q}$ and $\hat{p}$ have real and continuous eigenvalues q and p, respectively:

$$\hat{q}|q\rangle = q|q\rangle, \quad \hat{p}|p\rangle = p|p\rangle, \quad -\infty \leq q, p \leq \infty. \tag{1.22}$$

Various combinations of the inner product of the eigenfunctions $\{|q\rangle\}_{\Re}$ and $\{|p\rangle\}_{\Re}$ are given as following:

$$\langle q'|q\rangle = \delta(q' - q), \quad \langle p'|p\rangle = \delta(p' - p), \quad \langle q|p\rangle = (2\pi)^{-1/2} e^{iqp}. \tag{1.23}$$

These eigenfunctions also satisfy the following completeness relation:

$$\int dq|q\rangle\langle q| = \int dp|p\rangle\langle p| = \mathbb{1} \tag{1.24}$$

The eigenfunctions $\{|q\rangle\}_{\Re}$ and $\{|p\rangle\}_{\Re}$ are related by a Fourier transform:

$$\begin{aligned} |q\rangle =& \frac{1}{\sqrt{2\pi}} \int dp\, e^{-iqp} |p\rangle, \\ |p\rangle =& \frac{1}{\sqrt{2\pi}} \int dq\, e^{iqp} |q\rangle. \end{aligned} \tag{1.25}$$

We can also describe n-mode CV system using field operators $\hat{a}_i$ and $\hat{a}_i^\dagger$ ($i = 1, 2, \ldots, n$), where $\hat{a}_i$ and $\hat{a}_i^\dagger$ are called annihilation and creation operators respectively. The field operators and the quadrature operators are related as

$$\hat{a}_i = \frac{1}{\sqrt{2}}(\hat{q}_i + i\hat{p}_i), \quad \hat{a}_i^\dagger = \frac{1}{\sqrt{2}}(\hat{q}_i - i\hat{p}_i). \tag{1.26}$$

We arrange the annihilation operators and their conjugate creation operators in a column vector as

$$\hat{\xi}^{(c)} = (\xi_i^{(c)}) = (\hat{a}_1, \hat{a}_1^\dagger, \cdots, \hat{a}_n, \hat{a}_n^\dagger)^T \quad i = 1, 2, \ldots, 2n. \tag{1.27}$$

The canonical commutation relations for the field operators are given by

$$[\hat{\xi}_i^{(c)}, \hat{\xi}_j^{(c)}] = \Omega_{ij}, \quad (i, j = 1, 2, ..., 2n). \tag{1.28}$$

The Hilbert space of the i^{th} mode, $\mathcal{H}_i$, is spanned by the Fock states $|n_i\rangle$, $\quad \{n_i = 0,\, 1, \ldots, \infty\}$. These Fock states are the eigenvectors of the number operator $N_i = a_i^\dagger a_i$ with eigenvalues n_i. The eigenvalue n_i represents the number of photons in the i^{th} mode. The combined Hilbert space $\mathcal{H}^{\otimes n} = \otimes_{i=1}^n \mathcal{H}_i$ of the n-mode state is spanned by the product basis vector $|n_1 \ldots n_i \ldots n_n\rangle$ with $\{n_1, \ldots, n_i, \ldots, n_n = 0,\, 1, \ldots, \infty\}$. The field operators $\hat{a}_i$ and $\hat{a}_i^\dagger$ act irreducibly on the Hilbert space $\mathcal{H}_i$ and their action on the number state $|n_i\rangle$ can be easily determined by the commutation relations (1.28):

$$\begin{aligned} \hat{a_i}|n_i\rangle =& \sqrt{n_i}|n_i - 1\rangle \quad n_i \geq 1, \quad \hat{a_i}|0\rangle = 0 \\ \hat{a_i}^\dagger|n_i\rangle =& \sqrt{n_i + 1}|n_i + 1\rangle \quad n_i \geq 0 \end{aligned} \tag{1.29}$$

Note: The quadrature operators can be also be arranged in column vector in a different ordering as compared to Eq. (1.19):

$$\hat{\xi} = (\hat{q}_1 \cdots \hat{q}_n, \hat{p}_1, \cdots, \hat{p}_n)^T. \tag{1.30}$$

Consequently, the commutation relations are given by ($\hbar = 1$):

$$[\hat{\xi}_i, \hat{\xi}_j] = i\beta_{ij}, \quad \beta = \begin{pmatrix} 0_{n\times n} & \mathbb{1}_{n\times n} \\ -\mathbb{1}_{n\times n} & 0_{n\times n} \end{pmatrix}. \tag{1.31}$$

1.2.1 Phase space representation of CV systems

The phase space formulation of quantum mechanics is convenient for describing continuous variable quantum systems. We can represent an n-mode CV system in $2n$-dimensional phase space. We represent the $2n$ phase space variables as

$$\xi = (\xi_i) = (q_1, p_1, \ldots q_n, p_n)^T. \tag{1.32}$$

One problem in the phase space formulation of quantum mechanics stems from the fact that the classical variables q and p commute, whereas the quadrature operators $\hat{q}$ and $\hat{p}$ do not commute. Thus, the c-number correspondence, $\hat{q} \to q$ and $\hat{p} \to p$, is not one-to-one, when applied to functions in phase space. To illustrate this problem, let us consider the operator $\hat{q}\hat{p}$. Using the commutation relation $[\hat{q}, \hat{p}] = i$, we can express $\hat{q}\hat{p}$ in different ordered form as

$$\underbrace{\hat{q}\hat{p}}_{\text{standard}} = \underbrace{i + \hat{p}\hat{q}}_{\text{antistandard}} = \underbrace{(i + \hat{q}\hat{p} + \hat{p}\hat{q})/2}_{\text{symmetric}} \tag{1.33}$$

The corresponding c-numbers for different operator orderings are obviously not equal:

$$qp \neq i + qp \neq (i + 2qp)/2. \tag{1.34}$$

We also illustrate this problem for the field operators $\hat{a}$ and $\hat{a}^\dagger$, where we consider three different ordered forms: symmetric, antinormal, and normal. Let us consider the operator $(\hat{a} + \hat{a}^\dagger)^2$ and use the commutation relation $[\hat{a}, \hat{a}^\dagger] = 1$ to expand it in different ordered forms. The c-numbers are obtained in this case by the replacement $\hat{a} \to \alpha$, $\hat{a}^\dagger \to \alpha^*$. As we can see from Table 1.1 that the c-numbers for different operator orderings are not equal. To overcome this problem, we set up a one-to-one

Table 1.1: Different operator orderings and c-number correspondence

Symmetric (W)		Antinormal (P)		Normal (Q)
$\sum_{m,n} c^S_{m,n} \{\hat{a}^{\dagger m} \hat{a}^n\}_S$		$\sum_{m,n} c^A_{m,n} \hat{a}^m \hat{a}^{\dagger n}$		$\sum_{m,n} c^N_{m,n} \hat{a}^{\dagger m} \hat{a}^n$
$\hat{a}^2 + \hat{a}^{\dagger 2} + \hat{a}\hat{a}^\dagger + \hat{a}^\dagger\hat{a}$	=	$\hat{a}^2 + \hat{a}^{\dagger 2} + 2\hat{a}\hat{a}^\dagger - 1$	=	$\hat{a}^2 + \hat{a}^{\dagger 2} + 2\hat{a}^\dagger\hat{a} + 1$
$\alpha^2 + \alpha^{*^2} + 2\lvert\alpha\rvert^2$	$\neq$	$\alpha^2 + \alpha^{*^2} + 2\lvert\alpha\rvert^2 - 1$	$\neq$	$\alpha^2 + \alpha^{*^2} + 2\lvert\alpha\rvert^2$ +1

correspondence between operators on the Hilbert space and c-numbers on the phase space by specifying a definite operator ordering. As we shall see later in this chapter

that infinitely different orderings are possible. Symmetric or Weyl ordering, normal ordering, and antinormal ordering are the three most used operator orderings.

Converting an arbitrary ordered operator into a specific ordered form through repeated application of commutation relation might become a complicated task. However, such a task can be easily accomplished with the help of displacement operators. We define the displacement operator as

$$D(\alpha) = e^{\alpha\hat{a}^\dagger - \alpha^*\hat{a}}, \quad \text{or} \quad D(q,p) = e^{i(p\hat{q}-q\hat{p})}, \tag{1.35}$$

with $\alpha = (q+ip)/\sqrt{2}$. The composition rule for the displacement operators can be written as

$$\begin{aligned} D(\alpha)D(\beta) &= e^{(\alpha\beta^* - \alpha^*\beta)/2} D(\alpha+\beta), \quad \text{or} \\ D(q',p')D(q,p) &= e^{i(p'q-q'p)/2} D(q'+q, p'+p). \end{aligned} \tag{1.36}$$

The action of the displacement operator on the quadrature operators and the field operators can be written in a compact form as

$$D(\alpha)^\dagger \left(\hat{q},\hat{p},\hat{a},\hat{a}^\dagger\right) D(\alpha) = \left(\hat{q}+q, \hat{p}+p, \hat{a}+\alpha, \hat{a}^\dagger+\alpha^*\right). \tag{1.37}$$

The displacement operator serves as an ideal orthonormal basis for the Hilbert-Schmidt operators on the Hilbert space $\mathcal{H}$. The inner product of two Hilbert-Schmidt operators $\hat{A}$ and $\hat{B}$ is given by

$$(\hat{A},\hat{B}) = \text{Tr}\left(\hat{A}^\dagger \hat{B}\right). \tag{1.38}$$

Thus, the inner products of the displacement operators can be written as

$$\begin{aligned} (D(\alpha), D(\beta)) = \text{Tr}[D(\alpha)^\dagger D(\beta)] &= \pi\delta^2(\alpha-\beta), \quad \text{or} \\ (D(q',p')D(q,p)) = \text{Tr}[D(q',p')^\dagger D(q,p)] &= 2\pi\delta(q'-q)\delta(p'-p). \end{aligned} \tag{1.39}$$

In the next section, we use different ordered forms of displacement operator for defining various quasiprobability distributions.

1.2.2 Quasiprobability distributions

Any quantum state $|\Psi\rangle$ can be expanded using a complete set of basis states; for instance, the state $|\Psi\rangle$ can be written in the $|q\rangle$ basis as

$$|\Psi\rangle = \int dq |q\rangle\langle q|\Psi\rangle. \tag{1.40}$$

The generalization for the Hilbert-Schmidt operators follows in an analogous way. Any operator $\hat{A}$ can be expanded as

$$\begin{aligned}\hat{A} &= \int \frac{d^2\alpha}{\pi} D(\alpha)(D(\alpha), \hat{A}) \quad \text{Projection on } D(\alpha) \\ &= \underbrace{\int \frac{d^2\alpha}{\pi} D(\alpha)\text{Tr}[D(\alpha)^\dagger \hat{A}]}_{\text{Fourier transform on operator space}}.\end{aligned} \tag{1.41}$$

The conventional form can be obtained by replacing $\alpha \to -\alpha$ in the above equation:

$$\hat{A} = \int \frac{d^2\alpha}{\pi} D(\alpha)^\dagger \text{Tr}[D(\alpha)\hat{A}]. \tag{1.42}$$

For real variables, Eq. (1.42) can be written as

$$\hat{A} = \int \frac{dq\, dp}{2\pi} D(q,p)^\dagger \text{Tr}[D(q,p)\hat{A}]. \tag{1.43}$$

The displacement operator $D(\alpha)$ or $D(q,p)$ is symmetrically ordered and the above procedure puts any given operator $\hat{A}$ in symmetric ordered form. We now describe the procedure for ordering any operator in different ordered forms.

The displacement operator $D(\alpha)$ can be written in different ordered forms using the Baker-Campbell-Hausdorff formula as follows:

$$D(\alpha) = \underbrace{e^{\alpha\hat{a}^\dagger - \alpha^*\hat{a}}}_{\text{Symmetric}} = e^{-\frac{1}{2}|\alpha|^2} \underbrace{e^{\alpha\hat{a}^\dagger} e^{-\alpha^*\hat{a}}}_{\text{Normal}} = e^{\frac{1}{2}|\alpha|^2} \underbrace{e^{-\alpha^*\hat{a}} e^{\alpha\hat{a}^\dagger}}_{\text{Antinormal}}. \tag{1.44}$$

In fact, we can parameterize different orderings of $D(\alpha)$ through parameter σ as

$$D_\sigma(\alpha) = e^{\sigma\frac{1}{2}|\alpha|^2} D(\alpha), \quad -1 \le \sigma \le 1, \tag{1.45}$$

with following special cases:

$$\begin{aligned}\sigma = -1: &\quad D_{-1}(\alpha) = e^{-\frac{1}{2}|\alpha|^2} D(\alpha), \quad \text{Antinormal} \\ \sigma = 0: &\quad D_0(\alpha) = D(\alpha), \quad \text{Symmetric} \\ \sigma = 1: &\quad D_{+1}(\alpha) = e^{+\frac{1}{2}|\alpha|^2} D(\alpha). \quad \text{Normal}\end{aligned} \tag{1.46}$$

Now, Eq. (1.42) in terms of parameter σ can be written using Eq. (1.45) as follows:

$$\begin{aligned}\hat{A}_\sigma(\hat{a}, \hat{a}^\dagger) &= \int \frac{d^2\alpha}{\pi} \text{Tr}[D(\alpha)\hat{A}] e^{\frac{-\sigma|\alpha|^2}{2}} D_\sigma^\dagger(\alpha), \\ &= \int \frac{d^2\alpha}{\pi} \text{Tr}[D_{-\sigma}(\alpha)\hat{A}] D_\sigma^\dagger(\alpha).\end{aligned} \tag{1.47}$$

We consider Eq. (1.47) for the special case of $\sigma = +1$:

$$\begin{aligned}\hat{A}_{+1}(\hat{a}, \hat{a}^\dagger) &= \int \frac{d^2\alpha}{\pi} Tr[D_{-1}(\alpha)\hat{A}]D^\dagger_{+1}(\alpha), \\ &= \int \frac{d^2\alpha}{\pi} \mathrm{Tr}[e^{-\alpha^*\hat{a}} e^{\alpha\hat{a}^\dagger}\hat{A}]e^{-\alpha\hat{a}^\dagger} e^{\alpha^*\hat{a}}.\end{aligned} \tag{1.48}$$

Since $\hat{A}_{+1}(\hat{a}, \hat{a}^\dagger)$ is the normally ordered form of the operator $\hat{A}$, the corresponding c-number function on the phase space is obtained by replacing $\hat{a} \to \beta$, $\hat{a}^\dagger \to \beta^*$:

$$A_{+1}(\beta, \beta^*) = \int \frac{d^2\alpha}{\pi} \underbrace{\widetilde{A}_{+1}(\alpha, \alpha^*)}_{\mathrm{Tr}[e^{-\alpha^*\hat{a}} e^{\alpha\hat{a}^\dagger}\hat{A}]} \exp(\beta\alpha^* - \alpha\beta^*). \tag{1.49}$$

Here $A_{+1}(\beta, \beta^*)$ and $\widetilde{A}_{+1}(\alpha, \alpha^*)$ form a two-dimensional Fourier transform pairs. We can similarly define c-number function on the phase space for σ-ordered operators as follows:

$$A_\sigma(\beta, \beta^*) = \int \frac{d^2\alpha}{\pi} \underbrace{\widetilde{A}_\sigma(\alpha, \alpha^*)}_{\mathrm{Tr}[D_{-\sigma}(\alpha)\hat{A}]} \exp(\beta\alpha^* - \alpha\beta^*). \tag{1.50}$$

In the special case, when the operator $\hat{A}$ represents a density operator $\hat{\rho}$, $Tr[D_{-\sigma}(\alpha)\hat{\rho}]$ is called characteristic function and is denoted as $\chi_\sigma(\alpha, \alpha^*)$. For the case of density operator $\hat{\rho}$, Eq. (1.50) becomes

$$\rho_\sigma(\beta, \beta^*) = \int \frac{d^2\alpha}{\pi} \underbrace{\chi_\sigma(\alpha, \alpha^*)}_{\mathrm{Tr}[D_{-\sigma}(\alpha)\hat{\rho}]} \exp(\beta\alpha^* - \alpha\beta^*). \tag{1.51}$$

The relation between c-number functions $\rho_\sigma(\beta, \beta^*)$ for $\sigma = -1, 0, +1$, and different quasiprobability distributions is given below:

$$\begin{aligned}P(\beta, \beta^*) &= \frac{1}{\pi}\rho_{-1}(\beta, \beta^*), \quad \text{Antinormal} \\ W(\beta, \beta^*) &= \frac{1}{\pi}\rho_0(\beta, \beta^*), \quad \text{Symmetric} \\ Q(\beta, \beta^*) &= \frac{1}{\pi}\rho_{+1}(\beta, \beta^*). \quad \text{Normal}\end{aligned} \tag{1.52}$$

Here P, W, and Q represents Glauber-Sudarshan distribution, Wigner distribution, and Husimi distribution. Table 1.2 summarizes the relationship between the characteristic functions and quasiprobability distributions.

Table 1.2: Characteristic functions and quasiprobability distributions

Characteristic function	Two-dimensional Fourier transform	Quasiprobability distribution
$\chi_P(\alpha,\alpha^*) = \text{Tr}[\hat{\rho}e^{\alpha\hat{a}^\dagger}e^{-\alpha^*\hat{a}}]$	$\int \frac{d^2\alpha}{\pi^2} e^{\alpha^*\beta-\alpha\beta^*}\chi_P(\alpha,\alpha^*)$	Sudarshan-Glauber $P(\beta,\beta^*)$
$\chi_W(\alpha,\alpha^*) = \text{Tr}[\hat{\rho}e^{\alpha\hat{a}^\dagger-\alpha^*\hat{a}}]$	$\int \frac{d^2\alpha}{\pi^2} e^{\alpha^*\beta-\alpha\beta^*}\chi_W(\alpha,\alpha^*)$	Wigner $W(\beta,\beta^*)$
$\chi_Q(\alpha,\alpha^*) = \text{Tr}[\hat{\rho}e^{-\alpha^*\hat{a}}e^{\alpha\hat{a}^\dagger}]$	$\int \frac{d^2\alpha}{\pi^2} e^{\alpha^*\beta-\alpha\beta^*}\chi_Q(\alpha,\alpha^*)$	Husimi $Q(\beta,\beta^*)$

Properties of quasiprobability distributions

The distribution functions P, W, and Q are called quasiprobability distributions as they fail to satisfy one or more of the three Kolomogrov axioms of probability as shown in Table 1.3. Wigner distribution and Glauber-Sudarshan distribution can attain positive

Table 1.3: Kolomogrov axioms and probability $\mathcal{P}(\alpha)$

Axiom	Condition	
1	$0 \leq \mathcal{P}(\alpha) \leq 1$	✓/✗
2	$\int d^2\alpha \mathcal{P}(\alpha) = 1$	✓
3	Mutually exclusive	✗

as well as negative values, whereas Husimi distribution is always positive. However, all three quasiprobability distributions fail to satisfy the third axiom related to mutually exclusive events as two different coherent states are not orthogonal, and thus these phase space distributions do not represent the probability of mutually exclusive events in the phase space.

Relations among different phase space functions

We now describe the connection between various quasiprobability distributions and their Fourier transforms. Equation (1.44) implies the following relation between different characteristic functions:

$$\chi_W(\alpha) = e^{-\frac{1}{2}|\alpha|^2}\chi_P(\alpha) = e^{\frac{1}{2}|\alpha|^2}\chi_Q(\alpha). \tag{1.53}$$

Let $F(\omega)$ represents the Fourier transform of $f(t)$: $f(t) \xrightarrow{F.T.} F(\omega)$. Then, the convolution theorem states that the Fourier transform of the convolution of two function is equal to the multiplication of their Fourier transform and vice versa.

$$\underbrace{f_1(t) * f_2(t)}_{\text{Convolution}} \xrightarrow{F.T.} \underbrace{F_1(\omega) \times F_2(\omega)}_{\text{Multiplication}}, \quad | \quad \underbrace{f_1(t) \times f_2(t)}_{\text{Multiplication}} \xrightarrow{F.T.} \underbrace{F_1(\omega) * F_2(\omega)}_{\text{Convolution}}. \tag{1.54}$$

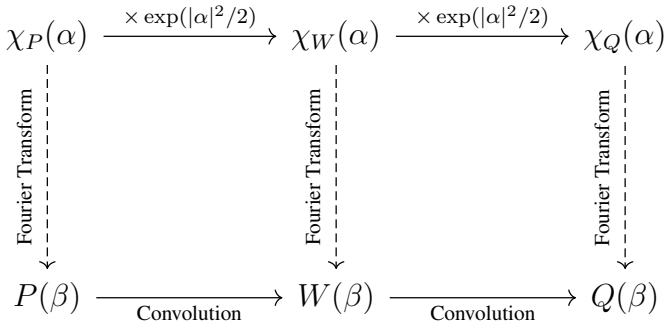
Hence, we can obtain the Wigner distribution from the P-distribution by a Gaussian convolution:

$$W(\beta) = \frac{2}{\pi} \int d^2\gamma \, P(\gamma) \exp(-2|\beta - \gamma|^2). \tag{1.55}$$

Similarly, the Q-distribution can be obtained from the Wigner distribution by convolution with a Gaussian function:

$$Q(\beta) = \frac{2}{\pi} \int d^2\gamma \, W(\gamma) \exp(-2|\beta - \gamma|^2). \tag{1.56}$$

Since convolution smoothens a function, the Wigner distribution, which is the Gaussian convolution of the P-distribution, has no singularities (derivatives of delta function), and the Husimi distribution, a Gaussian convolution of the Wigner distribution, is always positive. The relation between the characteristic functions and quasiprobability distributions can be illustrated through the following diagram:



We now describe optical equivalence theorem, which enables us to compute averages using phase space distributions.

Optical equivalence theorem

We first introduce optical equivalence theorem for normally ordered operators, which was devised by Sudarshan [43]:

$$\langle f^N(\hat{a}, \hat{a}^\dagger) \rangle = \frac{1}{\pi} \int d^2\alpha \, \hat{\rho}^{(A)}(\alpha, \alpha^*) f^{(N)}(\alpha, \alpha^*). \tag{1.57}$$

This theorem provides an elegant method to evaluate the average of normally ordered operators in the phase space. We can further write Eq. (1.57) using Eq. (1.52) as

$$\langle f^N(\hat{a},\hat{a}^\dagger)\rangle = \int d^2\alpha\, P(\alpha,\alpha^*) f^{(N)}(\alpha,\alpha^*). \tag{1.58}$$

Thus the average of normally ordered operator $f^N(\hat{a},\hat{a}^\dagger)$ is the P distribution weighted average of $f^{(N)}(\alpha,\alpha^*)$. Since the Glauber-Sudarshan representation of the coherent state $|\alpha_0\rangle$ is $\delta^2(\alpha-\alpha_0)$, the average number of photons in the coherent state can be easily evaluated using the optical equivalence theorem as follows:

$$\langle \hat{a}^\dagger\hat{a}\rangle = \int d^2\alpha\, |\alpha|^2\delta^2(\alpha-\alpha_0) = |\alpha_0|^2. \tag{1.59}$$

Equation (1.57) was later generalized for evaluating the averages of general ordered operators [44, 45, 46, 47]:

$$\langle f^{(\sigma)}(\hat{a},\hat{a}^\dagger)\rangle = \frac{1}{\pi}\int d^2\alpha\, \hat{\rho}^{(\overline{\sigma})}(\alpha,\alpha^*) f^{(\sigma)}(\alpha,\alpha^*). \tag{1.60}$$

Here $\overline{\sigma}$ represents the reciprocal ordering of σ. The normal ordering and the antinormal ordering are reciprocal of each other, while the symmetric ordering is reciprocal of itself. Therefore, while the normal ordering and the antinormal ordering of a density operator correspond to the Q and P representations, respectively, they are used for evaluating the averages of normally ordered and antinormally ordered operators.

Properties of the Wigner distribution

The Wigner distribution is one of the most widely used distribution functions. Here we study some of its properties. It can be written in terms of real canonical conjugate variables q and p as follows:

$$\begin{aligned} W(q,p) &= \int \frac{dq'dp'}{(2\pi)^2}\exp(i(q'p-p'q))\mathrm{Tr}[\exp[D(q',p')\hat{\rho}], \\ &= \int \frac{dq'dp'}{(2\pi)^2}\exp(i(q'p-p'q))\mathrm{Tr}[\exp[i(p'\hat{q}-q'\hat{p})]\hat{\rho}], \\ &= \int \frac{dq'}{2\pi}\exp(iq'p)\langle q-\frac{q'}{2}|\hat{\rho}|q+\frac{q'}{2}\rangle. \end{aligned} \tag{1.61}$$

We can deduce some basic properties of the Wigner distribution from the properties of the density operator $\hat{\rho}$ (1.1):

$$\begin{aligned} \hat{\rho}^\dagger = \hat{\rho} &\implies W(q,p) \text{ is real}, \\ \mathrm{Tr}\hat{\rho} = 1 &\implies \int_{\mathcal{R}^2} dqdp\, W(q,p) = 1. \end{aligned} \tag{1.62}$$

However, $\hat{\rho} \geq 0$ does not mean that $W(q,p) \geq 0$. Table 1.4 illustrates the important differences between the Hilbert space and the phase space picture for an n-mode CV system.

Table 1.4: The Hilbert space and the phase space picture for an n-mode CV system

	Hilbert space	Phase space
Dimension	∞	$2n$
Structure	$\bigotimes$	$\bigoplus$
State	$\hat{\rho}$	P/W/Q, χ_P/χ_W/χ_Q

1.2.3 Moments and Gaussian states

Moments play an important role in characterizing the Wigner distribution and its Fourier transform. We define the first order moment, also known as the displacement vector, for any state represented by the density operator ρ as follows:

$$\langle \hat{\xi} \rangle = \text{Tr}[\hat{\rho}\hat{\xi}]. \tag{1.63}$$

We can change the first order moment of any state, without affecting its quantum correlations, by applying the displacement operator. Similarly, the second order moments represented in the form of a matrix, also called the covariance matrix, is defined as

$$V = (V_{ij}) = \frac{1}{2}\langle \{\Delta\hat{\xi}_i, \Delta\hat{\xi}_j\} \rangle, \tag{1.64}$$

where $\Delta\hat{\xi}_i = \hat{\xi}_i - \langle\hat{\xi}_i\rangle$, and $\{\ ,\ \}$ denotes the anticommutator. The covariance matrix is a $2n \times 2n$ real, symmetric matrix. The uncertainty principle can be expressed easily in terms of the covariance matrix as

$$V + \frac{i}{2}\Omega \geq 0. \tag{1.65}$$

This equation also implies that the covariance matrix is positive definite i.e., $V > 0$. Any state obeying Eq. (6.8) is physically realizable. The covariance matrix of a single mode vacuum state $\hat{\rho} = |0\rangle\langle 0|$ is written as

$$V_{|0\rangle} = \frac{1}{2}\begin{pmatrix} \langle\{\Delta q, \Delta q\}\rangle & \langle\{\Delta q, \Delta p\}\rangle \\ \langle\{\Delta p, \Delta q\}\rangle & \langle\{\Delta p, \Delta p\}\rangle \end{pmatrix} = \frac{1}{2}\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}. \tag{1.66}$$

A single mode system with frequency ω in a thermal state corresponding to temperature T is represented by the following density operator:

$$\hat{\rho} = \sum_{n=0}^{\infty} \frac{\langle n \rangle^n}{(1+\langle n \rangle)^{n+1}} |n\rangle\langle n|, \tag{1.67}$$

where $\langle n \rangle = 1/(\exp(\omega/k_B T) - 1)$ is the average number of photons in the thermal state. The corresponding covariance matrix is given by

$$V_{\text{th}} = \frac{1}{2} \begin{pmatrix} 2\langle n \rangle + 1 & 0 \\ 0 & 2\langle n \rangle + 1 \end{pmatrix}. \tag{1.68}$$

Gaussian states are an important class of states in CV systems, which are states with Gaussian Wigner function. We can completely specify a Gaussian state by its first and second order moments. The vacuum state and the thermal state discussed above are examples of Gaussian states. For the special case of a Gaussian state, the Wigner distribution (1.61) can be written as [15]

$$W(\xi) = \frac{\exp[-(1/2)(\xi - \overline{\xi})^T V^{-1} (\xi - \overline{\xi})]}{(2\pi)^n \sqrt{\det V}}, \tag{1.69}$$

where V is the covariance matrix, and $\overline{\xi}$ denotes the displacement of an n-mode Gaussian state.

1.3 Gaussian operations

Gaussian operations are those operations which map Gaussian states to Gaussian states. We discuss various Gaussian operations including displacement operation and symplectic operations, for instance, phase change operation, squeezing operation and beam splitter operation.

1.3.1 Displacement operator and coherent states

We have already introduced the displacement operator in Sec. 1.2.1. It is one of the most important Gaussian operations, which displaces the mean of a quantum state. For instance, the action of the displacement operator $\hat{D}(q_0, p_0)$ on the vacuum state, centered at $(0, 0)$, generates the coherent state, centered at (q_0, p_0):

$$D(\alpha)|0\rangle = |\alpha\rangle, \quad \alpha = \frac{q_0 + i p_0}{\sqrt{2}}, \tag{1.70}$$

where $|0\rangle$ is the vacuum state and $|\alpha\rangle$ represents the coherent state. The displacement of the vacuum state in the phase space is shown in Fig. 1.1. Further, the coherent state $|\alpha\rangle$ is also defined as the eigenstate of the annihilation operator $\hat{a}$:

$$\hat{a}|\alpha\rangle = \alpha|\alpha\rangle, \quad \hat{a}|0\rangle = 0. \tag{1.71}$$

The Fock state representation of the coherent state reads

$$|\alpha\rangle = e^{-|\alpha|^2/2} \sum_{n=0}^{\infty} \frac{\alpha^n}{\sqrt{n!}} |n\rangle. \tag{1.72}$$

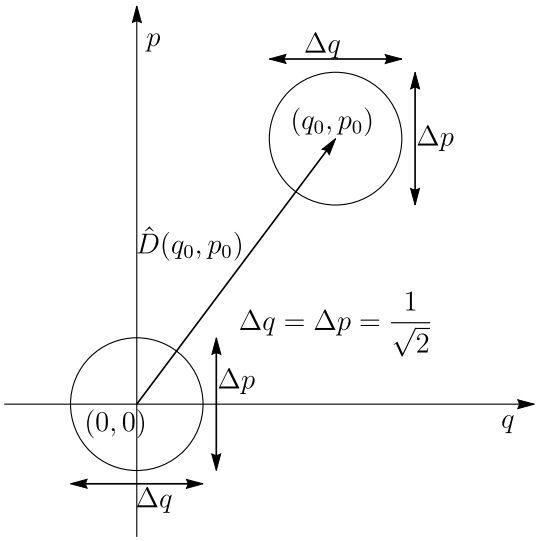


Figure 1.1: Representation of the quadrature uncertainties for the vacuum state and the coherent state in phase space.

We list some of the important properties of the coherent states below.

(i) Two different coherent states $|\alpha\rangle$ and $|\beta\rangle$ are not orthogonal, and their inner product is given by

$$\langle\alpha|\beta\rangle = \exp\left[-\frac{|\alpha|^2}{2} - \frac{|\beta|^2}{2} + \alpha^*\beta\right]. \tag{1.73}$$

(ii) The completeness relation for the coherent states is

$$\frac{1}{\pi}\int d^2\alpha\, |\alpha\rangle\langle\alpha| = \mathbb{1}. \tag{1.74}$$

(iii) The above two properties show that the coherent states form an overcomplete basis. As a consequence of this, any quantum state can be determined using only the diagonal matrix elements in the coherent state basis. For instance, an arbitrary density operator $\hat{\rho}$ of a single mode system can be written as

$$\hat{\rho} = \int d^2\alpha\, \phi(\alpha)|\alpha\rangle\langle\alpha|, \tag{1.75}$$

where $\phi(\alpha)$ is a quasi-probability distribution called Glauber-Sudarshan distribution [43, 48]. The Glauber-Sudarshan distribution also corresponds to the anti-normal ordering of an operator, as discussed in Eq. (1.52).

1.3.2 Symplectic transformations

The linear homogeneous transformations specified by real $2n \times 2n$ matrices S act on the quadratures operators as

$$\hat{\xi}_i \to \hat{\xi}_i' = S_{ij}\hat{\xi}_j, \tag{1.76}$$

such that the canonical commutation relations (1.20) are preserved, satisfy the condition

$$S\Omega S^T = \Omega. \tag{1.77}$$

These real matrices form a non-compact group called the symplectic group in $2n$ dimensions and is denoted as $Sp(2n,\, \mathcal{R})$. We have shown different linear transformations occurring in two dimensions in Table 1.5. The determinant of a symplectic matrix is equal to $+1$, and therefore only rotation, squeezing, and shear transformations are symplectic transformations.

For each $S \in Sp(2n,\, \mathcal{R})$, we can write a corresponding infinite dimensional unitary representation $\mathcal{U}(S)$ acting on the Hilbert space. For instance, the infinite dimensional unitary representation $\mathcal{U}(S)$ of S transforms the density operator $\hat{\rho}$ as $\hat{\rho} \to \mathcal{U}(S)\hat{\rho}\,\mathcal{U}(S)^\dagger$. The generators of these unitary transformations are quadratic functions of the quadrature operators. Further, we can decompose any symplectic matrix $S \in Sp(2n,\, \mathcal{R})$ as

$$S = PK(X, Y), \tag{1.78}$$

where $P \in \Pi(4)$ is a subset of $Sp(2n,\, \mathcal{R})$ defined as

$$\Pi(n) = \{S \in Sp(2n,\, \mathcal{R}) \,|\, S^T = S,\ S > 0\}, \tag{1.79}$$

and $K(X, Y)$ is the maximal compact subgroup of $Sp(2n,\, \mathcal{R})$, which is isomorphic to the unitary group $U(n) = X + iY$ in n dimensions. The action of the $U(n)$ transformation on the annihilation and creation operators is given as

$$\hat{\boldsymbol{a}} \to U\hat{\boldsymbol{a}}, \quad \hat{\boldsymbol{a}}^\dagger \to U^*\hat{\boldsymbol{a}}^\dagger, \tag{1.80}$$

Table 1.5: Different linear transformations in two dimensions

Transformation	Matrix	$S\Omega S^T = \Omega$	$\text{Det}[S] = +1$
Rotation	$\begin{bmatrix} \cos\theta & \sin\theta \\ -\sin\theta & \cos\theta \end{bmatrix}$	✓	✓
Reflection	$\underbrace{\begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}}_{\text{About } y=x}$	✓	✗
Scaling	$\begin{bmatrix} a & 0 \\ 0 & a \end{bmatrix}$	✗	✗
Squeezing	$\begin{bmatrix} c & 0 \\ 0 & 1/c \end{bmatrix}$	✓	✓
Shear $\equiv$ Rotation + squeezing	$\begin{bmatrix} 1 & b \\ 0 & 1 \end{bmatrix}$	✓	✓
Projection	$\underbrace{\begin{bmatrix} 1 & 0 \\ 0 & 0 \end{bmatrix}}_{\text{x-axis}}$	✗	✗
Contraction/ Expansion	$\underbrace{\begin{bmatrix} b & 0 \\ 0 & 1 \end{bmatrix}}_{\text{horizontal}}$	✗	✗

where $\hat{\boldsymbol{a}} = (\hat{a}_1, \hat{a}_2, \ldots, \hat{a}_n)^T$ and $\hat{\boldsymbol{a}}^\dagger = (\hat{a}_1^\dagger, \hat{a}_2^\dagger, \ldots, \hat{a}_n^\dagger)^T$. The transformation matrix $K(X, Y)$ acting on the quadrature operators can be easily obtained using Eqs. (1.26) and (1.80). The elements of the unitary part $U(n)$ act on the Hilbert space through its infinite dimensional unitary representation, and conserve the total photon number. These operations are also called passive operations. Few examples include phase change operation and beam splitter operation. These transformations do not change the quantum optical classicality or non-classicality status of a state. However, such transformations have the potential to convert separable non-classical states into entangled non-classical states. On the other hand, the elements of $\Pi(n)$, while acting via its

infinite dimensional unitary representation, do not conserve the total photon number. These transformations are also called active operations and can generate nonclassicality as they can transform a classical state to a non-classical one. The squeezing transformation is an example of an active transformation.

We discuss four symplectic operations in detail: phase change, single-mode squeezing, two-mode beam splitter, and two-mode squeezing operator.

Phase change operation

The phase change operation acting on the quadrature operators $(\hat{q}_i, \hat{p}_i)^T$ can be represented by the following symplectic matrix:

$$R_i(\phi) = \begin{pmatrix} \cos\phi & \sin\phi \\ -\sin\phi & \cos\phi \end{pmatrix}. \tag{1.81}$$

This operation belongs to the $U(1)$ subgroup of $Sp(2,\mathcal{R})$, and can be generated by quadratic Hamiltonian of the form $H = \hat{a}_i^\dagger \hat{a}_i$. The corresponding infinite dimensional unitary representation is given by

$$\mathcal{U}(R_i(\phi)) = \exp(-i\phi \underbrace{\hat{a}_i^\dagger \hat{a}_i}_{\text{Quadratic}}). \tag{1.82}$$

The action of the phase change operation on the annihilation operator turns out to be

$$\mathcal{U}(R_i(\phi))^\dagger \hat{a}_i \, \mathcal{U}(R_i(\phi)) = e^{-i\phi}\hat{a}_i. \tag{1.83}$$

Single mode squeezing operation

The symplectic matrix for the single mode squeezing operation acting on the quadrature operators $\hat{q}_i$ and $\hat{p}_i$ is given by

$$S_i(r) = \begin{pmatrix} e^{-r} & 0 \\ 0 & e^{r} \end{pmatrix}. \tag{1.84}$$

The corresponding infinite dimensional unitary representation for the single mode squeezing operation is given by

$$\mathcal{U}(S_i(r)) = \exp[r \underbrace{(a_i^2 - \hat{a}_i^{\dagger 2})}_{\text{Quadratic}}/2]. \tag{1.85}$$

The annihilation operator $\hat{a}_i$ transforms as follows under the action of the infinite dimensional unitary representation $\mathcal{U}(S(r))$:

$$\mathcal{U}(S_i(r))^\dagger \hat{a}_i \, \mathcal{U}_i(S(r)) = (\cosh r)\hat{a}_i - (\sinh r)\hat{a}_i^\dagger. \tag{1.86}$$

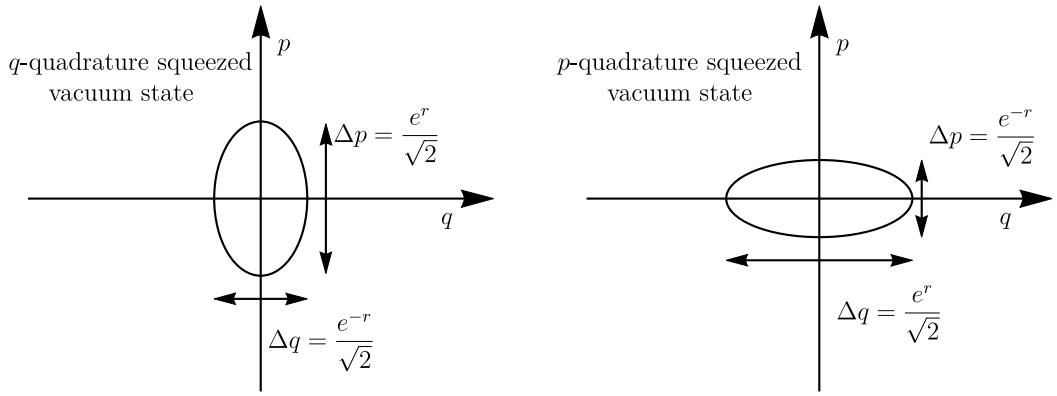


Figure 1.2: Representation of the quadrature uncertainties for squeezed vacuum state in the phase space.

The action of the squeezing operator on a single mode vacuum state generates a single mode squeezed vacuum state, which can be written in the Fock basis as follows:

$$\mathcal{U}(S_i(r))|0\rangle = \frac{1}{\sqrt{\cosh r}} \sum_{n=0}^{\infty} \frac{\sqrt{(2n)!}}{2^n n!} (\tanh r)^n |2n\rangle. \tag{1.87}$$

The covariance matrix for the single mode squeezed vacuum state is given by

$$V = S(r) V_{|0\rangle} S(r)^T = \frac{1}{2} \begin{pmatrix} e^{-2r} & 0 \\ 0 & e^{2r} \end{pmatrix}. \tag{1.88}$$

We have depicted $\hat{q}$ and $\hat{p}$ quadrature squeezed vacuum state in Fig. 1.84. Single mode squeezing operation can be implemented experimentally using parametric down-conversion in a nonlinear crystal [49].

Beam splitter operation

The action of a beam splitter $B_{ij}(\theta)$ on the quadrature operators $\hat{\xi} = (\hat{q}_i,\, \hat{p}_i,\, \hat{q}_j,\, \hat{p}_j)^T$ of a two mode system can be expressed as

$$B_{ij}(\theta) = \begin{pmatrix} \cos\theta\, \mathbb{1} & \sin\theta\, \mathbb{1} \\ -\sin\theta\, \mathbb{1} & \cos\theta\, \mathbb{1} \end{pmatrix}. \tag{1.89}$$

Similarly, the beam splitter transforms the annihilation operators $(\hat{a}_i, \hat{a}_j)^T$ of a two mode system as follows:

$$\begin{pmatrix} \hat{a}_i \\ \hat{a}_j \end{pmatrix} \rightarrow \begin{pmatrix} \cos\theta & \sin\theta \\ -\sin\theta & \cos\theta \end{pmatrix} \begin{pmatrix} \hat{a}_i \\ \hat{a}_j \end{pmatrix}. \tag{1.90}$$

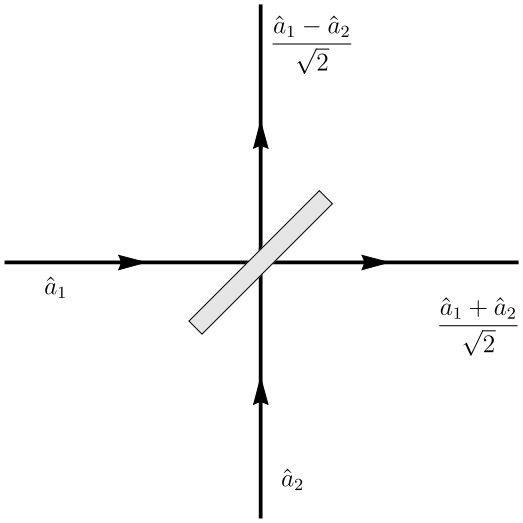


Figure 1.3: The effect of a balanced beam splitter on the annihilation operators

The above transformation matrix is an element of the $U(2)$ compact group. The corresponding infinite dimensional unitary representation of the beam splitter transformation is

$$\mathcal{U}(B_{ij}(\theta)) = \exp[\theta \underbrace{(\hat{a}_i^\dagger \hat{a}_j - \hat{a}_i \hat{a}_j^\dagger)}_{\text{Quadratic}}]. \tag{1.91}$$

Here θ specifies the transmissivity of the beam splitter through the relation $\tau = \cos^2\theta$. The action of a $50:50$ or balanced beam splitter ($\theta = \pi/4$) on the annihilation operators is shown in Fig. 1.3. We now demonstrate through a simple example that beam splitter can generate entanglement from separable but nonclassical input states. Consider a vacuum state $|0\rangle$ (classical) and single photon state $|1\rangle$ (nonclassical) mixed through a balanced beam splitter. The final state is an entangled state given by

$$|1\rangle|0\rangle \xrightarrow{\mathcal{U}(B_{12}(\pi/4))} \frac{1}{\sqrt{2}}(|1\rangle|0\rangle - |0\rangle|1\rangle) \tag{1.92}$$

Two mode squeezing operation

The symplectic transformation for a two mode squeezing operator acting on the quadrature operators $(\hat{q}_i, \hat{p}_i, \hat{q}_j, \hat{p}_j)$ is given by

$$S_{ij}(r) = \begin{pmatrix} \cosh r\, \mathbb{1} & \sinh r\, \mathbb{Z} \\ \sinh r\, \mathbb{Z} & \cosh r\, \mathbb{1} \end{pmatrix}, \tag{1.93}$$

where $\mathbb{Z} = \text{diag}(1, -1)$. The corresponding infinite dimensional unitary operator acting on the Hilbert space is

$$\mathcal{U}(S_{ij}(r)) = \exp[r \underbrace{(\hat{a}_i \hat{a}_j - \hat{a}_i^\dagger \hat{a}_j^\dagger)}_{\text{Quadratic}} /2]. \tag{1.94}$$

The quadratic expressions appearing in Eqs. (1.82) and (1.91) are photon number conserving, while the quadratic expressions appearing in Eqs. (1.85) and (1.94) do not conserve the photon number. We can generate a two mode squeezed vacuum (TMSV) state by applying a two mode squeezing operator on a two mode vacuum state:

$$\mathcal{U}(S_{ij}(r))|0\rangle_i|0\rangle_j = \frac{1}{\cosh r} \sum_{n=0}^{\infty} (-\tanh r)^n |n\rangle_i |n\rangle_j. \tag{1.95}$$

The covariance matrix for a TMSV state is given by

$$V = S_{12}(r)(V_{|0\rangle} \oplus V_{|0\rangle}) S_{12}^T(r) = \begin{pmatrix} \cosh(2r)\,\mathbb{1} & \sinh(2r)\,\mathbb{Z} \\ \sinh(2r)\,\mathbb{Z} & \cosh(2r)\,\mathbb{1} \end{pmatrix}. \tag{1.96}$$

We show the schematic for the generation of a TMSV state using vacuum states, single mode squeezers, and balanced beam splitter in Fig. 1.4.

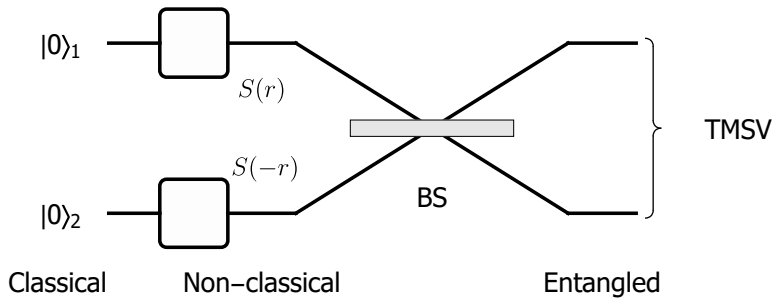


Figure 1.4: The squeezing operations convert vacuum states (classical) into squeezed vacuum states (non-classical). We mix the two single mode squeezed vacuum states using a balanced beam splitter to generate a TMSV state, which is entangled. We note that the output is an entangled state even if we mix a single mode vacuum state with a single mode squeezed state using a beam splitter.

1.4 Gaussian measurements

Gaussian measurements are those measurements for which the probability distribution corresponding to a measurement on a Gaussian state is a Gaussian. We describe two

Gaussian measurements, namely homodyne measurement and heterodyne measurement. These measurements have been thoroughly investigated in Chapter 2, and also used in Chapters 5 and 6.

Homodyne measurement

Homodyne measurement is one of the most important measurement techniques in CV systems and corresponds to the measurement of either $\hat{q}$ or $\hat{p}$ or any other phase rotated quadrature operators of the radiation mode. The measurement of the $\hat{q}$ quadrature corresponds to the projection on $|q\rangle\langle q|$ projectors, and the probability density $P(q)$ of obtaining the outcome 'q' is obtained by integrating the Wigner function over the p variable:

$$P(q) = \int W(q,p)\, dp. \tag{1.97}$$

Similarly, the measurement of the $\hat{p}$ quadrature corresponds to the projection on $|p\rangle\langle p|$ projectors, and the probability density $P(p)$ of obtaining the outcome 'p' is obtained by integrating the Wigner function over the q variable:

$$P(p) = \int W(q,p)\, dq. \tag{1.98}$$

Experimentally, the homodyne measurement is implemented by mixing the signal beam with a strong local oscillator and measuring the photon number difference between the resulting beams as shown in Fig. 1.5. Here the local oscillator and the signal beam are derived from the same source, and therefore have the same frequency. This is in contrast with heterodyne detection scheme, where the frequencies of the local oscillator and the signal beam are different. Now we show how the measurement of photon number difference with discrete outcome relates to the measurement of quadrature operators with continuous outcome [50, 51]. Let $\hat{a}_1$ and $\hat{a}_2$ represent the modes of the local oscillator and the signal, respectively. Then the transformed field operators $\hat{a}_1'$ and $\hat{a}_2'$ due to the action of the beam splitter are given by

$$\hat{a}_1' = \frac{\hat{a}_1 - \hat{a}_2}{\sqrt{2}}, \quad \hat{a}_2' = \frac{\hat{a}_1 + \hat{a}_2}{\sqrt{2}}. \tag{1.99}$$

The two detectors measure the average photon numbers $I_{a_1'} = \langle {a_1'}^\dagger a_1' \rangle$ and $I_{a_2'} = \langle {a_2'}^\dagger a_2' \rangle$ in the two output beams. We define photon number difference operator $\hat{\Delta}$ as

$$\hat{\Delta} = \hat{n}_1' - \hat{n}_2' = \hat{a}_1'^\dagger \hat{a}_1' - \hat{a}_2'^\dagger \hat{a}_2' = -\hat{a}_1^\dagger \hat{a}_2 - \hat{a}_2^\dagger \hat{a}_1. \tag{1.100}$$

We assume the local oscillator to be in a coherent state $|\alpha e^{-i\omega t}\rangle$ with $\alpha = |\alpha| e^{-i\psi}$. We also assume that the signal is derived from the same local oscillator, and $\hat{a}_2 = \hat{a}_0 e^{-i\omega t}$.

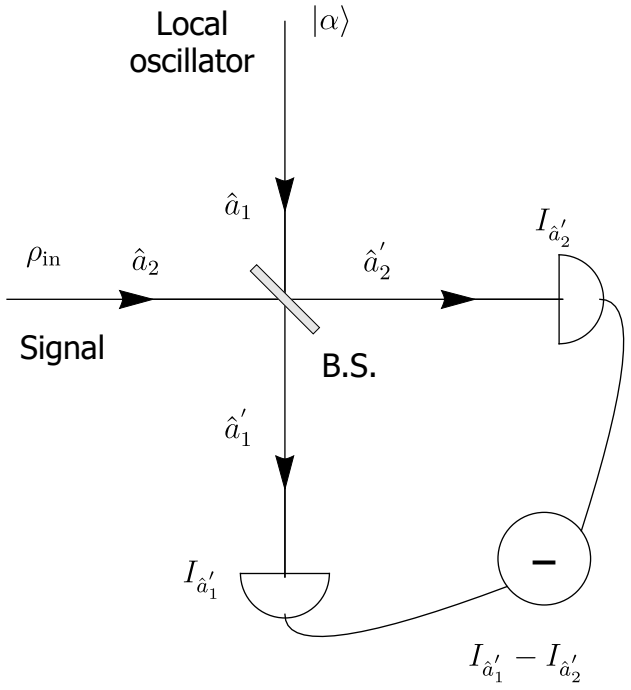


Figure 1.5: Experimental implementation of the homodyne measurement scheme.

Hence, the expectation value of the operator $\hat{\Delta}$ becomes

$$\langle\hat{\Delta}\rangle = |\alpha|\langle\hat{a}e^{i\theta} + \hat{a}^\dagger e^{-i\theta}\rangle = \sqrt{2}|\alpha|\langle\hat{x}_\theta\rangle, \tag{1.101}$$

where $\theta = \psi + \pi$. Similarly, the second moment of the operator $\hat{\Delta}$ can be evaluated as

$$\langle\hat{\Delta}^2\rangle = |\alpha|^2\Big(e^{2i\theta}\langle\hat{a}_0^2\rangle + e^{-2i\theta}\langle\hat{a}_0^{\dagger 2}\rangle + 2\langle\hat{a}_0^\dagger\hat{a}_0\rangle + 1\Big) + \langle\hat{a}_0^\dagger\hat{a}_0\rangle = 2|\alpha|^2\langle\hat{x}_\theta^2\rangle + \langle\hat{a}_0^\dagger\hat{a}_0\rangle. \tag{1.102}$$

In the limit of strong local oscillator, i.e., $|\alpha| \to \infty$, the above equation can be written as

$$\langle\hat{\Delta}^2\rangle \approx \langle(\sqrt{2}|\alpha|\hat{x}_\theta)^2\rangle. \tag{1.103}$$

Furthermore, one can show the following for the n^{th} moment of the operator $\hat{\Delta}$ in the strong local oscillator limit:

$$\langle\hat{\Delta}^n\rangle \approx \langle(\sqrt{2}|\alpha|\hat{x}_\theta)^n\rangle. \tag{1.104}$$

Since different order moments of the operators $\hat{\Delta}$ and $\sqrt{2}|\alpha|\hat{x}_\theta$ are the same for strong local oscillator, we conclude that the distribution function for both of them should also be the same. We had noted earlier that the operator $\hat{\Delta}$ has a discrete spectrum,

while the quadrature operator $\hat{x_\theta}$ has a continuous spectrum. Since we are considering the case of a strong local oscillator, i.e., the operator $|\alpha| \to \infty$, $\Delta/|\alpha|$ also has a continuous spectrum. Thus, one can measure the quadrature distribution by measuring the photon number difference distribution. Furthermore, we can measure the moments of the quadrature operators along different directions by changing the phase ψ of the local oscillator.

Heterodyne measurement

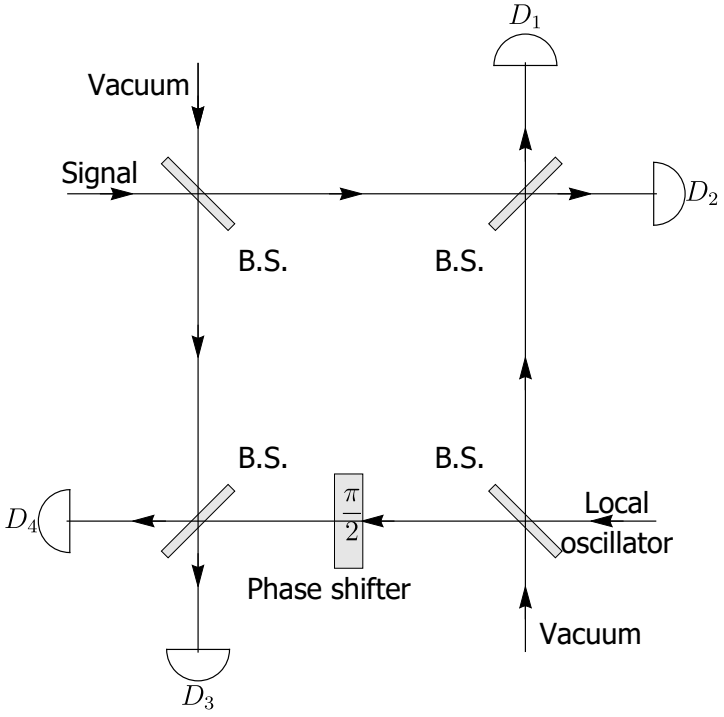


Figure 1.6: Experimental implementation of heterodyne measurement scheme.

Heterodyne measurement corresponds to the simultaneous measurement of $\hat{q}$ and $\hat{p}$ quadrature operators, and the measurement operators are projection over coherent state basis $E_\alpha = (2\pi)^{-1}|\alpha\rangle\langle\alpha|$. Experimentally, the heterodyne measurement is implemented by splitting the signal using a beam splitter, and then homodyning each of the two signal as shown in Fig. 1.6. As a consequence of the simultaneous measurement of the conjugate observables, an extra vacuum noise is added in the variances of the probability distribution of both $\hat{q}$ and $\hat{p}$ quadrature operators.

1.5 Miscellaneous techniques

In this section, we discuss various mathematical concepts and techniques, which are frequently used while dealing with CV systems.

Symplectic diagonalisation

Since the covariance matrix V is a $2n \times 2n$ real symmetric matrix, it can be diagonalized by a special orthogonal matrix $SO(2n, \mathcal{R})$. However, a theorem by Williamson [52] states that a positive definite or negative definite matrix of even dimension can be diagonalized by a symplectic matrix $Sp(2n, \mathcal{R})$. The diagonalized matrix, also known as the Williamsom form, is given by

$$SVS^T = \bigoplus_{i=1}^{n} \begin{pmatrix} k_i & 0 \\ 0 & k_i \end{pmatrix}, \tag{1.105}$$

where the k_i are called symplectic eigenvalues of V. These symplectic eigenvalues are the positive-defined eigenvalues of $i\Omega V$, and satisfy the relation $k_i \geq 1/2$, which is another statement of the uncertainty relation (6.8).

Effect of symplectic transformation

If the density operator transforms as $\rho \to \mathcal{U}(S)\rho\,\mathcal{U}(S)^\dagger$ under the infinite dimensional unitary representation $\mathcal{U}(S)$ of a symplectic transformation S, the transformations of the Wigner distribution, the displacement vector, and the covariance matrix are given by [39]

$$W(\xi) \to W(S^{-1}\xi), \quad \bar{\hat{\xi}} \to S\bar{\hat{\xi}}, \quad \text{and} \quad V \to SVS^T. \tag{1.106}$$

Euler decomposition

The Euler decomposition of a symplectic matrix S is given by [39]

$$S = UDV, \tag{1.107}$$

where U and V are unitary matrices and

$$D = \bigoplus_{k=1}^{n} D_{k_i} \quad \text{with} \quad D_{k_i} = \begin{pmatrix} k_i & 0 \\ 0 & 1/k_i \end{pmatrix}, \tag{1.108}$$

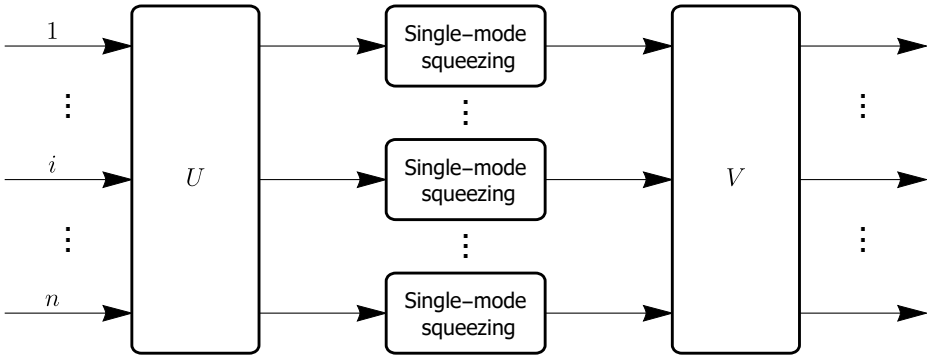


Figure 1.7: A general symplectic transformation matrix acting on an n-mode system can be decomposed as a product of $n \times n$ unitary matrix U, n single mode squeezing operators, and another $n \times n$ unitary matrix V.

represents n single mode squeezing operators. The schematic for the Euler decomposition is shown in Fig. 1.7. For instance, the Euler decomposition of the symplectic transformation corresponding to the two mode squeezing operator (1.93) is given by

$$S_{12}(r) = \underbrace{B_{12}(\pi/4)}_{U}\underbrace{(S_1(r) \oplus S_2(-r))}_{D}\underbrace{B_{12}(-\pi/4)}_{V}. \tag{1.109}$$

Inner product of two operators in phase space

For a single mode system, the inner product of two density operators $\hat{\rho}_1$ and $\hat{\rho}_2$ can be expressed as overlap integral of their Wigner distributions [53]:

$$\begin{aligned}(\hat{\rho}_1, \hat{\rho}_2) =& \text{Tr}[\hat{\rho}_1\hat{\rho}_2], \\ =& 2\pi \int_{\mathcal{R}^2} dqdp\, W_{\hat{\rho}_1}(q,p) W_{\hat{\rho}_2}(q,p).\end{aligned} \tag{1.110}$$

The above equation can be proved explicitly, but one can easily see this relation from optical equivalence theorem (1.60). Now, the Wigner characteristic function $\chi(\tau, \sigma)$ of a single mode system is defined as

$$\chi(\tau,\sigma) = Tr[\hat{\rho}\, \exp(i\sigma\hat{q} - i\tau\hat{p})], \tag{1.111}$$

where $\Lambda = (\tau, \sigma)^T$. The inner product of two density operators $\hat{\rho}_1$ and $\hat{\rho}_2$ in the characteristic function formalism is given as [42]

$$\text{Tr}[\hat{\rho}_1\hat{\rho}_2] = \frac{1}{2\pi}\int_{\mathcal{R}^2} d\tau d\sigma\, \chi_{\hat{\rho}_1}(\tau,\sigma)\chi_{\hat{\rho}_2}(-\tau,-\sigma). \tag{1.112}$$

Hilbert space vs phase space

We discuss a simple calculation to show the working principle of the Hilbert space and the phase space formalism. Consider a single mode squeezed vacuum state generated by the action of the single mode squeezing operator $\mathcal{U}(S(r)) = \exp[r(a^2 - \hat{a}^{\dagger 2})/2]$ on the vacuum state $|0\rangle$. Now we evaluate the expectation value of the operator $\hat{q}^2$ for a single mode squeezed vacuum state.

Hilbert space approach

The expectation value of the operator $\hat{q}^2$ for a single mode squeezed vacuum state

$$\langle \hat{q}^2 \rangle = \langle 0|\mathcal{U}(S(r))^\dagger \hat{q}^2 \mathcal{U}(S(r))|0\rangle. \tag{1.113}$$

In the Heisenberg picture, the evolution of the operator $\hat{q}^2$ is given by

$$\mathcal{U}(S(r))^\dagger \hat{q}^2 \mathcal{U}(S(r)) = \mathcal{U}(S(r))^\dagger \hat{q}\, \mathcal{U}(S(r))\mathcal{U}(S(r))^\dagger \hat{q}\, \mathcal{U}(S(r)). \tag{1.114}$$

Using $\mathcal{U}(S(r))^\dagger \hat{a}\, \mathcal{U}(S(r)) = \cosh r\, \hat{a} - \sinh r\, \hat{a}^\dagger$ and $\hat{q} = (\hat{a} + \hat{a}^\dagger)/\sqrt{2}$, we get

$$\langle \hat{q}^2 \rangle = \frac{e^{-2r}}{2}. \tag{1.115}$$

Wigner function approach

The Wigner distribution of the vacuum state can be written as

$$W_{|0\rangle}(q,p) = \frac{e^{-q^2-p^2}}{\pi}. \tag{1.116}$$

The symplectic matrix for the single mode squeezing transformation is given by

$$S(r) = \begin{pmatrix} e^{-r} & 0 \\ 0 & e^{r} \end{pmatrix}. \tag{1.117}$$

Since the Wigner distribution transforms as $W(\xi) \to W(S(r)^{-1}\xi)$ under squeezing transformation $S(r)$, the Wigner distribution of the single mode squeezed vacuum state becomes

$$W(q,p) = \frac{1}{\pi} \exp\left(-\frac{q^2}{e^{-2r}} - \frac{p^2}{e^{2r}}\right). \tag{1.118}$$

The expectation value of the operator $\hat{q}^2$ is computed as

$$\begin{aligned} \langle \{\hat{q}^2\}_{sym} \rangle =& \int dqdp\, q^2 W(q,p) \\ =& \frac{e^{-2r}}{2}. \end{aligned} \tag{1.119}$$

Wigner characteristic function approach

The Wigner characteristic function (1.111) for a Gaussian state takes the following simple form [15, 42]:

$$\chi(\Lambda) = \exp[-\frac{1}{2}\Lambda^T(\Omega V \Omega^T)\Lambda - i(\Omega\overline{\xi})^T\Lambda], \tag{1.120}$$

where V and $\overline{\xi}$ represent the covariance matrix and the displacement of the Gaussian state, respectively. Therefore, the Wigner characteristic function of the vacuum state is

$$\chi(\tau,\sigma) = \exp\left(-\frac{\tau^2}{4} - \frac{\sigma^2}{4}\right). \tag{1.121}$$

The Wigner characteristic function transforms as $\chi(\Lambda) \rightarrow \chi(S^{-1}\Lambda)$ ($\Lambda = (\tau,\sigma)^T$) under the squeezing transformation (1.117). Thus, the Wigner characteristic function of the single mode squeezed vacuum state is

$$\chi(\tau,\sigma) = \exp\left(-\frac{\tau^2}{4e^{-2r}} - \frac{\sigma^2}{4e^{2r}}\right). \tag{1.122}$$

For a single mode system, the symmetrically ordered form of the operator $\hat{q}^m\hat{p}^n$ can be obtained by differentiating the displacement operator $\exp(i\sigma\hat{q} - i\tau\hat{p})$ with respect to τ and σ:

$$\{\hat{q}^m\hat{p}^n\}_{\text{sym}} = \left(\frac{1}{i}\right)^m\left(\frac{1}{-i}\right)^n \frac{\partial^{m+n}}{\partial\sigma^m\partial\tau^n} e^{i\sigma\hat{q}-i\tau\hat{p}}\Big|_{\tau=\sigma=0}. \tag{1.123}$$

Hence, the average of a symmetrically ordered operator can be obtained by differentiating the Wigner characteristic function:

$$\begin{aligned}\left(\frac{1}{i}\right)^m\left(\frac{1}{-i}\right)^n \frac{\partial^{m+n}}{\partial\sigma^m\partial\tau^n}\chi(\tau,\sigma) &= \left(\frac{1}{i}\right)^m\left(\frac{1}{-i}\right)^n \frac{\partial^{m+n}}{\partial\sigma^m\partial\tau^n} Tr\left(\hat{\rho}e^{i\sigma\hat{q}-i\tau\hat{p}}\right)\Big|_{\tau=\sigma=0}, \\ &= Tr\left(\hat{\rho}\{\hat{q}^m\hat{p}^n\}_{\text{sym}}\right), \\ &= \langle\{\hat{q}^m\hat{p}^n\}_{\text{sym}}\rangle.\end{aligned} \tag{1.124}$$

Therefore, the average of the operator $\hat{q}^2$ can be evaluated by differentiating the Wigner characteristic function of the single mode squeezed vacuum state (1.122) twice with respect to σ as shown below:

$$\begin{aligned}\langle\{\hat{q}^2\}_{sym}\rangle &= \left(\frac{1}{i}\right)^2 \frac{\partial^2\chi(\tau,\sigma)}{\partial\sigma^2}\Big|_{\tau=\sigma=0}, \\ &= \frac{e^{-2r}}{2}.\end{aligned} \tag{1.125}$$

These examples exclusively show the utility of different calculations method. All the techniques mentioned in this chapter have been extensively used in this thesis. The interested readers can look Arvind *et. al.* [39], an extraordinary reference for acquiring such techniques.

1.6 Two different notions of quantumness

In this section, we discuss two different notions of quantumness namely quantum optical non-classicality and Bell nonlocality. The relation between these two notions of quantumness has been investigated in Chapter 4.

1.6.1 Quantum optical nonclassicality

In the quantum optical context, nonclassicality of quantum states is defined through the Glauber-Sudarshan representation. Generalizing Eq. (1.75), we can write the Glauber-Sudarshan distribution $\phi(\boldsymbol{\alpha})$ for an arbitrary quantum state of an n-mode system as

$$\hat{\rho} = \frac{1}{\pi^n} \int d^{2n}\boldsymbol{\alpha}\, \phi(\boldsymbol{\alpha}) |\boldsymbol{\alpha}\rangle\langle\boldsymbol{\alpha}|. \tag{1.126}$$

If the function $\phi(\boldsymbol{\alpha})$ is positive and no more singular than a delta function, the state is said to be classical, otherwise it is nonclassical[1]. This definition allows for a probability interpretation of the Glauber-Sudarshan representation. For instance, the Glauber-Sudarshan representation of the coherent state $|\alpha_0\rangle$ is

$$\phi(\alpha) = \delta^2(\alpha - \alpha_0), \tag{1.127}$$

a Dirac-delta function, and thus coherent states are classical. Similarly, the Glauber-Sudarshan representation of the thermal state (1.67) is given by

$$\phi(\alpha) = \frac{1}{\pi\langle n\rangle} \exp\left(-\frac{|\alpha|^2}{\langle n\rangle}\right), \tag{1.128}$$

which is a Gaussian, and thus thermal states are also classical. On the other hand, the Glauber-Sudarshan representation of the Fock state $|n\rangle$ is

$$\phi(\alpha) = e^{|\alpha|^2} \frac{1}{n!} \frac{\partial^{2n}}{\partial\alpha^n \partial\alpha^{*n}} \delta^2\alpha, \tag{1.129}$$

which is a higher order derivative of Dirac-delta function, and thus Fock states are nonclassical. Other examples of nonclassical states include squeezed states and superposition of coherent states.

[1] Distributions that are more singular than a delta function are always negative somewhere.

1.6.2 Bell's inequalities

After EPR paper [8], Bell's inequalities arose in an effort to devise local hidden variable theories compatible with quantum mechanics. Bell observed that there are certain correlations in quantum mechanics that cannot be explained by classical local models. Soon after Bell's 1964 paper, several other formulations of Bell's inequality were proposed. Here we briefly describe one of the most famous forms of Bell's inequalities known as the Clauser-Horne-Shimony-Holt (CHSH) inequality [54, 55].

We consider a pair of spin one-half particles moving in opposite directions. Two observers A and B measure the spin of the particles. Observer A can orient his apparatus at either θ_1, or θ_1' angle to a reference axis and get the outcome $a = \pm 1$, or $a' = \pm 1$. Similarly, observer B can orient his apparatus at either θ_2 or θ_2' angle and get the outcome $b = \pm 1$ or $b' = \pm 1$. The schematic is illustrated in Fig. 1.8.

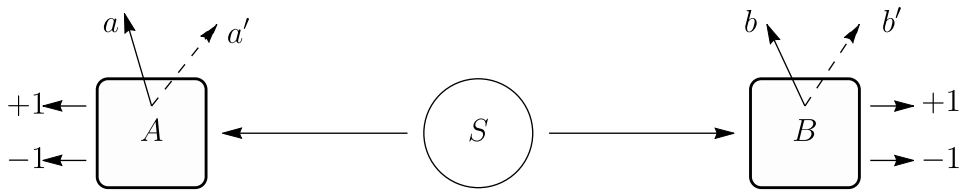


Figure 1.8: Schematic representation of the measurements in CHSH inequality.

The outcomes a, a', b, and b' identically satisfy

$$(a + a')b + (a - a')b' \equiv \pm 2. \tag{1.130}$$

Similarly, the j^{th} pair of spin one-half particles satisfy the relation

$$a_j b_j + a_j' b_j + a_j b_j' - a_j' b_j' \equiv \pm 2. \tag{1.131}$$

Taking average of the above equation yields the CHSH inequality:

$$|P(a, b) + P(a', b) + P(a, b') - P(a', b')| \leq 2. \tag{1.132}$$

Thus, there is an upper bound on the correlations of two distant particles according to classical local model. The quantum mechanical version of the CHSH inequality for a two qubit system can be written by associating the observable $\sigma_\theta = \vec{\sigma} \cdot \hat{\theta}$ with the measurement corresponding to the apparatus being oriented at angle an θ from the axis. Here $\vec{\sigma}$ is the Pauli vector and $\hat{\theta}$ is a unit vector oriented in the θ direction. The observed values for the operator $\vec{\sigma} \cdot \hat{\theta}$ are also ± 1. The correlation of the outcomes for two apparatus measuring spin of a particle at angles θ_1 and θ_2 from an arbitrary axis is given by

$$\langle \sigma_{\theta_1} \otimes \sigma_{\theta_2} \rangle = \cos\, 2(\theta_1 - \theta_2). \tag{1.133}$$

Thus, Eq. (1.132) can be written as

$$|\cos 2(\theta_1 - \theta_2) + \cos 2(\theta_1' - \theta_2) + \cos 2(\theta_1 - \theta_2') - \cos 2(\theta_1' - \theta_2')| \leq 2. \quad (1.134)$$

The above inequality is violated by quantum mechanical systems. As an example, we consider the singlet state of a bipartite qubit system given by

$$|\psi\rangle_S = \frac{1}{\sqrt{2}} \left(|10\rangle - |01\rangle\right). \quad (1.135)$$

When the various measurements directions are separated from each other by 22.5°, the left hand side of the Eq. (1.134) turns out to be $2\sqrt{2}$ [56], which is greater than 2, and thus the singlet state violates the CHSH inequality. The states violating the Bell's inequalities are known as non-local states. The correlations generated between distant parties through classical communications always satisfy Bell inequalities. Since the correlations obtained by performing measurement on entangled states violate Bell inequalities, we can discriminate separable from entangled state by studying their measurement statistics. Although entangled states are nonlocal, there are mixed entangled states, which do not violate any Bell inequalities. There have been some efforts to establish a quantitative relation between nonlocality and entanglement [57, 58, 59].

1.7 Motivations and arrangement of the thesis

In this section, we briefly describe the motivation behind the research undertaken in this thesis. The work could be broadly divided into three related topics: estimation of quantum states and quantum processes, quantum nonlocality, and quantum key distribution.

Quantum state tomography (QST) refers to the determination of the quantum states of an unknown system based on the results of experiments. It is one of the major tasks in various quantum communication and information protocols, and thus there has been a continuous development of innovative and efficient tomographic techniques. Usually a projective measurement is employed for measuring a set of incompatible observables, and the state is estimated from the measurement results. Since results of such measurements are statistical, one requires several copies of a system prepared identically to determine its state. Besides projective measurements, we can think of sequential measurement of a pair of conjugate observables in CV systems, where the observables are measured one after another [60, 61, 62, 63]. Similarly, one can also consider the joint measurement of conjugate observables for estimation of quantum states [64]. Ideal quantum state tomography requires infinite copies of the system, which is impractical in the real world. Usually, an experimentalist is provided with a fixed number of

identically prepared systems, and thus one would like to know the limitations of various measurement schemes and select the best as per their requirements [62, 65]. This question has been thoroughly investigated in Chapter 2.

We emphasize the utility of phase space formalism and symplectic group techniques in dealing with sequential measurement and Arthurs-Kelly measurement. Since the interaction Hamiltonians appearing in the sequential measurement and the Arthurs-Kelly measurement are quadratic expressions in the quadrature operators, the corresponding transformation matrix acting on the quadrature operators or phase space variables for Gaussian operations can be evaluated by exponentiation of the corresponding Lie algebra [39]. Once the transformation matrix is obtained, the mean and the covariance matrix of the transformed state can be readily evaluated. Further, the mean and covariance matrix of the reduced state of any system is readily obtained by ignoring the entries corresponding to all the other systems.

Quantum process tomography (QPT) refers to the determination of unknown quantum processes, which are generally completely positive quantum dynamical maps. In standard QPT, output states corresponding to probe states are estimated using QST. For CV systems, one possibility is to use homodyne measurement to measure the output states corresponding to coherent state probes [66]. Several theoretical as well as experimental investigations have been undertaken by several authors along similar lines [67, 68, 69]. In this thesis, we take a different approach and look at QST and QPT based on photon number resolving measurements.

Quantumness of a state in quantum optical context is based on the diagonal coherent state representation function for the state [43, 48]. If this function is positive and no more singular than a delta function, the state is classified as classical, otherwise it is considered to be non-classical. On the other hand, nonlocality of a quantum state arises in composite systems, when they violate the upper bound on the correlations of distant objects based on a classical local realistic model. It is worth exploring whether passive optical elements, which do not affect the classical or nonclassical status of a state, can convert quantum optical nonclassicality to nonlocality [70, 71]. In this thesis, we explore the connection between these two types of nonclassicalities from the perspective of Bell's inequality violation for several Gaussian and non-Gaussian states.

Here again, the calculations for Gaussian as well as non-Gaussian states of CV systems have been performed in phase space. For Gaussian as well as non-Gaussian states, Wigner function as well as its Fourier transform are useful because of their transformation properties under symplectic transformations. For non-Gaussian states, the Wigner function corresponding to the reduced state of the part of the system can be evaluated by integrating out all the other modes of the system. Similarly, the inner product of two density operators can be evaluated by integrating the product of the corresponding Wigner functions over the phase space.

QKD refers to the secure communication of random secret keys between two parties. While many security proofs for CV QKD have appeared in literature [72, 73], security under side channel attacks still remains an open problem since it is hard to take into account every detail of the experimental implementations of various devices and detectors. Based on the idea of entanglement swapping, measurement-device-independent (MDI) QKD protocol was developed, which is secure against all detector side-channel attacks [74, 75]. To enhance the transmission distances, photon subtracted two mode squeezed vacuum (PSTMSV) state has been considered as a resource state for CV-MDI-QKD. In this work, we consider a new resource state, which further enhances the transmission distances in CV-MDI-QKD.

Photon subtraction for multi-mode systems can be easily handled in the phase space formalism using the generating function and matrix integration techniques [39, 76]. For instance, the averages of symmetric ordered operators, appearing in the covariance matrix, can be evaluated as a weighted average of the Wigner function. The Wigner characteristic function provides an alternate and efficient method to evaluate the averages of symmetric ordered operators.

Most of the real life implementation of long distance QKD is based on optical system involving photons [77]. However, it is worth exploring if QKD can be carried out by other physical systems. In this direction, we consider a different CV system namely superconducting rings with a Josephson junction for implementation of QKD. The advantage of this system is that the actually measurements can be delayed to a time when the key is actually required, while the transport of the relevant quantum states can be completed before hand.

This thesis is organized as follows. In Chapter 2, we investigate the relative performance of various measurement schemes in Gaussian states estimation, while in Chapter 3, we propose an optimal scheme for the tomography of Gaussian states and Gaussian channels using photon number measurements. In Chapter 4, we study the conversion of quantum-optical nonclassicality into Bell-type nonlocality via passive operations. In Chapter 5, we study QKD using photon subtracted two mode squeezed coherent state, while in Chapter 6, we explore QKD using superconducting rings with a mesoscopic Josephson junction. Finally, in Chapter 7, we provide a summary of the thesis and discuss future directions.

Chapter 2

Estimation of Wigner distribution of Gaussian states: a comparative study

2.1 Introduction

Reconstruction of quantum states by performing measurements on an ensemble of identical but unknown systems is known as quantum state estimation (QSE) or quantum state tomography (QST) [78, 79, 80]. QSE is an important problem in quantum mechanics and in quantum information processing and finding schemes for its efficient execution is an active area of research [81, 82, 83]. Ideal QSE requires infinite copies of a quantum system, which is impractical in the real world. Usually, an experimentalist is provided with a fixed number of identically prepared systems, and thus one would like to know the advantages and limitations of various measurement schemes and select the best scheme as per the requirements. We consider several different measurement schemes that can be employed for the purpose of QSE of continuous variable (CV) systems.

Homodyne measurement (Hom) is one of the most widely employed measurement scheme in CV systems, which measures either the $\hat{q}$ quadrature or the $\hat{p}$ quadrature or any other phase rotated quadrature operator [84, 85, 86, 87]. It has been shown that various quasiprobability distributions such as Glauber-Sudarshan distribution, Wigner distribution, and Husimi distribution [88] can be estimated using measurements of the rotated quadrature operators. Further, Wigner distribution and Glauber-Sudarshan distribution have been determined experimentally for certain states using homodyne measurement [89, 90]. One can also think of sequential measurement (SM) of a pair of conjugate observables in CV systems, where the observables are measured one after another [60, 61, 62]. The sequential measurement of two non-commuting observ-

ables has been employed to reconstruct the Moyal M function, which is the Fourier transform of the Wigner function [61]. In a first of its kind, Arthurs and Kelly (AK) extended the von Neumann measurement scheme for the joint measurement of two non-commuting observables [64]. However, the joint measurement induces an additional noise in the probability distributions of both the non-commuting observables.

Similarly, a heterodyne measurement (Het), which is equivalent to an eight-port measurement (double-homodyne), is employed for the joint measurement of two non-commuting observables [91, 92, 93, 94, 95, 96, 97, 98, 99, 100, 101, 102]. In the heterodyne measurement, the vacuum noise is added in both the non-commuting observables, whereas in the Arthurs-Kelly scheme, the noise added in the non-commuting observables can be varied. It has been shown that the heterodyne measurement can do a better estimation of the first and the second order moments of the quadrature operators of Gaussian and non-Gaussian states compared to the homodyne measurement [65, 103, 104]. The superiority of localized phase space sampling with unbalanced homodyne measurement [105] compared to delocalized heterodyne measurement has also been shown [106].

In this chapter, we attempt to provide a complete picture and a comparative study of state estimation efficiency of different measurement schemes including homodyne measurement, sequential measurement, Arthurs-Kelly measurement, and heterodyne measurement. To this end, we consider an ensemble of N identically prepared single mode Gaussian states. A Gaussian state can be completely specified by its first order moments determined by the mean values of the quadrature operators and second order moments determined by the variances of the quadrature operators that can be arranged in the form of a covariance matrix. We therefore need to estimate the mean and the covariance matrix of a Gaussian state to completely reconstruct its Wigner distribution. We further assume that the Gaussian states are either squeezed in the $\hat{q}$ quadrature or the $\hat{p}$ quadrature. Such types of state have been considered in squeezed state CV quantum key distribution protocols [107, 108, 109]. Furthermore, to estimate such Gaussian states is simpler, as we perform measurements only along $\hat{q}$ and $\hat{p}$-quadratures.

We provide analytical expressions of the estimation efficiency of the mean and the variance of an ensemble of N identically prepared Gaussian states. We show that the optimal performance of the Arthurs-Kelly scheme and the sequential measurement is equal to the heterodyne measurement. For mean estimation, the heterodyne measurement outperforms the homodyne measurement for squeezed coherent state ensemble, but for variance estimation, the homodyne measurement outperforms the heterodyne measurement for a certain squeezing parameter range. Then we proceed to a modified Hamiltonian [110, 111] in the Arthurs-Kelly scheme that can entangle the two meters. Here the results show that the optimal performance of the scheme can only be obtained when the meters are uncorrelated. Since the Hamiltonians involved in the sequential

measurement and the Arthurs-Kelly scheme are quadratic expressions in quadrature operators, the corresponding symplectic transformations acting on the quadrature operators or the phase space variables belong to the real symplectic group $Sp(4,\mathcal{R})$ and $Sp(6,\mathcal{R})$ [112], respectively. We exploit this fact and explicitly work in phase space for calculation simplicity. We expect that these techniques along with the results obtained in this work will be useful in undertaking various studies in different quantum information and quantum communication protocols [15, 40].

This chapter is organized as follows. In Sec. 2.2, we introduce various measurement schemes and obtain the variance of probability distributions corresponding to different quadratures measurements. In Sec. 2.3, we derive and examine the results of the fidelities of the mean and the variance estimation. In Sec. 2.4, we consider Arthurs-Kelly scheme with a modified interaction Hamiltonian. Finally, in Sec. 2.5, we provide some concluding remarks and discuss future prospects.

2.2 Measurement schemes

We consider a single mode continuous variable quantum system with quadrature operators $\hat{q}$ and $\hat{p}$ satisfying the bosonic commutation relation

$$[\hat{q},\hat{p}] = i\hbar. \tag{2.1}$$

We assume that the system is in a Gaussian state with displacement vector $\overline{\hat{\xi}}$ and covariance matrix V given by

$$\overline{\hat{\xi}} = \begin{pmatrix} q_0 \\ p_0 \end{pmatrix}, \quad V = \begin{pmatrix} (\Delta q)^2 & 0 \\ 0 & (\Delta p)^2 \end{pmatrix}, \tag{2.2}$$

where $q_0 = \langle \hat{q} \rangle$, $p_0 = \langle \hat{p} \rangle$, $(\Delta q)^2 = \langle \hat{q}^2 \rangle - (\langle \hat{q} \rangle)^2$, and $(\Delta p)^2 = \langle \hat{p}^2 \rangle - (\langle \hat{p} \rangle)^2$. The corresponding Wigner function of the Gaussian state can be readily obtained using Eq. (1.69) as

$$W(q,p) = \frac{1}{2\pi\Delta q\Delta p} \exp\left[-\frac{(q-q_0)^2}{2(\Delta q)^2} - \frac{(p-p_0)^2}{2(\Delta p)^2} \right]. \tag{2.3}$$

For analysis purposes in the later sections, we shall use the explicit form of the covariance matrix for squeezed coherent thermal state corresponding to temperature T of a single mode system with frequency ω, which can be written as follows using Eqs. (1.68) and (1.84):

$$V = S(r)V_{\rm th}S(r)^T = \frac{1}{2}\begin{pmatrix} (2\langle n\rangle + 1)e^{-2r} & 0 \\ 0 & (2\langle n\rangle + 1)e^{2r} \end{pmatrix}, \tag{2.4}$$

where $\langle n\rangle = 1/(\exp(\omega/k_BT) - 1)$ is the average number of photons in the thermal state. In the following sections, we discuss various measurement schemes, which are employed for the estimation of Gaussian states. The measurements considered are Gaussian measurements, *i.e.*, the probability distributions of the outcomes are Gaussian. These measurements are performed on an ensemble of identically prepared Gaussian states, and different outcomes are obtained according to the probability distribution of the corresponding observable of the state. The variance of the probability distributions signify the accuracy of the corresponding measurement schemes. Here we consider the case that the measurement apparatuses have infinite precision and the variance in the outcomes for any measurement is due to the inherent uncertainty in the observables.

2.2.1 Homodyne measurement

In homodyne measurement, we measure either the $\hat{q}$ quadrature or the $\hat{p}$ quadrature on the system. The probability distribution function $P(q)$ of obtaining the outcome 'q' corresponding to the measurement of the $\hat{q}$ quadrature on the state (2.2) can be evaluated as

$$P(q) = \int W(q,p)dp = \frac{1}{\sqrt{2\pi(\Delta q)^2}} \exp\left[-\frac{(q-q_0)^2}{2(\Delta q)^2}\right]. \tag{2.5}$$

Therefore, the corresponding variance for the $\hat{q}$ quadrature measurement is

$$V^{\text{Hom}}(\hat{q}) = (\Delta q)^2. \tag{2.6}$$

Similarly, the probability distribution function $P(p)$ of obtaining the outcome 'p' corresponding to the measurement of the $\hat{p}$ quadrature on the state (2.2) can be evaluated as

$$P(p) = \int W(q,p)dq = \frac{1}{\sqrt{2\pi(\Delta p)^2}} \exp\left[-\frac{(p-p_0)^2}{2(\Delta p)^2}\right]. \tag{2.7}$$

Therefore, the corresponding variance for the $\hat{p}$ quadrature measurement is

$$V^{\text{Hom}}(\hat{p}) = (\Delta p)^2. \tag{2.8}$$

2.2.2 Heterodyne measurement

In heterodyne measurement, we measure jointly the $\hat{q}$ quadrature and the $\hat{p}$ quadrature on the system. Since the heterodyne measurement corresponds to the projection over coherent state basis $E_\alpha = (2\pi)^{-1}|\alpha\rangle\langle\alpha|$, the probability of obtaining the outcomes 'q'

and 'p' on the joint measurement of the q and p-quadratures on a system with density operator ρ can be written as

$$P(q,p) = \frac{1}{2\pi}\mathrm{Tr}[\hat{\rho}|\alpha\rangle\langle\alpha|]. \tag{2.9}$$

For simplicity, we move to the phase space and evaluate the trace in the Wigner function description as follows:

$$P(q,p) = \int_{\mathcal{R}^2} dqdp\, W_{\hat{\rho}}(q,p) W_{|\alpha\rangle}(q,p). \tag{2.10}$$

A straightforward calculation yields the probability distribution as

$$P(q,p) = \frac{\exp\left[-\frac{(q-q_0)^2}{1+2(\Delta q)^2} - \frac{(p-p_0)^2}{1+2(\Delta p)^2}\right]}{\pi\sqrt{\left(1+2(\Delta q)^2\right)\left(1+2(\Delta p)^2\right)}}. \tag{2.11}$$

Therefore, the corresponding variance of the marginals $P(q)$ and $P(p)$ of the probability distribution $P(q,p)$ is

$$V^{\text{Het}}(\hat{q}) = \frac{1}{2} + (\Delta q)^2, \quad \text{and} \quad V^{\text{Het}}(\hat{p}) = \frac{1}{2} + (\Delta p)^2. \tag{2.12}$$

We note that the vacuum noise (equal to $1/2$) is added to the variance of both the marginals $P(q)$ and $P(p)$ of the probability distribution $P(q,p)$.

2.2.3 Sequential measurement

In the sequential measurement scheme, the weak measurement of one quadrature is followed by the strong measurement of its conjugate quadrature [60]. To carry out the first measurement, we use the von-Neumann measurement model, where we couple the system with a meter in sufficiently wide wave functions. This measurement disturbs the state a little and does not lead to the collapse of the wave function. Such type of measurements are called weak or unsharp measurements [113, 114, 115, 116, 117]. Although weak measurement disturbs the state a little, we obtain comparatively less information about the system [118]. Since the state does not collapse after the weak measurement, it can be reused for the measurement of the conjugate observable [119]. The second measurement, a strong one, is a homodyne measurement. To remove the biasedness in the order of the measurements, we divide the ensemble in two halves [62]. On the first half, we measure the $\hat{Q}$-quadrature of the meter weakly, which renders information about the $\hat{q}$-quadrature of the system. This is followed by a homodyne measurement of the $\hat{p}$-quadrature on the system, as shown in Fig. 2.1. Similarly, on the

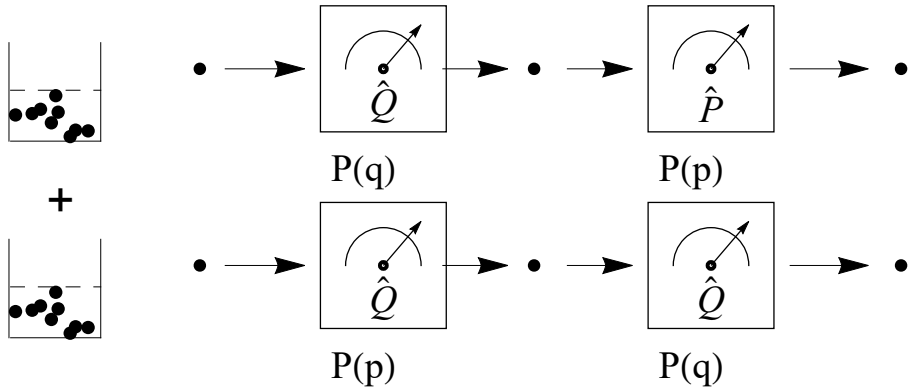


Figure 2.1: Schematic representation of the sequential measurement scheme. The whole ensemble is divided in two halves. On the first half, the sequential measurement of the $\hat{Q}$-quadrature of the meter, which renders information about the $\hat{q}$-quadrature of the system, is followed by a homodyne measurement of the $\hat{p}$-quadrature of the system. Similarly, on the second half, the sequential measurement of the $\hat{Q}$-quadrature of the meter, which renders information about the $\hat{p}$-quadrature of the system, is followed by a homodyne measurement of the $\hat{q}$-quadrature of the system.

second half, the weak measurement of $\hat{Q}$-quadrature of the meter renders information about the $\hat{p}$-quadrature of the system, which is followed by a homodyne measurement of the $\hat{q}$-quadrature of the system.

We now describe the exact details of the scheme. While the system is represented by the quadrature operators $\hat{q}$ and $\hat{p}$, we consider the apparatus also to be a one mode CV system representing a meter with quadrature operators $\hat{Q}_1$ and $\hat{P}_1$. The corresponding phase space is four-dimensional and can be represented by four variables, which can be arranged in a column vector form as $\xi = (q, p, Q_1, P_1)^T$. We assume that the system is in a squeezed coherent thermal state and the meter is in a squeezed vacuum state, and thus they satisfy the following uncertainty relations:

$$\Delta q \Delta p \geq 1/2, \quad \Delta Q_1 \Delta P_1 = 1/2. \tag{2.13}$$

Since the system and the meter are in Gaussian states, the system-meter state can be specified by the following displacement vector and covariance matrix:

$$\bar{\hat{\xi}} = \begin{pmatrix} \langle \hat{q} \rangle = q_0 \\ \langle \hat{p} \rangle = p_0 \\ \langle \hat{Q}_1 \rangle = 0 \\ \langle \hat{P}_1 \rangle = 0 \end{pmatrix}, \quad V = \begin{pmatrix} (\Delta q)^2 & 0 & 0 & 0 \\ 0 & (\Delta p)^2 & 0 & 0 \\ 0 & 0 & (\Delta Q_1)^2 & 0 \\ 0 & 0 & 0 & (\Delta P_1)^2 \end{pmatrix}. \tag{2.14}$$

Now we consider the interaction Hamiltonian of the form

$$\hat{H}(t) = \delta(t - t_1) \hat{q} \hat{P}_1, \tag{2.15}$$

which entangles the system and the meter. The unitary operator acting on the joint system-meter Hilbert space is given by

$$\mathcal{U}(\hat{H}(t)) = \mathrm{e}^{-i\int \hat{H}(t)\,dt} = \mathrm{e}^{-i\hat{q}\hat{P}_1}. \tag{2.16}$$

The corresponding symplectic transformation acting on the quadrature operators $\hat{\xi} = (\hat{q}, \hat{p}, \hat{Q}_1, \hat{P}_1)^T$ is given by (see Appendix A)

$$S = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & -1 \\ 1 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}. \tag{2.17}$$

The above symplectic transformation is an element of the real symplectic group $Sp(4,\, \mathcal{R})$ and satisfies the symplectic condition (1.77). As a result of the above transformation, the final displacement vector and covariance matrix V (2.14) can be written as follows according to Eq. (1.106):

$$\overline{\hat{\xi}'} = \begin{pmatrix} \langle \hat{q} \rangle = q_0 \\ \langle \hat{p} \rangle = p_0 \\ \langle \hat{Q}_1 \rangle = q_0 \\ \langle \hat{P}_1 \rangle = 0 \end{pmatrix}, \quad V' = \begin{pmatrix} (\Delta q)^2 & 0 & (\Delta q)^2 & 0 \\ 0 & (\Delta p)^2 + (\Delta P_1)^2 & 0 & -(\Delta P_1)^2 \\ (\Delta q)^2 & 0 & (\Delta q)^2 + (\Delta Q_1)^2 & 0 \\ 0 & -(\Delta P_1)^2 & 0 & (\Delta P_1)^2 \end{pmatrix}. \tag{2.18}$$

One can easily find the transformed Wigner distribution of the system-meter using Eq. (1.69), which is specified by the displacement vector and the covariance matrix (2.18). The Wigner distribution of the reduced state of the meter can be evaluated by integrating the system-meter Wigner distribution over the system variables q and p. The displacement vector and the covariance matrix of the reduced state can be readily evaluated using the Wigner function of the reduced state. An alternative to this approach is to work at the covariance matrix level. The displacement vector and the covariance matrix of the reduced state of the meter can be obtained by ignoring the matrix elements corresponding to the system mode. This can be easily seen through the Wigner characteristic function of a Gaussian state [14, 42]. Thus, the displacement vector and the covariance matrix of the reduced state of the meter are

$$\overline{\hat{\xi}'_{\mathrm{M}}} = \begin{pmatrix} \langle \hat{Q}_1 \rangle = q_0 \\ \langle \hat{P}_1 \rangle = 0 \end{pmatrix}, \quad V'_{\mathrm{M}} = \begin{pmatrix} (\Delta q)^2 + (\Delta Q_1)^2 & 0 \\ 0 & (\Delta P_1)^2 \end{pmatrix}. \tag{2.19}$$

The corresponding Wigner function for the reduced state of the meter can be written using Eq. (1.69) as

$$W(Q_1, P_1) = \frac{1}{2\pi\Delta P_1 \sqrt{(\Delta q)^2 + (\Delta Q_1)^2}} \exp\left[-\frac{(Q_1 - q_0)^2}{2((\Delta q)^2 + (\Delta Q_1)^2)} - \frac{P_1^2}{2(\Delta P_1)^2} \right]. \tag{2.20}$$

The probability density to obtain the outcome Q_1 after a measurement of the $\hat{Q}_1$-quadrature on the meter is

$$P(Q_1) = \frac{1}{\sqrt{2\pi((\Delta q)^2 + (\Delta Q_1)^2)}} \exp\left[-\frac{(Q_1 - q_0)^2}{2((\Delta q)^2 + (\Delta Q_1)^2)}\right]. \tag{2.21}$$

Clearly, the variance of the probability distribution is

$$V_1^{\rm SM}(\hat{q}) = (\Delta q)^2 + (\Delta Q_1)^2, \tag{2.22}$$

which we could have directly written from Eq. (2.18) as the element corresponding to the variance of Q_1. Similarly, the displacement vector and the covariance matrix of the reduced state of the system are given by

$$\overline{\xi_{\rm S}^{'}} = \begin{pmatrix} \langle \hat{Q}_1 \rangle = q_0 \\ \langle \hat{P}_1 \rangle = p_0 \end{pmatrix}, \quad V_{\rm S}^{'} = \begin{pmatrix} (\Delta q)^2 & 0 \\ 0 & (\Delta p)^2 + (\Delta P_1)^2 \end{pmatrix}. \tag{2.23}$$

The variance of the probability distribution corresponding to the homodyne measurement of the $\hat{p}$-quadrature is given by

$$V_1^{\rm SM}(\hat{p}) = (\Delta p)^2 + (\Delta P_1)^2. \tag{2.24}$$

To perform weak measurement of quadrature $\hat{Q}_1$, we prepare the meter in a state with large ΔQ_1, which implies $\Delta P_1 \to 0$. Thus in this limit, the covariance matrix of the reduced state $V_{\rm S}^{'}$ of the system is equal to the covariance matrix of the initial state of the system.

We now discuss the weak measurement of the $\hat{p}$-quadrature followed by a homodyne measurement of the $\hat{q}$-quadrature. We again consider the initial state of the joint system-meter state being represented by the displacement vector and the covariance matrix as given in Eq. (2.14). We consider the interaction Hamiltonian of the form

$$\hat{H}(t) = \delta(t - t_1)\hat{p}\hat{Q}_1, \tag{2.25}$$

which is the generator of the following symplectic transformation:

$$S = \begin{pmatrix} 1 & 0 & 0 & 1 \\ 0 & 1 & 0 & 0 \\ 0 & 1 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}. \tag{2.26}$$

The above symplectic transformation is also an element of the real symplectic group $Sp(4,\, \mathcal{R})$ and satisfies the symplectic condition (1.77). The final system-meter state after the action of the above symplectic transformation can be specified by the following

displacement vector and covariance matrix:

$$\overline{\hat{\xi}'} = \begin{pmatrix} \langle \hat{q} \rangle = q_0 \\ \langle \hat{p} \rangle = p_0 \\ \langle \hat{Q}_1 \rangle = p_0 \\ \langle \hat{P}_1 \rangle = 0 \end{pmatrix}, \quad V' = \begin{pmatrix} (\Delta q)^2 + (\Delta P_1)^2 & 0 & 0 & (\Delta P_1)^2 \\ 0 & (\Delta p)^2 & (\Delta p)^2 & 0 \\ 0 & (\Delta p)^2 & (\Delta p)^2 + (\Delta Q_1)^2 & 0 \\ (\Delta P_1)^2 & 0 & 0 & (\Delta P_1)^2 \end{pmatrix}. \tag{2.27}$$

The displacement vector (2.27) shows that the mean of the $\hat{Q}_1$-quadrature for the meter is p_0. Thus, the measurement of the $\hat{Q}_1$-quadrature of the meter yields information about the $\hat{p}$ quadrature of the system. We can directly write the variance of the probability distributions corresponding to the sequential measurement of the $\hat{Q}_1$-quadrature of the meter followed by a homodyne measurement of the $\hat{q}$-quadrature from Eq. (2.27) as

$$\begin{aligned} V_2^{\mathrm{SM}}(\hat{p}) =& (\Delta q)^2 + (\Delta P_1)^2, \quad \text{and} \\ V_2^{\mathrm{SM}}(\hat{q}) =& (\Delta p)^2 + (\Delta Q_1)^2. \end{aligned} \tag{2.28}$$

Here we are measuring $\hat{Q}_1$ quadrature weakly by preparing the meter in a state with large ΔQ_1, which implies $\Delta P_1 \to 0$. Thus in this limit, the reduced state covariance matrix of the system

$$V_{\mathrm{S}}' = \begin{pmatrix} (\Delta q)^2 + (\Delta P_1)^2 & 0 \\ 0 & (\Delta p)^2 \end{pmatrix} \tag{2.29}$$

is equal to the covariance matrix of the initial state of the system.

2.2.4 Arthurs-Kelly measurement scheme

Arthurs-Kelly proposed a scheme by extending the von Neumann model, which enables us to measure simultaneously conjugate quadratures $\hat{q}$ and $\hat{p}$. To this end, two meters, one for each quadrature measurement, are introduced, as shown in Fig. 2.2. We represent the system and two meters using three pairs of Hermitian quadrature operators arranged in column vector as $\hat{\xi} = (\hat{q}, \hat{p}, \hat{Q}_1, \hat{P}_1, \hat{Q}_2, \hat{P}_2)^T$, where $(\hat{q}, \hat{p})$ corresponds to the system and $(\hat{Q}_1, \hat{P}_1)$ and $(\hat{Q}_2, \hat{P}_2)$ correspond to the two meters. We assume the system to be in a squeezed coherent thermal state and the meters to be in a squeezed vacuum state, and thus they satisfy the following uncertainty relations:

$$\Delta q \Delta p \geq 1/2, \quad \Delta Q_1 \Delta P_1 = 1/2, \quad \Delta Q_2 \Delta P_2 = 1/2. \tag{2.30}$$

We analyze our joint system in a six-dimensional phase space represented by six variables, which can be arranged in a column vector form as $\xi = (q, p, Q_1, P_1, Q_2, P_2)^T$.

We represent the system-meters initial state by the displacement vector $\bar{\hat{\xi}}$ given as

$$\bar{\hat{\xi}} = \begin{pmatrix} \langle \hat{q} \rangle = q_0 \\ \langle \hat{p} \rangle = p_0 \\ \langle \hat{Q}_1 \rangle = 0 \\ \langle \hat{P}_1 \rangle = 0 \\ \langle \hat{Q}_2 \rangle = 0 \\ \langle \hat{P}_2 \rangle = 0 \end{pmatrix}, \tag{2.31}$$

and the covariance matrix V given as

$$V = \begin{array}{c} \overbrace{}^{\text{System}} \quad \overbrace{}^{\text{Meter 1}} \quad \overbrace{}^{\text{Meter 2}} \\ \begin{array}{cc|cc|cc} q & p & Q_1 & P_1 & Q_2 & P_2 \end{array} \\ \left(\begin{array}{cc|cc|cc} (\Delta q)^2 & 0 & 0 & 0 & 0 & 0 \\ 0 & (\Delta p)^2 & 0 & 0 & 0 & 0 \\ \hline 0 & 0 & (\Delta Q_1)^2 & 0 & 0 & 0 \\ 0 & 0 & 0 & (\Delta P_1)^2 & 0 & 0 \\ \hline 0 & 0 & 0 & 0 & (\Delta Q_2)^2 & 0 \\ 0 & 0 & 0 & 0 & 0 & (\Delta P_2)^2 \end{array} \right) \begin{array}{c} q \\ p \\ Q_1 \\ P_1 \\ Q_2 \\ P_2 \end{array} \end{array} . \tag{2.32}$$

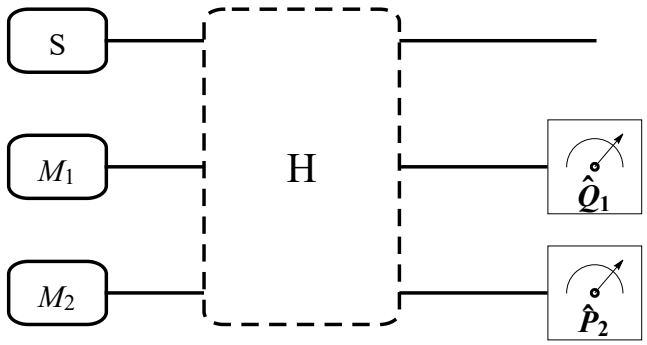


Figure 2.2: Schematic representation of the Arthurs-Kelly scheme. The system is labeled by S, while the two meters are labeled by M_1 and M_2. H represents the interaction Hamiltonian. Measurement of $\hat{Q}_1$-quadrature on meter M_1 and measurement of $\hat{P}_2$-quadrature on meter M_2 yield information about the $\hat{q}$-quadrature and the $\hat{p}$-quadrature of the system, respectively.

The interaction Hamiltonian through which we intend to measure both the system quadratures by coupling them to different meters is considered to be of the form

$$H = \delta(t - t_1)(\hat{q}\hat{P}_1 - \hat{p}\hat{Q}_2), \tag{2.33}$$

which entangles the system with both the meters. The corresponding symplectic transformation acting on the quadrature operators $\hat{\xi}$ is given by

$$S = \begin{array}{c} \begin{matrix} q & p & Q_1 & P_1 & Q_2 & P_2 \end{matrix} \\ \left(\begin{array}{cc|cc|cc} 1 & 0 & 0 & 0 & -1 & 0 \\ 0 & 1 & 0 & -1 & 0 & 0 \\ \hline 1 & 0 & 1 & 0 & -\frac{1}{2} & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 \\ \hline 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & -\frac{1}{2} & 0 & 1 \end{array}\right) \end{array} \begin{matrix} q \\ p \\ Q_1 \\ P_1 \\ Q_2 \\ P_2 \end{matrix} . \tag{2.34}$$

The above symplectic transformation is an element of the real symplectic group $Sp(6, \mathcal{R})$ and satisfies the symplectic condition (1.77). The displacement vector of the transformed joint system-meters state can be written as

$$\overline{\hat{\xi}'} = \begin{pmatrix} \langle \hat{q} \rangle = q_0 \\ \langle \hat{p} \rangle = p_0 \\ \langle \hat{Q}_1 \rangle = q_0 \\ \langle \hat{P}_1 \rangle = 0 \\ \langle \hat{Q}_2 \rangle = 0 \\ \langle \hat{P}_2 \rangle = p_0 \end{pmatrix} . \tag{2.35}$$

Similarly, the covariance matrix of the transformed joint system-meters state evaluates to

$$V' = \begin{array}{c} \begin{matrix} \overbrace{\qquad\qquad}^{\text{System}} & & \overbrace{\qquad\qquad}^{\text{Meter 1}} & & \overbrace{\qquad\qquad}^{\text{Meter 2}} & \\ q & p & Q_1 & P_1 & Q_2 & P_2 \end{matrix} \\ \begin{pmatrix} (\Delta q)^2 + (\Delta Q_2)^2 & 0 & (\Delta q)^2 + \frac{(\Delta Q_2)^2}{2} & 0 & -(\Delta Q_2)^2 & 0 \\ 0 & (\Delta p)^2 + (\Delta P_1)^2 & 0 & -(\Delta P_1)^2 & 0 & (\Delta p)^2 + \frac{(\Delta P_1)^2}{2} \\ (\Delta q)^2 + \frac{(\Delta Q_2)^2}{2} & 0 & V_{M_1}(Q_1) & 0 & -\frac{(\Delta Q_2)^2}{2} & 0 \\ 0 & -(\Delta P_1)^2 & 0 & (\Delta P_1)^2 & 0 & -\frac{(\Delta P_1)^2}{2} \\ -(\Delta Q_2)^2 & 0 & -\frac{(\Delta Q_2)^2}{2} & 0 & (\Delta Q_2)^2 & 0 \\ 0 & (\Delta p)^2 + \frac{(\Delta P_1)^2}{2} & 0 & -\frac{(\Delta P_1)^2}{2} & 0 & V_{M_2}(P_2) \end{pmatrix} \end{array}, \tag{2.36}$$

where

$$V_{M_1}(Q_1) = (\Delta q)^2 + (\Delta Q_1)^2 + \frac{(\Delta Q_2)^2}{4}, \text{ and } V_{M_2}(P_2) = (\Delta p)^2 + \frac{(\Delta P_1)^2}{4} + (\Delta P_2)^2. \tag{2.37}$$

The displacement vector and the covariance matrix of the reduced state of the system can be readily written using Eqs. (2.35) and (2.36) as

$$\overline{\xi_{\rm S}^{'}} = \begin{pmatrix} \langle \hat{Q}_1 \rangle = q_0 \\ \langle \hat{P}_1 \rangle = p_0 \end{pmatrix}, \quad V_{\rm S}^{'} = \begin{pmatrix} (\Delta q)^2 + (\Delta Q_2)^2 & 0 \\ 0 & (\Delta p)^2 + (\Delta P_1)^2 \end{pmatrix}. \tag{2.38}$$

Similarly, the displacement vector and the covariance matrix of meter 1 can be written as

$$\overline{\xi_{\rm M_1}^{'}} = \begin{pmatrix} \langle \hat{Q}_1 \rangle = q_0 \\ \langle \hat{P}_1 \rangle = 0 \end{pmatrix}, \quad V_{\rm M_1}^{'} = \begin{pmatrix} (\Delta q)^2 + (\Delta Q_1)^2 + \frac{(\Delta Q_2)^2}{4} & 0 \\ 0 & (\Delta P_1)^2 \end{pmatrix}. \tag{2.39}$$

Finally, meter 2 is represented by the following displacement vector and covariance matrix:

$$\overline{\xi_{\rm M_2}^{'}} = \begin{pmatrix} \langle \hat{Q}_1 \rangle = 0 \\ \langle \hat{P}_1 \rangle = p_0 \end{pmatrix}, \quad V_{\rm M_2}^{'} = \begin{pmatrix} (\Delta Q_2)^2 & 0 \\ 0 & (\Delta p)^2 + \frac{(\Delta P_1)^2}{4} + (\Delta P_2)^2 \end{pmatrix}. \tag{2.40}$$

The variance of the probability distribution for the measurement of the $\hat{Q}_1$-quadrature on the meter 1 and $\hat{P}_2$-quadrature on meter 2 can be directly written from Eq. (2.36) as

$$\begin{aligned} V^{\rm AK}(\hat{q}) =& (\Delta q)^2 + (\Delta Q_1)^2 + \frac{(\Delta Q_2)^2}{4}, \\ V^{\rm AK}(\hat{p}) =& (\Delta p)^2 + \frac{(\Delta P_1)^2}{4} + (\Delta P_2)^2. \end{aligned} \tag{2.41}$$

2.3 Results

Our aim in this section is to examine the performance of various measurement schemes in the estimation of the Wigner distribution of an ensemble with a fixed number of identically prepared states. Specifically, we wish to analyze the estimation efficiency of the mean and the variance of an ensemble of N identically prepared Gaussian states. To this end, we define measure of fidelity F_1 for the mean of the Gaussian state as

$$F_1 = \langle (q^A - q^M)^2 \rangle + \langle (p^A - p^M)^2 \rangle, \tag{2.42}$$

where q^A and p^A are the actual values of the mean of the $\hat{q}$ and $\hat{p}$ quadratures of the Gaussian state and are thus fixed, whereas q^M and p^M are the measured values of the $\hat{q}$ and $\hat{p}$ quadratures of the Gaussian state and are different for measurements on different copies of the system. The magnitude of the fidelity measure F_1 signifies how well the mean (q_0, p_0) of the Gaussian state has been estimated. We define another measure of fidelity F_2 for the variance of the Gaussian state as

$$F_2 = \langle (V_q^A - V_q^M)^2 \rangle + \langle (V_p^A - V_p^M)^2 \rangle, \tag{2.43}$$

where V_q^A and V_p^A are the actual values of the variance of $\hat{q}$ and $\hat{p}$ quadratures, while V_q^M and V_p^M are the measured values of the variance of $\hat{q}$ and $\hat{p}$ quadratures. Here F_2 signifies how well the variance $(\Delta q)^2$ and $(\Delta p)^2$ has been estimated. In the case of perfect estimation, both the fidelities F_1 and F_2 should approach zero.

2.3.1 Analytical expressions of the fidelity F_1

Now we evaluate the fidelity F_1 for various measurements, which are employed for the estimation of Gaussian states. To estimate the state using the homodyne measurement, we divide the ensemble in two halves. On the first half of the ensemble, the $\hat{q}$-quadrature is measured, while on the other half of the ensemble, the $\hat{p}$-quadrature is measured. Thus, we can write the fidelity measure F_1 for the homodyne measurement using Eqs. (2.6) and (2.8) as

$$F_1^{\mathrm{Hom}} = \frac{(\Delta q)^2}{N/2} + \frac{(\Delta p)^2}{N/2}. \tag{2.44}$$

Here we have used the fact that the probability distribution involved in the homodyne measurement is Gaussian, and the sample variance for a Gaussian (normal) distribution $\mathcal{N}(\mu, \sigma)$ with mean μ and variance σ^2 for a sample of size N is given by σ^2/N. The fidelity measure F_1 for the heterodyne measurement can be written using Eq. (2.12) as

$$F_1^{\mathrm{Het}} = \frac{(\Delta q)^2 + 1/2}{N} + \frac{(\Delta p)^2 + 1/2}{N}. \tag{2.45}$$

We can analytically derive from Eqs. (2.44) and (2.45) that $F_1^{\mathrm{Hom}} \geq F_1^{\mathrm{Het}}$, where the equality sign only holds for a coherent state ensemble. Therefore, the homodyne measurement and the heterodyne measurement perform the same for a coherent state ensemble, whereas the heterodyne measurement outperforms the homodyne measurement for a squeezed state ensemble as far as the mean estimation is concerned.

For the sequential measurement scheme, we again divide the ensemble in two halves and perform measurement according to the procedure described in Sec. 2.2.3. The expression of the fidelity F_1 in this case can be given as

$$F_1^{\mathrm{SM}} = \left\langle \left(q^A - \frac{q_1^M + q_2^M}{2} \right)^2 \right\rangle + \left\langle \left(p^A - \frac{p_1^M + p_2^M}{2} \right)^2 \right\rangle, \tag{2.46}$$

which can be written as follows using Eqs. (2.22), (2.24), and (2.28):

$$F_1^{\mathrm{SM}} = \frac{(\Delta q)^2 + (\Delta p)^2 + (\Delta Q_1)^2 + (\Delta P_1)^2}{N}. \tag{2.47}$$

It can be seen from the above equation that the optimal performance in the mean estimation for the sequential measurement scheme corresponds to $\Delta Q_1 = \Delta P_1 = 1/\sqrt{2}$. Further, at the optimal conditions, $F_1^{\rm SM} = F_1^{\rm Het}$. Similarly, we can write the fidelity expression F_1 for the Arthurs-Kelly scheme using Eq. (2.41) as

$$F_1^{\rm AK} = \frac{(\Delta q)^2 + (\Delta Q_1)^2 + \frac{(\Delta Q_2)^2}{4}}{N} + \frac{(\Delta p)^2 + \frac{(\Delta P_1)^2}{4} + (\Delta P_2)^2}{N}. \tag{2.48}$$

For the Arthurs-Kelly scheme, the optimal performance in the mean estimation corresponds to

$$\Delta Q_1 = 1/2, \quad \Delta P_2 = 1/2, \tag{2.49}$$

and at the optimal conditions, $F_1^{\rm AK} = F_1^{\rm Het}$. This means that the optimal performance in the mean estimation of the sequential measurement requires only classical resources, *i.e.*, the meter should be prepared in a coherent state, while the Arthurs-Kelly scheme requires nonclassical resources, *i.e.*, the meters should be prepared in a squeezed state.

Now we illustrate the dependence of the fidelity F_1 on the initial width of the meter ΔQ_1, the squeezing parameter r, and the average number of photons $\langle n \rangle$ graphically. We have considered an ensemble of size $N = 20$ in all different plots in this chapter.

We show the plot of the fidelity F_1 as a function of the initial width of the meter ΔQ_1 for a coherent state ensemble in Fig. 6.2(a). The results show that the homodyne measurement and the heterodyne measurement perform the same and the optimal performance of the Arthurs-Kelly scheme and the sequential measurement schemes are equal to that of the homodyne measurement and the heterodyne measurement. Similarly, Fig. 6.2(b) shows the plot of fidelity F_1 as a function of the initial width of the meter ΔQ_1 for a squeezed coherent state ensemble with squeezing parameter $r = 1$. In this case, the heterodyne measurement outperforms the homodyne measurement. Further, an increase or a decrease in the size of the ensemble changes only the magnitude of the fidelity, while the performance trend of the various measurement schemes remain the same. It should be noted that these conclusions about the relative performances of the various measurement schemes are based on the mean estimation efficacy.

We plot the fidelity F_1 as a function of the squeezing parameter r in Fig. 2.4(a). The results show that both the homodyne measurement and the heterodyne measurement estimate the mean of the Gaussian state with the same fidelity for a coherent state ensemble $(r = 0)$, while for a squeezed coherent state ensemble $(r > 0)$, the heterodyne measurement outperforms the homodyne measurement. The plot of the fidelity F_1 as a function of the average number of photons $\langle n \rangle$ is shown in Fig. 2.4(b). The results show that the fidelity of the mean estimation increases, *i.e.*, the estimation efficiency decreases, for a thermal state $(\langle n \rangle > 0)$ ensemble as compared to a pure state $(\langle n \rangle = 0)$ ensemble.

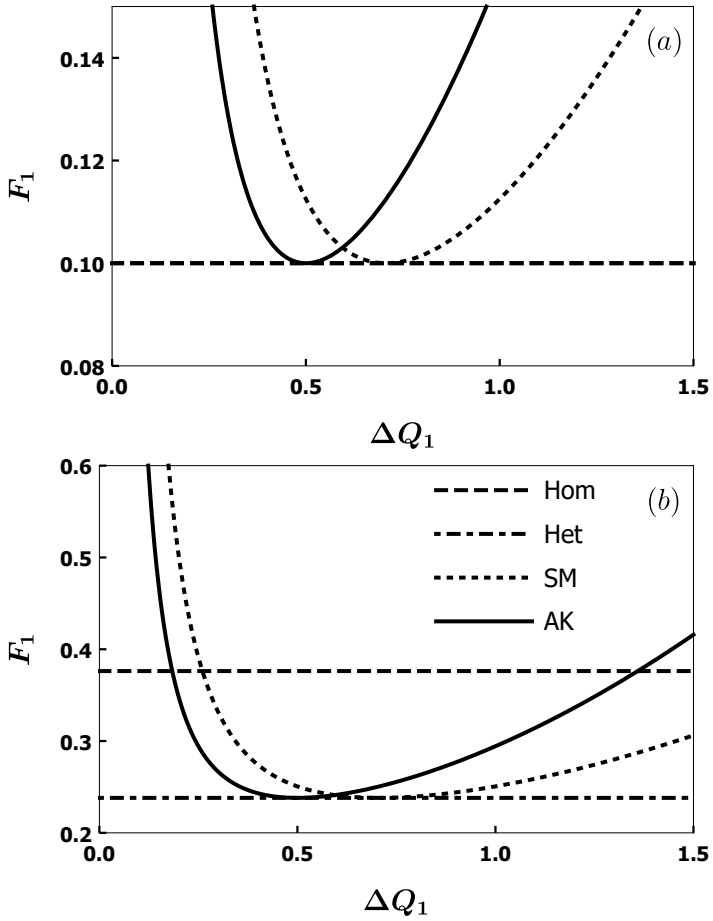


Figure 2.3: Both the plots show the fidelity F_1 as a function of the initial width of the meter ΔQ_1 for an ensemble of size $N = 20$. Additionally, we have taken $\Delta P_2 = 1/2$ in all the graphs for the Arthurs-Kelly scheme, which is the condition for the optimal performance (2.49). (a) The ensemble consists of identically prepared coherent states. The homodyne measurement and the heterodyne measurement perform equally in this case. (b) The ensemble consists of identically prepared squeezed coherent states with squeezing parameter $r = 1$.

2.3.2 Analytical expressions of the fidelity F_2

We now proceed to derive expressions of fidelity measure F_2 (2.43) for the various measurement schemes. For the homodyne measurement, the expression of the fidelity F_2 evaluates to

$$F_2^{\mathrm{Hom}} = \frac{2(\Delta q)^4}{N/2} + \frac{2(\Delta p)^4}{N/2}. \tag{2.50}$$

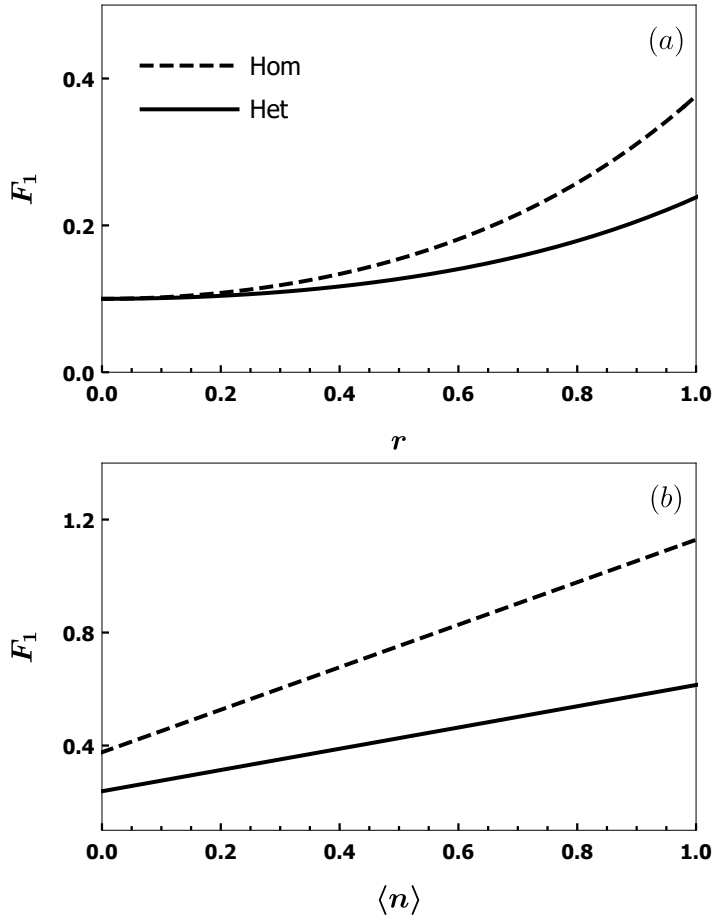


Figure 2.4: (a) The fidelity F_1 as a function of the squeezing parameter r. Here average number of photon is $\langle n \rangle = 0$. (b) The fidelity F_1 as a function of the average photon number $\langle n \rangle$. Here squeezing parameter has been taken as $r = 1$. An ensemble of size $N = 20$ has been considered for both the plots.

Here we have used the fact that the variance of the sample variance for a Gaussian (normal) distribution $\mathcal{N}(\mu, \sigma)$ with mean μ and variance σ^2 for a sample of size N is given by $2\sigma^4/N$. Similarly, the expression of the fidelity F_2 for the heterodyne measurement evaluates to

$$F_2^{\text{Het}} = \frac{2\left((\Delta q)^2 + 1/2\right)^2}{N} + \frac{2\left((\Delta p)^2 + 1/2\right)^2}{N}. \tag{2.51}$$

For the sequential measurement scheme, the expression of the fidelity F_2 can be written in an analogous way as Eq. (2.46). The final expression of the fidelity in this case

evaluates to

$$F_2^{\mathrm{SM}} = \frac{2}{N}\Big[(\Delta p)^4 + (\Delta q)^2\left((\Delta Q_1)^2 + (\Delta q)^2\right)^2 + (\Delta Q_1)^2\left((\Delta Q_1)^2 + (\Delta p)^2\right)^2 + (\Delta P_1)^2\left((\Delta q)^2 + (\Delta p)^2 + (\Delta P_1)^2\right)^2\Big]. \tag{2.52}$$

Similarly, the fidelity F_2 for the Arthurs-Kelly scheme can be written as

$$F_2^{\mathrm{AK}} = \frac{2\left((\Delta q)^2 + (\Delta Q_1)^2 + \frac{(\Delta Q_2)^2}{4}\right)^2}{N} + \frac{2\left((\Delta p)^2 + \frac{(\Delta P_1)^2}{4} + (\Delta P_2)^2\right)^2}{N}. \tag{2.53}$$

We note here that the fidelity expressions F_1 and F_2 for different measurement schemes are independent of the actual values of the mean q_0 and p_0 of the Gaussian states and depend only on the actual variances $(\Delta q)^2$ and $(\Delta p)^2$ of the quadratures. Now we turn to study the dependence of fidelity F_2 on the initial width of the meter ΔQ_1, the squeezing parameter r, and the average number of photons $\langle n\rangle$.

We show the plot of the fidelity F_2 as a function of the initial width of the meter ΔQ_1 for a coherent state ensemble in Fig. 2.5(a). The results show that the homodyne measurement outperforms the heterodyne measurement in estimating the variance for a coherent state ensemble. We also notice that the optimal performance of the Arthurs-Kelly scheme and the sequential measurement equal the heterodyne measurement. We note that the optimal performance of the Arthurs-Kelly scheme occurs at $\Delta Q_1 = \Delta P_2 = 1/2$, while the optimal performance of the sequential measurement occurs at $\Delta Q_1 = 1/\sqrt{2}$.

Similarly, Fig. 2.5(b) shows the plot of the fidelity F_2 as a function of the initial width of the meter ΔQ_1 for a squeezed coherent state ensemble with squeezing parameter $r = 1$. The results show that the heterodyne measurement outperforms the homodyne measurement in estimating the variance of a squeezed state ensemble with squeezing parameter $r = 1$. Here too, the optimal performance of the Arthurs-Kelly scheme and the sequential measurement equal the heterodyne measurement.

We plot the fidelity F_2 as a function of the squeezing parameter r in Fig. 2.6(a) for $\langle n\rangle = 0$. The results show that the homodyne measurement outperforms the heterodyne measurement up to a certain value of the squeezing parameter $r_c = 0.53$. This result is in contrast with the fidelity F_1 result, where the heterodyne measurement outperforms the homodyne measurement for all non-zero squeezing parameter. The critical value of the squeezing parameter r_c at a given $\langle n\rangle$, where the relative performance of the homodyne measurement is equal to the heterodyne measurement can be written as

$$e^{2r_c} = \frac{1 + \sqrt{3 + 2n_1^2} + \sqrt{2(2 - n_1^2 + \sqrt{3 + 2n_1^2})}}{2n_1}, \tag{2.54}$$

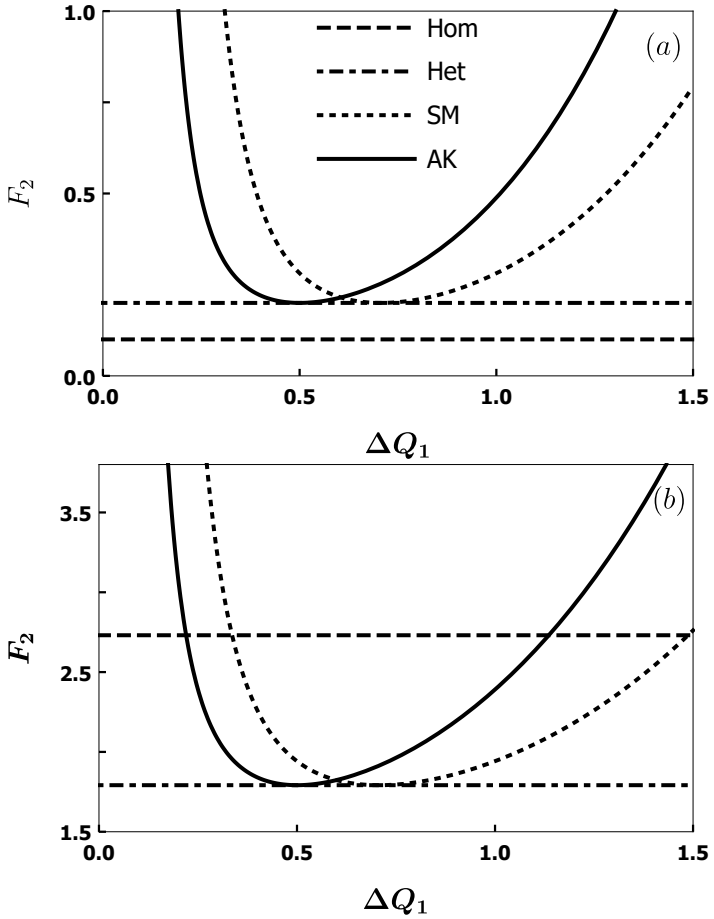


Figure 2.5: Both the plots show the fidelity F_2 as a function of the initial width of the meter ΔQ_1 for an ensemble of size $N = 20$. (a) The ensemble consists of identically prepared coherent states. (b) The ensemble consists of identically prepared squeezed coherent states with squeezing parameter $r = 1$.

where $n_1 = 2\langle n\rangle + 1$. Further, the plot of the fidelity F_2 as a function of the average number of photons $\langle n\rangle$ is shown in Fig. 2.6(b). The results reveal that the variance estimation for a thermal state ensemble is less precise as compared to a pure state ensemble.

2.3.3 Average estimation efficiency

We now move on to compare the relative performances of the various measurement schemes on a large number of randomly generated squeezed coherent thermal states with squeezing parameter r varying uniformly between -1 to $+1$. Such an ensemble

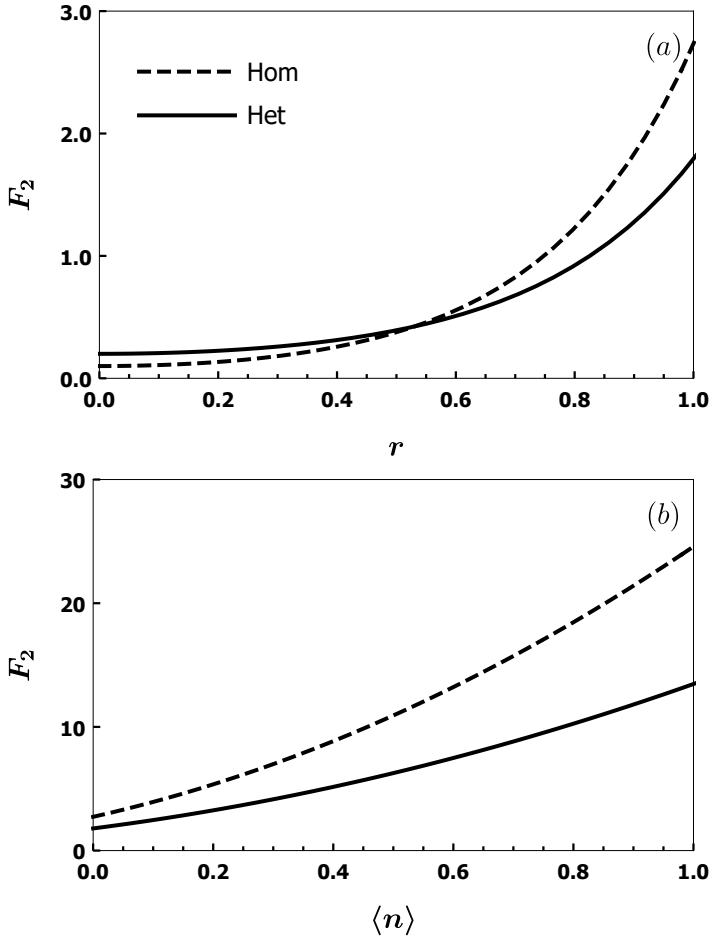


Figure 2.6: (a) The fidelity F_2 as a function of the squeezing parameter r. Here average number of photon has been set as $\langle n \rangle = 0$. (b) The fidelity F_2 as a function of the average photon number $\langle n \rangle$. Here squeezing parameter has been taken as $r = 1$. An ensemble of size $N = 20$ has been considered for both the plots.

can be produced by a parametric down converter operating at a fixed temperature, which generates states with squeezing parameter r uniformly distributed between -1 to $+1$. We note that the squeezing parameter range -1 to $+1$ can be easily achieved in experiments. For evaluating the average fidelities $\overline{F_1}$ and $\overline{F_2}$, we consider the state of the system to be parameterized by the squeezing parameter r and the average number of photons $\langle n \rangle$ as given in Eq. (2.4).

2.3.3.1 Calculation of the mean fidelity $\overline{F_1}$

The mean fidelity $\overline{F_1}^{\text{Hom}}$ for the homodyne measurement is calculated as

$$\overline{F_1}^{\text{Hom}} = \frac{1}{2}\int_{-1}^{+1} F_1^{\text{Hom}}(r, \langle n\rangle)dr, = \frac{n_1 \sinh(2)}{N}, \tag{2.55}$$

where $n_1 = 2\langle n\rangle + 1$. Similarly, the final expressions of the average fidelity for the other measurement schemes are

$$\begin{aligned}
\overline{F_1}^{\text{Het}} &= \frac{2 + n_1 \sinh(2)}{2N}, \\
\overline{F_1}^{\text{SM}} &= \frac{2\left((\Delta Q_1)^2 + (\Delta P_1)^2\right) + n_1 \sinh(2)}{2N}, \\
\overline{F_1}^{\text{AK}} &= \frac{1}{4N}\Big[(\Delta Q_2)^2 + (\Delta P_1)^2 + 4\left((\Delta Q_1)^2 + (\Delta P_2)^2\right) + 2n_1 \sinh(2)\Big].
\end{aligned} \tag{2.56}$$

The results for the mean fidelity $\overline{F_1}$ for various measurement schemes are shown in Fig. 2.7.

We see from Fig. 2.7(a) that the heterodyne measurement outperforms the homodyne measurement, and the optimal performance of the Arthurs-Kelly scheme and the sequential measurement equal the heterodyne measurement. Figure 2.7(b) shows that the performance trend for the thermal state ensembles is similar to the pure state ensembles except the estimation efficiency of the mean is reduced for the thermal state ensemble as compared to the pure state ensemble.

2.3.3.2 Calculation of the mean fidelity $\overline{F_2}$

We now calculate the expressions of the mean fidelity $\overline{F_2}$ averaged over different squeezed coherent thermal state ensembles with squeezing parameter r uniformly distributed between -1 to $+1$ for different measurement schemes. The mean fidelity $\overline{F_2}$ for the homodyne measurement and the heterodyne measurement evaluate to

$$\begin{aligned}
\overline{F_2}^{\text{Hom}} &= \frac{n_1^2 \sinh(4)}{2N}, \\
\overline{F_2}^{\text{Het}} &= \frac{4 + 4n_1 \sinh(2) + n_1^2 \sinh(4)}{4N}.
\end{aligned} \tag{2.57}$$

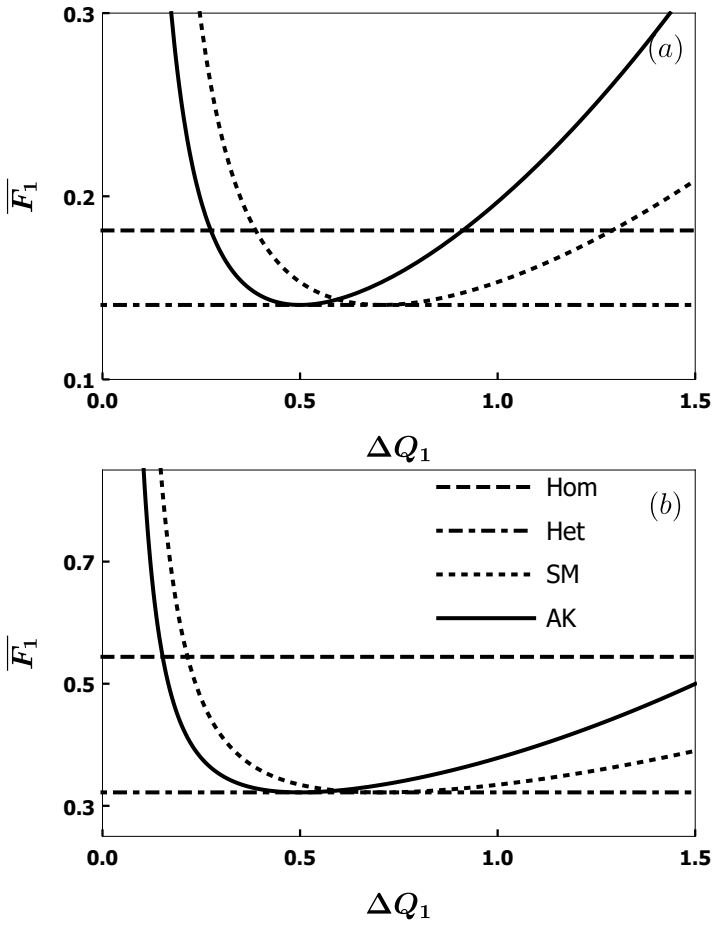


Figure 2.7: Both the plots show the mean fidelity $\overline{F_1}$ as a function of the initial width of the meter ΔQ_1 for an ensemble of size $N = 20$. (a) The averaging is done over identically prepared squeezed coherent state with $\langle n \rangle = 0$, whose squeezing parameter r is uniformly distributed between -1 to $+1$. (b) The averaging is done over identically prepared squeezed coherent thermal state with $\langle n \rangle = 1$, whose squeezing parameter r is uniformly distributed between -1 to $+1$.

Similarly, the expressions of the mean fidelity for the sequential measurement and the Arthurs-Kelly scheme evaluate to

$$\overline{F_2}^{\text{SM}} = \frac{1}{4N}\left[4\left((\Delta Q_1)^2 + (\Delta P_1)^2\right)\left(2 + n_1 \sinh(2)\right) + n_1^2 \sinh(4)\right],$$

$$\overline{F_2}^{\text{AK}} = \frac{1}{8N}\Big[2n_1^2 \sinh(4) + \left(4(\Delta Q_1)^2 + (\Delta Q_2)^2\right)\left(4(\Delta Q_1)^2 + (\Delta Q_2)^2 + 2n_1 \sinh(2)\right)$$
$$+ \left((\Delta P_1)^2 + 4(\Delta P_2)^2\right)\left((\Delta P_1)^2 + 4(\Delta P_2)^2 + 2n_1 \sinh(2)\right)\Big]. \tag{2.58}$$

The results for the mean fidelity $\overline{F_2}$ for various measurement schemes are shown in

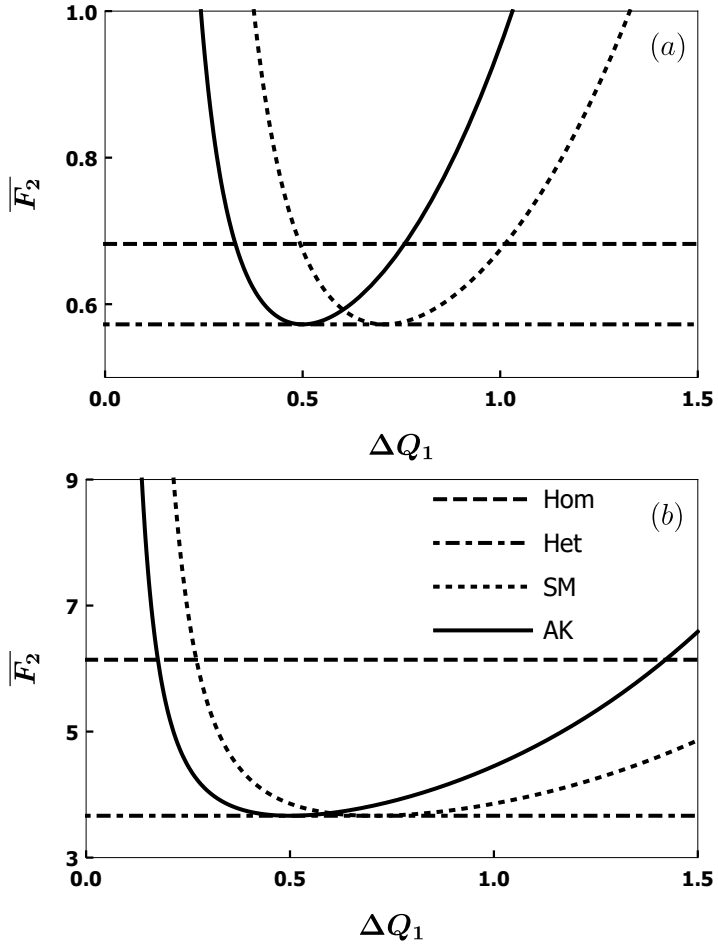


Figure 2.8: Both the plots show the mean fidelity $\overline{F_2}$ as a function of the initial width of the meter ΔQ_1 for an ensemble of size $N = 20$. (a) The averaging is done over identically prepared squeezed coherent state with $\langle n \rangle = 0$, whose squeezing parameter r is uniformly distributed between -1 to $+1$. (b) The averaging is done over identically prepared squeezed coherent thermal state with $\langle n \rangle = 1$, whose squeezing parameter r is uniformly distributed between -1 to $+1$.

Fig. 2.8. As can be seen from Fig. 2.8(a), the heterodyne measurement outperforms the homodyne measurement, and the optimal performance of the Arthurs-Kelly scheme and the sequential measurement scheme equal the heterodyne measurement. For the thermal state ensembles, the performance trend remains the same; however, the estimation efficiency $\overline{F_2}$ of the variance is reduced for the thermal state ensembles as compared to the pure state ensembles as can be seen from Fig. 2.8(b).

We summarize the relative performances of the homodyne measurement and the heterodyne measurement in Table 3.1. We further note that the optimal performance of the sequential measurement and the Arthurs-Kelly scheme is equal to the heterodyne measurement for both the mean and the variance estimation.

Table 2.1: Homodyne measurement versus heterodyne measurement. d_1 and d_2 represent the accuracy of the mean and the variance estimation.

Ensemble	Distance measure	Relative performance
Coherent state ($r = 0$)	$d_1^{\text{Hom}} = d_1^{\text{Het}}$	Hom = Het
Squeezed state ($r > 0$)	$d_1^{\text{Hom}} > d_1^{\text{Het}}$	Hom < Het
$r < r_c$ (Eq. (2.54))	$d_2^{\text{Hom}} < d_2^{\text{Het}}$	Hom > Het
$r > r_c$	$d_2^{\text{Hom}} > d_2^{\text{Het}}$	Hom < Het
$-1 \leq r \leq +1$	$\overline{d_1}^{\text{Hom}} > \overline{d_1}^{\text{Het}}$	Hom < Het
$-1 \leq r \leq +1$	$\overline{d_2}^{\text{Hom}} > \overline{d_2}^{\text{Het}}$	Hom < Het

2.4 Modified Hamiltonian in the Arthurs-Kelly scheme

We now consider a scenario where the measuring apparatuses can influence each other [110]. Here we want to analyze the performance of the Arthurs-Kelly scheme. To this end, we consider a modified form of the interaction Hamiltonian [110, 111] in the Arthurs-Kelly scheme

$$H = \delta(t - t_1)\left(\hat{q}\hat{P}_1 - \hat{p}\hat{Q}_2 + \frac{\kappa}{2}\hat{P}_1\hat{Q}_2\right), \tag{2.59}$$

where κ determine the coupling strength between the two probes. This Hamiltonian entangles the system with both the meters and also the two meters among themselves. The corresponding symplectic transformation acting on the quadrature operators is

$$S = \begin{array}{c} \begin{array}{cccccc} q & p & Q_1 & P_1 & Q_2 & P_2 \end{array} \\ \left(\begin{array}{cc|cc|cc} 1 & 0 & 0 & 0 & -1 & 0 \\ 0 & 1 & 0 & -1 & 0 & 0 \\ \hline 1 & 0 & 1 & 0 & \frac{\kappa-1}{2} & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 \\ \hline 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & \frac{-\kappa-1}{2} & 0 & 1 \end{array}\right) \end{array} \begin{array}{c} q \\ p \\ \\ Q_1 \\ P_1 \\ Q_2 \\ P_2 \end{array}, \tag{2.60}$$

The covariance matrix and the displacement vector corresponding to system-meters state after time t_1 can be evaluated using Eq. (1.106). The covariance matrix of the reduced state of the two meters is given by

$$V_{M_1M_2}^{\mathrm{RED}} = \begin{pmatrix} V_{M_1}(Q_1) & 0 & \frac{(\kappa-1)}{2}(\Delta Q_2)^2 & 0 \\ 0 & (\Delta P_1)^2 & 0 & -\frac{(\kappa+1)}{2}(\Delta P_1)^2 \\ \frac{(\kappa-1)}{2}(\Delta Q_2)^2 & 0 & (\Delta Q_2)^2 & 0 \\ 0 & -\frac{(\kappa+1)}{2}(\Delta P_1)^2 & 0 & V_{M_2}(P_2) \end{pmatrix}, \quad (2.61)$$

where

$$\begin{aligned} V_{M_1}(Q_1) =& (\Delta q)^2 + (\Delta Q_1)^2 + \frac{(\kappa-1)^2}{4}(\Delta Q_2)^2, \\ V_{M_2}(P_2) =& (\Delta p)^2 + \frac{(\kappa+1)^2}{4}(\Delta P_1)^2 + (\Delta P_2)^2. \end{aligned} \quad (2.62)$$

We find using Simon's entanglement criteria [120] that the reduced state of the two meters is entangled for $|\kappa| \geq 1$. The variance of the probability distribution for the measurement of the $\hat{q}$-quadrature on the meter 1 and the $\hat{p}$-quadrature on the meter 2 can be written as the variance corresponding to $\hat{Q}_1$ and $\hat{P}_2$ in the covariance matrix for the reduced state of the meters (2.61):

$$\begin{aligned} V^{\mathrm{COR}}(\hat{q}) =& (\Delta q)^2 + (\Delta Q_1)^2 + \frac{(\kappa-1)^2}{4}(\Delta Q_2)^2, \\ V^{\mathrm{COR}}(\hat{p}) =& (\Delta p)^2 + \frac{(\kappa+1)^2}{4}(\Delta P_1)^2 + (\Delta P_2)^2. \end{aligned} \quad (2.63)$$

Thus, the fidelity expression F_1 for the modified Arthurs-Kelly scheme reads

$$F_1^{\mathrm{COR}} = \frac{V^{\mathrm{COR}}(\hat{q})}{N} + \frac{V^{\mathrm{COR}}(\hat{p})}{N}. \quad (2.64)$$

We optimize the fidelity F_1^{COR} with respect to the parameters ΔQ_1 and ΔP_2. The optimal value of the fidelity F_1^{COR} evaluates to

$$F_{1\,\mathrm{OPT}}^{\mathrm{COR}} = \begin{cases} \frac{1+(\Delta q)^2+(\Delta p)^2}{N} & |\kappa| \leq 1, \\ \frac{|\kappa|+(\Delta q)^2+(\Delta p)^2}{N} & |\kappa| > 1. \end{cases} \quad (2.65)$$

We note that the optimal fidelity $F_{1\,\mathrm{OPT}}^{\mathrm{COR}}$ for $|\kappa| \leq 1$ equals the fidelity for the heterodyne measurement F_1^{Het} (2.45).

The plot of the fidelity as a function of the coupling strength κ for a coherent state ensemble is shown in Fig. 2.9(a). The results show that the estimation of the coherent state ensemble using the modified Arthurs-Kelly scheme is best in the range $|\kappa| \leq 1$,

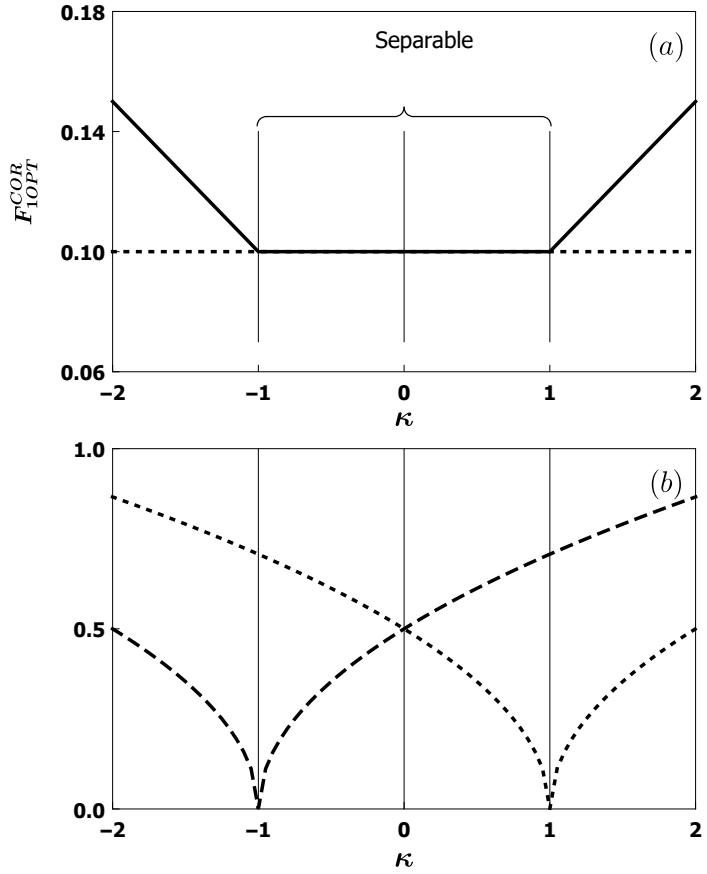


Figure 2.9: (a) Optimal fidelity $F_{1\,\mathrm{OPT}}^{\mathrm{COR}}$ for the modified Arthurs-Kelly scheme, represented by the solid curve, as a function of the coupling strength κ. The dashed curve represents the fidelity for the heterodyne measurement F_1^{Het}. (b) The plot of ΔQ_1 (dashed) and ΔP_2 (dotted) for the optimal performance of the modified Arthurs-Kelly scheme as a function of the coupling strength κ. We have considered an ensemble of coherent states for both the plots.

which corresponds to uncorrelated probes. The corresponding value of ΔQ_1 and ΔP_2, which optimizes the fidelity F_1^{COR} turns out to be

$$\Delta Q_1 = \begin{cases} \frac{\sqrt{1+\kappa}}{2} & \kappa > 1, \\ \frac{\sqrt{1+\kappa}}{2} & |\kappa| < 1, \\ \frac{\sqrt{-1-\kappa}}{2} & \kappa < -1, \end{cases} , \quad \Delta P_2 = \begin{cases} \frac{\sqrt{-1+\kappa}}{2} & \kappa > 1, \\ \frac{\sqrt{1-\kappa}}{2} & |\kappa| < 1, \\ \frac{\sqrt{1-\kappa}}{2} & \kappa < -1. \end{cases} \tag{2.66}$$

We have also plotted ΔQ_1 and ΔP_2 as a function of the coupling strength κ corresponding to the optimal performance of the modified Arthurs-Kelly scheme in Fig. 2.9(b). For the coupling strength $\kappa = 0$, the modified Arthurs-Kelly scheme reduces to the

original Arthurs-Kelly scheme. This can also be verified from from Fig. 2.9(b), where at $\kappa = 0$, $\Delta Q_1 = \Delta P_1 = 1/2$, which is the same as Eq. (2.49).

2.5 Discussion and Conclusion

In this chapter, we have explored the estimation of the mean and the variance of an ensemble with a fixed number of identically prepared Gaussian states by employing various measurement schemes with view to compare their efficiencies. To carry out the calculation, we employed the phase space formalism. Since we were dealing with Gaussian states and quadratic Hamiltonians, the covariance matrix and symplectic group techniques provided an elegant and intuitive way to handle the analysis. We have provided analytical expressions of the fidelity of the mean and the variance estimation. The study of the fidelity expressions revealed that the optimal performance of the Arthurs-Kelly scheme requires non-classical resources in the sense that the meters should be initially prepared in a squeezed state; however, the optimal performance of the sequential measurement only requires classical resources, *i.e.*, the meter should be initially prepared in a coherent state. Further, we showed that the optimal performance of the Arthurs-Kelly scheme and the sequential measurement equal heterodyne measurement for both the mean and the variance estimation. For mean estimation, the analysis revealed that the performance of the homodyne measurement and the heterodyne measurement is the same for a coherent state ensemble, whereas, for a squeezed state ensemble, the heterodyne measurement performs better than the homodyne measurement. For variance estimation, the homodyne measurement outperforms the heterodyne measurement for a squeezed coherent thermal state ensemble up to a certain squeezing parameter range. Finally, we analyzed the relative performance of various measurement schemes for an ensemble of Gaussian states with varying squeezing parameters. The results show that the heterodyne measurement always perform better than the homodyne measurement for both the mean and the variance estimation. Further, the optimal performance of the sequential measurement and the Arthurs-Kelly scheme is equal to the heterodyne measurement for both the mean and the variance estimation. We then proceeded to a modified Hamiltonian in the Arthurs-Kelly scheme that can correlate the two meters. The results show that the optimal performance of the scheme can only be obtained when the meters are uncorrelated.

We expect that these results will find applications in various quantum information and quantum communication protocols. One natural extension that we are pursuing is to extend the analysis for Gaussian states squeezed in arbitrary directions. It would be interesting to generalize the theory for non-Gaussian states, where we are required to estimate higher order moments.

Chapter 3

Optimal characterization of Gaussian channels using photon-number-resolving detectors

3.1 Introduction

In this chapter, we report a quantum state tomography (QST) scheme for Gaussian states and quantum process tomography (QPT) scheme for Gaussian channels based on photon number measurements. To measure the quadrature operators, homodyne and heterodyne measurements are employed in general, which was the focus of Chapter 2. However, the prospect of QST via photon number measurements has opened up with the recent development of experimental techniques in photon-number-resolving-detectors (PNRDs) [34, 35]. In this direction, Cerf *et al*. proposed a scheme to estimate the trace and determinant of the covariance matrix of a Gaussian state using beam splitters and on-off detectors [121, 122]. In a similar effort, Parthasarathy *et al*. devised a theoretical scheme to determine a Gaussian state by estimating its mean and covariance matrix using passive and active optical elements and PNRDs [123].

Another ongoing quest in quantum information processing is the characterization of quantum processes, which is formally called quantum process tomography (QPT). For CV systems, several theoretical as well as experimental research works have already been carried out [66, 67, 68, 69, 124, 125, 126, 127, 128, 129]. Originally, Lobino *et al*. characterized quantum processes using coherent state probes and homodyne measurements [66]. In another scheme, Ghalaii *et al*. devised a coherent state probe based QPT scheme, where they have measured normally-ordered moments using homodyne detection [69]. In a similar direction, Parthasarathy *et al*. have character-

ized Gaussian channel using QST schemes based on photon number measurements for Gaussian states [123].

In this chapter, we present a variant of the scheme given by Parthasarathy *et al*. [123] for QST of Gaussian states based on PNRDs, which utilizes less number of optical elements. An n-mode Gaussian state is fully determined by its $2n$ first moments and second-order moments arranged in the form of a covariance matrix, which has $2n^2+n$ parameters. Therefore, we require a total of $2n^2+3n$ parameters to completely specify an n-mode Gaussian state. To determine all the $2n^2+3n$ parameters of the state, we require exactly $2n^2+3n$ distinct measurements, and thus our scheme based on photon number measurements is optimal. We next turn to the characterization of Gaussian channels, where we employ our QST scheme to estimate the output states corresponding to coherent state probes. A Gaussian channel between two n-mode systems is described by a pair of $2n \times 2n$ real matrices A and B with $B = B^T \geq 0$, which satisfy certain complete positivity and trace-preserving conditions [130, 131, 132]. Matrix A is specified by $4n^2$ parameters, while matrix B is specified by $2n^2+n$ parameters, and thus an n-mode Gaussian channel is completely described by $6n^2+n$ parameters. We show that we can characterize a Gaussian quantum channel optimally, *i.e*., we require exactly $6n^2+n$ distinct measurements to determine all the $6n^2+n$ parameters of the Gaussian channel. To get an insight into the efficiency of the scheme, we compare the variances of different transformed number operators arising in our QST scheme. Finally, we express the variance of the quadrature operators in terms of variances of transformed number operators. In CV quantum key distribution (QKD) protocols, we need to send an intense local oscillator pulse along with the signal pulse for reference purpose, which is in itself a difficult task and can also lead to security loopholes [133, 134]. The PNRDs based measurement scheme proposed in this chapter does not require an intense local oscillator pulse, and thus may be quite effective in CV-QKD protocols.

The chapter is structured as follows. In Sec. 3.2, we describe our optimal QST scheme based on PNRDs for Gaussian states. In Sec. 3.3, we present the scheme for the optimal characterization of Gaussian channels. In Sec. 3.4, we compare the variances of different transformed number operators arising in the state tomography scheme. Finally, in Sec. 4.4, we provide conclusions based on our results.

3.2 Estimation of Gaussian states using photon number measurements

In this section, we describe a modified version of the original QST scheme reported in [123]. The original QST scheme uses active as well as passive optical elements

and PNRDs to estimate the mean and covariance matrix of a Gaussian state. Our QST scheme uses less number of optical elements and thus provides an economical implementation of the scheme. In the scheme, photon number measurement is performed on the original and transformed Gaussian states. The involved transformations or gates are displacement, phase rotation, single mode squeezing, and beam splitter operation denoted by $\hat{D}_i(q,p)$, $\mathcal{U}(R_i(\theta))$, $\mathcal{U}(S_i(r))$, and $\mathcal{U}(B_{ij}(\theta))$, respectively. However, before proceeding further with the QST scheme, we define our system and evaluate averages of transformed number operators that shall be required later.

3.2.1 Mean of transformed number operators

For this work, we consider an n-mode Gaussian state described by n pairs of Hermitian quadrature operators $\hat{q}_i, \hat{p}_i$ ($i = 1, \ldots, n$). Our system can also be described by field annihilation and creation operators $\hat{a}_i$ and $\hat{a}_i^\dagger$ ($i = 1, 2, \ldots, n$), which are related to the quadrature operators according to Eq. (1.26). The number operator for the i^{th} mode and total number operator for the n-mode system can be written as

$$\hat{N}_i = \hat{a}_i^\dagger \hat{a}_i = \frac{1}{2}\left(\hat{q}_i^{\,2} + \hat{p}_i^{\,2} - 1\right), \tag{3.1a}$$

$$\hat{N} = \sum_{i=1}^{n} \hat{N}_i. \tag{3.1b}$$

For calculation simplicity, we work in the phase space formalism using the Wigner function description. Our n-mode system can be represented by $2n$ phase space variables $\boldsymbol{\xi} = (q_1, p_1, \ldots, q_n, p_n)^T$. The Wigner distribution for a Gaussian state can be written as [15]

$$W(\boldsymbol{\xi}) = \frac{\exp[-(1/2)(\boldsymbol{\xi} - \boldsymbol{d})^T V^{-1} (\boldsymbol{\xi} - \boldsymbol{d})]}{(2\pi)^n \sqrt{\det V}}, \tag{3.2}$$

where $\boldsymbol{d}$ is the displacement, and V is the covariance matrix of the Gaussian state in phase space. We now evaluate averages of transformed number operators that are required later, in phase space formalism. Since the total number operator

$$\hat{N} = \sum_{j=1}^{n} \hat{N}_i = \frac{1}{2} \sum_{j=1}^{n} \left(\hat{q}_i^{\,2} + \hat{p}_i^{\,2} - 1\right) \tag{3.3}$$

is symmetrically ordered in $\hat{q}$ and $\hat{p}$ operators, the average number of photons $\langle \hat{N} \rangle$ for the n-mode Gaussian state can be evaluated as follows in the phase space formalism

using the Wigner distribution [123, 135]:

$$\langle \hat{N} \rangle \;=\; \frac{1}{2}\sum_{j=1}^{n}\int d^{2n}\boldsymbol{\xi}\left(q_i^2+p_i^2-1\right)W(\boldsymbol{\xi}) = \frac{1}{2}\left[\text{Tr}\left(V-\frac{1}{2}\mathbb{1}_{2n}\right)+||\boldsymbol{d}||^2\right]. \tag{3.4}$$

In the Schrödinger picture, quantum states transform as $\rho \rightarrow \mathcal{U}\rho\,\mathcal{U}^\dagger$ under a unitary transformation $\mathcal{U}$, while in the Heisenberg picture, the number operator transforms as $\hat{N} \rightarrow \mathcal{U}^\dagger \hat{N}\,\mathcal{U}$. Since the displacement operator, $D(\boldsymbol{r})$, transforms the mean of the Gaussian state as $\boldsymbol{d} \rightarrow \boldsymbol{d}+\boldsymbol{r}$, the average number of photon for a state transformed via a displacement operator $D(\boldsymbol{r})$ can be written as

$$\langle \hat{D}(\boldsymbol{r})^\dagger \hat{N} \hat{D}(\boldsymbol{r})\rangle = \frac{1}{2}\left[\text{Tr}\left(V-\frac{1}{2}\mathbb{1}_{2n}\right)+||\boldsymbol{d}+\boldsymbol{r}||^2\right]. \tag{3.5}$$

Therefore,

$$\langle \hat{D}(\boldsymbol{r})^\dagger \hat{N} \hat{D}(\boldsymbol{r})\rangle - \langle \hat{N}\rangle = \frac{1}{2}\left(||\boldsymbol{d}+\boldsymbol{r}||^2-||\boldsymbol{d}||^2\right). \tag{3.6}$$

Further, using Eqs. (3.4) and (1.106), the average of the number operator after a metaplectic transformation $\hat{\mathcal{U}}(S)$ of the state can be readily evaluated as

$$\langle \hat{\mathcal{U}}(S)^\dagger \hat{N} \hat{\mathcal{U}}(S)\rangle = \frac{1}{2}\text{Tr}\left(VS^TS-\frac{1}{2}\mathbb{1}_{2n}\right)+\frac{1}{2}\boldsymbol{d}^TS^TS\boldsymbol{d}. \tag{3.7}$$

Therefore,

$$\langle \hat{\mathcal{U}}(S)^\dagger \hat{N} \hat{\mathcal{U}}(S)\rangle - \langle \hat{N}\rangle = \frac{1}{2}\text{Tr}\left[V(S^TS-\mathbb{1}_{2n})\right]+\frac{1}{2}\boldsymbol{d}^T(S^TS-\mathbb{1}_{2n})\boldsymbol{d}. \tag{3.8}$$

The above derived expressions will be helpful in relating the Gaussian state parameters to photon number measurements, as we shall see later. We now resume the discussion of our QST scheme.

3.2.2 Mean estimation

To estimate the mean of an n-mode Gaussian state, we first obtain $\langle \hat{N}\rangle$ by measuring the photon number of the original state. We then measure the photon number of the state that has been displaced by a unit amount along one of the $2n$ phase space variables. In Fig. 3.1, we show displacement gate $\hat{D}_i(1,0)$ acting on the i^{th} mode, which displaces the original state by a unit amount along $\hat{q}_i$ quadrature. We consider two distinct photon number measurements, when the original state has been transformed by

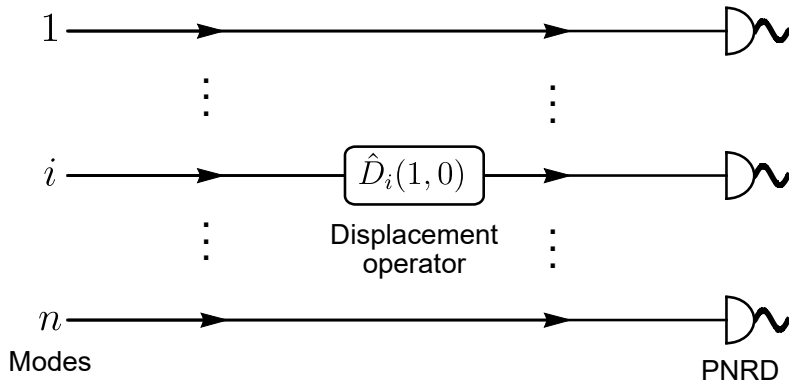


Figure 3.1: Scheme for the estimation of the mean of an n-mode Gaussian state. For estimating the mean of $\hat{q}_i$-quadrature, we displace the $\hat{q}_i$-quadrature by a unit amount by applying a displacement gate $\hat{D}_i(1,0)$ before measuring the photon number of each of the modes.

displacement operator $\hat{D}_i(1,0)$ and $\hat{D}_i(0,1)$, providing us $\langle \hat{D}_i(1,0)^\dagger \hat{N} \hat{D}_i(1,0)\rangle$ and $\langle \hat{D}_i(0,1)^\dagger \hat{N} \hat{D}_i(0,1)\rangle$. We, therefore, obtain by using Eq. (3.6):

$$\begin{aligned} \langle \hat{D}_i(1,0)^\dagger \hat{N} \hat{D}_i(1,0)\rangle - \langle \hat{N}\rangle &= \frac{1}{2}\left(1+2d_{q_i}\right), \\ \langle \hat{D}_i(0,1)^\dagger \hat{N} \hat{D}_i(0,1)\rangle - \langle \hat{N}\rangle &= \frac{1}{2}\left(1+2d_{p_i}\right), \end{aligned} \tag{3.9}$$

which can be rewritten as

$$\begin{aligned} d_{q_i} &= \langle \hat{D}_i(1,0)^\dagger \hat{N} \hat{D}_i(1,0)\rangle - \langle \hat{N}\rangle - \frac{1}{2}, \\ d_{p_i} &= \langle \hat{D}_i(0,1)^\dagger \hat{N} \hat{D}_i(0,1)\rangle - \langle \hat{N}\rangle - \frac{1}{2}. \end{aligned} \tag{3.10}$$

Thus, once the values of $\langle \hat{D}_i(1,0)^\dagger \hat{N} \hat{D}_i(1,0)\rangle$, $\langle \hat{D}_i(0,1)^\dagger \hat{N} \hat{D}_i(0,1)\rangle$, and $\langle \hat{N}\rangle$ have been obtained, we can estimate the mean values of $\hat{q}_i$ and $\hat{p}_i$-quadratures. Therefore, we need to make $2n$ photon number measurements after displacing the state by a unit amount along $2n$ different phase space variables along with photon number measurement on the original state in order to obtain all the $2n$ elements of the mean $\boldsymbol{d}$ of the Gaussian state. To measure these averages, we need to repeat the measurements many times. Further, we can estimate $\mathrm{Tr}(V)$ once the mean $\boldsymbol{d}$ of the Gaussian state has been estimated.

$$\mathrm{Tr}(V) = 2\langle \hat{N}\rangle - ||\boldsymbol{d}||^2 + n. \tag{3.11}$$

Thus, a total of $2n+1$ photon number measurements is required to estimate $2n$ elements of the mean $\boldsymbol{d}$ and the trace of the covariance matrix $\mathrm{Tr}(V)$ of the Gaussian state.

3.2.3 Estimation of intra-mode covariance matrix

We take the covariance matrix of the n-mode Gaussian state of the following form for the convenience of calculations:

$$V = \begin{pmatrix} V_{1,1} & V_{1,2} & \cdots & V_{1,n} \\ V_{2,1} & \ddots & \ddots & \vdots \\ \vdots & \ddots & \ddots & V_{n-1,n} \\ V_{n,1} & \cdots & V_{n,n-1} & V_{n,n} \end{pmatrix}, \tag{3.12}$$

where $V_{i,j}$ is a 2×2 matrix. Also, we take the mean and intra-mode covariance matrix for mode i (or covariance matrix of the marginal state of mode i) as follows:

$$d_i = \begin{pmatrix} d_{q_i} \\ d_{p_i} \end{pmatrix}, \quad V_{i,i} = \begin{pmatrix} \sigma_{qq} & \sigma_{qp} \\ \sigma_{qp} & \sigma_{pp} \end{pmatrix}. \tag{3.13}$$

To estimate the intra-mode covariance matrix, we apply a single-mode symplectic gate $P_i(r, \phi)$ comprising of a squeezer followed by a phase shifter acting on the i^{th} mode of the Gaussian state before measuring photon number on each of the modes. The gate $P_i(r, \phi)$ is mathematically represented as

$$P_i(r, \phi) = S_i(r) R_i(\phi) = \begin{pmatrix} e^{-r} & 0 \\ 0 & e^{r} \end{pmatrix} \begin{pmatrix} \cos\phi & \sin\phi \\ -\sin\phi & \cos\phi \end{pmatrix}. \tag{3.14}$$

Figure 3.2 illustrates the measurement scheme for the estimation of the intra-mode covariance matrix of the i^{th} mode of the Gaussian state.

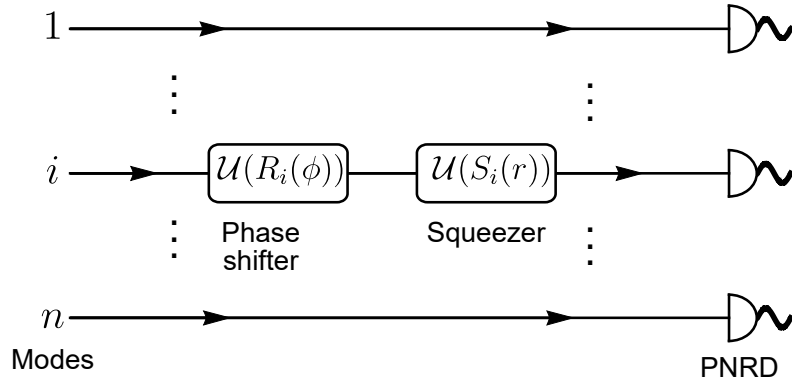


Figure 3.2: Scheme for the estimation of the intra-mode covariance matrix of an n-mode Gaussian state. For estimating the intra-mode covariance matrix of the i^{th} mode, we apply a phase shifter $\mathcal{U}(R_i(\phi)))$ followed by a squeezer $\mathcal{U}(S_i(r))$ on the i^{th} mode of the state before measuring the photon number of each of the modes.

Equation (3.8) reduces to the following under the action of single-mode symplectic gate $P_i(r,\phi)$:

$$\langle\hat{\mathcal{U}}(P_i)^\dagger\hat{N}\hat{\mathcal{U}}(P_i)\rangle - \langle\hat{N}\rangle = \frac{1}{2}\text{Tr}\left[V_{i,i}(P_i^TP_i - \mathbb{1}_2)\right] + \frac{1}{2}d_i^T(P_i^TP_i - \mathbb{1}_2)d_i, \tag{3.15}$$

where

$$P_i^TP_i = \begin{pmatrix} e^{-2r}\cos^2\phi + e^{2r}\sin^2\phi & -\sinh 2r\sin 2\phi \\ -\sinh 2r\sin 2\phi & e^{-2r}\sin^2\phi + e^{2r}\cos^2\phi \end{pmatrix}. \tag{3.16}$$

For compactness, we define

$$P_i^TP_i - \mathbb{1}_2 = \begin{pmatrix} k_1 & k_3 \\ k_3 & k_2 \end{pmatrix}, \tag{3.17}$$

and thus Eq. (3.15) becomes

$$\begin{aligned}\langle\hat{\mathcal{U}}(P_i)^\dagger\hat{N}\hat{\mathcal{U}}(P_i)\rangle - \langle\hat{N}\rangle = \frac{1}{2}\Big[&k_1\sigma_{qq} + k_2\sigma_{pp} + 2k_3\sigma_{qp} \\ &+ k_1{d_{q_i}}^2 + k_2{d_{p_i}}^2 + 2k_3d_{q_i}d_{p_i}\Big].\end{aligned} \tag{3.18}$$

We get the following on the rearrangement of the above equation:

$$\begin{aligned}k_1\sigma_{qq} + k_2\sigma_{pp} + 2k_3\sigma_{qp} = 2\left(\langle\hat{\mathcal{U}}(P_i)^\dagger\hat{N}\hat{\mathcal{U}}(P_i)\rangle - \langle\hat{N}\rangle\right) \\ - (k_1{d_{q_i}}^2 + k_2{d_{p_i}}^2 + 2k_3d_{q_i}d_{p_i}).\end{aligned} \tag{3.19}$$

The above equation has three unknown parameters σ_{qq}, σ_{pp}, and σ_{qp} since d_{q_i} and d_{p_i} have already been estimated in Sec. 3.2.2 (Eq. (3.10)). In order to estimate these three unknown parameters, we choose three proper combinations of squeezing parameter r and phase rotation angle ϕ such that the corresponding photon number measurements on the P_i transformed Gaussian state yield the unknown parameters. We present one such triplet of combinations below.

(i) For $e^r = \sqrt{2}$ and $\phi = 0$, we get

$$-\frac{1}{2}\left(\sigma_{qq} - 2\sigma_{pp}\right) = c_1. \tag{3.20}$$

(ii) For $e^r = \sqrt{3}$ and $\phi = 0$, we get

$$-\frac{2}{3}\left(\sigma_{qq} - 3\sigma_{pp}\right) = c_2. \tag{3.21}$$

(iii) For $e^r = \sqrt{2}$ and $\phi = \pi/4$, we get

$$\frac{1}{4}\left(\sigma_{qq} + \sigma_{pp} - 6\sigma_{qp}\right) = c_3. \tag{3.22}$$

Here c_1, c_2, and c_3 represent the right-hand side (RHS) of Eq. (3.19), which can be easily determined once the photon number distribution has been measured on the transformed Gaussian states. Matrix elements σ_{qq} and σ_{pp} can be obtained by solving Eqs. (3.20) and (3.21), which can be substituted in Eq. (3.22) to yield σ_{qp}. Thus, the estimation of $V_{i,i}$ requires three distinct photon number measurements on the transformed Gaussian states. Therefore, for the estimation of all $V_{i,i}$ $(1 \leq i \leq n-1)$, we require $3(n-1)$ measurements. However, for the estimation of $V_{n,n}$, we need to estimate σ_{qp} and one of σ_{qq} or σ_{pp}, as $\mathrm{Tr}(V)$ has already been estimated. Thus, the estimation of all the parameters of the intra-mode covariance matrix $V_{i,i}$ $(1 \leq i \leq n)$ of a Gaussian state require a total of $3(n-1)+2 = 3n-1$ distinct photon number measurements.

3.2.4 Estimation of inter-mode correlations matrix

To estimate the inter-mode correlations matrix, we apply two-mode symplectic operations on the Gaussian state before measuring the photon number of each of the modes. The covariance matrix of the reduced state of the i and j modes can be written as follows using the notation of Eq. (3.12):

$$\begin{pmatrix} V_{i,i} & V_{i,j} \\ V_{i,j}^T & V_{j,j} \end{pmatrix}. \tag{3.23}$$

We note that $i < j$ need not be successive modes. Here we need to estimate only $V_{i,j}$, the inter-mode correlations matrix corresponding to the modes i and j, since $V_{i,i}$ and $V_{j,j}$ has already been estimated in Sec. 3.2.3. We assume the elements of matrix $V_{i,j}$ as

$$V_{i,j} = \begin{pmatrix} \gamma_{qq} & \gamma_{qp} \\ \gamma_{pq} & \gamma_{pp} \end{pmatrix}. \tag{3.24}$$

The two-mode symplectic gate consists of the following three optical elements in the order given: a phase shifter acting on the i^{th} mode, a balanced beam splitter acting on modes i and j, and a squeezer acting on mode i. The symplectic transformation matrix for the aforementioned gate is given by

$$\begin{aligned} Q_{ij}(r,\phi) &= (S_i(r) \oplus \mathbb{1}_2) B_{ij}\left(\frac{\pi}{4}\right)(R_i(\phi) \oplus \mathbb{1}_2), \\ &= \begin{pmatrix} S_i(r) & 0 \\ 0 & \mathbb{1}_2 \end{pmatrix} \frac{1}{\sqrt{2}} \begin{pmatrix} \mathbb{1}_2 & \mathbb{1}_2 \\ -\mathbb{1}_2 & \mathbb{1}_2 \end{pmatrix} \begin{pmatrix} R_i(\phi) & 0 \\ 0 & \mathbb{1}_2 \end{pmatrix}. \end{aligned} \tag{3.25}$$

The schematic representation of the measurement scheme for the estimation of the inter-mode correlations matrix $V_{i,j}$ is illustrated in Fig. 3.3.

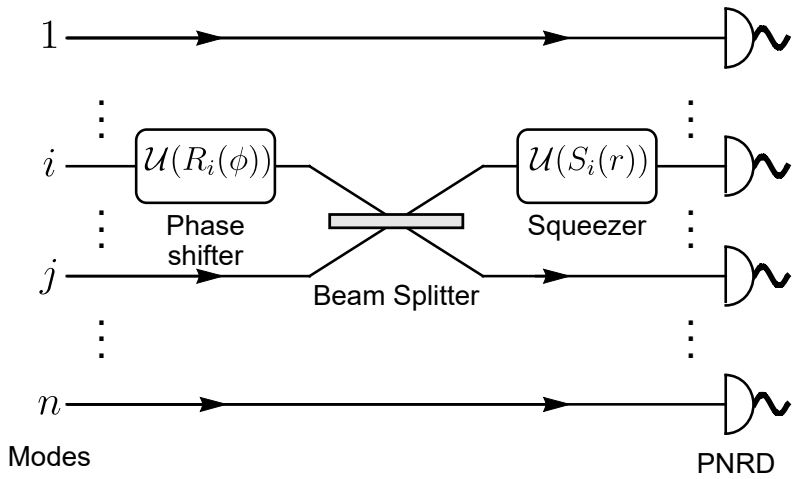


Figure 3.3: Scheme for estimation of inter-mode correlations matrix of an n-mode Gaussian state. For estimating the inter-mode correlations matrix of the modes i and j, we first apply a phase shifter $\mathcal{U}(R_i(\phi)))$ on the i^{th} mode followed by a balanced beam splitter $\mathcal{U}(B_{ij}(\frac{\pi}{4})))$ on i and j modes of the state. Finally, we apply a squeezer $\mathcal{U}(S_i(r))$ on the i^{th} mode of the state before measuring the photon number of each of the modes.

Equation (3.8) reduces to the following under the action of the gate $Q_{ij}(r,\phi)$ on the modes i and j of the Gaussian state:

$$\begin{aligned}\langle\hat{\mathcal{U}}(Q_{ij})^\dagger\hat{N}\hat{\mathcal{U}}(Q_{ij})\rangle - \langle\hat{N}\rangle = \frac{1}{2}\text{Tr}\left[\begin{pmatrix} V_{i,i} & V_{i,j} \\ V_{i,j}^T & V_{j,j}\end{pmatrix}\begin{pmatrix} K-\mathbb{1}_2 & M \\ M^T & L-\mathbb{1}_2\end{pmatrix}\right] \\ + \frac{1}{2}\begin{pmatrix} d_{q_i} \\ d_{p_i} \\ d_{q_j} \\ d_{p_j}\end{pmatrix}^T\begin{pmatrix} K-\mathbb{1}_2 & M \\ M^T & L-\mathbb{1}_2\end{pmatrix}\begin{pmatrix} d_{q_i} \\ d_{p_i} \\ d_{q_j} \\ d_{p_j}\end{pmatrix},\end{aligned} \tag{3.26}$$

where we have used

$$Q_{ij}^T Q_{ij} = \begin{pmatrix} K & M \\ M^T & L\end{pmatrix}. \tag{3.27}$$

Using the following simplified form of trace

$$\begin{aligned}&\text{Tr}\left[\begin{pmatrix} V_{i,i} & V_{i,j} \\ V_{i,j}^T & V_{j,j}\end{pmatrix}\begin{pmatrix} K-\mathbb{1}_2 & M \\ M^T & L-\mathbb{1}_2\end{pmatrix}\right] \\ &= \text{Tr}\left[V_{i,i}(K-\mathbb{1}_2) + V_{j,j}(L-\mathbb{1}_2)\right] + 2\text{Tr}\left[V_{i,j}M^T\right],\end{aligned} \tag{3.28}$$

and a rearrangement of Eq. (3.26) leads to the equation

$$\begin{aligned}\mathrm{Tr}\left[V_{i,j}M^T\right] = \langle\hat{\mathcal{U}}(Q_{ij})^\dagger\hat{N}\hat{\mathcal{U}}(Q_{ij})\rangle - \langle\hat{N}\rangle - \frac{1}{2}\mathrm{Tr}\left[V_{i,i}(K-\mathbb{1}_2) + V_{j,j}(L-\mathbb{1}_2)\right] \\ - \frac{1}{2}\begin{pmatrix} d_{q_i} \\ d_{p_i} \\ d_{q_j} \\ d_{p_j}\end{pmatrix}^T \begin{pmatrix} K-\mathbb{1}_2 & M \\ M^T & L-\mathbb{1}_2\end{pmatrix}\begin{pmatrix} d_{q_i} \\ d_{p_i} \\ d_{q_j} \\ d_{p_j}\end{pmatrix}.\end{aligned} \tag{3.29}$$

The left-hand side (LHS) of the above equation can be written as following after taking the trace:

$$\begin{aligned}\mathrm{Tr}\left[V_{i,j}M^T\right] = \frac{1}{2}\Big[\left(e^{-2r}-1\right)\cos\phi\,\gamma_{qq} + \left(e^{2r}-1\right)\cos\phi\,\gamma_{pp} \\ + \left(1-e^{2r}\right)\sin\phi\,\gamma_{qp} + \left(e^{-2r}-1\right)\sin\phi\,\gamma_{pq}\Big].\end{aligned} \tag{3.30}$$

Since various terms, for instance, $V_{i,i}$, $V_{j,j}$, d_{q_i}, d_{p_i}, d_{q_j}, d_{p_j} , have already been estimated, the four unknowns γ_{qq}, γ_{pp}, γ_{qp}, γ_{pq} on the LHS of Eq. (3.29) can be estimated by performing four distinct photon number measurements on the Q_{ij} transformed Gaussian states for proper combinations of squeezing parameter r and phase rotation angle ϕ. We present one such quartet of combinations below to determine the four unknowns.

(i) For $e^r = \sqrt{2}$ and $\phi = 0$, we get

$$-\frac{1}{4}\left(\gamma_{qq} - 2\gamma_{pp}\right) = d_1. \tag{3.31}$$

(ii) For $e^r = \sqrt{3}$ and $\phi = 0$, we get

$$-\frac{1}{3}\left(\gamma_{qq} - 3\gamma_{pp}\right) = d_2. \tag{3.32}$$

(iii) For $e^r = \sqrt{2}$ and $\phi = \pi/2$, we get

$$-\frac{1}{4}\left(2\gamma_{qp} + \gamma_{pq}\right) = d_3. \tag{3.33}$$

(iv) For $e^r = \sqrt{3}$ and $\phi = \pi/2$, we get

$$-\frac{1}{3}\left(3\gamma_{qp} + \gamma_{pq}\right) = d_4. \tag{3.34}$$

Here d_1, d_2, d_3, and d_4 corresponds to the RHS of Eq. (3.29), which can be easily determined once the photon number distribution has been measured on the transformed Gaussian states. Parameters γ_{qq} and γ_{pp} can be obtained by solving Eqs. (3.31) and (3.32), while γ_{qp} and γ_{pq} can be obtained by solving Eqs. (3.33) and (3.34). Since the correlations matrix $V_{i,j}$ estimation requires four distinct measurements, estimation of all the inter-mode correlations matrices of the n-mode Gaussian states thus require $4 \times n(n-1)/2 = 2n(n-1)$ measurements. The total number of measurements add up to $(2n+1) + (3n-1) + 2n(n-1) = 2n^2 + 3n$, and therefore estimation of $2n^2 + 3n$ parameters of the n-mode Gaussian state require $2n^2 + 3n$ measurements. Thus, our tomography scheme for Gaussian states using photon number measurements is optimal in the sense that we require exactly the same number of distinct measurements as the number of independent real parameters of the Gaussian state. Table 3.1 summarizes the above results.

Table 3.1: Tomography of an n-mode Gaussian state by photon number measurements

Estimate type	Parameter number	Gaussian operations	Measurement number
Mean ($\boldsymbol{d}$)	$2n$	Displacement	$2n+1$
Intra-mode covariance ($V_{i,i}$)	$3n$	Phase shifter, squeezer	$3n-1$
Inter-mode correlations ($V_{i,j}$)	$2n(n-1)$	Phase shifter, squeezer, beam splitter	$2n(n-1)$
Total	$\boldsymbol{2n^2+3n}$		$\boldsymbol{2n^2+3n}$

3.3 Characterization of Gaussian channels

In this section, we employ the QST scheme developed in Section 3.2 for the characterization of a Gaussian channel using coherent state probes [66, 67, 124]. Gaussian channels are those channels that transform Gaussian states into Gaussian states [131, 132]. A Gaussian channel between two n-mode systems is described by a pair of $2n \times 2n$ real matrices A and B with $B = B^T \geq 0$ [130]. The matrices A and B are determined by a total of $4n^2 + 2n(2n+1)/2 = 6n^2 + n$ real parameters and satisfy the following complete positivity and trace preserving condition:

$$B + i\Omega - iA\Omega A^T \geq 0. \tag{3.35}$$

A Gaussian state with mean $\boldsymbol{d}$ and covariance matrix V transform as follows under the action of the Gaussian channel:

$$\boldsymbol{d} \to A\boldsymbol{d}, \quad V \to AVA^T + \frac{1}{2}B. \tag{3.36}$$

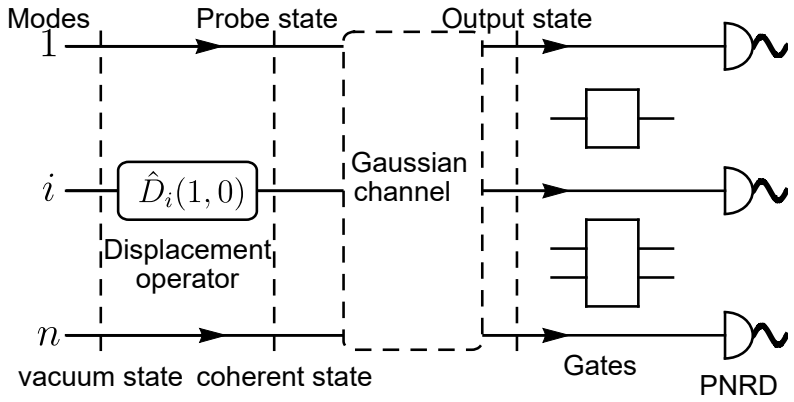


Figure 3.4: Scheme for a complete characterization of an n-mode Gaussian channel. We displace the $\hat{q}_i$ quadrature by applying the displacement operator $\hat{D}_i(1,0)$ on an n-mode vacuum state to obtain one of the coherent state probes. A total of $2n$ distinct coherent state probes, prepared by displacing the n-mode vacuum state along one of the $2n$ different phase space variables, are sent into the channel, and the corresponding output states are fully or partially tomographed using photon number measurements. Gates indicate single and two-mode optical elements involved in state tomography as described in Sec. 3.2.

We again follow the scheme given in [123]. The scheme requires $2n$ distinct coherent state probes, which can be generated by displacing n-mode vacuum state by a unit amount along one of the $2n$ different phase space variables. These coherent state probes are sent through the channel, and the corresponding output states are fully or partially tomographed using photon number measurements. Figure 3.4 shows the schematic diagram. The information thus obtained about the output state parameters allows us to characterize the Gaussian channel. We now proceed to discuss the exact scheme with mathematical details. We define a $2n$ dimensional column vector as follows for convenience:

$$\boldsymbol{e}_j = (0, 0, \ldots, 1, \ldots, 0, 0)^T, \tag{3.37}$$

with 1 present at the j^{th} position. An n-mode vacuum state $|\mathbf{0}\rangle$ has the following mean and covariance matrix:

$$\boldsymbol{d} = \mathbf{0}, \quad V = \frac{1}{2}\mathbb{1}_{2n}. \tag{3.38}$$

We displace the n-mode vacuum state by a unit amount along n different $\hat{q}$-quadratures to generate the first set of n coherent state probes. For example, the displacement operator $\hat{D}_j(1,0)$ acts on the n-mode vacuum state to give one of the coherent state probe displaced by a unit amount along $\hat{q}_j$ quadrature:

$$|\boldsymbol{e}_{2j-1}\rangle = \hat{D}_j(1,0)|\mathbf{0}\rangle. \tag{3.39}$$

The mean and covariance matrix of the coherent state $|\boldsymbol{e}_{2j-1}\rangle$ is given by

$$\boldsymbol{d} = \boldsymbol{e}_{2j-1}, \quad V = \frac{1}{2}\mathbb{1}_{2n}. \tag{3.40}$$

After passing through the Gaussian channel, the mean and covariance matrix of the probe state $|\boldsymbol{e}_{2j-1}\rangle$ transform as per Eq. (3.36):

$$\boldsymbol{d}_G = A\boldsymbol{e}_{2j-1}, \quad V_G = \frac{1}{2}(AA^T + B). \tag{3.41}$$

A full state tomography is performed on the output state ρ_G ($j = 1$) corresponding to the coherent state probe $|\boldsymbol{e}_1\rangle$, which requires $2n^2+3n$ measurements. This gives the matrix $AA^T + B$ and the first column of matrix A. We then measure only the mean of the rest of the output state ρ_G ($2 \leq j \leq n$), which allows us to estimate the remaining odd columns of matrix A.

However, as mentioned in Sec. 3.2.2, we have to make $2n + 1$ measurements to estimate the $2n$ parameters of the mean vector $\boldsymbol{d}_G$. This leads to the overshooting of the number of measurements compared to the number of channel parameters, which renders the scheme non-optimal. Here we notice that since all the output states have the same covariance matrix, $\text{Tr}(V) = \text{Tr}(AA^T + B)/2$ is also the same for all the output states, which has already been obtained during the full state tomography of the first output state ($j = 1$). We now exploit this fact to obtain the value of $\langle\hat{N}\rangle$ for the other output states ($2 \leq j \leq n$), which results in an optimal characterization of the Gaussian channel. We make $2n$ measurements on the displaced output state ρ_G ($j = 2$), which yields $2n$ equations:

$$\begin{aligned} d_{q_i} &= \langle\hat{D}_i(1,0)^\dagger\hat{N}\hat{D}_i(1,0)\rangle - \langle\hat{N}\rangle - \frac{1}{2}, \quad 1 \leq i \leq n, \\ d_{p_i} &= \langle\hat{D}_i(0,1)^\dagger\hat{N}\hat{D}_i(0,1)\rangle - \langle\hat{N}\rangle - \frac{1}{2}, \quad 1 \leq i \leq n. \end{aligned} \tag{3.42}$$

We put d_{q_i} and d_{p_i} ($1 \leq i \leq n$) in Eq. (3.11) and get a quadratic equation in $\langle\hat{N}\rangle$. After solving for $\langle\hat{N}\rangle$, we substitute its value in Eq. (3.42) to obtain d_{q_i} and d_{p_i} ($1 \leq i \leq n$). Thus, for the other output states ρ_G ($2 \leq j \leq n$), we require only $2n$ measurements to estimate the mean vector $\boldsymbol{d}_G$.

We now displace the n-mode vacuum state by a unit amount along n different $\hat{p}$-quadratures to generate the other set of n coherent state probes. For example, displacement operator $\hat{D}_j(0,1)$ acts on the n-mode vacuum state to give one of the coherent state probe displaced by a unit amount along $\hat{p}_j$ quadrature:

$$|\boldsymbol{e}_{2j}\rangle = \hat{D}_j(0,1)|\mathbf{0}\rangle. \tag{3.43}$$

The mean and covariance matrix of the coherent state $|\boldsymbol{e}_{2j}\rangle$ are given by

$$\boldsymbol{d} = \boldsymbol{e}_{2j}, \quad V = \frac{1}{2}\mathbb{1}_{2n}. \tag{3.44}$$

After passing through the Gaussian channel, the mean and covariance matrix of the probe state $|\boldsymbol{e}_{2j}\rangle$ transform as per Eq. (3.36):

$$\boldsymbol{d}_G = A\boldsymbol{e}_{2j}, \quad V_G = \frac{1}{2}(AA^T + B). \tag{3.45}$$

We again measure only the mean for the output states ρ_G ($1 \leq j \leq n$) corresponding to the $\hat{p}$-displaced coherent state probes. This allows us to determine all the even columns of matrix A, which lead to the complete specification of matrix A as we have already determined odd columns of matrix A using the first set of $\hat{q}$-displaced coherent state probes. Further, matrix B is also determined as matrix $AA^T + B$ was already known from the full state tomography on the first coherent state probe. Thus, the total number of measurements add up to $2n^2 + 3n + 2n(2n-1) = 6n^2 + n$, which is exactly equal to the number of parameters specifying a Gaussian channel. Table 3.2 summarizes the result. Thus by exploiting the fact that $\mathrm{Tr}(V)$ is the same for all the output states corresponding to coherent state probes input, we eliminate the need for extra $2n-1$ measurements as reported by Parthasarathy *et al.* [123], which leads to the optimality of our scheme. We note here that the scheme is optimal even when the coherent state probes have different mean since $\mathrm{Tr}(V)$ is the same for all the output states in this case too.

3.4 Variance in photon number measurements

We analyze and compare the variance of the photon number of the original and gate transformed states, which were required for the QST in Sec. 3.2. This analysis will offer us an insight into the quality of our estimates of the Gaussian states and channels.

We again work in phase space formalism to evaluate the variance of the photon number. The square of the number operator can be written in a symmetrically ordered

Table 3.2: Tomography of an n-mode Gaussian channel

Coherent state probe	Information obtained	Measurement number
$\hat{q}$-displaced	Odd columns of A & $(AA^T + B)$	$2n^2 + 3n + (n-1) \times 2n$
$\hat{p}$-displaced	Even columns of A	$n \times 2n$
	Total	$\boldsymbol{6n^2 + n}$

form as follows:

$$\begin{aligned}\hat{N}^2 &= \frac{1}{4}\sum_{i,j=1}^{n}\left(\hat{q_i}^2 + \hat{p_i}^2 - 1\right)\left(\hat{q_j}^2 + \hat{p_j}^2 - 1\right)\\ \{\hat{N}^2\}_{\text{sym}} &= f(\hat{q},\hat{p}) = \frac{1}{4}\sum_{\substack{i,j=1\\ i\neq j}}^{n}\left(\hat{q_i}^2 + \hat{p_i}^2 - 1\right)\left(\hat{q_j}^2 + \hat{p_j}^2 - 1\right)\\ &+\frac{1}{4}\sum_{i=1}^{n}\left[\hat{q_i}^4 + \hat{p_i}^4 - 2\hat{q_i}^2 - 2\hat{p_i}^2 + \frac{1}{3}(\hat{q_i}^2\hat{p_i}^2 + \hat{q_i}\hat{p_i}\hat{q_i}\hat{p_i} + \hat{q_i}\hat{p_i}^2\hat{q_i})\right].\end{aligned} \tag{3.46}$$

Thus, the average of $\hat{N}^2$ can be evaluated in a straightforward manner in phase space formalism using the expression

$$\langle\hat{N}^2\rangle = \int d^{2n}\boldsymbol{\xi}\; f(q,p)W(\boldsymbol{\xi}). \tag{3.47}$$

Using the above equation and Eq. (3.4), the variance of number operator can be expressed in an elegant form as [123, 135, 136]

$$\text{Var}(\hat{N}) = \langle\hat{N}^2\rangle - \langle\hat{N}\rangle^2 = \frac{1}{2}\text{Tr}\left[\left(V - \frac{1}{2}\mathbb{1}_{2n}\right)\left(V + \frac{1}{2}\mathbb{1}_{2n}\right)\right] + \boldsymbol{d}^T V\boldsymbol{d}. \tag{3.48}$$

To get some intuition about the mean and variance of the photon number, we consider a single-mode Gaussian state with mean $\boldsymbol{d} = (u,u)^T$ and covariance matrix

$$V(\beta) = \frac{1}{2}(2\mathcal{N}+1)R(\beta)S(2s)R(\beta)^T, \tag{3.49}$$

where $\mathcal{N}$ is the thermal noise parameter, β is the phase shift angle, and s is the squeezing. The mean and variance of the number operator for the above state are given by

$$\begin{aligned}\langle\hat{N}\rangle &= \mathcal{N}\cosh 2s + \sinh^2 s + u^2,\\ \text{Var}(\hat{N}) &= \left(\mathcal{N}+\frac{1}{2}\right)^2\cosh 4s - \frac{1}{4}\\ &\quad +2u^2\left(\mathcal{N}+\frac{1}{2}\right)(\cosh 2s + \sin 2\beta\sinh 2s)\,. \end{aligned} \tag{3.50}$$

It can be seen from the above equation that the mean photon number depends only on displacement u and squeezing s of the state, whereas the variance of the photon number depends on all three parameters, displacement u, squeezing s, and phase shift angle β of the state. The variance of the displaced number operator is given by

$$\text{Var}\left(\hat{D}(\boldsymbol{r})^\dagger\hat{N}\hat{D}(\boldsymbol{r})\right) = (\boldsymbol{d}+\boldsymbol{r})^T V(\boldsymbol{d}+\boldsymbol{r}) + \frac{1}{2}\text{Tr}\left[\left(V-\frac{1}{2}\mathbb{1}_{2n}\right)\left(V+\frac{1}{2}\mathbb{1}_{2n}\right)\right]. \tag{3.51}$$

We show the plots of $\langle\hat{N}\rangle$ and $\langle D^\dagger(1,0)\hat{N}D(1,0)\rangle$ as a function of displacement parameter u for a single-mode squeezed coherent thermal state (3.49) in Fig. 3.5(a). The plots reveal that while $\langle D^\dagger(1,0)\hat{N}D(1,0)\rangle$ is larger than $\langle\hat{N}\rangle$, the mean value of both the operators increases with the displacement parameter u. Further, Fig. 3.5(b) reveals that mean values $\langle\hat{N}\rangle$ and $\langle D^\dagger(1,0)\hat{N}D(1,0)\rangle$ also increase with squeezing s. Fig. 3.5(c) plots the variance of the operators $\hat{N}$ and $D^\dagger(1,0)\hat{N}D(1,0)$ as a function of displacement parameter u. The plots reveal that while the variance of operator $D^\dagger(1,0)\hat{N}D(1,0)$ is larger than the variance of the operator $\hat{N}$, the variance of both the operators increase with displacement parameter u. Similarly, Fig. 3.5(d) reveals that the variance of the operators $\hat{N}$ and $D^\dagger(1,0)\hat{N}D(1,0)$ increases with squeezing s.

The variance of the photon number after a symplectic transformation S of the state is given by

$$\text{Var}\big(\mathcal{U}(S)^\dagger\hat{N}\mathcal{U}(S)\big)\big) = \boldsymbol{d}^T V\boldsymbol{d} + \frac{1}{2}\text{Tr}\left[\left(SVS^T-\frac{1}{2}\mathbb{1}_{2n}\right)\left(SVS^T+\frac{1}{2}\mathbb{1}_{2n}\right)\right]. \tag{3.52}$$

The variance of the number operator under the action of $P_i(r,\phi)$ gate (Eq. (3.14)) for different values of the parameters r and ϕ (Eqs. (3.20)-(3.22)) has been compared using the above expression. Figure 3.6(a) shows the plots of the variance of different $P_i(r,\phi)$ gate transformed number operators as a function of displacement u for the single-mode squeezed coherent thermal state (3.49). The plots reveal that the variance of different $P_i(r,\phi)$ gate transformed number operators increase with displacement u. While the variance of $\mathcal{U}^\dagger(P)\hat{N}\mathcal{U}(P)$ with $e^r=\sqrt{2}$, $\phi=\pi/4$ is always lower than the variance of $\hat{N}$ and the variance of $\mathcal{U}^\dagger(P)\hat{N}\mathcal{U}(P)$ with $e^r=\sqrt{3}$, $\phi=0$ is always higher

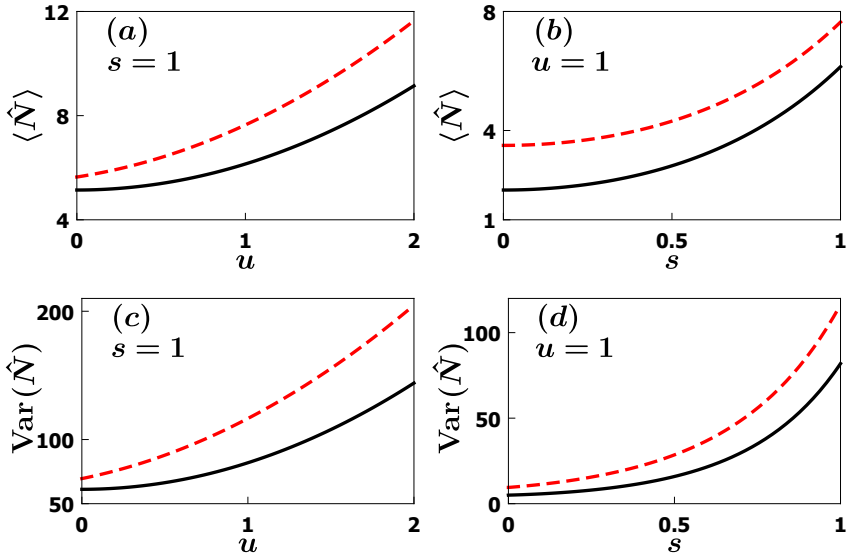


Figure 3.5: For all four panels, single-mode squeezed coherent thermal state (3.49) with parameters $\beta = \pi/3$ and $\mathcal{N} = 1$ has been considered. Mean and variance of $\hat{N}$ have been represented by the solid black line, while mean and variance of $D^{\dagger}(1,0)\hat{N}D(1,0)$ have been represented by the dashed red line. (a) Mean photon number versus displacement u. (b) Mean photon number versus squeezing s. (c) Variance of photon number versus displacement u. (d) Variance of photon number versus squeezing s.

than the variance of $\hat{N}$, the variance of $\mathcal{U}^{\dagger}(P)\hat{N}\mathcal{U}(P)$ with $e^r = \sqrt{2}$, $\phi = 0$ crosses over the variance of $\hat{N}$ at a certain value of displacement u. Figure 3.6(b) shows the plots of the variance of the photon number as a function of squeezing parameter s. The plots reveal that the variance of different $P_i(r,\phi)$ gate transformed number operators shows a similar dependence on squeezing s as that of displacement u.

In order to compare the variance of the photon number under the action of two mode gates $Q_{ij}(r,\phi)$ (Eq. (3.25)), we consider a two mode Gaussian state with mean $\boldsymbol{a} = (u,u,u,u)^T$ and covariance matrix V

$$V = B_{12}\left(\frac{\pi}{4}\right)[V(\beta_1) \oplus V(\beta_2)]B_{12}\left(\frac{\pi}{4}\right)^T, \tag{3.53}$$

where $V(\beta)$ has already been defined in Eq. (3.49). The variance of the $Q_{ij}(r,\phi)$ gate transformed number operator corresponding to the above state can be evaluated using Eq. (3.52). Figure 3.6(c) shows the plots of the variance of the different $Q_{ij}(r,\phi)$ gate transformed number operators as a function of displacement u for two-mode squeezed coherent thermal state (3.53). The plots reveal that the variance of the different $Q_{ij}(r,\phi)$ gate transformed number operators increases with displacement. While

the variance of $\mathcal{U}^{\dagger}(Q)\hat{N}\mathcal{U}(Q)$ with $e^r = \sqrt{2}$, $\phi = 0$, and $e^r = \sqrt{3}$, $\phi = 0$ always remain higher than the variance of $\hat{N}$, the variance of $\mathcal{U}^{\dagger}(Q)\hat{N}\mathcal{U}(Q)$ with $e^r = \sqrt{2}$, $\phi = \pi/2$ and $e^r = \sqrt{3}$, $\phi = \pi/2$ crosses over the variance of $\hat{N}$ at a certain value of the displacement parameter u. Figure 3.6(d) shows the plots of the variance of different $Q_{ij}(r, \phi)$ gate transformed number operators as a function of squeezing s. The plots reveal that the squeezing dependence of different variances exhibits a similar trend as that of dependence on displacement.

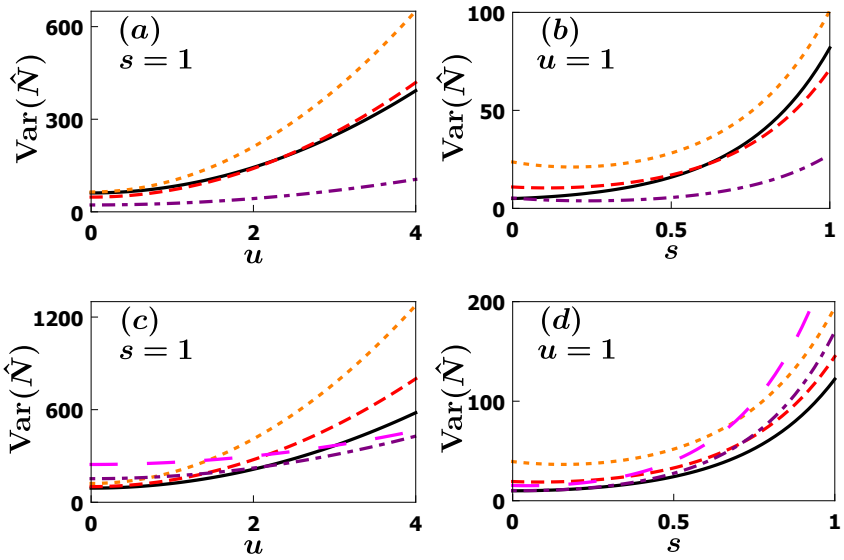


Figure 3.6: (a) Variance of photon number versus displacement u for single-mode squeezed thermal state (3.49). (b) Variance of photon number versus squeezing s for single-mode squeezed thermal state (3.49). For both panel (a) and (b), different lines represent Var$(\mathcal{U}^{\dagger}(P)\hat{N}\mathcal{U}(P))$ with $e^r = \sqrt{2}$, $\phi = 0$ (red dashed), $e^r = \sqrt{3}$, $\phi = 0$ (orange dotted), $e^r = \sqrt{2}$, $\phi = \pi/4$ (purple dot dashed), while the solid black line represents Var$(\hat{N})$, and parameter $\beta = \pi/3$. (c) Variance of photon number versus displacement u for two-mode squeezed coherent thermal state (3.53). (d) Variance of photon number versus squeezing s for two-mode squeezed coherent thermal state (3.53). For both panel (c) and (d), different lines represent Var$(\mathcal{U}^{\dagger}(Q)\hat{N}\mathcal{U}(Q))$ with $e^r = \sqrt{2}$, $\phi = 0$ (red dashed), $e^r = \sqrt{3}$, $\phi = 0$ (orange dotted), $e^r = \sqrt{2}$, $\phi = \pi/2$ (purple dot dashed), $e^r = \sqrt{3}$, $\phi = \pi/2$ (magenta large dashed), while the solid black line represents Var$(\hat{N})$. Thermal parameter has been set as $\mathcal{N} = 1$ for all four panels.

To see the quality of estimation, we express the variance of estimated Gaussian parameters in terms of the variances of transformed number operators. For an n-mode

system, quadrature operators $\hat{q}_i$ and $\hat{p}_i$ can be expressed as

$$\begin{aligned} \hat{q}_i &= \hat{D}_i(1,0)^\dagger \hat{N} \hat{D}_i(1,0) - \hat{N} - \frac{1}{2}, \\ \hat{p}_i &= \hat{D}_i(0,1)^\dagger \hat{N} \hat{D}_i(0,1) - \hat{N} - \frac{1}{2}. \end{aligned} \tag{3.54}$$

We note that taking the average of the above equation yields Eq. (3.10). Since $\hat{N}$ and $\hat{D}_i(1,0)^\dagger \hat{N} \hat{D}_i(1,0)$ are measured on different states, these operators are uncorrelated and the expressions for the variance of the quadratures can be written as

$$\begin{aligned} \text{Var}(\hat{q}_i) &= \text{Var}(\hat{D}_i(1,0)^\dagger \hat{N} \hat{D}_i(1,0)) + \text{Var}(\hat{N}), \\ \text{Var}(\hat{p}_i) &= \text{Var}(\hat{D}_i(0,1)^\dagger \hat{N} \hat{D}_i(0,1)) + \text{Var}(\hat{N}). \end{aligned} \tag{3.55}$$

Here $\text{Var}(\hat{q}_i)$ and $\text{Var}(\hat{p}_i)$ represent the quality of estimation of quadrature $\hat{q}_i$ and $\hat{p}_i$, respectively. As can be seen from the above analysis that both $\text{Var}(\hat{q}_i)$ and $\text{Var}(\hat{p}_i)$ depend on displacement u and squeezing s. An optimization of displacement gate $D_i(q_i, p_i)$ parameters q_i and p_i is required in order to minimize $\text{Var}(\hat{q}_i)$ and $\text{Var}(\hat{q}_i)$. Such optimization is needed for the best estimation of Gaussian state parameters. Similarly, we can write $\hat{q}_i^2$ as

$$\hat{q}_i^2 = 6\Bigg[\underbrace{\hat{\mathcal{U}}(P_i)^\dagger \hat{N} \hat{\mathcal{U}}(P_i)}_{e^r=\sqrt{3},\phi=0} - 2\underbrace{\hat{\mathcal{U}}(P_i)^\dagger \hat{N} \hat{\mathcal{U}}(P_i)}_{e^r=\sqrt{2},\phi=0} - \hat{N}\Bigg]. \tag{3.56}$$

Thus the variance of $\hat{q}_i^2$ becomes

$$\text{Var}(\hat{q}_i^2) = 6\Bigg[\underbrace{\text{Var}(\hat{\mathcal{U}}(P_i)^\dagger \hat{N} \hat{\mathcal{U}}(P_i))}_{e^r=\sqrt{3},\phi=0} + 2\underbrace{\text{Var}(\hat{\mathcal{U}}(P_i)^\dagger \hat{N} \hat{\mathcal{U}}(P_i))}_{e^r=\sqrt{2},\phi=0} + \text{Var}(\hat{N})\Bigg]. \tag{3.57}$$

It can be seen from the above analysis that the variance of $\hat{q}_i^2$ also depends on both displacement u and squeezing s. An optimization of $P_i(r,\phi)$ gate parameters in order to minimize $\text{Var}(\hat{q}_i^2)$ is required in this case too. Likewise, we can express various intra-mode correlation terms such as $\text{Var}(\hat{p}_i^2)$ and $\text{Var}(\hat{q}_i\hat{p}_i)$, as well as various inter-mode correlation terms such as $\text{Var}(\hat{q}_i\hat{q}_j)$ and $\text{Var}(\hat{q}_i\hat{p}_j)$ in terms of the variances of different transformed number operators.

3.5 Concluding remarks

In this chapter, we report photon number measurements based Gaussian state tomography and Gaussian process tomography scheme. While the work builds upon the

scheme given in [123], the current scheme provides an optimal solution to the problem, with a smaller number of optical elements, which makes the scheme more accessible to experimentalists. After describing our optimal scheme for Gaussian state tomography, we use it for the estimation of a Gaussian channel in an optimal way, where we require a total number of $6n^2 + n$ measurements to estimate $6n^2 + n$ parameters specifying a Gaussian channel. Here we have exploited the fact that $\mathrm{Tr}(V)$ is the same for all the output states corresponding to coherent state probes with the same or different mean. Value of $\mathrm{Tr}(V)$ obtained from the full state tomography of the first output state can be used to estimate $\langle \hat{N} \rangle$ for each of the remaining coherent state probes, which renders the scheme optimal. This, in some sense, completes the problem of finding an optimal solution of the Gaussian channel characterization posed in [123].

We note here that the scheme proposed in this chapter is an improvement over existing schemes based on PNRDs and not the traditional homodyne and heterodyne measurement schemes. Similarly, the optimality demonstrated is in terms of numbers of distinct measurements performed, where each distinct measurement has to be performed several times to estimate the averages. Several efforts have already been made to develop measurement schemes using weak oscillators and PNRDs [83, 137], which could be quite beneficial in scenarios where strong local oscillators are not available, which are required for homodyne measurements. Thus, our scheme based on PNRDs is an advancement in this direction as it requires no local oscillator. We expect that with the photon number measurements becoming more and more feasible in recent times, our scheme can be easily implemented in the near future. In current analysis, we have considered estimation of Gaussian states using PNRDs, while prevalent homodyne and heterodyne measurement scheme can estimate even non-Gaussian states. In principle, the current PNRDs based scheme can be extended to non-Gaussian states, however, it requires further investigation.

The study of variance in photon number measurements of the original and transformed states reveals that the variance increases with the mean or displacement and squeezing parameter of the state. Thus, this scheme is preferable for states with small mean and squeezing values. One direction of research could be to improve the scheme performance for states with large mean values. In order to extract information about the parameters of the state, we have chosen certain specific values of gate parameters (see Eqs. (3.20)-(3.22) or Eqs. (3.31)-(3.34)). The effect of different values of gate parameters on the quality of estimates and determination of optimal parameters that maximize the performance of the scheme needs further investigation. Further, the consequences of inefficient PNRDs [138] on Gaussian state tomography and Gaussian process tomography needs to be explored. The results of this chapter are published in Phys. Rev. A **102**, 012616 (2020).

Chapter 4

Using Multiphoton Bell's inequalities to unearth nonlocality of continuous variable states

4.1 Introduction

In their famous 1935 paper, Einstein, Podolsky, and Rosen, despite their controversial conclusion, brought out some of the strangest features of the Quantum Theory [8]. The idea of an entangled state was introduced in this paper, and was elaborated in subsequent papers by Schrödinger [9, 10]. These discussions by Schrödinger further, led to the concept of steering. Later on, Bell introduced the concept of quantum nonlocality in contrast to Einsteinian locality [11]. Entanglement, steering, and nonlocality are all examples of nontrivial quantum correlations, and have turned out to be indispensable resources in quantum information processing [12, 139]. The violation of a Bell inequality indicates nonlocality, which is the strongest form of all quantum correlations [140]. The concept of non locality is useful in a wide range of areas including quantum communication and secure quantum key distribution [141, 142, 143, 144, 145]. Although the original EPR paper considered continuous variable (CV) systems, most of the subsequent research in the field of nonlocality and its violation have been done using discrete variable (DV) systems. The most famous version of Bell inequality, known as CHSH inequality, was formulated for the DV two dimensional bipartite systems [54, 55]. Since the CHSH inequality is valid only for bipartite two-dimensional systems [37, 54, 55, 140], there have been several attempts to generalize the Bell-CHSH inequality for multipartite systems [146, 147, 148, 149, 150, 151] as well as multidimensional systems [152, 153].

4. Using Multiphoton Bell's inequalities to unearth nonlocality of continuous variable states

A problem of major importance is to construct Bell inequalities for CV systems as it enables us to relate to quantum optical nonclassicality of optical systems. Several attempts have already been made to construct Bell-type inequality for CV systems with different number of modes [154, 155, 156, 157, 158, 159]. Specifically, measurement operators with two outcomes, for instance, displaced parity operator measurements, displaced on-off measurements, and pseudo-spin operator measurements, have been employed in CHSH inequality for constructing Bell inequalities for the CV systems [154, 155, 156]. These Bell inequalities have been shown to be effective in detecting nonlocality in various Gaussian and non-Gaussian states [160, 161, 162, 163, 164]. However, the problem of constructing an universal Bell-type inequality for CV systems remains open to this day.

In a different context in quantum optics, a state is said to be classical if diagonal coherent staterepresentation function corresponding to a quantum state is positive and no more singular than a delta function, otherwise the state is classified as nonclassical [43, 48]. Classical states correspond to ensemble of solutions the of Maxwell equations, while nonclassical states have intrinsic quantum properties. The classicality or nonclassicality status of a state remains unchanged by the action of passive optical elements, for instance, beam splitters, phase shifters, and wave plates. The two distinct concepts of classicality based on locality and quantum optical context are called C-classicality and P-classicality, respectively [71]. The inter conversion between these two distinct notions of classicality is possible via passive optics and has been widely studied [70, 71, 165, 166, 167, 168, 169, 170]. This work provides an experimentally implementable connection via multiphoton Bell-type inequalities between these two distinct types of classicality.

In this chapter, we demonstrate the usefulness of the multiphoton Bell-type inequality [154] in unearthing the nonlocality in different four mode state of the CV systems. We first apply the inequality to different two-photon states, where the results show that the multiphoton Bell-type inequality can detect nonlocality only if the correlations exists between the modes corresponding to different propagation directions. We then move on to states with an arbitrary number of photons. We consider optical circuits comprising of phase shifters, beam splitters, and wave plates to generate quantum correlations from nonclassical squeezing in four mode Gaussian states. The nonlocality analysis reveals that the results of the four mode pure Gaussian states are consistent with two photon states. We analyze thermal Gaussian states where the findings reveal that the nonlocality vanishes above a certain temperature. Thereafter, dissipation due to photon loss is modeled using beam splitters, where we find that nonlocality is preserved for all non-zero transmittance values of the beam splitters. Finally, going beyond Gaussian states, we consider pair coherent states and entangled coherent states, which are important non Gaussian states. The results show that these states

violate the inequality, and are thus nonlocal.

This chapter has been structured as follows. In Sec. 4.2, we briefly discuss the formalism of the CV system and the multiphoton Bell violation setup used in this work. Nonlocality in two-photon states has been considered in Sec. 4.3.1, while nonlocality in four-mode general Gaussian states has been considered in Sec. 4.3.2. Non-Gaussian states have been dealt with in Sec. 4.3.3. Finally, we provide a summary of our results and future aspects in Sec. 4.4.

4.2 Background

In this section, we briefly recapitulate the mathematical formalism of four mode CV system and the multiphoton Bell's inequality setup involving the same.

4.2.1 CV system

The Bell violation setup considered for this work is a four-mode optical system as depicted in Fig. 4.1. The two polarization directions $\hat{x}$ and $\hat{y}$ associated with the wave vector $\boldsymbol{k}$ are represented by the annihilation operators $\hat{a}_1$ and $\hat{a}_2$, while the two polarization directions $\hat{x}'$ and $\hat{y}'$ associated with the wave vector $\boldsymbol{k}'$ are represented by the annihilation operators $\hat{a}_3$ and $\hat{a}_4$. These annihilation operators and their corresponding creation operators satisfy the usual commutation relation (1.28).

Alternatively, we can describe our optical setup using four pairs of Hermitian operator, $\hat{q}_i, \hat{p}_i$ ($i = 1, 2, 3, 4$), also known as quadrature operators. The linear homogeneous transformations specified by real 8×8 matrices S acting on the quadrature operators form a non-compact group called the symplectic group in 8 dimensions, and is denoted as $Sp(8, \mathcal{R})$. Further, any arbitrary element of the $Sp(8, \mathcal{R})$ group can be decomposed into active and passive operations. While the single mode squeezing operation is the most basic operation of the active part, the beam splitter and the phase shifter serve as the basic elements of the passive part which form a compact group $U(4)$. The classicality or non-classicality status of a state does not change under the action of passive transformations. However, a separable non-classical state can get entangled by such transformations.

Since the Bell violation setup being considered has two polarization modes associated with each of the wave vectors, a beam splitter cannot be used to transform the two polarization modes associated with a specific wave vector. We thus need to consider compact transformations generated by wave plates, which can act on the two polarization modes associated with a specific wave vector. We discuss the action of half and quarter wave plates on the annihilation operators and how to decompose an arbitrary

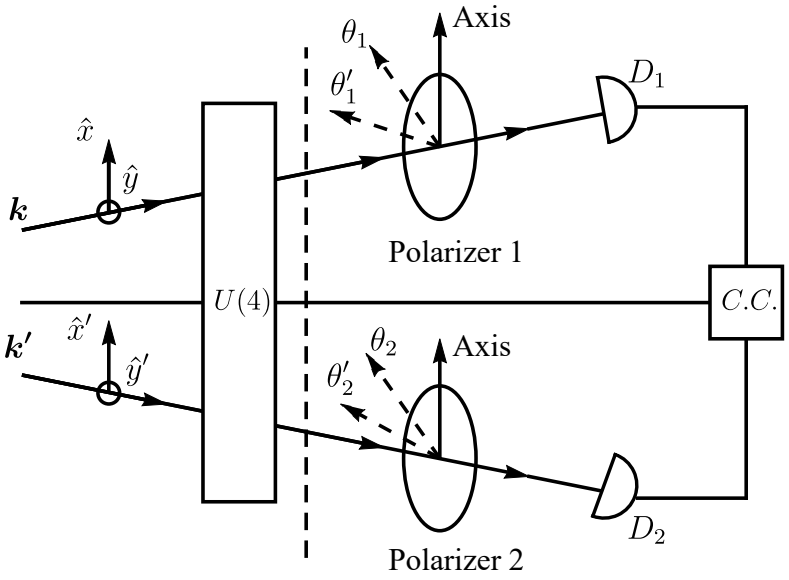


Figure 4.1: Setup to study Bell inequality violation for the states of a four-mode radiation field. The two linear polarization directions $\hat{x}$ and $\hat{y}$ are associated with the propagation direction $\boldsymbol{k}$, while the two linear polarization directions $\hat{x}'$ and $\hat{y}'$ are associated with the propagation direction $\boldsymbol{k}'$. Passive operations comprising of beam splitters, phase shifters, and wave plates are represented by $U(4)$. Angles θ_1 and θ_1' represent the orientation of the polarizer 1 with respect to the x-axis, whereas angles θ_2 and θ_2' represent the orientation of the polarizer 2 with respect to the x'-axis. The detectors are denoted by D_1 and D_2 and $C.C.$ denotes the coincidence counter.

4×4 compact unitary transformation using beam splitters, phase shifters, and wave plates using Cosine-Sine decomposition for our specific setup.

Wave plates: We consider a half-wave plate with slow axis at an angle ϕ to the transverse direction of the electric field. The corresponding transformation matrix acting on the annihilation operators $(\hat{a}_i, \hat{a}_j)^T$ is given by [171]

$$Q(\phi) = \nu(\phi) C(\pi/2) \nu(\phi)^{-1}, \tag{4.1}$$

with

$$\nu(\phi) = \begin{pmatrix} \cos\phi & -\sin\phi \\ \sin\phi & \cos\phi \end{pmatrix}, \; C(\eta) = \begin{pmatrix} e^{i\eta/2} & 0 \\ 0 & e^{-i\eta/2} \end{pmatrix}. \tag{4.2}$$

We also consider a quarter-wave plate with slow axis at an angle ϕ to the transverse direction of the electric field. The corresponding transformation matrix acting on the annihilation operators $(\hat{a}_i, \hat{a}_j)^T$ is given by

$$Q(\phi) = \nu(\phi) C(\pi) \nu(\phi)^{-1}. \tag{4.3}$$

We note that any $SU(2)$ compact transformations can be obtained as a combination of quarter- and half-wave plates.

Cosine-Sine decomposition : Cosine-Sine decomposition allows us to implement all $U(4)$ passive transformations in terms of basic passive elements including beam splitter, phase shifter, and quarter and half wave plates, which can act on state of our system. An arbitrary 4×4 compact unitary transformation can be decomposed as following using Cosine-Sine decomposition [172]:

$$U = \begin{pmatrix} U_1 & 0 \\ 0 & U_2 \end{pmatrix} \underbrace{\begin{pmatrix} C & S \\ -S & C \end{pmatrix}}_{D} \begin{pmatrix} V_1^T & 0 \\ 0 & V_2^T \end{pmatrix}, \tag{4.4}$$

where matrix D, with

$$C = \begin{pmatrix} \cos\theta_1 & 0 \\ 0 & \cos\theta_2 \end{pmatrix}, \; S = \begin{pmatrix} \sin\theta_1 & 0 \\ 0 & \sin\theta_2 \end{pmatrix}, \tag{4.5}$$

can be produced by combining passive elements like beam splitters and wave plates, while U_1, U_2, V_1, and V_2 denote 2×2 unitary transformations that can be produced by combining passive elements like wave plates and phase shifter [173].

4.2.1.1 Phase space description

Wigner distribution corresponding to a density operator $\hat{\rho}$ of a quantum system is defined as

$$W(\xi) = (2\pi)^{-4} \int d^4q' \, \langle \underline{\mathfrak{q}} - \frac{1}{2}\underline{\mathfrak{q}}'|\hat{\rho}|\underline{\mathfrak{q}} + \frac{1}{2}\underline{\mathfrak{q}}'\rangle \exp(i\underline{\mathfrak{q}}' \cdot \underline{\mathfrak{p}}), \tag{4.6}$$

where $\underline{\mathfrak{q}} = (q_1, q_2, q_3, q_4)^T$, $\underline{\mathfrak{p}} = (p_1, p_2, p_3, p_4)^T$ and $\xi = (q_1, \, p_1, \ldots, q_4, \, p_4)^T$. Thus, $W(\xi)$ is a function of eight real phase space variables for a four mode quantum system.

In this work, without any loss of generality, we take the first order moments to be zero as we can change the first order moment of any state without affecting its quantum correlations by applying the displacement operator. The Wigner distribution (4.6) of a general zero-centered four-mode Gaussian states takes a simple form

$$W(\xi) = \frac{\exp[-(1/2)(\xi)^T V^{-1}(\xi)]}{(2\pi)^4 \sqrt{\det V}}, \tag{4.7}$$

where V is the covariance matrix of the four mode Gaussian state.

4.2.2 The Multiphoton Bell violation scenario

We consider the Bell violation setup described in Fig. 4.1. We first apply compact passive transformations $U(4)$ generated by a combination of beam splitters, phase shifters,

and wave plates on a nonclassical and separable state to prepare the state. Thereafter, in each propagation direction, a polarizer placed in a particular direction selects photons with a certain linear polarization. Finally, the coincidence counts are measured using on-off detectors, which performs a coarse-grained measurement in the sense it differentiates between "light" and "no light". The on-off detectors for a single mode system are mathematically described by the set of operator $\{|0\rangle\langle 0|, I - |0\rangle\langle 0|\}$.

To evaluate the coincidence count rates, we define four dichotomous Hermitian operators as following:

$$\begin{aligned} \hat{A}_1 &= (I_{2\times 2} - |00\rangle\langle 00|)_{\boldsymbol{k}}, \\ \hat{A}_2 &= (I_{2\times 2} - |00\rangle\langle 00|)_{\boldsymbol{k'}}, \\ \hat{A}_1(\theta_1) &= (I_{\theta_1} - |0\rangle_{\theta_1\theta_1}\langle 0|)I_{\theta_1+\frac{\pi}{2}}, \\ \hat{A}_2(\theta_2) &= (I_{\theta_2} - |0\rangle_{\theta_2\theta_2}\langle 0|)I_{\theta_2+\frac{\pi}{2}}. \end{aligned} \tag{4.8}$$

The subscripts θ_1 and θ_2 are the directions of the polarizers with subscripts 1 and 2 denoting propagation directions $\boldsymbol{k}$ and $\boldsymbol{k}'$, respectively. We have taken the quantum mechanical action of the polarizer into account while defining these operators. The operators $\hat{A}_1$ and $\hat{A}_1(\theta_1)$ act on the Hilbert space of the modes $\hat{a_1}$ and $\hat{a_2}$, the operator $I_{2\times 2}$ represents a unit operator acting on the Hilbert space of these two modes. Further, the operator I_{θ_1} represents a unit operator for the single mode system with wave vector $\boldsymbol{k}$ and polarization θ_1, whereas the operator $I_{\theta_1+\frac{\pi}{2}}$ represents a unit operator for the orthogonal polarization. Similarly, the operators $\hat{A}_2$ and $\hat{A}_2(\theta_2)$ act on the Hilbert space of the modes $\hat{a_4}$ and $\hat{a_4}$. The probability of detecting at least one photon with no polarizer placed in the path is represented by the expectation value of $\hat{A}_1$, while the probability of detecting at least one photon after a polarizer has been placed in the path is represented by the expectation value of $\hat{A}_1(\theta_1)$. Similarly, the probability of detecting at least one photon with no polarizer placed in the path is represented by the expectation value of $\hat{A}_2$, while the probability of detecting at least one photon after a polarizer has been placed in the path is represented by the expectation value of $\hat{A}_2(\theta_2)$.

Based on different orientations of the two polarizers, we define four different types of coincidence count rates as following:

(i) $P(\theta_1, \theta_2)$ =$\langle A_1(\theta_1)A_2(\theta_2)\rangle$= P_1 at θ_1 and P_2 at θ_2,

(ii) $P(\theta_1, \ )$ = $\langle A_1(\theta_1)A_2\rangle$= P_1 at θ_1 and P_2 removed,

(iii) $P(\ , \theta_2)$ = $\langle A_1A_2(\theta_2)\rangle$= P_1 removed and P_2 at θ_2,

(iv) $P(\ , \ )$ =$\langle A_1A_2\rangle$= P_1 and P_2 removed,

where P_1 and P_2 represent polarizer 1 and polarizer 2, respectively. If the quantum state of the four mode field is known, then the coincidence count rates can be calculated readily using the above relations.

We now derive the general constraint on the correlation between the measurement observables in the hidden variable frame work. If the hidden variable description exists, then the outcomes of individual measurements can be predicted if we are provided with the density operator of the state and the hidden variable λ. Let the actual values of the dynamical variables A_1, A_2, $A_1(\theta_1)$, and $A_1(\theta_2)$ is given by $a_1(\lambda)$, $a_2(\lambda)$, $a_1(\theta_1, \lambda)$, and $a_1(\theta_2, \lambda)$ for a particular value of λ. The averages of various dynamical variables in the hidden variable framework can be evaluated as follows:

$$\begin{aligned}
\langle A_1\rangle_{\text{hv}} &= \int a_1(\lambda)\mathcal{P}(\lambda)d\lambda, \\
\langle A_2\rangle_{\text{hv}} &= \int a_2(\lambda)\mathcal{P}(\lambda)d\lambda, \\
\langle A_1(\theta_1)\rangle_{\text{hv}} &= \int a_1(\theta_1, \lambda)\mathcal{P}(\lambda)d\lambda, \\
\langle A_1(\theta_2)\rangle_{\text{hv}} &= \int a_1(\theta_2, \lambda)\mathcal{P}(\lambda)d\lambda,
\end{aligned} \tag{4.9}$$

where subscript “hv" represents ‘hidden variable and $\mathcal{P}$ is the probability distribution of the hidden variable λ. Similarly, we can write the various coincidence count rates in the local hidden variable frame work as follows:

$$\begin{aligned}
P(\ ,\ )_{\text{hv}} = \langle A_1A_2\rangle_{\text{hv}} &= \int a_{12}(\lambda)\mathcal{P}(\lambda)d\lambda = \int a_1(\lambda)a_2(\lambda)\mathcal{P}(\lambda)d\lambda, \\
P(\theta_1,\ )_{\text{hv}} = \langle A_1(\theta_1)A_2\rangle_{\text{hv}} &= \int a_{12}(\theta_1, \lambda)\mathcal{P}(\lambda)d\lambda = \int a_1(\theta_1, \lambda)a_2(\lambda)\mathcal{P}(\lambda)d\lambda, \\
P(\ ,\theta_2)_{\text{hv}} = \langle A_1A_2(\theta_2)\rangle_{\text{hv}} &= \int a_{21}(\theta_2, \lambda)\mathcal{P}(\lambda)d\lambda = \int a_1(\lambda)a_2(\theta_2, \lambda)\mathcal{P}(\lambda)d\lambda, \\
P(\theta_1, \theta_2)_{\text{hv}} = \langle A_1(\theta_1)A_2(\theta_2)\rangle_{\text{hv}} &= \int a_{12}(\theta_1, \theta_2, \lambda)\mathcal{P}(\lambda)d\lambda = \int a_1(\theta_1, \lambda)a_2(\theta_2, \lambda)\mathcal{P}(\lambda)d\lambda.
\end{aligned} \tag{4.10}$$

We assume that the polarizer can not add any photon and can only remove photons from a given state, which can be expressed as

$$\begin{aligned}
a_1(\theta_1, \lambda) \leq & a_1(\lambda), \\
a_2(\theta_2, \lambda) \leq & a_2(\lambda).
\end{aligned} \tag{4.11}$$

We consider the following inequality given in Ref. [174] for deriving the constraints on the correlation between the measurement observables.

If $0 \leq x, x' \leq X$ and $0 \leq y, y' \leq Y$, then

$$-XY \leq xy - xy' + x'y + x'y' - Yx' - Xy \leq 0. \tag{4.12}$$

Identifying $x = a_1(\theta_1, \lambda)$,$x' = a_1(\theta_1', \lambda)$, $y = a_2(\theta_2, \lambda)$, $y' = a_2(\theta_2', \lambda)$, $X = a_1(\lambda)$, $Y = a_2(\lambda)$, and using Eqs. (4.10) and (4.11), the inequality (4.12) can be written as

$$\begin{aligned} -a_1(\lambda)a_2(\lambda) \leq & a_1(\theta_1, \lambda)a_2(\theta_2, \lambda) - a_1(\theta_1, \lambda)a_2(\theta_2', \lambda) + a_1(\theta_1', \lambda)a_2(\theta_2, \lambda) \\ & + a_1(\theta_1', \lambda)a_2(\theta_2', \lambda) - a_2(\lambda)a_1(\theta_1', \lambda) - a_1(\lambda)a_2(\theta_2, \lambda) \leq 0. \end{aligned} \tag{4.13}$$

Integrating the above inequality over the λ variable with weight function $\mathcal{P}$, we obtain

$$\begin{aligned} -P(\ ,\ ) \leq & P(\theta_1, \theta_2) - P(\theta_1, \theta_2') + P(\theta_1', \theta_2) \\ & + P(\theta_1', \theta_2') - P(\theta_1',\ ) - P(\ , \theta_2) \leq 0. \end{aligned} \tag{4.14}$$

The above Bell-type inequality is obeyed by the coincidence count rates for any choices of angles θ_1, θ_2, θ_1', and θ_2'. Further, it is state independent and valid for general radiation states with either definite or arbitrary number of photons. Any quantum state violating the inequality (4.14) is said to have nonlocal quantum correlations, which cannot be explained in realist hidden variable models based on local theory. We would like to stress that we have considered operators defined on the four mode field, and did not treat photon as a single particle traveling along a path.

4.3 Nonlocality using Multiphoton Bell-type Inequality

In this section, we analyze the capacity of the multiphoton Bell-type inequality in revealing the nonlocality of any given four mode state of the quantum optical field. To gain insights into the working principle of the Bell violation setup, we first consider two-photon states.

4.3.1 Two photon States

We consider two different two-photon states. To produce the first two-photon state $|\psi_1\rangle$, we consider the U transformation (4.4) with

$$U_1 = U_2 = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & -1 \\ 1 & 1 \end{pmatrix}, \ V_1 = V_2 = \mathbb{1}_2, \ D = \mathbb{1}_4, \tag{4.15}$$

and apply on a nonclassical and separable state as follows:

$$\begin{aligned} |1\rangle_1|0\rangle_2|1\rangle_3|0\rangle_4 & \xrightarrow{\mathcal{U}(U_1)\otimes\mathcal{U}(U_2)} \frac{1}{2}(|10\rangle - |01\rangle)_{12}(|10\rangle - |01\rangle)_{34} \\ = |\psi_1\rangle = & \frac{1}{2}(|1\rangle_1|0\rangle_2|1\rangle_3|0\rangle_4 - |1\rangle_1|0\rangle_2|0\rangle_3|1\rangle_4 \\ & -|0\rangle_1|1\rangle_2|1\rangle_3|0\rangle_4 + |0\rangle_1|1\rangle_2|0\rangle_3|1\rangle_4, \end{aligned} \tag{4.16}$$

where $\mathcal{U}(U_1)$ and $\mathcal{U}(U_2)$ represent the infinite dimensional unitary (metaplectic) representation of U_1 and U_2 and act on the modes 1 & 2 ($\boldsymbol{k}$) and modes 3 & 4 ($\boldsymbol{k'}$), respectively. We note that the final state (4.16) generated after the passive transformation is entangled.

Similarly, to generate the second state $|\psi_2\rangle$, we consider the following passive transformation (4.4) with

$$C = -S = (1/\sqrt{2})\mathbb{1}_2,\ U_1 = U_2 = V_1 = V_2 = \mathbb{1}_2, \tag{4.17}$$

and apply on a nonclassical and separable state as follows:

$$\begin{aligned} |1\rangle_1|1\rangle_2|0\rangle_3|0\rangle_4 &\xrightarrow{\mathcal{U}(D)} \frac{1}{2}(|10\rangle - |01\rangle)_{13}(|10\rangle - |01\rangle)_{24} \\ = |\psi_2\rangle &= \frac{1}{2}(|1\rangle_1|1\rangle_2|0\rangle_3|0\rangle_4 - |1\rangle_1|0\rangle_2|0\rangle_3|1\rangle_4 \\ &\quad -|0\rangle_1|1\rangle_2|1\rangle_3|0\rangle_4 + |0\rangle_1|0\rangle_2|1\rangle_3|1\rangle_4). \end{aligned} \tag{4.18}$$

The pair of modes 1 & 2 ($\boldsymbol{k}$) are mixed with the pair of modes 3 & 4 ($\boldsymbol{k'}$) as a result of this transformation.

We now analyze the multiphoton Bell-type inequality (4.14) for states $|\psi_1\rangle$ and $|\psi_2\rangle$. The calculation results reveal that the inequality is not violated by the state $|\psi_1\rangle$ for any value of $\theta_1, \theta_2, \theta_1'$, and θ_2', whereas the inequality is violated by the state $|\psi_2\rangle$ for some values of $\theta_1, \theta_2, \theta_1'$, and θ_2'. This strange result is intimately related to the Bell violation setup. In state $|\psi_1\rangle$, the entanglement is present in modes $1-2$ and modes $3-4$, *i.e.*, the modes corresponding to two different directions are separable. This leads to the factorization of all the correlation functions, for instance,

$$P(\theta_1, \theta_2) = \langle \hat{A}_1(\theta_1)\hat{A}_2(\theta_2)\rangle = \langle \hat{A}_1(\theta_1)\rangle\langle \hat{A}_2(\theta_2)\rangle. \tag{4.19}$$

Thus, the multiphoton Bell-type inequality is not violated. On the other hand, modes $1-3$ and modes $2-4$ of the state $|\psi_2\rangle$ are entangled, *i.e.*, the modes corresponding to two different directions are entangled. Therefore, the correlation functions do not factorize, for example,

$$\langle \hat{A}_1(\theta_1)\hat{A}_2(\theta_2)\rangle \neq \langle \hat{A}_1(\theta_1)\rangle\langle \hat{A}_2(\theta_2)\rangle. \tag{4.20}$$

This fact leads to the violation of the Bell-type inequality. Thus, we can conclude that if the entanglement exists between either of the modes along different directions, the multiphoton Bell-type inequality (4.14) is capable of detecting nonlocality.

4.3.2 Four-mode Gaussian states

In this section, we examine different cases of four mode Gaussian states. We analyze pure as well as mixed states along with leakage modeled by beam splitters.

4.3.2.1 Generic four-mode Gaussians

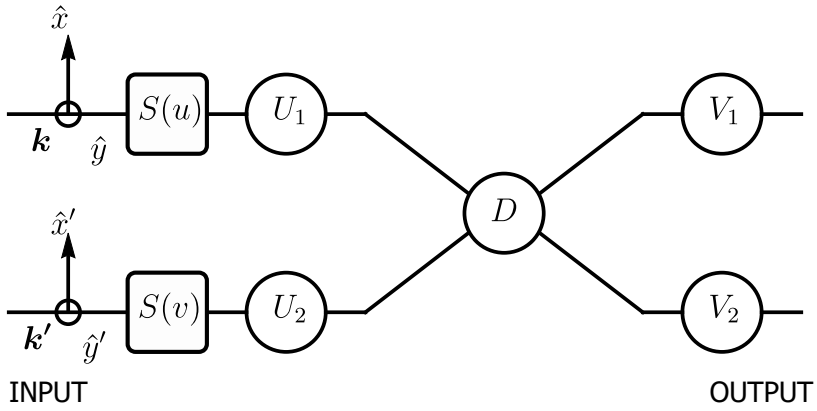


Figure 4.2: Schematic to produce a four-mode generic Gaussian state. Active squeezing transformations are denoted by $S(u)$ and $S(v)$. Passive transformations generated by combinations of quarter and half wave plates and phase shifters are denoted by U_1, U_2, V_1, and V_2, while D denotes transformations that can be generated using beam splitters and quarter and half wave plates. The active operations squeeze the individual modes, and consequently, the state becomes nonclassical. The final state obtained after the passive transformations is entangled.
Classical $\xrightarrow{\text{Squeezing}}$ Non-classical $\xrightarrow{\text{Passive operations}}$ Entangled.

We first generate a generic four mode Gaussian state starting with a four-mode vacuum state or a thermal state. We squeeze the first and the second modes by an equal amount u and the third and the fourth modes by an equal amount v. The resultant squeezing transformation $S(u,v) = S(u)\oplus S(u)\oplus S(v)\oplus S(v)$ can be mathematically represented as

$$S(u,v) = \begin{array}{c} \begin{array}{cccccccc} q_1 & p_1 & q_2 & p_2 & q_3 & p_3 & q_4 & p_4 \end{array} \\ \left(\begin{array}{cccc|cccc} e^{-u} & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & e^{u} & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & e^{-u} & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & e^{u} & 0 & 0 & 0 & 0 \\ \hline 0 & 0 & 0 & 0 & e^{-v} & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & e^{v} & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & e^{-v} & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & e^{v} \end{array}\right) \end{array} \begin{array}{c} q_1 \\ p_1 \\ q_2 \\ p_2 \\ q_3 \\ p_3 \\ q_4 \\ p_4 \end{array} \tag{4.21}$$

We now consider a passive transformation comprised of beam splitter, phase shifters,

and quarter and half wave plates as illustrated in Fig. 4.2, and apply it on the squeezed state to generate an entangled state. The combined action of the passive transformation on the annihilation operators $(\hat{a}_1, \hat{a}_2, \hat{a}_3, \hat{a}_4)^T$ is represented by the matrix

$$U = \frac{1}{2}\begin{pmatrix} 1 & 1 & 1 & 1 \\ -1 & 1 & -1 & 1 \\ -1 & -1 & 1 & 1 \\ 1 & -1 & -1 & 1 \end{pmatrix}. \tag{4.22}$$

This passive transformation generates the maximum amount of entanglement while acting on a four mode system. We can decompose this matrix in the form given in Eq. (4.4) and the submatrices evaluates to be

$$\begin{aligned} &U_1 = U_2 = \frac{1}{\sqrt{2}}\begin{pmatrix} 1 & -1 \\ 1 & 1 \end{pmatrix},\ V_1 = V_2 = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix},\ \text{and} \\ &C = S = \frac{1}{\sqrt{2}}\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}. \end{aligned} \tag{4.23}$$

The action of the passive transformation matrix (4.22) on the Hermitian quadrature operators $\hat{\xi}$ is given by

$$K = \frac{1}{2}\left(\begin{array}{cccc|cccc} q_1 & p_1 & q_2 & p_2 & q_3 & p_3 & q_4 & p_4 & \\ \hline 1 & 0 & 1 & 0 & 1 & 0 & 1 & 0 & q_1 \\ 0 & 1 & 0 & 1 & 0 & 1 & 0 & 1 & p_1 \\ -1 & 0 & 1 & 0 & -1 & 0 & 1 & 0 & q_2 \\ 0 & -1 & 0 & 1 & 0 & -1 & 0 & 1 & p_2 \\ \hline -1 & 0 & -1 & 0 & 1 & 0 & 1 & 0 & q_3 \\ 0 & -1 & 0 & -1 & 0 & 1 & 0 & 1 & p_3 \\ 1 & 0 & -1 & 0 & -1 & 0 & 1 & 0 & q_4 \\ 0 & 1 & 0 & -1 & 0 & -1 & 0 & 1 & p_4 \end{array}\right) \tag{4.24}$$

The covariance matrix of the final state produced by the symplectic transformation $S = KS(u, v)$ is given by

$$V = SV_0S^T, \tag{4.25}$$

where

$$V_0 = \frac{1}{2\kappa}\mathbb{1}_{8\times 8},\ \text{where}\ \kappa = \tanh\left(\frac{\hbar\omega}{2kT}\right)\ \&\, 0 \leq \kappa \leq 1, \tag{4.26}$$

is the four mode thermal state. The corresponding Wigner function can be evaluated using Eq. 4.7. After the state has been generated, we now move to examine the nonlocality of the four-mode generic Gaussian state. To this end, we define the average of

the Bell operator as follows:

$$\begin{aligned} f(\theta_1,\theta_2,\theta_1',\theta_2') =& P(\theta_1,\theta_2)_{\text{qm}}^{\text{gauss}} - P(\theta_1,\theta_2')_{\text{qm}}^{\text{gauss}} \\ &+ P(\theta_1',\theta_2)_{\text{qm}}^{\text{gauss}} + P(\theta_1',\theta_2')_{\text{qm}}^{\text{gauss}} \\ &- P(\theta_1', \quad)_{\text{qm}}^{\text{gauss}} - P(\quad,\theta_2)_{\text{qm}}^{\text{gauss}}. \end{aligned} \tag{4.27}$$

The calculation for one of the correlation functions is shown below:

$$\begin{aligned} P(\theta_1,\theta_2)_{\text{qm}}^{\text{gauss}} =& 1 - Tr(\rho|0\rangle_{\theta_1\theta_1}\langle 0|) - Tr(\rho|0\rangle_{\theta_2\theta_2}\langle 0|) \\ &+ Tr(\rho|0\rangle_{\theta_1\theta_1}\langle 0||0\rangle_{\theta_2\theta_2}\langle 0|). \end{aligned} \tag{4.28}$$

Phase space techniques proves to be convenient for calculations involving states with arbitrary number of photons. We show the calculation for one term of Eq. (4.28) below, while the rest of the terms can be calculated similarly:

$$Tr(\rho|0\rangle_{\theta_1\theta_1}\langle 0|) = 2\pi \int W(U(\theta_1,0)\xi) W_0(q_1,p_1) d\xi, \tag{4.29a}$$

$$= 2\sqrt{\text{Det}(G)}\sqrt{\text{Det}[U(\theta_1,0)^T G U(\theta_1,0) + e_{11} + e_{22}]^{-1}}, \tag{4.29b}$$

where G is related to the covariance matrix as $G = (1/2)V^{-1}$ and $U(\theta_1,\theta_2) = R(\theta_1) \oplus R(\theta_2) \oplus R(\theta_1) \oplus R(\theta_2)$ with

$$R(\theta) = \begin{pmatrix} \cos\theta & -\sin\theta \\ \sin\theta & \cos\theta \end{pmatrix}, \tag{4.30}$$

is the rotation in phase space (ξ) due to the polarizers.

We now examine different families of the four mode Gaussian states using the calculation techniques illustrated above.

4.3.2.2 Four-mode pure squeezed vacuum state

We first examine the nonlocality for the case $\kappa = 1$ in Eq. (4.25) , which corresponds to four-mode pure squeezed vacuum state. The plot of $f(\theta_1,\theta_2,\theta_1',\theta_2')$ as a function of the squeezing parameter u for two different cases $v = -u$, and $v = 0$ has been shown in Fig. 4.3. The case $v = -u$ is represented by the thick solid line, which violates the multiphoton Bell-type inequality. The input state in this case assumes a simple form $|\text{TMSV}\rangle_{13}|\text{TMSV}\rangle_{24}$, where TMSV denotes two mode squeezed vacuum state. The entanglement structure of the aforementioned state is the same as the state $|\psi_2\rangle$, which has been considered in Sec. 4.3.1. The case $v = 0$ is represented by the dashed line, and it also violates the inequality, although to a smaller degree. Therefore, we conclude that both the states corresponding to the two different cases are nonlocal. We note that the chosen value of the parameters $\theta_1, \theta_2, \theta_1'$ and θ_2' corresponds to the maximum violation of the inequality.

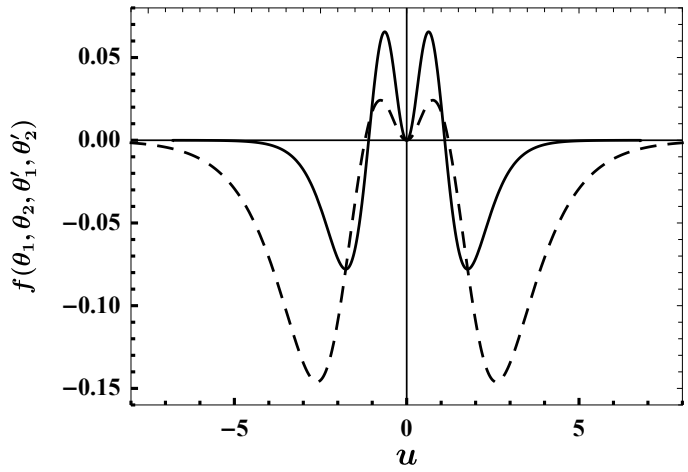


Figure 4.3: Average of the Bell operator as a function of the squeezing parameter u for a four-mode pure squeezed vacuum state. The thick solid curve and the dashed curve represent the case $v = -u$ and $v = 0$, respectively. The multiphoton Bell's inequality is violated for both the cases. We have set the angles as $\theta_1 = 1.32$, $\theta_2 = 0.93$, $\theta_1' = 3.66$, $\theta_2' = 3.32$, which corresponds to the maximum violation of the inequality.

4.3.2.3 Four-mode squeezed thermal state

Thermal states arise in a situation when the system is in thermodynamic equilibrium with an environment. Thermal states are a classical mixture of photon number states (energy eigen states) with weight factors given by the Boltzmann factor [15]. The Wigner distribution of a thermal state is Gaussian and is classical in the quantum optical context. Squeezed thermal states, another class of nonclassical Gaussian states, are generated by applying squeezing transformations on a thermal state.

Here we analyze the nonlocality in the four-mode squeezed thermal state for the maximum violation case $v = -u$. The plot of $f(\theta_1, \theta_2, \theta_1', \theta_2')$ as a function of the squeezing parameter u for different values of the thermal parameter κ is shown in Fig. 4.4. The findings reveal that the state is nonlocal even at a finite temperature. However, the nonlocal correlations in the state vanishes as the temperature is increased further.

4.3.2.4 Leakage model

We now turn our attention to a situation relevant to practical systems, where there is a leakage in the system causing information loss and energy dissipation.Such leakage processes can have adverse effects on the effectiveness of different quantum information protocols [175], for example, continuous variable quantum key distribution [176].

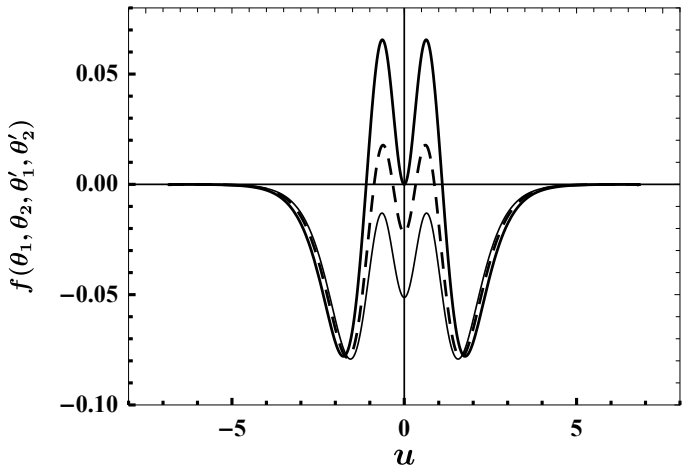


Figure 4.4: Average of the Bell operator as a function of the squeezing parameter u for a four-mode squeezed thermal state for the case $v = -u$. Various curves correspond to $\kappa = 1$ (thick solid), $\kappa = 0.8$ (dashed) and $\kappa = 0.7$ (thin solid). The plot shows that there is a loss of nonlocal correlations with an increase in the temperature. We have set the angles as $\theta_1 = 1.32$, $\theta_2 = 0.93$, $\theta_1' = 3.66$, $\theta_2' = 3.32$.

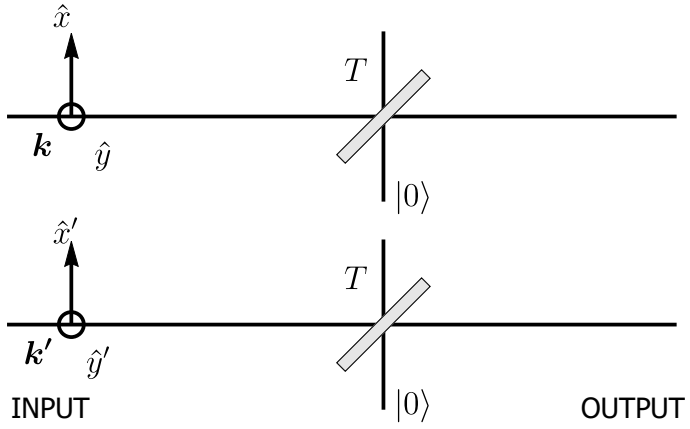


Figure 4.5: Modeling leakage with beam splitters. We mix each mode of the pure input state with the vacuum state using beam splitters of transmittance T. Afterwards, we discard the modes corresponding to the vacuum state, and the reduced state is a mixed Gaussian state.

Thus, it is of significant importance to characterize the effect of leakage processes on the state properties.Generally, dissipative processes are responsible for leakages and can be modeled using beam splitters. The schematic for the leakage processes is shown in Fig. 4.5, where we mix each mode of the system with the vacuum state using

beam splitters of transmittance T. Thereafter, we trace out the mode corresponding to the vacuum, and the reduced state is a mixed Gaussian state. It should be noted that we have considered the leakage for the maximum violation case $v = -u$.

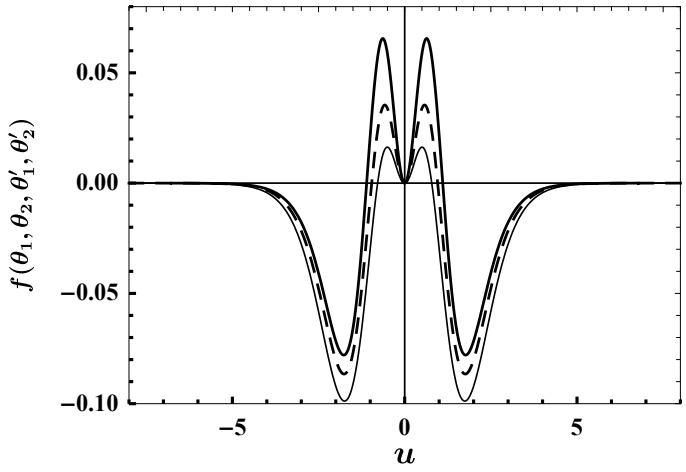


Figure 4.6: Average of the Bell operator as a function of the squeezing parameter u for a four-mode pure squeezed vacuum state $|\text{TMSV}\rangle_{13}\,|\text{TMSV}\rangle_{24}$ in the presence of leakage. Various curves correspond to $T = 1$ (thick solid), $T = 0.8$ (dashed), and $T = 1$ (thin solid). Results indicate that the nonlocal correlations of state remains preserved under leakage. We have set the angles as $\theta_1 = 1.32$, $\theta_2 = 0.93$, $\theta_1' = 3.66$, $\theta_2' = 3.32$.

The plot of $f(\theta_1, \theta_2, \theta_1', \theta_2')$ as a function of the squeezing parameter u for different values of transmittance T is shown in Fig. 4.6. The results show that as the transmittance is decreased, there is a decrease in the detected nonlocal correlations, although it never vanishes even for low transmittance. Thus, the leakage processes preserve the nonlocality of the squeezed Gaussian state. This result is in contrast with the thermal states, where the state becomes local after a certain threshold temperature.

4.3.3 Non-Gaussian states

This section examines the nonlocality in pair coherent states and entangled coherent states, which are important examples of non-Gaussian states.

4.3.3.1 Pair coherent states

Pair coherent states are defined as the simultaneous eigenkets of $\hat{a}_1\hat{a}_2$ and $\hat{a}_1\hat{a}_1^\dagger - \hat{a}_2\hat{a}_2^\dagger$ with eigenvalues ζ and q, respectively [177]:

$$\hat{a}_1\hat{a}_2 \left|\zeta, q\right\rangle = \zeta \left|\zeta, q\right\rangle, \quad \left(\hat{a}_1\hat{a}_1^\dagger - \hat{a}_2\hat{a}_2^\dagger\right) \left|\zeta, q\right\rangle = q \left|\zeta, q\right\rangle, \tag{4.31}$$

where ζ is in general complex and q represents the photon number difference between the two modes. The pair coherent states can also be written in the Fock basis as follows:

$$\left|\zeta, q\right\rangle = A_q \sum_{n=0}^{\infty} \frac{\zeta^n}{\left[n!(n+q)!\right]^{1/2}} \left|n+q, n\right\rangle, \tag{4.32}$$

with

$$A_q = \left[\left|\zeta\right|^{-q} J_q\left(2\left|\zeta\right|\right)\right]^{-1/2}, \tag{4.33}$$

where J_q is the modified Bessel function of the first kind of order q. Several quantum properties, for instance, entanglement, nonclassicality, and squeezing have been analyzed in pair coherent states [178, 179, 180] and these states can also serve as a resource state for quantum teleportation [181]. Despite the fact that the covariance matrix only captures information about the second order correlation and leaves the information about the higher order correlation, it has been shown that inequalities based on the second-order correlation can detect entanglement in the pair coherent states [178].

However, we do not consider the Gaussian approximation of the pair coherent states for this work. To study nonlocality for the pair coherent states, the average of the Bell operator (4.27), which is valid for non-Gaussian states as well, is evaluated. To compute the correlation functions in the phase space, for instance, Eq. (4.29a), we use the Wigner function for the pair coherent states [182].

The average of the Bell operator (4.27) is computed for the input state $\left|PCS\right\rangle_{13}\left|PCS\right\rangle_{24}$ with $q = 0$ and Im(ζ)$= 0$. We plot the numerically computed averages in Fig. 4.7. The result reveals that the multiphoton Bell-type inequality is violated by the pair coherent states.

4.3.3.2 Entangled Coherent State

Entangled coherent state (ECS) are defined for two mode system as [183]

$$\left|ECS\right\rangle = N_o\left(\left|\frac{\alpha}{\sqrt{2}}\right\rangle\left|\frac{-\alpha}{\sqrt{2}}\right\rangle - \left|\frac{-\alpha}{\sqrt{2}}\right\rangle\left|\frac{\alpha}{\sqrt{2}}\right\rangle\right), \tag{4.34}$$

where $N_o = [2 - 2\exp(-2|\alpha|^2)]^{-1/2}$.

We prepare modes 1 and 2 (direction $\boldsymbol{k}$) in the odd coherent state $|\psi_o\rangle = N_o(|\alpha\rangle - |-\alpha\rangle)$ and modes 3 and 4 (direction $\boldsymbol{k'}$) in the vacuum state. The pair of modes 1 &

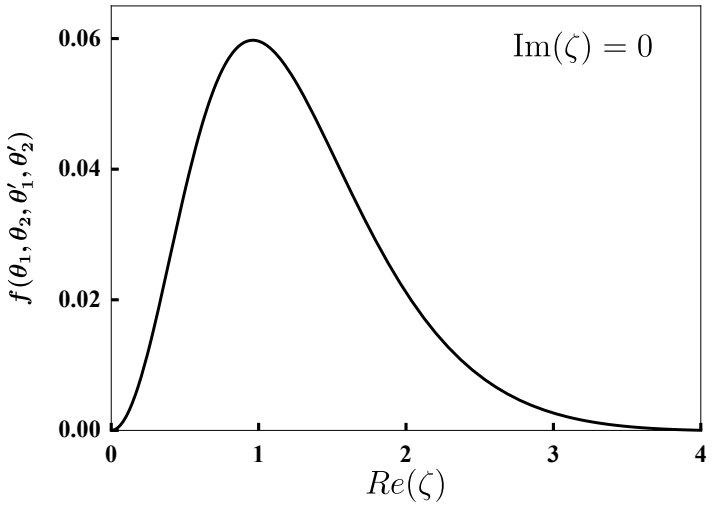


Figure 4.7: Average of the Bell operator as a function of the parameter Re(ζ) for pair coherent state with $q = 0$. The result shows that the pair coherent states are nonlocal. We have set the angles as $\theta_1 = 3.67$, $\theta_2 = 3.29$, $\theta_1' = 2.30$, $\theta_2' = 5.75$.

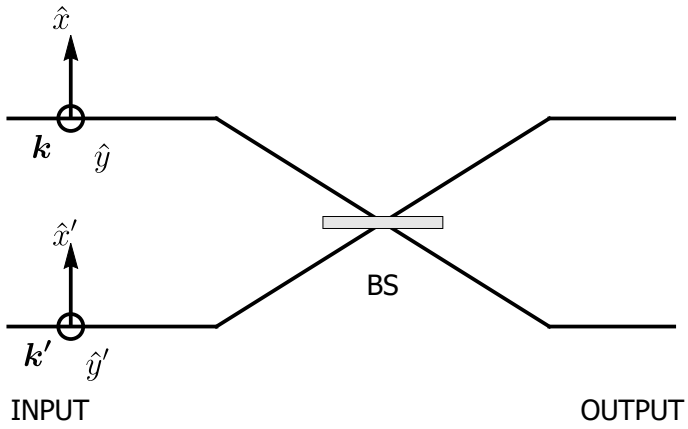


Figure 4.8: Set up for the generation of entangled coherent state (ECS). We mix modes 1 and 2 ($\boldsymbol{k}$) prepared in the odd coherent state $|\psi_o\rangle = N_o(|\alpha\rangle - |-\alpha\rangle)$ with modes 3 and 4 ($\boldsymbol{k'}$) in the vacuum state via a balanced beam splitter. The final state is$|ECS\rangle_{13}|ECS\rangle_{24}$.

2 are mixed with the pair of modes 3 & 4 using a balanced beam splitter as shown in Fig. 4.8. This transformation can be mathematically represented in the form given in Eq. (4.4) with

$$C = -S = (1/\sqrt{2})\mathbb{1}_2,\ U_1 = U_2 = V_1 = V_2 = \mathbb{1}_2. \tag{4.35}$$

The final state obtained is $|ECS\rangle_{13}|ECS\rangle_{24}$:

$$N_o^2(|\alpha\rangle - |-\alpha\rangle)_1(|\alpha\rangle - |-\alpha\rangle)_2|0\rangle_3|0\rangle_4 \xrightarrow{\mathcal{U}(D)} N_o^2\left(\left|\frac{\alpha}{\sqrt{2}}\right\rangle\left|\frac{-\alpha}{\sqrt{2}}\right\rangle - \left|\frac{-\alpha}{\sqrt{2}}\right\rangle\left|\frac{\alpha}{\sqrt{2}}\right\rangle\right)_{13} \left(\left|\frac{\alpha}{\sqrt{2}}\right\rangle\left|\frac{-\alpha}{\sqrt{2}}\right\rangle - \left|\frac{-\alpha}{\sqrt{2}}\right\rangle\left|\frac{\alpha}{\sqrt{2}}\right\rangle\right)_{24}. \tag{4.36}$$

The Wigner function $W(\xi)$ of the state $N_o^2(|\alpha\rangle - |-\alpha\rangle)_1(|\alpha\rangle - |-\alpha\rangle)_2|0\rangle_3|0\rangle_4$ can be readily evaluated using Eq. (4.6). To obtain the Wigner function of the final state in Eq. (4.36), we transform the Wigner function as $W(\xi) \to W\left(E^{-1}\xi\right)$, where E is the passive transformation corresponding to Eq. (4.35) acting on the quadrature operators $\hat{\xi}$ as follows:

$$E = \frac{1}{\sqrt{2}} \begin{array}{c} \begin{array}{cccc|cccc} q_1 & p_1 & q_2 & p_2 & q_3 & p_3 & q_4 & p_4 \end{array} \\ \left(\begin{array}{cccc|cccc} 1 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 1 \\ \hline -1 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & -1 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & -1 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & -1 & 0 & 0 & 0 & 1 \end{array}\right) \end{array} \begin{array}{c} q_1 \\ p_1 \\ q_2 \\ p_2 \\ q_3 \\ p_3 \\ q_4 \\ p_4 \end{array} \tag{4.37}$$

The Bell operator can be evaluated analytically for the entangled coherent state, for instance, Eq. (4.29a) turns out to be

$$Tr(\rho|0\rangle_{\theta_1\theta_1}\langle 0|) = 2\frac{e^{d^2}}{(e^{d^2}-1)^2}\left[-\cosh\left(\frac{1}{4}d^2\cos(2\theta_1)\right) + \cosh\left(\frac{3}{4}d^2\right)\cosh\left(\frac{1}{4}d^2\sin(2\theta_1)\right)\right], \tag{4.38}$$

where $d = \text{Re}(\alpha)$ and $\text{Im}(\alpha) = 0$. We plot the average of the Bell operator as a function of $\text{Re}(\alpha)$ in Fig. 4.9. The result shows that the multiphoton Bell-type inequality is violated by the entangled coherent state.

Expanding both sides of Eq. (4.36) in the Fock basis and then taking the limit $|\alpha| \to 0$, we get

$$|1\rangle_1|1\rangle_2|0\rangle_3|0\rangle_4 \xrightarrow{\mathcal{U}(D)} \frac{1}{2}(|10\rangle - |01\rangle)_{13}(|10\rangle - |01\rangle)_{24}. \tag{4.39}$$

This equation is same as Eq. (4.18) considered in Sec. (4.3.1), where the final state obtained has been shown to violate the multiphoton Bell-type inequality.

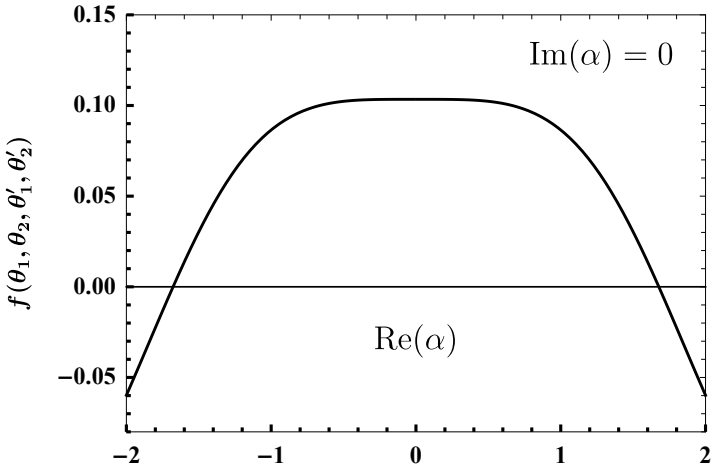


Figure 4.9: Average of Bell operator as a function of $\mathrm{Re}(\alpha)$ for entangled coherent state. The result shows that entangled coherent states are nonlocal. We have set the angles as $\theta_1 = 2.67$, $\theta_2 = 5.59$, $\theta_1' = 1.88$, $\theta_2' = 3.24$.

4.4 Conclusion

In this chapter, we investigated the potential of the multiphoton Bell-type inequality, which is based on the Clauser-Horne 1974 Bell test inequality, in revealing the nonlocality of continuous variable systems. To this end, we examined various states ranging from states with a finite number of photons to an arbitrary number of photons, Gaussian to non-Gaussian. The role of the compact passive transformations in converting quantum optical nonclassicality into quantum nonlocality is also demonstrated through several examples. The studies show that the multiphoton Bell-type inequality is capable of detecting nonlocality in a variety of situations.

The input state for the multiphoton Bell-type inequality is a four mode radiation field. The only requirement for the inequality to detect nonlocality in a given state is that the correlation should not be limited to modes 1 and 2 and modes 3 and 4 as these pairs of modes travel along the same physical directions. The results for the thermal state revealed that the quantum nonlocality vanishes after a certain threshold temperature. However, the results for the leakage modeled by beam splitters showed that the violation decreases with increasing the beam splitter transmissivity, but never vanishes.

In this study, the coincidence count is measured using on-off detectors with two outcomes, which basically differentiates between the presence and the absence of light. Although, the multiphoton Bell-type inequality based on two outcomes is capable of detecting nonlocality, it is desirable to construct inequality based on more fine grained

measurements using photon number resolving detectors.

Chapter 5

Coherence assisted non-Gaussian measurement device independent quantum key distribution

5.1 Introduction

In this chapter, we report continuous variable measurement-device-independent quantum key distribution (CV-MDI-QKD) using photon subtraction on two-mode squeezed coherent (PSTMSC) states as a resource. Quantum key distribution (QKD) protocols [144, 184] allow us to share unconditionally secure keys between two distant parties which is not possible in the classical world. In quantum mechanics, simultaneous measurement of two non-commuting observables introduces an additional noise in the measurement outcomes for both. Bennett and Brassard exploited this fundamental feature of quantum physics to develop a secure key distribution scheme for cryptography [13, 185]. Security of QKD schemes is based on the laws of nature which cannot be violated [73, 144, 186]. This is in contrast with classical key distribution schemes where the security is based on computationally difficult to solve problems. Later on, unconditional security [109, 187, 188] of various QKD schemes used other important quantum features, like no-cloning theorem [189, 190], entanglement [144], Bell-nonlocality [191, 192], and monogamy of quantum correlations [145, 193].

We can classify the existing QKD schemes into two major categories: discrete variable QKD (DV-QKD) [13, 191] and continuous variable QKD (CV-QKD) [109, 190, 194, 195]. DV-QKD requires costly single photon sources which renders its physical realization difficult. On the other hand, the realization of CV-QKD, based on the quadrature amplitudes of quantum optical sources, is relatively easier. While DV-

QKD protocols are more suitable for long distances, CV-QKD provides a better key rate for short distances [196]. CV-QKD protocols have been shown to be unconditionally secure against collective attacks [72, 73, 197, 198, 199] in the finite key size and asymptotic regime, which has also been realized experimentally [77, 200, 201].

However, one of the major setbacks in the experimental realizations of QKD protocols is due to imperfect and compromised devices that have not been accounted for in the theoretical models. Therefore, one needs to fully characterize these devices in order to identify security loopholes or side channels, which in itself is a difficult task. To eliminate the gaps between theoretical models and physical devices, discrete variable device-independent quantum key distribution (DV-DI-QKD) protocol was invented [202]. However, the protocol remains impractical due to low secret key rate and small transmission distances. Later on, discrete variable measurement-device-independent quantum key distribution (DV-MDI-QKD) protocol [74, 203] was proposed to eliminate all the security loopholes arising due to imperfect detectors. This protocol has a favourable performance and also enhances the secret key rate. In this protocol, Bell state measurements are performed by an untrusted third party, who publicly communicates the result, which Alice and Bob use to generate a secure key. Significant progress has been made in theoretical [204, 205, 206] as well as experimental [207, 208, 209] aspect of DV-MDI-QKD protocol. The concept of entanglement swapping was extended to CV-QKD protocols, which gave rise to CV-MDI-QKD protocol [75, 210, 211]. Significant progress has been made in theoretical [212, 213, 214] as well as experimental [75] aspect of this protocol. However, CV-MDI-QKD protocols yield lower transmission distances than DV-MDI-QKD.

Studies have shown that entanglement content of the two-mode squeezed vacuum (TMSV) state can be enhanced using non-Gaussian operations, like photon addition and subtraction [22, 23, 24, 25, 27, 215, 216, 217]. Thus, it is natural to expect that these states can improve the maximum transmission distances [32, 33, 218]. It has already been shown that photon subtraction on a two-mode squeezed vacuum (PSTMSV) state yields higher transmission distances than a TMSV state [32].

In this chapter, we apply non-Gaussian operations on two-mode squeezed coherent (TMSC) states to generate a resource for CV-MDI-QKD protocol. To be more specific, we consider photon subtraction on a two-mode squeezed coherent (PSTMSC) state. It should be noted that both the TMSV and TMSC states have the same covariance matrix, and since the key rate depends only on the covariance matrix, the performance of both the states in CV-MDI-QKD protocol is the same. However, for non-Gaussian operations like photon subtraction, the covariance matrix is different for the PSTMSV and PSTMSC states, and thus the performance of both the states in CV-MDI-QKD protocol will be different. Our results show that the PSTMSC state based CV-MDI-QKD protocol significantly improves the transmission distance at the price of reduction in

the maximum achievable secure key rate. For our PSTMSC state based protocol, transmission distances can go up to $60-70$ km, which is considerably more than the earlier protocols. We further show that our protocol is a generalization of previous CV-MDI-QKD protocols and their results can be obtained as a special case of ours. We present the results of numerical simulations of the secure key rate, which reveal coherence along with non-Gaussianity improves the transmission distances of the protocol. Here we have defined coherence as the amount of displacement of the coherent state, that is fed into the non-linear optical down-converter, from the vacuum state to generate the TMSC state. We emphasize here that it is easier to produce a TMSC state than a TMSV state as the starting point for the former is the coherent state and the latter is the vacuum state. Further, the theoretical study of non-Gaussian operations on the TMSC state is quite complicated and is not available in the literature to the best of our knowledge. In this work, we also provide the calculation of the covariance matrix for the PSTMSC state in phase space formalism, which can find utility in the other quantum information processing (QIP) protocols.

This chapter is structured as follows. In Sec. 5.2.1, we review the CV-MDI-QKD protocol, while in Sec. 5.2.2, we provide a detailed calculation of the covariance matrix of the PSTMSC state. In Sec. 5.2.3, we present a redesigned version of the CV-MDI-QKD protocol suited for the PSTMSC state. In Sec. 5.3, we provide the mathematical framework to evaluate the secret key rate of the QKD protocol. In Sec. 5.4 we present numerical simulation studies of the performance of the PSTMSC state based CV-MDI-QKD protocol. Finally, in Sec. 5.5 we provide conclusions based on our results and discuss future directions.

5.2 Description of the QKD protocol

In this section, we briefly review the entanglement based CV-MDI-QKD protocol, and then provide a detailed calculation of the covariance matrix of the k-photon subtracted TMSC state. Finally, the modified CV-MDI-QKD protocol tailored for the PSTMSC state is presented.

5.2.1 CV-MDI-QKD

In the entanglement based CV-MDI-QKD, each of the two remotely located parties Alice and Bob generate a TMSV state with quadrature variances V_A and V_B, respectively. We consider $V_A = V_B$ for the rest of the chapter. We label the pair of modes as A_1, A_2 for Alice and B_1, B_2 for Bob. An untrusted third party, Charlie, is connected to Alice and Bob through quantum channels of lengths L_{AC} and L_{BC}, respectively. Alice and

Bob send one of their modes (A_2 for Alice and B_2 for Bob) to Charlie, while the modes A_1 and B_1 are retained with them, respectively. The total transmission length equals $L = L_{AC} + L_{BC}$. Charlie combines the two modes using a 50:50 beam splitter (BS) and the two output modes are labeled as C and D. He then measures the x quadrature on mode C and the p quadrature on mode D using a homodyne detection system and publicly declares the obtained results $\{X_C, P_D\}$.

In the next step, Bob applies a displacement operator $D(\alpha)$ transforming his mode B_1 to B_1'. Here $\alpha = g(X_C + iP_D)$, where g is the gain factor. This operation entangles the modes A_1 and B_1'. Thereafter, both Alice and Bob perform joint measurement of the x and p quadratures on their respective modes A_1 and B_1' using heterodyne detection system. The results thus obtained by Alice, $\{X_A, P_A\}$, are correlated with the results obtained by Bob, $\{X_B, P_B\}$. Finally, the secret key is obtained after information reconciliation and privacy amplification on the correlated data. Furthermore, this work considers the case of reverse reconciliation, where Alice corrects her results in reference to Bob's results.

5.2.2 Photon subtraction on a two-mode squeezed coherent state

This section contains illustration and detailed analytical calculations of the probability and the covariance matrix for k photon subtraction on one mode of the TMSC state. The calculations have been done in the phase space formalism using the Wigner function representation.

Photon subtraction scheme

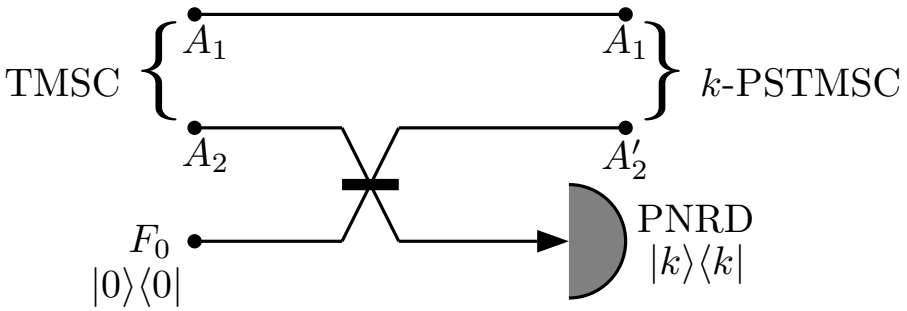


Figure 5.1: Schematic representation of the photon subtraction operation on a TMSC state. Modes A_1 and A_2 are initialized in the TMSC state, while mode F_0 is initialized in the vacuum state. A photon number resolving detector (PNRD), described by the POVM $\{\Pi_k, \mathbb{1} - \Pi_k\}$, where $\Pi_k = |k\rangle\langle k|$, is applied to the mode F_1.

Alice sends a coherent beam of light through a non-linear optical down converter [219] and generates a TMSC state $|\psi\rangle_{A_1A_2} = S_{12}(r)D_1(d)D_2(d)|00\rangle$ with variance $V_A = \cosh(2r)$, where $S_{12}(r) = \exp[r(\hat{a}^\dagger_{A_1}\hat{a}^\dagger_{A_2} - \hat{a}_{A_1}\hat{a}_{A_2})]$ represents the two-mode squeezing operator with r as a real squeezing parameter, and $D_i(d) = \exp[d(\hat{a}^\dagger_{A_i} - \hat{a}_{A_i})]$ represents the displacement operator, which displaces the mode A_i by an amount d along the x quadrature. Thereafter, Alice sends one of her modes A_2 to Fred, who uses a beam splitter of transmittivity τ to combine the mode A_2 with the mode F_0 initialized in the vacuum state $|0\rangle$. Fred then measures mode F_1 using a photon number resolving detector (PNRD) described by the POVM $\{\Pi_k, \mathbb{1} - \Pi_k\}$, where $\Pi_k = |k\rangle\langle k|$ is a projection on the k-photon state. A successful k-photon subtraction corresponds to the click of the POVM element Π_k, and the state corresponding to the modes A_1 and A_2' is k-PSTMSC state. The schematic for the same is given in Fig. 5.1, which can be represented through the following flow diagram in the Hilbert space:

$$|\psi\rangle_{A_1A_2}|0\rangle_{F_0} \xrightarrow{\text{Beam Splitter}} |\Psi\rangle_{A_1A_2'F_1} = \mathcal{U}(B_{A_2F_0}(\tau))|\psi\rangle_{A_1A_2}|0\rangle_{F_0} \xrightarrow[\text{PNRD}]{\text{Projection on } |k\rangle_{F_1}\langle k|} |\Psi\rangle^k_{A_1A_2'} = {}_{F_1}\langle k|\Psi\rangle_{A_1A_2'F_1}. \tag{5.1}$$

Here the state $|\Psi\rangle^k_{A_1A_2'}$ is unnormalized and the normalized state $|\widetilde{\Psi}\rangle^k_{A_1A_2'}$ is given by

$$|\widetilde{\Psi}\rangle^k_{A_1A_2'} = \frac{1}{\sqrt{P^k_{PS}}}{}_{F_1}\langle k|\Psi\rangle_{A_1A_2'F_1}, \tag{5.2}$$

where P^k_{PS} is the probability of detection of k photon, which can be evaluated as

$$P^k_{PS} = \sum_m \sum_l |{}_{A_1}\langle m|_{A_2'}\langle l|_{F_1}\langle k|\Psi\rangle_{A_1A_2F_1}|^2 = \sum_m \sum_l |{}_{A_1}\langle m||\Psi\rangle^k_{A_1A_2'}|^2. \tag{5.3}$$

Wigner function approach

We now present a stepwise calculation of the Wigner function of the TMSC state, the effect of the beam splitter transformation on the input state and the probability of k photon detection. We then calculate the covariance matrix of the k-PSTMSC state.

Wigner function of the TMSC state

We compute explicitly the Wigner function of the TMSC state starting from the two-mode coherent state. A two-mode coherent state, represented by quadrature field operators $\hat{\xi} = (\hat{x_1}, \hat{p_1}, \hat{x_2}, \hat{p_2})^T$ ($[\hat{x_i}, \hat{p_j}] = 2i\delta_{ij}$ with $i, j \in \{1, 2\}$), is sent through a two-mode squeezer. The Wigner function of the two-mode coherent state with the

displacement vector $\overline{\xi} = (d, 0, d, 0)^T$ can be written using Eq. (1.69) as

$$W^C_{A_1A_2}(\xi_1, \xi_2) = \frac{1}{4\pi^2} \exp\left[-\frac{1}{2}\left((x_1 - d)^2 + p_1^2 + (x_2 - d)^2 + p_2^2\right)\right]. \tag{5.4}$$

Now, the two-mode coherent state is sent through a two-mode squeezer given by the two-mode squeezing transformation matrix S_{12} (1.93). Consequently, the Wigner function transforms as $W(\xi) \to W(S_{12}^{-1}\xi)$. The transformation $\xi \to S_{12}^{-1}\xi$ can be written as

$$\begin{aligned} x_1 &\to x_1 \cosh r - x_2 \sinh r, \quad p_1 \to p_1 \cosh r + p_2 \sinh r, \\ x_2 &\to x_2 \cosh r - x_1 \sinh r, \quad p_2 \to p_1 \sinh r + p_2 \cosh r. \end{aligned} \tag{5.5}$$

Thus, the Wigner function of the TMSC state becomes

$$W_{A_1A_2}(\xi_1, \xi_2) = \frac{1}{4\pi^2} \exp\Bigg[-\frac{1}{2}\big((x_1 \cosh r - x_2 \sinh r - d)^2 + (p_1 \cosh r + p_2 \sinh r)^2 + (x_2 \cosh r - x_1 \sinh r - d)^2 + (p_1 \sinh r + p_2 \cosh r)^2\big)\Bigg]. \tag{5.6}$$

The Wigner function of the Fock state $|k\rangle$ is given by

$$W(q, p)_{|k\rangle} = \frac{(-1)^k}{2\pi} \exp\left(-\frac{q^2}{2} - \frac{p^2}{2}\right) L_k(q^2 + p^2), \tag{5.7}$$

which reduces to the Wigner function of the vacuum state for $k = 0$.

Probability of k-photon detection

In the next step, Fred mixes the vacuum mode F_0 with the mode A_2 of the TMSC state, obtained from Alice, using a beam splitter of transmittivity τ represented by the transformation matrix $B(\tau)$ (1.89). The Wigner function transforms as $W(\xi) \to W(B(\tau)^{-1}\xi)$. Thus, the transformation $\xi \to B(\tau)^{-1}\xi$

$$\begin{aligned} x_2 &\to \sqrt{\tau}x_2 - \sqrt{1-\tau}x_3, \quad p_2 \to \sqrt{\tau}p_2 - \sqrt{1-\tau}p_3, \\ x_3 &\to \sqrt{1-\tau}x_2 + \sqrt{\tau}x_3, \quad p_3 \to \sqrt{1-\tau}p_2 + \sqrt{\tau}p_3, \end{aligned} \tag{5.8}$$

yields a three mode entangled state whose Wigner function is described by

$$W_{A_1A_2'F_1}(\xi_1, \xi_2, \xi_3) = W'_{A_1A_2'}(x_1, p_1, x_2, p_2) W'_{F_1}(x_3, p_3)_{|0\rangle}. \tag{5.9}$$

After a successful photon subtraction, *i.e.*, when the POVM element $\Pi_k = |k\rangle\langle k|$ clicks, the unnormalized Wigner function of the k-PSTMSC state can be written as

$$W^k_{A_1A_2'}(\xi_1, \xi_2) = 4\pi \int dx_3 dp_3 \underbrace{W'_{A_1A_2}(x_1, p_1, x_2, p_2) W'_{|0\rangle}(x_3, p_3)}_{\text{Three mode entangled state}} \underbrace{W_{|k\rangle}(x_3, p_3)}_{\text{Projection on } |k\rangle\langle k|}. \tag{5.10}$$

As we shall see, we do not need to explicitly calculate the Wigner function of the k-PSTMSC state for the calculation of the probability and the covariance matrix. Here we compute the probability of k-photon detection and evaluate it using the multidimensional Gaussian integral. First, we integrate $W^k_{A_1A_2'}(\xi_1,\xi_2)$ with respect to the ξ variables, which yields the probability expression given by

$$\begin{aligned} P^k_{PS} &= \int dx_1 dp_1 dx_2 dp_2\, W^k_{A_1A_2'}(\xi_1,\xi_2), \\ &= 4\pi \int d^6\underline{\xi} W'_{A_1A_2}(x_1,p_1,x_2,p_2) W'_{|0\rangle}(x_3,p_3) W_{|k\rangle}(x_3,p_3), \end{aligned} \tag{5.11}$$

with $\underline{\xi} = (x_1,p_1,x_2,p_2,x_3,p_3)^T$. Using the generating function for the Laguerre polynomial

$$\partial^k_s \partial^k_t (e^{st+s(q+ip)-t(q-ip)})\big|_{s=t=0} = k! L_k(q^2+p^2), \tag{5.12}$$

the probability expression (5.17) can be written as

$$\begin{aligned} P^k_{PS} = 4\pi \partial^k_s \partial^k_t e^{st} \int d^6\underline{\xi} W'_{A_1A_2}(x_1,p_1,x_2,p_2) W'_{|0\rangle}(x_3,p_3) \frac{(-1)^k}{2\pi k!} \\ \times e^{\frac{-x_3^2-p_3^2}{2}} e^{st+s(x_3+ip_3)-t(x_3-ip_3)} \Big|_{s=t=0}. \end{aligned} \tag{5.13}$$

This substitution turns the integrand into a Gaussian integral, which can be recast as a multidimensional Gaussian integral as follows:

$$P^k_{PS} = \frac{(-1)^k}{4\pi^3} \frac{1}{k!} e^{-d^2}\, \partial^k_s \partial^k_t e^{st} \int d^6\underline{\xi} \exp\big(-\underline{\xi}^T M \underline{\xi} + N^T \underline{\xi}\big)\Big|_{s=t=0}, \tag{5.14}$$

with

$$M = \begin{pmatrix} m_1 \mathbb{I}_2 & m_4 \mathbb{Z}_2 & m_5 \mathbb{Z}_2 \\ m_4 \mathbb{Z}_2 & m_2 \mathbb{I}_2 & m_6 \mathbb{I}_2 \\ m_5 \mathbb{Z}_2 & m_6 \mathbb{I}_2 & m_3 \mathbb{I}_2 \end{pmatrix}, \quad N = \begin{pmatrix} -dn_1 \\ 0 \\ -dn_1\sqrt{T} \\ 0 \\ s-t+dn_1\sqrt{1-T} \\ i(s+t) \end{pmatrix}, \tag{5.15}$$

where $m_1 = -(1+2\alpha^2)/2$, $m_2 = -(1+2\alpha^2\tau)/2$, $m_3 = -(1+\alpha^2(1-\tau))$, $m_4 = \alpha\sqrt{(1+\alpha^2)\tau}$, $m_5 = -\alpha\sqrt{(1+\alpha^2)(1-\tau)}$, $m_6 = \alpha^2\sqrt{\tau(1-\tau)}$, $n_1 = \alpha - \sqrt{1+\alpha^2}$ and $\alpha = \sinh r$. This form facilitates the use of the multidimensional Gaussian integral formula

$$\int_{\mathbb{R}^n} \exp\big(-X^T M X + V^T X\big) dX = \sqrt{\frac{\pi^n}{\det M}} \exp\left(\frac{N^T M^{-1} N}{4}\right), \tag{5.16}$$

which enables us to obtain the desired expression without performing multiple integrations. Thus, the expression of the probability reduces to

$$P_{PS}^{k} = \frac{(-1)^k}{1+\alpha^2(1-\tau)}\frac{1}{k!}\exp\left[-\frac{d^2\left(1+2\alpha(\alpha+\sqrt{1+\alpha^2})\right)(1-\tau)}{4(1+\alpha^2(1-\tau))}\right] \times \partial_s^k\partial_t^k \exp(-Ast+Bs+Ct)|_{s=0,t=0}\,, \tag{5.17}$$

where $A = \frac{\alpha^2(1-\tau)}{1+\alpha^2(1-\tau)}$ and $B = -C = -\frac{d(\alpha+\sqrt{1+\alpha^2})\sqrt{1-\tau}}{2(1+\alpha^2(1-\tau))}$. Again using

$$\partial_s^k\partial_t^k \exp\left(-Ast+Bs+Ct\right)|_{s=0,t=0} = (-1)^k A^k k! L_k(\frac{BC}{A}), \tag{5.18}$$

the probability expression (5.17) can be brought in a closed form:

$$P_{PS}^{k} = \frac{A^k}{1+\alpha^2(1-\tau)}\exp\left[-\frac{d^2\left(1+2\alpha(\alpha+\sqrt{1+\alpha^2})\right)(1-\tau)}{4(1+\alpha^2(1-\tau))}\right]L_k(D), \tag{5.19}$$

with $D = \frac{CB}{A} = -\frac{d^2\left(\alpha+\sqrt{1+\alpha^2}\right)^2}{4\alpha^2(1+\alpha^2(1-\tau))}$. The probability of photon subtraction attains a maximum at a certain value of transmittivity τ and both the maximum probability and the corresponding transmittivity τ depends on the number of photon subtracted as shown in Fig. 5.2.

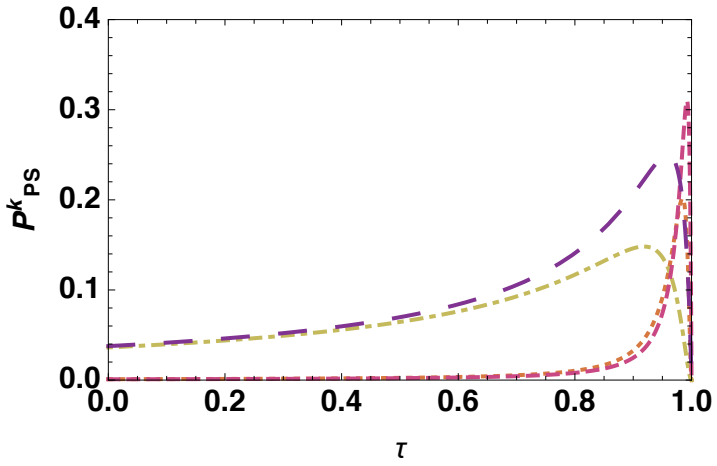


Figure 5.2: Probability of photon subtraction versus BS transmittance τ. Different lines represent 1-PSTMSC (red dashed), 2-PSTMSC (orange dotted), 1-PSTMSV (purple large dashed) and 2-PSTMSV (yellow dash dotted). We have set variance as $V_A = 50$ and displacement as $d = 2$.

Covariance matrix of the k-PSTMSC state

The normalized Wigner function of the k-PSTMSC state is

$$\widetilde{W}^{k}_{A_1A_2'}(\xi_1,\xi_2) = \left(P^{k}_{PS}\right)^{-1} W^{k}_{A_1A_2'}(\xi_1,\xi_2), \tag{5.20}$$

Using the Wigner function of the k-PSTMSC state, the averages of the symmetrically ordered operators can be easily evaluated by using parametric differentiation technique:

$$\begin{aligned}\langle\{\hat{x_1}^{r_1}\hat{p_1}^{s_1}\hat{x_2}^{r_2}\hat{p_2}^{s_2}\}_{\text{sym}}\rangle &= \int d^4\xi x_1^{r_1}p_1^{s_1}x_2^{r_2}p_2^{s_2}\widetilde{W}^{k}_{A_1A_2'}(\xi_1,\xi_2),\\ &= \partial^{r_1}_{u_1}\partial^{s_1}_{v_1}\partial^{r_2}_{u_2}\partial^{s_2}_{v_2}\int d^4\xi\widetilde{W}^{k}_{A_1A_2'}(\xi_1,\xi_2)e^{x_1u_1+p_1v_1+x_2u_2+p_2v_2}\Big|_{u_1=v_1=u_2=v_2=0},\end{aligned} \tag{5.21}$$

where the symbol $\{\}_{\text{sym}}$ denotes symmetrically ordered operators. We follow the same approach as in the probability calculations to evaluate the above expression. By suitably choosing the values of r_1, s_1, r_2, s_2 in Eq. (5.21), all the elements of the covariance matrix can be calculated. The averages of all the quantities appearing in the covariance matrix has been shown in Appendix B.0.3. The covariance matrix takes the following form:

$$\Sigma_{A_1A_2'} = \begin{pmatrix} \gamma_A^x & 0 & \gamma_C^x & 0\\ 0 & \gamma_A^p & 0 & \gamma_C^p\\ \gamma_C^x & 0 & \gamma_B^x & 0\\ 0 & \gamma_C^p & 0 & \gamma_B^p \end{pmatrix}, \tag{5.22}$$

where $(\Sigma_{A_1A_2'})_{ij} = \frac{1}{2}\langle\{\hat{\xi}_i,\hat{\xi}_j\}\rangle - \langle\hat{\xi}_i\rangle\langle\hat{\xi}_j\rangle$. The covariance matrix can also be obtained in the Wigner characteristic function representation (see Appendix B).

5.2.3 CV-MDI-QKD using a PSTMSC state

Since we consider entanglement based CV-MDI-QKD with the PSTMSC state as a resource state, we have an additional parameter in our protocol resulting from the fact that our starting point is a coherent state rather than the vacuum state. Here we explain the schematic of the protocol tailored for PSTMSC state as illustrated in Fig. 5.3. The protocol consists of the following steps.

Step 1: Alice generates a TMSC state in mode A_1A_2 with variance V_A.

Step 2: In the next step, Alice sends one of her modes A_2 to Fred, an untrusted party, who performs k photon subtraction operation on the TMSC state. After a successful photon subtraction, the A_2 mode transforms to A_2', which is transmitted to Charlie through the quantum channel.

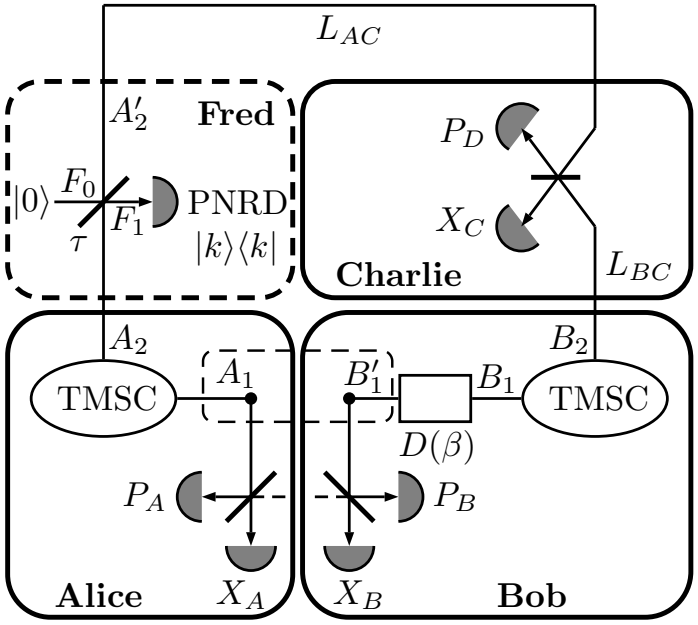


Figure 5.3: Schematic representation of the CV-MDI-QKD tailored for the PSTMSC state. Charlie combines the two modes sent by Alice and Bob on a 50:50 beam splitter and performs homodyne measurements of the x quadrature of the output mode C and the p quadrature of the output mode D. After displacement of mode B_1 by Bob based on results announced by Charlie, the modes A_1 and B_1' become correlated. Of the four parties, Alice, Bob, Charlie, and Fred, the latter two are untrusted.

Step 3: Bob also generates a TMSC state in mode B_1B_2 with variance $V_B = V_A$ and transmits the mode B_2 to Charlie.
Step 4: Charlie interferes the two modes A_2' and B_2 received from Alice and Bob, respectively, using a 50:50 BS and obtains the output modes C and D. He then measures the x quadrature of C and the p quadrature of D using homodyne detection. Then he publicly announces the results of the measurements.
Step 5: Bob then applies the displacement operation $D(\alpha)$ as defined in Section 5.2.1, which transforms his mode B_1 to B_1'. As a result, the two modes A_1 and B_1' get entangled. Thereafter, both Alice and Bob implement heterodyne detection on the modes A_1 and B_1' respectively and obtain correlated results.
Step 6: In the final step, Alice and Bob carry out information reconciliation and privacy amplification to distill a secure key from the correlated results.

5.2.4 Special cases

One of the specialties of our study of CV-MDI-QKD using the PSTMSC state is its generality. As we show below, several of the previous results in CV-MDI-QKD can be obtained as a special case of our results.

In the first special case, we set $k = 0$ and Fred's BS transmittivity $\tau = 1$ in the covariance matrix of the PSTMSC state. This yields the covariance matrix of the TMSC state, which is identical to the TMSV state. Thus, the results obtained for the aforementioned case reduce to the previous results obtained with the TMSV state [210].

In the second special case, we set $d = 0 \; \forall \; k \neq 0$ in the covariance matrix of the PSTMSC state. This yields the covariance matrix of the PSTMSV state, which has been studied in several CV-MDI-QKD protocols [32, 220]. This enables us to verify the previous results for the PSTMSV state as a special case of ours. In particular, we find that the results reported in [221] are incorrect. Several studies have also shown that a non-Gaussian post-selection of the data is equivalent to the PSTMSV state [218, 222].

Since the previous results with either the PSTMSV state or the non-Gaussian post-selection are subsumed in our CV-MDI-QKD using PSTMSC state, our study allows us to verify, compare and interpolate between various previous results available in the literature.

5.3 Eavesdropping, channel parameters and secure key rate

As discussed in the above section, two quantum channels and one classical channel are required in our CV-MDI-QKD using PSTMSC state. We consider that the entangling cloner attack is performed by an eavesdropper, Eve, on each of the quantum channels [223]. The most general attacks, known as two mode attacks, correspond to the case, where the attacks are correlated with each other [205, 224]. However, in this work, we assume that the two channels are non-interacting and well separated, and thus the correlated attack is reduced to independent one-mode collective attacks on each channel. Holevo bound, χ_{BE}, provides the upper bound of the information gained by Eve under the aforementioned strategy. We again reiterate that we have not considered a general attack.

We now move on to mathematically characterize various channel parameters which is used to calculate the Holevo bound and the secret key rate. We define the transmittance of the two channels T_A and T_B as

$$T_A = 10^{-l\frac{L_{AC}}{10}} \quad \text{and} \quad T_B = 10^{-l\frac{L_{BC}}{10}}, \tag{5.23}$$

where $l = 0.2$dB/km is the channel loss, L_{AC} is the total transmission distance between Alice and Charlie, and L_{BC} is the total transmission distance between Bob and Charlie. We consider the following two cases in our further analysis:
The symmetric case: This case assumes that Charlie is located midway between Alice and Bob, which implies $L_{AC} = L_{BC}$. The total transmission length then becomes $L = 2L_{AC} = 2L_{BC}$ with $T_A = T_B$.
The asymmetric case: This case assumes that Bob and Charlie are at the same place, *i.e.*, $L_{BC} = 0$. The total transmission length, in this case, is given by $L = L_{AC} = L_{AB}$ with $T_B = 1$, where L_{AB} is the total transmission distance between Alice and Bob.

We define a normalized parameter T, which depends on the channel parameter T_A and the gain of Bob's displacement operation g, as follows:

$$T = \frac{T_A g^2}{2}. \tag{5.24}$$

The total channel added noise is then given by

$$\chi_{line} = \frac{1-T}{T} + \varepsilon^{th}, \tag{5.25}$$

where ε^{th} is the thermal excess noise in the equivalent one-way protocol, which can be determined using the following equation [32, 210]:

$$\varepsilon^{th} = \frac{T_B}{T_A}(\chi_B - 1) + \chi_A + 1 + \frac{T_B}{T_A}\left(\sqrt{\frac{2}{T_B g^2}}\sqrt{V_B - 1} - \sqrt{V_B + 1}\right)^2, \tag{5.26}$$

with

$$\chi_A = \frac{1-T_A}{T_A} + \epsilon_A^{th},\ \chi_B = \frac{1-T_B}{T_B} + \epsilon_B^{th}, \tag{5.27}$$

where ε_A^{th} and ε_B^{th} represent the thermal excess noise in the quantum channels between Alice-Charlie and Bob-Charlie. The thermal excess noise ε^{th} in the equivalent one-way protocol is minimized with respect to the gain. The minimized thermal noise is given by

$$\varepsilon^{th} = \frac{T_B}{T_A}(\varepsilon_B - 2) + \varepsilon_A + \frac{2}{T_A}, \tag{5.28}$$

and the corresponding gain is

$$g = \sqrt{\frac{2(V_A - 1)}{T_B(V_A + 1)}}. \tag{5.29}$$

We consider that the homodyne detectors used by Charlie are imperfect, and the corresponding noise is given by

$$\chi_{homo} = \frac{\nu_{el} + 1 - \eta}{\eta}, \tag{5.30}$$

where ν_{el} represents the variance of the electronic noise and η represents the detector's efficiency. Therefore, the total noise added by the channel and the detectors is given by

$$\chi_{tot} = \chi_{line} + \frac{2\chi_{homo}}{T_A}. \tag{5.31}$$

We provide numerical results in the following sections assuming Charlie's homodyne detectors to be perfect, *i.e.*, $\chi_{homo} = 0$, except in Sec. 5.4.4, where we explore the effect of the noisy detectors on the secure key rate and the total transmission length. Assuming Eve performs a one-mode collective attack on each of the quantum channels, the secure key rate is given by

$$K = P_{PS}^{k} \left(\beta I_{AB} - \chi_{BE}\right), \tag{5.32}$$

where β is the reverse reconciliation efficiency, I_{AB} is the mutual information between Alice and Bob, and χ_{BE} is the Holevo bound between Bob and Eve, which represents the maximum amount of information Eve can gain about Bob's outcome. In the numerical simulations, we optimize various parameters for maximum secure key rate K, while keeping the others fixed.

The state $\rho_{A_1B_1'}$ obtained after step 5 of the protocol, given in Sec. 5.2.3, can be described by the following covariance matrix:

$$\begin{aligned}\Sigma_{A_1B_1'} &= \begin{pmatrix} \gamma_A^x & 0 & \sqrt{T}\gamma_C^x & 0 \\ 0 & \gamma_A^p & 0 & \sqrt{T}\gamma_C^p \\ \sqrt{T}\gamma_C^x & 0 & T(\gamma_B^x + \chi_{tot}) & 0 \\ 0 & \sqrt{T}\gamma_C^p & 0 & T(\gamma_B^p + \chi_{tot}) \end{pmatrix}, \\ &= \begin{pmatrix} a_1 & 0 & c_1 & 0 \\ 0 & a_2 & 0 & c_2 \\ c_1 & 0 & b_1 & 0 \\ 0 & c_2 & 0 & b_2 \end{pmatrix}.\end{aligned} \tag{5.33}$$

We then calculate the mutual information between Alice and Bob, I_{AB} as follows [225]:

$$I_{AB} = \frac{1}{2}\log_2\left(\frac{\Sigma^x_{A_1M}}{\Sigma^x_{A_1M|B_{1M}'}}\right) + \frac{1}{2}\log_2\left(\frac{\Sigma^p_{A_1M}}{\Sigma^p_{A_1M|B_{1M}'}}\right), \tag{5.34}$$

with

$$\Sigma^{\xi}_{A_1M} = \frac{\Sigma^{\xi}_{A_1} + 1}{2}, \tag{5.35}$$

where $\xi \in \{x, p\}$ and $\Sigma^{\xi}_{A_M|B_M}$ stands for the conditional variance of Alice's outcome conditioned on Bob's outcome of his heterodyne measurement, which is given as,

$$\Sigma^{\xi}_{A_1M|B_{1M}'} = \frac{\Sigma^{\xi}_{A_1|B_1'} + 1}{2}, \tag{5.36}$$

where $\Sigma^{\xi}_{A_1|B_1'}$ is evaluated from the matrix,

$$\begin{aligned}\Sigma_{A_1|B_1'} =&\Sigma_{A_1} - \Sigma_C \left(\Sigma_{B_1'} + I_2\right)^{-1} (\Sigma_C)^T, \\ =&\begin{pmatrix} a_1 - \frac{c_1^2}{b_1+1} & 0 \\ 0 & a_2 - \frac{c_2^2}{b_2+1} \end{pmatrix}.\end{aligned} \tag{5.37}$$

We now evaluate the upper bound on the information gained by Eve. To this end, we assume that she has got access to Fred's mode F, and thus her state can be represented by ρ_{EF}. We also assume that she can purify the state $\rho_{A_1B_1'EF}$. The Holevo bound χ_{BE} between Bob and Eve can be obtained as

$$\begin{aligned}\chi_{BE} &= S(\rho_{EF}) - \int dm_B p(m_B) S(\rho_{EF}^{m_B}) \\ &= S(\rho_{A_1B_1'}) - S(\rho_{A_1|B_1'}^{m_{B_1'}}),\end{aligned} \tag{5.38}$$

where $S(\rho)$ represents the von-Neumann entropy of the state ρ, m_B is the measurement outcomes of Bob with probability density $p(m_B)$, $\rho_{A_1|B_1'}^{m_{B_1'}}$ is the state of Alice's mode A_1 conditioned on Bob's outcome on mode B_1' and $\rho_{EF}^{m_B}$ is the Eve's state conditioned on Bob's outcomes.

The state $\rho_{A_1B_1'}$ is described by the covariance matrix $\Sigma_{A_1B_1'}$ as given in Eq. (5.33), whereas state $\rho_{A_1|B_1'}^{m_{B_1'}}$ is described by the covariance matrix $\Sigma_{A_1|B_1'}^{m_{B_1'}}$ as given in Eq. (5.37), since the covariance matrix does not depend on the measurement result m. The von-Neumann entropy $S(\rho_{A_1B_1'})$ and $S(\rho_{A_1|B_1'}^{m_{B_1'}})$ are given as

$$S(\rho_{A_1B_1'}) = G\left[\frac{\lambda_1 - 1}{2}\right] + G\left[\frac{\lambda_2 - 1}{2}\right], \tag{5.39}$$

and

$$S(\rho_{A_1|B_1'}^{m_{B_1'}}) = G\left[\frac{\lambda_3 - 1}{2}\right], \tag{5.40}$$

where λ_1, λ_2 are doubly degenerate symplectic eigenvalues of $\Sigma_{A_1B_1'}$, λ_3 is the symplectic eigenvalue of $\Sigma_{A_1|B_1'}^{m_{B_1'}}$, and

$$G(x) = (x+1)\log_2(x+1) - x\log_2 x, \tag{5.41}$$

is the von-Neumann entropy of the thermal state. The symplectic eigenvalues λ_1 and λ_2 evaluates as

$$\lambda_{1,2} = \frac{1}{\sqrt{2}}\left[I_1 + I_2 + 2I_3 \pm \sqrt{(I_1 + I_2 + 2I_3)^2 - 4I_4}\right]^{1/2} \tag{5.42}$$

where $I_1 = a_1 a_2$, $I_2 = b_1 b_2$, $I_3 = c_1 c_2$, and $I_4 = (a_1 b_1 - c_1^2)(a_2 b_2 - c_2^2)$, while the symplectic eigenvalue λ_3 evaluates as

$$\lambda_3 = \sqrt{\left(a_1 - \frac{c_1^2}{b_1 + 1}\right)\left(a_2 - \frac{c_2^2}{b_2 + 1}\right)}. \tag{5.43}$$

5.4 Simulation results

After describing the protocol in detail, we now discuss numerical results in this section for both the symmetric case and the asymmetric case. Here we perform optimization of a few parameters, while keeping the others fixed, to obtain maximum secure key rate.

It has already been shown in [32] that transmission distances for secure key rate in CV-MDI-QKD can be enhanced by using photon subtraction on a TMSV state. Their results for the asymmetric case show that one can reach up to distances of approximately $60 - 70$ km for PSTMSV state, whereas only $40 - 50$ km is achievable using a TMSV state. We show in the following sections that the PSTMSC state can further enhance the performance compared to the PSTMSV state.

5.4.1 Effect of displacement on distance for a fixed key rate

We first study the variation of transmission distances as a function of displacement for several fixed values of the key rate. We show the results for the symmetric and asymmetric cases in Figs. 5.4 and 5.5, respectively. The results for the symmetric case reveal that the PSTMSC state improves the transmission distance by 0.5 km compared to the PSTMSV state for a given secure key rate of 10^{-4} bits per pulse. However, in the asymmetric case for the same key rate, an increment of approximately 10 km is observed. Thus, the above results imply that transmission distance increases with coherence, and the effect is much more visible in the asymmetric case. However, we also notice that a larger coherence has a negative impact on the transmission distance. For our further discussions, we set coherence $d = 2$, which maximizes the transmission distances. Furthermore, the value of Fred's beam splitter transmittivity τ used in the numerical simulations maximizes the secure key rate (5.32), and not the photon subtraction probability (5.19).

5.4.2 Effect of Variance on key rate for a fixed distance

Along with the coherence and photon subtraction transmittivity τ, the secure key rate also depends on the variance V_A of the TMSC state used by Alice and Bob. Figures 5.6

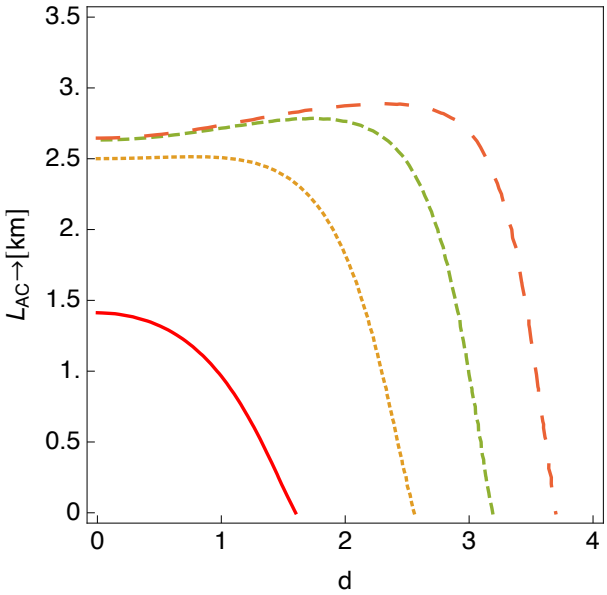


Figure 5.4: Plots of L_{AC} versus vacuum state displacement d for different values of the secret key for the symmetric case for 1-PSTMSC. The different values of the fixed secret key rate are $K = 10^{-1}$ (red solid line), $K = 10^{-2}$ (yellow dotted line), $K = 10^{-3}$ (green short-dashed line) and $K = 10^{-4}$ (orange long-dashed line). The total transmission length is $L = 2L_{AC}$. Other parameters are set as follows: $V_A = 50$, $\eta = 1$, $\varepsilon_A^{th} = 0.002 = \varepsilon_B^{th}$ and $\beta = 96\%$.

and 5.7 show the plots of the secure key rate as a function of V_A for the symmetric and the asymmetric cases, respectively.

The results show that the TMSV state performs better than all the other states, including PSTMSC for a fixed transmission length $L_{AB} = 4$ km in the symmetric case. Further, the PSTMSC state yields a lower key rate than the PSTMSV state for a given transmission distance and variance. For the asymmetric case with length fixed as $L_{AB} = L_{AC} = 20$ km, the TMSV state still performs better than the other states. However, the other states, including the PSTMSV state and the PSTMSC state perform better than the TMSV state for variance larger than 250. We also notice that the PSTMSC state yields a higher secure key rate than the PSTMSV state for small variances. In order to optimize the secure key rate for large transmission distances, a small value of variance, $V_A = 50$, is enough.

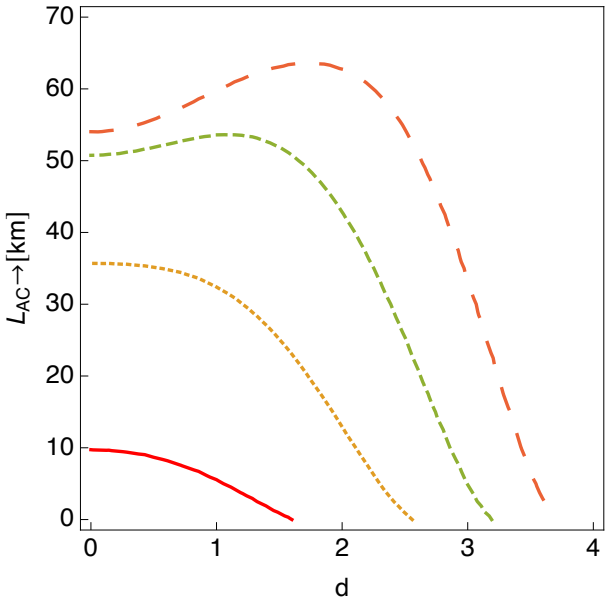


Figure 5.5: Plots of L_{AC} versus vacuum state displacement d for different values of the fixed secret key for the extreme asymmetric case for 1-PSTMSC. The different values of the fixed secret key rates are $K = 10^{-1}$ (red solid line), $K = 10^{-2}$ (yellow dotted line), $K = 10^{-3}$ (green short-dashed line) and $K = 10^{-4}$ (orange long-dashed line). The total transmission length is $L = L_{AC}$ and other parameters are set as follows: $V_A = 50$, $\varepsilon_A^{th} = 0.002 = \varepsilon_B^{th}$ and $\beta = 96\%$.

5.4.3 Effect of Length on the secure key rate

In the previous sections, we have determined approximate values of τ, d and V_A that maximize the transmission lengths for the PSTMSC state. We now plot the secure key rate as a function of L_{AC} in Figs. 5.8 and 5.9 for the symmetric and asymmetric cases, respectively. The total transmission length is $L_{AB} = 2L_{AC}$ in the symmetric case, whereas the total transmission length is $L_{AB} = L_{AC}$ in the asymmetric case.

The symmetric case results show that the TMSV state yields a higher key rate than any other state for any transmission length. Although the maximum key rate offered by the PSTMSV state is more than the PSTMSC state, the latter allows a longer transmission length than the PSTMSV state. The benefit of using the PSTMSC state is visible in the asymmetric case, where it performs significantly better than the others by approximately 10 km at the price of a reduction in the secure key rate. The above results suggest that a small amount of coherence can increase the transmission distances. Although the maximum achievable key rate is less for the PSTMSC state, the distances over which QKD can be performed is substantially increased for this state. Thus, the

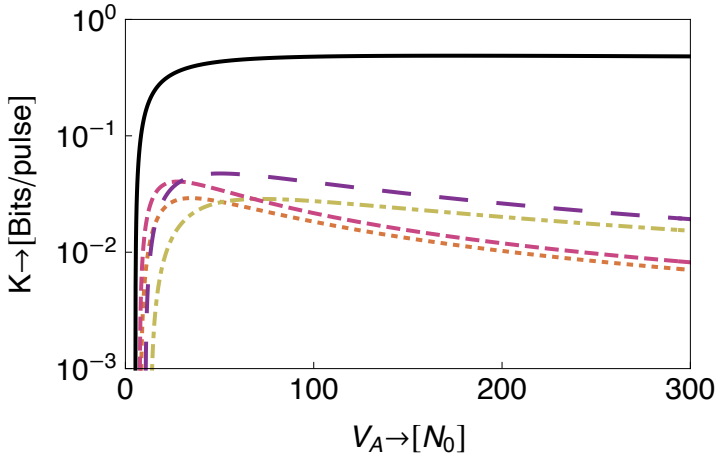


Figure 5.6: Secret key rate versus V_A in the symmetric case where $L_{AC} = L_{BC} = 2$ km and total transmission distance $L = 2L_{AC}$. Different lines represent 1-PSTMSC (red dashed), 2-PSTMSC (orange dotted), 1-PSTMSV (purple large dashed), 2-PSTMSV (yellow dash dotted) and TMSV (black solid). Other parameters are set as follows: $\tau = 0.9$, $\varepsilon_A^{th} = 0.002 = \varepsilon_B^{th}$, $\beta = 96\%$ and displacement $d = 2$.

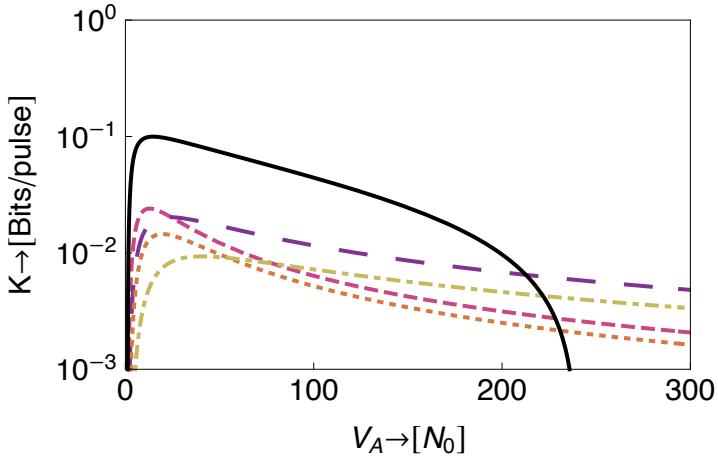


Figure 5.7: Secret key rate as a function of V_A in the asymmetric case where $L_{AC} = 20$ km, $L_{BC} = 0$ and total transmission distance $L = L_{AC}$. Different lines represent 1-PSTMSC (red dashed), 2-PSTMSC (orange dotted), 1-PSTMSV (purple large dashed), 2-PSTMSV (yellow dash dotted) and TMSV (black solid). Other parameters are set as follows: $\tau = 0.9$, $\varepsilon_A^{th} = 0.002 = \varepsilon_B^{th}$, $\beta = 96\%$ and displacement $d = 2$.

PSTMSC state enhances the performance of CV-MDI-QKD protocol compared to the PSTMSV state. Further, our state is more accessible to experimentalists as it is easier

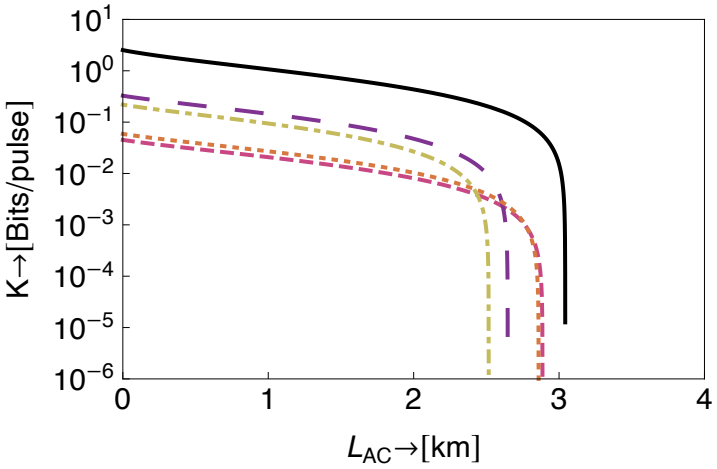


Figure 5.8: Secret key rate as a function of L_{AC} in the symmetric case where $L_{AC} = L_{BC}$, $V_A = 50$ and total transmission distance $L = 2L_{AC}$. Different lines represent 1-PSTMSC (red dashed), 2-PSTMSC (orange dotted), 1-PSTMSV (purple large dashed), 2-PSTMSV (yellow dash dotted) and TMSV (black solid). Other parameters are set as follows: $\tau = 0.9$, $\varepsilon_A^{th} = 0.002 = \varepsilon_B^{th}$, $\beta = 96\%$ and coherence $d = 2$.

to prepare squeezed coherent states as compared to squeezed vacuum states.

5.4.4 Noisy homodyne detectors

In this section, we discuss the case where Charlie's homodyne detectors are imperfect, *i.e.*, $\chi_{homo} \neq 0$. Figures 5.10 and 5.11 show that the PSTMSC state is more resilient against imperfect detectors as compared to the PSTMSV state. In order to maintain transmission distances upto 30 km, the detector's efficiency needs to be close to unity. Even for a small detector inefficiency of $\eta = 0.995$ and $\nu_{el} = 0.01$, we observe that the maximum transmission length drops to approximately 28 km. Moreover, detector's efficiency as low as $\eta = 0.86$ can yield secure key for small transmission lengths.

5.5 Conclusion

In this chapter, the PSTMSC state as a resource state for CV-MDI-QKD protocol was considered and it was shown that it can further improve the transmission distances as compared to the PSTMSV state. To compute the secret key rate, we derive the covariance matrix for the PSTMSC state in the phase space formalism. For the asymmetric case and perfect homodyne detectors, we observe that transmission length of 68 km

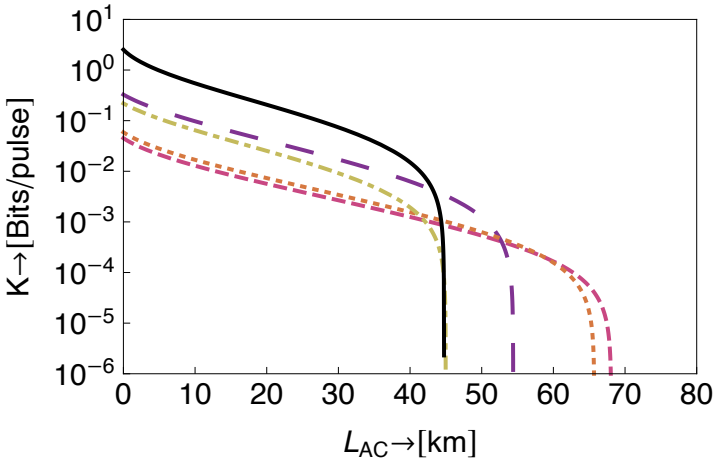


Figure 5.9: Secret key rate as a function of L_{AC} in the asymmetric case where $L_{BC} = 0$, $V_A = 50$ and total transmission distance $L = L_{AC}$. Different lines represent 1-PSTMSC (red dashed), 2-PSTMSC (orange dotted), 1-PSTMSV (purple large dashed), 2-PSTMSV (yellow dash dotted) and TMSV (black solid). Other parameters are set as follows: $\tau = 0.9$, $\varepsilon_A^{th} = 0.002 = \varepsilon_B^{th}$, $\beta = 96\%$ and displacement $d = 2$.

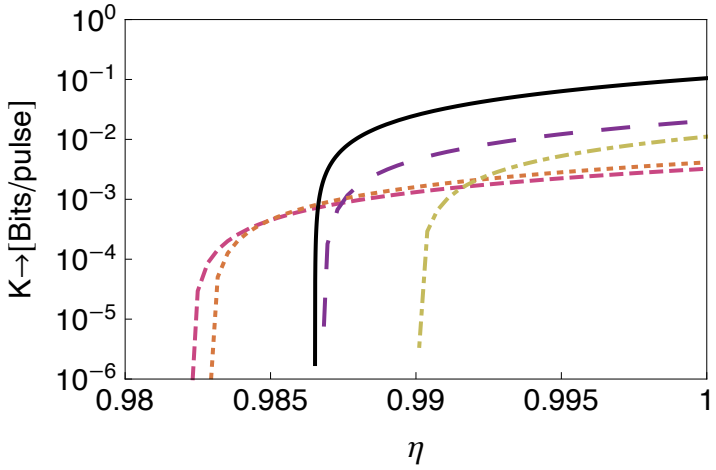


Figure 5.10: Secret key rate as a function of η in the asymmetric case where $L_{AC} = 20$ km and $V_A = 50$ with total transmission distance $L = L_{AC}$. Different lines represent 1-PSTMSC (red dashed), 2-PSTMSC (orange dotted), 1-PSTMSV (purple large dashed), 2-PSTMSV (yellow dash dotted) and TMSV (black solid). Other parameters are set as follows: $\tau = 0.9$, $\varepsilon_A^{th} = 0.002 = \varepsilon_B^{th}$, $\beta = 96\%$, displacement $d = 2$ and $\nu_{el} = 0.01$.

can be achieved for a small amount of coherence $d = 2$ in the PSTMSC state, which is significantly larger than the achievable distance with the PSTMSV state. However,

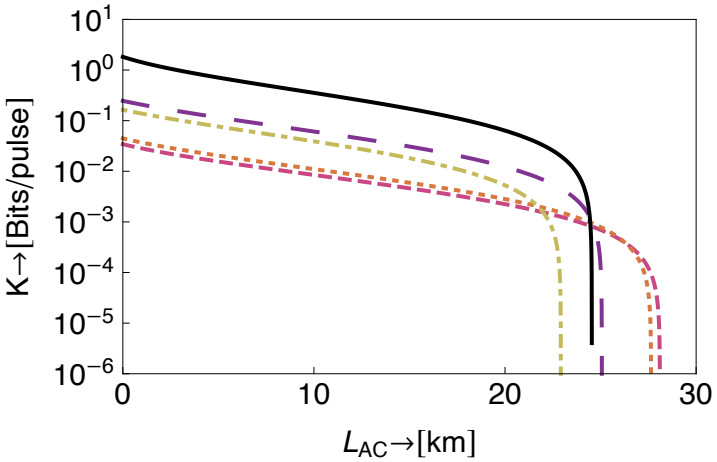


Figure 5.11: Secret key rate as a function of L_{AC} in the asymmetric case where $V_A = 50$ and total transmission distance $L = L_{AC}$. Different lines represent 1-PSTMSC (red dashed), 2-PSTMSC (orange dotted), 1-PSTMSV (purple large dashed), 2-PSTMSV (yellow dash dotted) and TMSV (black solid). Other parameters are set as follows: $\tau = 0.9$, $\varepsilon_A^{th} = 0.002 = \varepsilon_B^{th}$, $\beta = 96\%$, displacement $d = 2$ and detector efficiency $\eta = 0.995$.

in the symmetric case, no such improvement in transmission distance is observed. The results also show that transmission length of up to 28 km can be achieved using the PSTMSC state for imperfect homodyne detection, which renders our QKD protocol preferable for a small city. Further, the PSTMSC state outperforms the PSTMSV state for the imperfect detectors, which demonstrates the superiority of our PSTMSC state based CV-MDI-QKD protocol. Since PSTMSC states can be generated by feeding coherent states, which are readily available from well phase-stabilized lasers, in the down-converter, it is easier to implement our CV-MDI-QKD protocol as compared to CV-MDI-QKD protocol based on PSTMSV states, where one needs to deal with the vacuum states. Moreover, our QKD protocol is a generalization of many of the previous CV-MDI-QKD protocols. It is important to note that various non-Gaussian operations like photon addition, subtraction, and catalysis on the TMSV state have been considered in various QIP tasks; however, these non-Gaussian operations on the TMSC state largely remain unexplored. We expect that the covariance matrix calculated here will be useful in the characterization of the PSTMSC state and will find applications in various QIP tasks. The results of this chapter are published in Phys. Rev. A **100**, 052329 (2019).

5. Coherence assisted non-Gaussian measurement device independent quantum key distribution

Chapter 6

On-demand quantum key distribution using superconducting rings with a mesoscopic Josephson junction

6.1 Introduction

In this chapter, we propose a CV-QKD scheme based on superconducting rings with a Josephson junction. As noted in Chapter 5, the practical implementations of QKD schemes are largely based on light devices [77, 226, 227, 228, 229]. In the prepare and measure version of CV-QKD, Bob is required to measure the state immediately after receiving as quantum states of optical systems cannot be stored for long. Thus, the key generated has to be stored, and it is open to stealing attacks during the storage period. To prevent this, we present a novel CV-QKD scheme where Bob is not required to measure the state immediately after receiving it. In this scheme, Bob stores the states and measures them only when the key is required. Afterwards, Alice and Bob employ classical communication and post-processing operations to generate the key. This unique feature renders our CV-QKD scheme more secure and eventually more practical. The proposed CV-QKD scheme is based on superconducting rings with a Josephson junction [230, 231, 232] also known as rf-SQUIDs. We represent this system using the charge operator Q and total flux operator Φ', which have continuous eigenvalues, and therefore, is an example of CV systems. It has been shown that persistent currents can flow in such systems at sufficiently low temperatures [233, 234] making it is possible to engineer extremely long lived coherent states under no-dissipation conditions [235, 236, 237], which can be employed to carry out QKD.

The first step in the scheme is the preparation of Gaussian-modulated coherent

states of the rf-SQUID. These encoded states are then transferred to Bob, who stores them in a no-dissipation condition. These encoded states can be transferred to Bob in several ways and in principle over large distances. For instance, Alice can dip the squid arrays with encoded states in liquid helium, pack them in a suitcase, and send them to another continent via a flight. Now Bob measures the state whenever the key is required. During storage, the states evolve under the system Hamiltonian. Owing to the presence of a nonlinear term in the Hamiltonian, collapse and revival phenomena of the state are observed. In view of this, we provide two distinct measurement schemes that Bob can perform to generate the key. In the first scheme, measurement is performed at arbitrary times, while in the second scheme, measurement is performed at specific times. The second scheme requires Alice and Bob to share a clock along with the exact time of the generation of states indicated on the rf-SQUID. The first and second measurement schemes yield a secure key rate of 0.20 bits and 0.50 bits, respectively. Under the assumption of individual attacks, the scheme turns out to be secure. Thus we have provided a CV-QKD scheme using a non-photonic system with a new feature of storing the encoded states. We name our scheme as on-demand QKD, since the QKD can be performed at any time after the state has been transferred. Furthermore, our scheme can be experimentally realized using existing superconducting technologies.

This chapter is organized as follows. In Sec. 6.2.1, we review CV-QKD using coherent states, while in Sec. 6.2.2, we introduce superconducting rings with a mesoscopic Josephson junction in details. In Secs. 6.2.3 and 6.2.4, we detail the preparation and evolution of a coherent state on a rf-SQUID. In Sec. 6.3, we describe our CV-QKD scheme, while in Sec. 6.4, we provide security proof. Finally, in Sec. 6.5, we provides some concluding remarks.

6.2 Background

In this section, we briefly review CV-QKD using coherent states and then discuss the preparation and evolution of a coherent state on a rf-SQUID.

6.2.1 Coherent state based CV-QKD

Here we briefly outline the coherent state based CV-QKD scheme as developed by Grosshans *et al.* [109]. In this scheme, two parties Alice and Bob want to establish a shared secret key. In the first step, Alice generates two random real numbers x_A and p_A from two independent Gaussian distributions. Each Gaussian distribution has variance $V_A N_0$, where $N_0 = 1$ is the vacuum noise variance. She then prepares the coherent state $|x_A + ip_A\rangle$ and transmits it to Bob through an insecure quantum channel

with Gaussian and white noise. After obtaining the state, Bob randomly performs the homodyne measurement of either the $\hat{x}$ quadrature or the $\hat{p}$ quadrature.

Bob communicates his measurement quadrature to Alice through a classically authenticated channel. Alice keeps the random number corresponding to the measured quadrature, while discards the other. Alice and Bob repeat the overall process many times to obtain the raw key. Thereafter, a sliced reconciliation scheme [189] may be used to transform the raw key into errorless bit strings. In the end, a secure key can be distilled from the errorless bit strings by performing a privacy amplification protocol.

Since the noise is white and has Gaussian statistics, the optimum information rate between Alice and Bob can be evaluated using the Shannon formula [238]. If Σ_B is the signal-to-noise ratio (SNR) as measured by Bob, then the optimum information rate is given by

$$I(A:B) = \frac{1}{2}\log_2(1+\Sigma_B). \tag{6.1}$$

Consider an eavesdropper, called Eve, who attempts to obtain information by manipulating the signal in the quantum channel. A secure key can be distilled only if the optimum information rate between Alice and Bob $I(A:B)$ exceeds the optimum information rate between Alice and Eve $I(A:E)$. This can be mathematically represented as

$$r_{\text{min}} = I(A:B) - I(A:E) > 0, \tag{6.2}$$

where r_{min} is the minimum rate at which a secure key can be distilled.

We evaluate the maximum amount of information that Eve can gain about Alice's key. For this purpose, we consider that Eve employs the best strategy possible. If the insecure quantum channel between Alice and Bob has transmissivity η, then she captures a fraction $1-\eta$ of the signal and let pass the remaining fraction η to Bob through her own lossless channel. This strategy enables her to obtain the maximum amount of information about Alice's key.

Let χN_0 be the amount of noise added in Bob's signal, then $\chi^{-1}N_0$ is the minimum noise that gets added in Eve's signal, where $\chi = (1-\eta)/\eta$ [239]. The above statement is another form of no-cloning theorem, and thus can also address the security of the QKD scheme when individual attacks are performed by Eve. For the coherent state based QKD scheme, the total variance of any quadrature of the state, leaving Alice's lab, is $VN_0 = V_A N_0 + N_0$. Thus, we find that

$$1+\Sigma_B = \frac{V+\chi}{1+\chi}, \quad 1+\Sigma_E = \frac{V+1/\chi}{1+1/\chi}. \tag{6.3}$$

Using the above expressions, the secret key rate (6.2) evaluates to

$$\begin{aligned} r_{\text{min}} &= \frac{1}{2}\log_2(1+\Sigma_B) - \frac{1}{2}\log_2(1+\Sigma_E), \\ &= \frac{1}{2}\log_2\left(\frac{V+\chi}{1+V\chi}\right). \end{aligned} \tag{6.4}$$

From the above equation, a secure key can be obtained if $\chi < 1$ or $\eta > \frac{1}{2}$. To put it in other words, we can successfully obtain a secure key in principle as long as the transmission efficiency of the Alice-Bob channel is greater than 50%.

6.2.2 Superconducting ring with a junction (rf-SQUID)

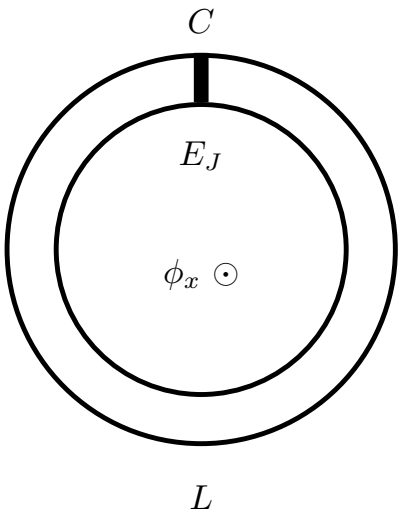


Figure 6.1: A superconducting ring of inductance L containing a mesoscopic Josephson junction with capacitance C. The Josephson coupling constant is E_J and ϕ_x is the external flux.

Here we provide a brief background of superconducting rings containing a mesoscopic Josephson junction, also called rf-SQUIDs. We describe the generation of coherent states [236, 237] and their evolution under the rf-SQUID Hamiltonian.

We consider a superconducting ring of inductance L containing a Josephson junction with capacitance C as shown in Fig. 6.1. Let E_J be the Josephson coupling constant and an external flux ϕ_x is applied on the ring, then the Hamiltonian for the junction is given by ($\hbar = k_B = c = 1$),

$$H = \frac{Q^2}{2C} + \frac{(\Phi' - \phi_x)^2}{2L} + E_J(1-\cos\theta). \tag{6.5}$$

Here Q represents the charge operator across the junction, and Φ' represents the operator corresponding to the total flux through the ring. The phase difference of the superconducting wavefunction across the junction is denoted by θ, and is related to the total flux Φ' by $\theta = 2e\Phi'$. The operators Q and Φ' are a canonically conjugate pair of operators satisfying the following canonical commutation relation:

$$[\Phi', Q] = i. \tag{6.6}$$

Generally, we measure voltage rather than charge in experiments, and thus we would like to develop the scheme using V' and Φ' operators. Since the voltage across the junction is given by $V' = Q/C$, the commutation relation for the V' and Φ' operators becomes

$$C\,[\Phi', V'] = i. \tag{6.7}$$

Therefore, the uncertainty relationship for the V' and Φ' quadratures is given by

$$\langle (\Delta\Phi')^2 \rangle \langle (\Delta V')^2 \rangle \geq \frac{1}{4C^2}. \tag{6.8}$$

The rf-SQUID Hamiltonian (6.5) is akin to a simple harmonic oscillator except for the presence of a coupling term proportional to the Josephson coupling energy. The first term in the Hamiltonian represents kinetic energy, while the last two terms represent potential energy. If we expand the last term in the Hamiltonian and retain terms up to the fourth order in θ, we obtain

$$\begin{aligned} H &= \frac{Q^2}{2C} + \frac{C}{2}\omega^2\Phi'^2 - \frac{\Phi'\phi_x}{L} - \frac{2}{3}E_J e^4 \Phi'^4, \\ &\text{with} \quad \omega = \left(\frac{1}{CL} + \frac{4e^2 E_J}{C}\right)^{\frac{1}{2}}. \end{aligned} \tag{6.9}$$

In order to simplify the calculations, we define new dimensionless quadrature operators as

$$\Phi = \sqrt{C\omega}\Phi', \quad \text{and} \quad V = \sqrt{\frac{C}{\omega}}V'. \tag{6.10}$$

The quadrature operators Φ and V are related to the annihilation and creation operators, b and $b^\dagger$ as

$$\Phi = \frac{1}{\sqrt{2}}(b + b^\dagger), \quad V = \frac{i}{\sqrt{2}}(b^\dagger - b). \tag{6.11}$$

Applying the rotating wave approximation in Eq. (6.9), and omitting all the terms independent of the annihilation and creation operators, we obtain

$$H = \Omega b^\dagger b - \mu(b + b^\dagger) - \nu(b^\dagger b)^2, \tag{6.12}$$

where

$$\nu = \frac{2E_J e^4}{3(\omega C)^2}, \quad \mu = \frac{\phi_x}{L\sqrt{2\omega C}}, \quad \Omega = \omega - \nu. \tag{6.13}$$

We put an experimentally realizable condition $\mu \gg \Omega \gg \nu$ [236, 237] for further discussion in the remainder of this chapter. We turn on the external driving field of appropriate strength such that $\mu \gg \Omega, \nu$. During this time, only the second term in the Hamiltonian (6.12) is effective, which can displace a state in the phase space along the V quadrature as μ is a real quantity. The corresponding unitary operator is essentially the displacement operator, which can be written as

$$D(\tau_1) = \mathrm{e}^{i\mu(b+b^\dagger)\tau_1}, \tag{6.14}$$

where τ_1 represents the time for which the external driving field is switched on. We can prepare an arbitrary coherent state displaced along the V quadrature by adjusting the external driving flux ϕ_x and time duration τ_1.

Once the driving field has been turned off, only the first and the third terms of the Hamiltonian are non-zero. Further, for short duration τ_2, only the first term prevails due to the condition $\Omega \gg \nu$, and the corresponding unitary operator is given by

$$R(\tau_2) = \mathrm{e}^{-i\Omega b^\dagger b\tau_2}. \tag{6.15}$$

This unitary operator is essentially the phase change operator, which produces a rotation in the phase space. However for long duration τ_3, both the first and the third terms turn out to be significant. The effective Hamiltonian in the interaction picture becomes $H = -\nu(b^\dagger b)^2$, and the corresponding unitary operator is given by

$$S(\tau_3) = \mathrm{e}^{i\nu(b^\dagger b)^2\tau_3}. \tag{6.16}$$

The above Hamiltonian squeezes and de-squeezes the coherent state in V and Φ quadrature, and therefore the state exhibits collapse and revival phenomenon. If the system is initially in a coherent state $|\alpha\rangle$, the state gets squeezed due to the nonlinear Hamiltonian. However, squeezing vanishes at time $\tau_3 = \pi/\nu$ and the state becomes $|-\alpha\rangle$. This state differs from the initial state by a π rotation in the phase space. As time proceeds, the state again gets squeezed. Again, the squeezing vanishes at time $\tau_3 = 2\pi/\nu$ and the state becomes $|\alpha\rangle$. Under no-dissipation conditions, this collapse and revival cycle continues indefinitely. At intermediate times, the state can be expressed as a superposition of coherent states.

6.2.3 Preparation of a coherent state on a rf-SQUID

We outline the stepwise details undertaken by Alice to prepare the desired coherent state $|\phi_A + iv_A\rangle$. The first step is to prepare the rf-SQUID in its ground state $|0\rangle$.

To accomplish this, Alice lets the rf-SQUID decohere in the low Josephson coupling limit [240]. She then turns on the driving field and suitably adjusts the external driving flux ϕ_x and the time duration τ_1 to obtain the following coherent state:

$$D\left(\frac{\phi_A}{\mu_1}\right)|0\rangle = |0 + i\phi_A\rangle. \tag{6.17}$$

The ground state has been displaced along the V quadrature as μ_1 is a real quantity. Afterwards, Alice turns off the driving field for a time τ_2 such that $\Omega\tau_2 = \pi/2$. Since we have assumed $\Omega \gg \nu$, thus for a small duration τ_2, we can neglect the nonlinear term in the Hamiltonian (6.12). The effective Hamiltonian $H = \Omega\hat{b}^\dagger\hat{b}$ causes a $\pi/2$ rotation of the state in the phase space:

$$R\left(\frac{\pi}{2\Omega}\right)|0 + i\phi_A\rangle = |\phi_A + 0\rangle. \tag{6.18}$$

Alice once again turns on the driving field and suitably adjusts the external driving flux ϕ_x and time duration τ_1 to obtain the desired coherent state $|\phi_A + iv_A\rangle$:

$$D\left(\frac{v_A}{\mu_2}\right)|\phi_A + 0\rangle = |\phi_A + iv_A\rangle. \tag{6.19}$$

To sum up, Alice applies the unitary operator

$$T(\phi_A, v_A) = D\left(\frac{v_A}{\mu_2}\right) R\left(\frac{\pi}{2\Omega}\right) D\left(\frac{\phi_A}{\mu_1}\right). \tag{6.20}$$

on the ground state of the rf-SQUID to obtain the desired coherent state $|\phi_A + iv_A\rangle$. By suitably adjusting the external driving flux ϕ_x and various time durations, Alice can prepare arbitrary coherent states.

6.2.4 Evolution of a coherent state during the storage

Alice now transfers the encoded ensemble of states to Bob, where it is stored. During the transfer as well as the storage period, no external field is applied and the Hamiltonian (6.12) effectively reduces to

$$H = \Omega b^\dagger b - \nu(b^\dagger b)^2. \tag{6.21}$$

We now discuss the evolution of a given coherent state due to the above Hamiltonian. Let the state at time $t = 0$ be $|\alpha\rangle = |\phi_A + iv_A\rangle$, then the evolved state at time t is given by

$$|\psi(t)\rangle = \mathrm{e}^{-i\Omega b^\dagger bt}\mathrm{e}^{i\nu(b^\dagger b)^2 t}|\alpha\rangle. \tag{6.22}$$

The above state can be written in the Fock basis as

$$|\psi(t)\rangle = e^{-\frac{|\alpha|^2}{2}} \sum_{n=0}^{\infty} e^{i\nu n^2 t} \frac{(\alpha e^{-i\Omega t})^n}{\sqrt{n!}} |n\rangle. \tag{6.23}$$

If we tune the value of the quantity Ω/ν to be an even integer, then at time $t = \pi/\nu$, the above state evolves to the coherent state $|-\alpha\rangle$, whereas at at time $t = 2\pi/\nu$, the above state becomes the original state $|\alpha\rangle$. In general, whenever $t = \pi p/\nu q$, where $p < q$ are mutually prime, we can write the state (6.23) as a superposition of coherent states of same magnitude $|\alpha|$, but different phases [241, 242]:

$$\begin{aligned} \left|\psi\left(t = \frac{\pi p}{\nu q}\right)\right\rangle &= \sum_{l=0}^{m-1} c_l^{p,q} \left|\alpha \mathrm{e}^{-i\pi\left(\frac{\Omega p}{\nu q} - \frac{2l}{m}\right)}\right\rangle, \\ \text{with} \qquad c_l^{p,q} &= \frac{1}{m} \sum_{r=0}^{m-1} \mathrm{e}^{i\pi r\left(\frac{pr}{q} - \frac{2l}{m}\right)} \end{aligned} \tag{6.24}$$

and $m = q$ if at most one of p or q is odd, and $m = 2q$ if both are odd. For instance, if $p = 1$ and $q = 2$, Eq. (6.24) is a superposition of two coherent states:

$$\left|\psi\left(t = \frac{\pi}{2\nu}\right)\right\rangle = \frac{1}{\sqrt{2}} \left[\mathrm{e}^{i(\pi/4)} \left|\alpha \mathrm{e}^{-i\Omega\pi/2\nu}\right\rangle + \mathrm{e}^{-i(\pi/4)} \left|-\alpha \mathrm{e}^{-i\Omega\pi/2\nu}\right\rangle\right]. \tag{6.25}$$

We now aim to find out the variance of the Φ and V quadratures for the state (6.22). To this end, we first compute the average values of a few required functions of the field operators b and $b^\dagger$:

$$\langle b(t)\rangle = \alpha \mathrm{e}^{-it(\Omega-\nu)} \mathrm{e}^{|\alpha|^2(e^{i2\nu t}-1)}, \tag{6.26}$$

$$\langle b^\dagger(t)\rangle = \alpha^* \mathrm{e}^{it(\Omega-\nu)} \mathrm{e}^{|\alpha|^2(e^{-i2\nu t}-1)}, \tag{6.27}$$

$$\langle b(t)^2\rangle = \alpha^2 \mathrm{e}^{-2it(\Omega-2\nu)} \mathrm{e}^{|\alpha|^2(e^{i4\nu t}-1)}, \tag{6.28}$$

$$\langle b^\dagger(t)^2\rangle = \alpha^{*^2} \mathrm{e}^{2it(\Omega-2\nu)} \mathrm{e}^{|\alpha|^2(e^{-i4\nu t}-1)}, \tag{6.29}$$

$$\langle b^\dagger(t) b(t)\rangle = |\alpha|^2, \tag{6.30}$$

where Eq. (6.30) shows that the average number of quanta $\langle b^\dagger(t) b(t)\rangle$ is conserved under the action of the nonlinear Hamiltonian (6.21). The variance of the Φ and V quadratures can be easily calculated using the above results:

$$\begin{aligned} \langle(\Delta\Phi)^2\rangle =& \frac{1}{2}\Bigg[1 + 2|\alpha|^2 + \alpha^2 \mathrm{e}^{\left(|\alpha|^2\left(\gamma^2-1\right)-2it\xi\right)} - \beta^2 \mathrm{e}^{\left(|\alpha|^2\left(\gamma^{-2}-1\right)+2it\xi\right)} \\ &+ \mathrm{e}^{-2it\zeta}\left(\beta^* \mathrm{e}^{\left(|\alpha|^2(\gamma-1)\right)} - \beta \mathrm{e}^{\left(|\alpha|^2\left(\gamma^{-1}-1\right)+2it\zeta\right)}\right)^2\Bigg], \end{aligned} \tag{6.31}$$

$$\langle(\Delta V)^2\rangle = \frac{1}{2}\Big[1+2|\alpha|^2-\alpha^2 e^{\left(|\alpha|^2\left(\gamma^2-1\right)-2it\xi\right)}+\beta^2 e^{\left(|\alpha|^2\left(\gamma^{-2}-1\right)+2it\xi\right)} - e^{-2it\zeta}\left(\beta^* e^{\left(|\alpha|^2(\gamma-1)\right)}+\beta e^{\left(|\alpha|^2\left(\gamma^{-1}-1\right)+2it\zeta\right)}\right)^2\Big], \tag{6.32}$$

where $\alpha = (\phi + iv)/\sqrt{2}$, $\xi = \Omega - 2\nu$, $\beta = (v + i\phi)/\sqrt{2}$, $\gamma = e^{2i\nu t}$ and $\zeta = \Omega - \nu$.

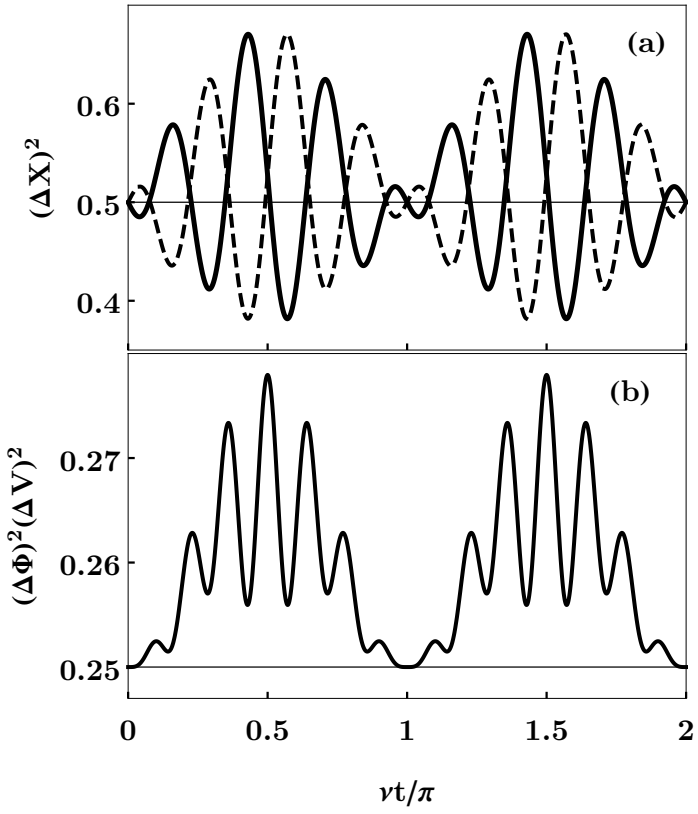


Figure 6.2: (a) Solid and dashed curves represent the variances of the Φ and V quadratures of the state (6.22). The squeezing condition in the quadrature X is $\langle(\Delta X)^2\rangle < 1/2$. We observe that when one quadrature is squeezed, its conjugate quadrature is de-squeezed. (b) The product of the variances of the state (6.22) satisfies $(\Delta\Phi)^2(\Delta V)^2 \geq 1/4$. The equality sign holds when the state revives to a coherent state. The parameters are set as $\Omega = 5\nu$, $\phi_A = 0.3$, and $v_A = 0.3$.

A state is squeezed in the quadrature $X \in \{\Phi, V\}$, if the variance falls below the coherent state value, *i.e.*, $\langle(\Delta X)^2\rangle < 1/2$. We first analyze the squeezing in the quadratures Φ and V for the state (6.22). As we can see from Fig. 6.2, the squeezing in the quadratures Φ and V appears and disappears with time. When one of the

quadratures is squeezed, its conjugate quadrature variance is above the coherent state value. Furthermore, the product of variances $(\Delta\Phi)^2(\Delta V)^2$ follows the uncertainty relation (6.8).

We now analyze the squeezing in the quadratures Φ and V for the state (6.25). Equations (6.31) and (6.32) reduce to

$$\langle(\Delta\Phi)^2\rangle = \begin{cases} \frac{1}{2} + \phi^2 - \mathrm{e}^{-2(\phi^2+v^2)}v^2 & \frac{\Omega}{\nu} \text{ is even,} \\ \frac{1}{2} + v^2 - \mathrm{e}^{-2(\phi^2+v^2)}\phi^2 & \frac{\Omega}{\nu} \text{ is odd,} \end{cases} \tag{6.33}$$

$$\langle(\Delta V)^2\rangle = \begin{cases} \frac{1}{2} + v^2 - \mathrm{e}^{-2(\phi^2+v^2)}\phi^2 & \frac{\Omega}{\nu} \text{ is even,} \\ \frac{1}{2} + \phi^2 - \mathrm{e}^{-2(\phi^2+v^2)}v^2 & \frac{\Omega}{\nu} \text{ is odd .} \end{cases} \tag{6.34}$$

The variance in the quadratures Φ and V for even Ω/ν are depicted on a contour plot in Fig. 6.3. The state is squeezed for the points inside the contour of value 0.50. Thus,

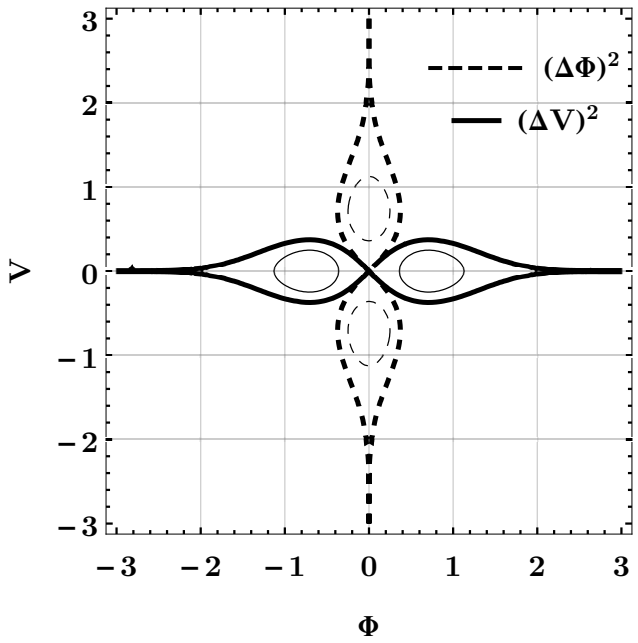


Figure 6.3: Thick-solid and thick-dashed curves represent a contour of value 0.5, while thin-solid and thin-dashed curves represent a contour of value 0.4. The state (6.25) is squeezed in Φ and V for the points inside the contour of value 0.5, whereas there is no second order squeezing for points outside this contour.

when the driving field is turned off, the encoded state exhibits collapse and revival phenomenon under the system Hamiltonian.

6.3 Protocol

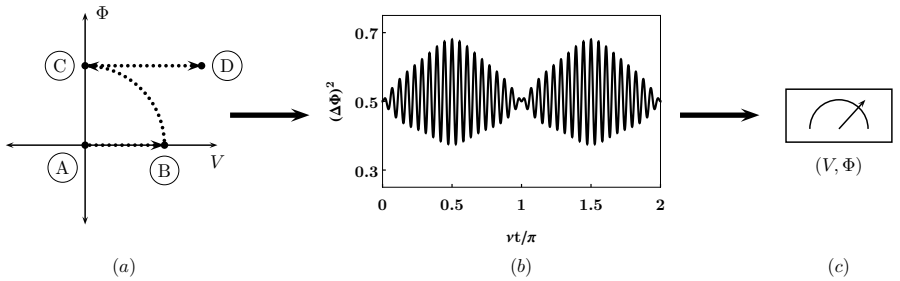


Figure 6.4: (a) Phase space illustration of coherent state preparation by Alice. The ground state is displaced from A to B followed by a rotation to C and final displacement to D. (b) Fluctuations in the variance of the Φ quadrature during the storage of the states. Parameters have been set as $\Omega = 20\nu$, $\phi_A = 0.3$, and $v_A = 0$. (c) Bob performs a homodyne measurement of randomly chosen quadrature V or Φ.

In this section, we present our on-demand QKD scheme based on coherent states generated on rf-SQUIDs. The following steps are required for a successful key distribution:

S1: Alice draws two random numbers ϕ_A and v_A from two independent Gaussian distributions where both of them are centered at ϕ_0, v_0 and have variance $V_A N_0$. She then generates the coherent state $|\phi_A + iv_A\rangle$ on a rf-SQUID as illustrated in Sec. 6.2.3. She repeats the above process and prepares an ensemble of coherent states on rf-SQUIDs with proper marking.

S2: The marked ensemble of rf-SQUIDs is sent to Bob through a quantum channel with Gaussian noise. We assume that both Alice and Bob are aware of the numbers of rf-SQUIDs in the ensemble.

S3: After receiving the ensemble, Bob stores it until the need for key distribution arises. The states of this ensemble evolve under the system Hamiltonian during the transfer as well as the storage period. As discussed in Sec. 6.2.4, the states exhibit collapse and revival phenomenon.

S4: Whenever the key is required, Bob randomly chooses the voltage V quadrature or the flux Φ quadrature and performs a homodyne measurement of the chosen quadrature on each marked state of the ensemble.

S5: In the next step, Bob communicates his measurement quadrature for each state of the ensemble to Alice through an authenticated classical channel. Thereafter, Alice retains the corresponding quadrature data for each state of the ensemble, while discards the other quadrature data. The data shared between Alice and Bob is thus correlated.

S6: Thereafter, using a sliced reconciliation scheme, the correlated data is transformed into errorless bit strings. Finally, a secure key can be obtained by performing privacy amplification on the errorless bit strings.

The schematic of the on-demand QKD scheme has been illustrated in Fig. 6.4. Two different measurement schemes can be implemented by Bob in the step S4 mentioned above. In the first scheme, Bob performs measurements at arbitrary times, while in the second scheme, he performs measurements at specific times in order to maximize the correlations of the data shared with Alice. We evaluate the average correlations of the shared data between Alice and Bob for both the measurement schemes, and it turns out that it is possible to carry out a successful QKD in both the measurement schemes as we shall see in the following sections.

Case 1: Measurement at an arbitrary time

In this scheme, Bob performs measurement at arbitrary times without being concerned about the time that has elapsed after state preparation. As discussed in Sec. 6.2.4, the state exhibits a periodic collapse and revival phenomenon under the system Hamiltonian. As a result, the behavior of the correlation between Alice's encoded data and Bob's measured results are periodic. Since Bob can perform measurement at any random time, his measurement can be considered to be uniformly distributed over a periodic cycle. Therefore, the required correlation is the time average of the time-dependent periodic correlation between Alice and Bob. We now proceed to evaluate this average correlation between Alice and Bob and the corresponding secure key rate.

To quantify the noise (correlation) between Bob's measurement result and Alice's encoded value of quadrature X, we define a quantity $C_{AB}(X)$ as follows:

$$\begin{aligned} C_{AB}(X) &= \langle (X^B - X^A)^2 \rangle \\ &= \langle (X^B)^2 \rangle + (X^A)^2 - 2X^A \langle X^B \rangle, \end{aligned} \tag{6.35}$$

where X^A represents the information encoded by Alice, X^B represents the homodyne measurement's results of the quadrature X, and the average is taken over all possible measurement results of Bob. We consider that Alice prepares the coherent state $|\alpha\rangle$

and Bob performs homodyne measurement of quadrature X at time t, then the noise $C_{AB}(\Phi)$ evaluates to

$$C_{AB}(\Phi) = \frac{1}{2}\Bigg[1 + 2|\alpha|^2 + 4\left(\mathrm{Re}\left(\alpha\right)\right)^2 + \alpha^2 \mathrm{e}^{|\alpha|^2\left(\gamma^2-1\right)-2it\xi} - \beta^2 \mathrm{e}^{\left(|\alpha|^2\left(\gamma^{-2}-1\right)+2it\xi\right)} - 4\mathrm{Re}\left(\alpha\right)\mathrm{e}^{-it\zeta}\left(\alpha \mathrm{e}^{|\alpha|^2(\gamma-1)} + \alpha^* \mathrm{e}^{\left(|\alpha|^2\left(\gamma^{-1}-1\right)+2it\zeta\right)}\right)\Bigg], \tag{6.36}$$

while the noise $C_{AB}(V)$ evaluates to

$$C_{AB}(V) = \frac{1}{2}\Bigg[1 + 2|\alpha|^2 + 4\left(\mathrm{Im}\left(\alpha\right)\right)^2 - \alpha^2 \mathrm{e}^{\left(|\alpha|^2\left(\gamma^2-1\right)-2it\xi\right)} + \beta^2 \mathrm{e}^{\left(|\alpha|^2\left(\gamma^{-2}-1\right)+2it\xi\right)} - 4\mathrm{Im}\left(\alpha\right)\mathrm{e}^{-it\zeta}\left(\beta \mathrm{e}^{\left(|\alpha|^2\left(\gamma^{-1}-1\right)+2it\zeta\right)} + \beta^* \mathrm{e}^{|\alpha|^2(\gamma-1)}\right)\Bigg], \tag{6.37}$$

where $\alpha = (\phi_A + iv_A)/\sqrt{2}$, $\xi = \Omega - 2\nu$, $\beta = (v_A + i\phi_A)/\sqrt{2}$, $\gamma = \mathrm{e}^{2i\nu t}$ and $\zeta = \Omega - \nu$. Let us suppose that Alice draws ϕ_A and v_A from two independent zero-centered Gaussian distributions with variance $V_A N_0 = 1/2$. The weighted average noise is evaluated by averaging over all the possible coherent states generated by Alice. The weighted average noise turns out to be equal for both the Φ and V quadratures and is given as

$$\begin{aligned} C_{AB}^{\{|\alpha\rangle\}}(X) &= \int_{-\infty}^{\infty}\int_{-\infty}^{\infty} dx_1 dx_2 \frac{1}{\pi}\mathrm{e}^{-(x_1^2+x_2^2)} C_{AB}(X) \\ &= \frac{3}{2} - \frac{9\cos(t(\nu-\Omega)) - 6\cos(t(\nu+\Omega)) + \cos(t(3\nu+\Omega))}{(5-3\cos(2\nu t))^2}, \end{aligned} \tag{6.38}$$

where $X \in \{\Phi, V\}$. The plots of the weighted average noise $C_{AB}^{\{|\alpha\rangle\}}(X)$ as a function of scaled time $\nu t/\pi$ for both odd and even values of Ω/ν is shown in Fig. 6.5. The weighted average noise has a period of π/ν and $2\pi/\nu$ for odd and even values of Ω/ν, respectively. Averaging the weighted average noise over one periodic cycle $t = 0$ to $t = 2\pi/\nu$ under the approximation $\Omega \gg \nu$, we obtain

$$C_{AB}^{\mathrm{T}}(X) = \frac{\nu}{2\pi}\int_0^{\frac{2\pi}{\nu}} dt\, C_{AB}^{\{|\alpha\rangle\}}(X) = \frac{3}{2}. \tag{6.39}$$

Thus, the optimum information rate between Alice and Bob $I(A:B)$ evaluates to

$$I(A:B) = \frac{1}{2}\log_2\left(1 + \frac{V_A N_0}{C_{AB}^{\mathrm{T}}(X)}\right). \tag{6.40}$$

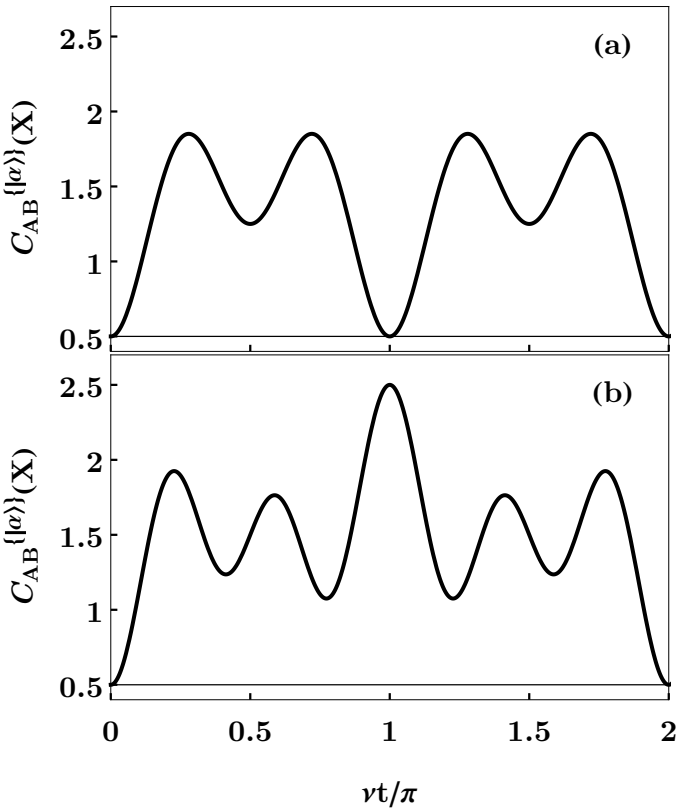


Figure 6.5: (a) Weighted average noise in either of the quadratures Φ or V as a function of the scaled time $\nu t/\pi$ for $\Omega/\nu = 5$, *i.e.*, for odd Ω/ν. The state (6.22) at time $t = 0$, π/ν and $2\pi/\nu$ is $|\alpha\rangle$, and thus the corresponding noise is equal to $1/2$. (b) Weighted average noise in either of the quadratures Φ or V as a function of the scaled time $\nu t/\pi$ for $\Omega/\nu = 6$, *i.e.*, for even Ω/ν. The state (6.22) at time $t = 0$, and $2\pi/\nu$ is $|\alpha\rangle$, and thus the corresponding noise is equal to $1/2$. However, at time π/ν, the state is $|-\alpha\rangle$, and thus the corresponding noise is maximum.

Taking $V_A N_0 = 1/2$ and using Eq. (6.39), the optimum information rate turns out to be $I(A : B) = 0.20$ bits. Therefore, the scheme generates correlated data, which can be distilled to generate secure key.

Case 2: Measurements at specific times

In this scheme, whenever the need for the key distribution arises, Bob only performs his measurement at those specific times which maximizes the correlation of the shared data. We have identified three such timings of which two correspond to the state (6.22) becoming a pure coherent state ($|\alpha\rangle$ or $|-\alpha\rangle$). The third timing corresponds to the

state (6.22) becoming a superposition of two coherent states as given by Eq. (6.25). The time period of the revival and collapse of the states are expected to be smaller compared to the storage time. Alice needs to indicate the time of generation of each state on the ensemble. Furthermore, Alice and Bob need to share synchronized clocks, since Bob has to perform measurement at specific timings.

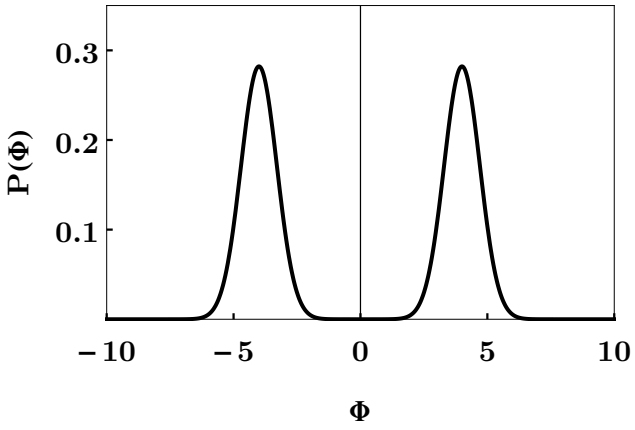


Figure 6.6: The probability distribution of the Φ quadrature for the state (6.25), when Alice Gaussian distribution is centered about $\phi_0 = v_0 = 4$, and $\Omega = 100\nu$.

In this scheme, the two Gaussian distributions have the same variance, but are centered around a larger value, for example, $\phi_0 = v_0 = 4$. Bob follows a slightly different scheme for recording the measurement readings, where he takes the absolute value of the obtained results. When Bob records the absolute value of the obtained results, the probability distribution of either of the quadratures is the same for both Alice and Bob at times $t = 0$, $t = \pi/2\nu$, $t = \pi/\nu$, $t = 3\pi/2\nu$ and $t = 2\pi/\nu$. This is true for both the cases of Ω/ν being an odd or an even integer. Bob obtains a bimodal distribution if he performs measurement at times $t = \pi/2\nu$ and $t = 3\pi/2\nu$, as shown in Fig. 6.6. We note that this distribution is bimodal only if we consider a large value of ϕ_0 and v_0. After taking the absolute value of his results, he obtains the same distribution as Alice's. Further, at other aforementioned specific times, Bob obtains the same distribution as Alice's if he records the absolute value of the obtained results.

The correlations for the measurements at any of the aforementioned specific timings is equal to the vacuum noise $N_0 = 1/2$. Thus, the average correlation is also equal to vacuum noise $N_0 = 1/2$, and the optimum information rate between Alice and Bob $I(A:B)$ evaluates to

$$I(A:B) = \frac{1}{2}\log_2\left(1 + \frac{V_A N_0}{N_0}\right) = 0.50 \text{ bits}. \tag{6.41}$$

It is necessary to perform measurements at precisely specified times to attain the aforementioned information rate. Furthermore, the need for the key distribution may arise after a long time leading to long storage of states. For a rf-SQUID with $\Omega \approx 10^4$Hz and $\Omega/\nu = 100$, the time period of collapse and revival is of the order of a few hundred microseconds (10^{-4}s). Commercially available atomic clocks allow measurement of time upto an error of 0.1μs per day. Thus, Bob can store the states for about 1000 days before the errors become of the order of collapse and revival time period. Moreover, measurement timings with a nanosecond resolution can be performed using computer processors in the GHz range . Thus, measurement at specific timings is feasible with the current technology for a storage period of around 1000 days.

6.4 Security

In this section, we provide the security proof for both the measurement schemes (at arbitrary and specific timings) for the case of an individual attack by an eavesdropper. As a result of eavesdropping, Gaussian noise is introduced in the rf-SQUIDs.

Security proof for our QKD scheme based on coherent states on rf-SQUIDs is similar to the continuous variable QKD based on coherent states [109]. Furthermore, we assume that Eavesdropper, Eve, has access to the ensemble of rf-SQUIDs while it is being transported through a quantum channel with Gaussian noise. As has already been stated in this chapter, if χN_0 is the amount of noise added in the Bob's signal, then $\chi^{-1}N_0$ is the minimum noise that gets added in the Eve's signal [239]. In view of this, the secure key rate for the case when Bob is performing measurement at arbitrary times is given by

$$\begin{aligned}\Delta I &= I(A:B) - I(A:E) \\ &= \frac{1}{2}\log_2\left(\frac{(V_A+\chi)\,N_0 + C^T_{AB}(X_i)}{\chi N_0 + C^T_{AB}(X)}\right) \\ &\quad - \frac{1}{2}\log_2\left(\frac{(1+V_A\chi)\,N_0 + C^T_{AE}(X)\chi}{C^T_{AE}(X)\chi + N_0}\right).\end{aligned} \tag{6.42}$$

Here $C^T_{AE}(X)$ is the time-averaged noise between Alice and Eve. Eve aims to minimize the noise and for that she could employ the measurement scheme at specific timings. This is also the best possible strategy as the noise at other timings is higher than the vacuum noise N_0. For $\chi < 1$, the secure key rate is positive and thus a secure key can be distilled. In the second case where Bob performs measurements at specific timings, the condition for positive secure key rate can be obtained by substituting $C^T_{AB}(X) = N_0 = 1/2$ in Eq. (6.42). The condition, in this case too, for a positive

secure key rate turns out to be $\chi < 1$. Thus, the secure key cannot be distilled for both measurement schemes if $\chi \geq 1$.

6.5 Conclusion

In this chapter, we investigated the possibility of accomplishing QKD with a non-photonic quantum system. The scheme requires Alice to prepare coherent states on rf-SQUIDs followed by the transfer of these states to Bob, who then stores it under no dissipation conditions [233, 234]. Whenever the need for a key arises, Bob performs measurements, and thereafter, classical information exchange and classical post-processing operations can be done to obtain a secure key. As the state evolves under the system Hamiltonian, the correlation between Alice and Bob exhibits collapse and revival phenomenon. Motivated by this fact, we devised two different measurement schemes, one without time stamping and the other with time stamping. The scheme without time stamping, where Bob performs measurement at arbitrary times, has a reasonable key rate of 0.20 bits. The scheme with time stamping has a higher key rate of 0.50 bits, however it is hard to implement.

Our proposed on-demand QKD scheme has several benefits over light-based QKD schemes, the most important being the possibility of storage of encoded states for years and therefore, the key generation can be carried out on demand. Furthermore, our scheme acts as a bridge between SQUIDs, which are currently utilized in several quantum information and quantum communication protocols [243, 244, 245]. We expect that this work will pave the way for the application of other condensed matter concepts to quantum communication. Specifically, one can explore the feasibility of entanglement assisted QKD using entangled states of SQUIDs. The results of this chapter are contained in arXiv:1808.06471v1.

6. On-demand quantum key distribution using superconducting rings with a mesoscopic Josephson junction

Chapter 7

Summary and Future Outlook

This thesis is a step further in the area of continuous variable quantum information processing, including quantum state tomography and quantum process tomography, nonlocality, and quantum key distribution. In the first work, we investigated the relative performances of various measurement schemes in the estimation of single mode Gaussian states. These studies will enable experimentalists to select the most efficient measurement scheme, which will enhance the performance of the QIP protocol under consideration. In our work, we had considered the state to be either squeezed in the $\hat{q}$-quadrature or the $\hat{p}$-quadrature. A possible future work would be, therefore, to extend the analysis for Gaussian states squeezed in arbitrary directions. Considering the increasing importance of non-Gaussian states in various QIP tasks, it is desirable to extend our analysis to non-Gaussian states, where we are required to estimate moments of all order.

In the next work, we provided a scheme for the optimal characterization of n-mode Gaussian states and n-mode Gaussian channels using photon number measurements. Since our state estimation scheme does not require local oscillators, it is well suited for scenarios where it is difficult to arrange local oscillators. For instance, in CV-QKD, transmitting an intense local pulse along with the signal pulse is a difficult task and can also lead to security loopholes [133, 134]. Further, it would be interesting to devise a scheme based on photon number measurements for the estimation of non-Gaussian states.

In a different direction, we undertook study of quantum nonlocality in a variety of quantum optical states ranging from a finite number of photons to an arbitrary number of photons, Gaussian to non-Gaussian. To this end, we considered multiphoton Bell-type inequality, which is based on the Clauser-Horne 1974 Bell test inequality. This inequality allows us to explore the role played by passive transformations in converting quantum optical nonclassicality to quantum nonlocality. We remark that on-off detectors are used for measurements in this inequality, which is very coarse-grained. Thus, it is desirable to construct Bell-type inequality based on more fine-grained measure-

ments.

The last part of the thesis dealt with CV quantum key distribution (QKD). To this end, we considered continuous variable measurement device independent quantum key distribution (CV-MDI-QKD), which is immune to attack on detectors. Here we have shown that photon subtraction on two mode squeezed coherent state enhances the performance of CV-MDI-QKD protocol as compared to photon subtraction on two mode squeezed vacuum state. However, the results revealed that multiple photon subtraction is detrimental to the performance of CV-MDI-QKD protocol as compared to single photon subtraction despite the fact that the entanglement content of multiple photon subtraction is more than single photon subtraction. This indicates that entanglement alone is not sufficient to enhance the performance of CV-MDI-QKD protocol. A thorough investigation is required in order to pinpoint the form of quantumness responsible for the enhancement of the CV-MDI-QKD protocol performance. Moreover, it remains an open problem whether other non-Gaussian states can be generated, which can further enhance the performance of the CV-MDI-QKD protocols.

In the last chapter of the thesis, we proposed a CV-QKD scheme based on long-lived coherent states prepared on superconducting rings with a mesoscopic Josephson junction. In this scheme, the key is generated whenever the actual need for the key arises, which is in contrast to light-based CV-QKD scheme, where the key is generated right after obtaining the state. This feature of our QKD scheme prevents the stealing of the key after generation.

To summarize, we believe that photon-number-resolving-detectors and non-Gaussian states are going to play an important role in the advancement of the quantum information processing field. On a positive note, with recent technological developments, the protocols involving these elements can be experimentally implemented.

Appendix A

Calculation of the symplectic transformation matrix for a given Hamiltonian

We provide two different methods to evaluate the symplectic transformation matrix for a given Hamiltonian.

A.1 Hilbert space and Baker-Campbell-Hausdorff formula

Consider the Hamiltonian $\hat{H}(t) = \delta(t - t_1)\hat{q}\hat{P}_1$ (Eq. 2.15). The corresponding infinite dimensional unitary representation is given by

$$\mathcal{U}(\hat{H}(t)) = \mathrm{e}^{-i\int \hat{H}(t)\,dt} = \mathrm{e}^{-i\hat{q}\hat{P}_1}. \tag{A.1}$$

In Heisenberg picture, the evolution of any operator $\hat{A}$ can be written as

$$\hat{A} \xrightarrow{\mathcal{U}(\hat{H}(t))} \mathcal{U}(\hat{H}(t))^\dagger\, \hat{A}\, \mathcal{U}(\hat{H}(t)). \tag{A.2}$$

Thus, the transformation of various quadrature operators using the Baker-Campbell-Hausdorff (BCH) formula can be evaluated as following:

$$\begin{aligned}
\mathrm{e}^{i\hat{q}\hat{P}_1}\, \hat{q}\, \mathrm{e}^{-i\hat{q}\hat{P}_1} &= \hat{q} \\
\mathrm{e}^{i\hat{q}\hat{P}_1}\, \hat{p}\, \mathrm{e}^{-i\hat{q}\hat{P}_1} &= \hat{p} - \hat{P}_1 \\
\mathrm{e}^{i\hat{q}\hat{P}_1}\, \hat{Q}_1\, \mathrm{e}^{-i\hat{q}\hat{P}_1} &= \hat{q} + \hat{Q}_1 \\
\mathrm{e}^{i\hat{q}\hat{P}_1}\, \hat{P}_1\, \mathrm{e}^{-i\hat{q}\hat{P}_1} &= \hat{P}_1
\end{aligned} \tag{A.3}$$

Thus, the quadrature operators transform as

$$\begin{pmatrix} \hat{q} \\ \hat{p} \\ \hat{Q} \\ \hat{P}_1 \end{pmatrix} \xrightarrow{\mathcal{U}(\hat{H}(t))} \underbrace{\begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & -1 \\ 1 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}}_{S} \begin{pmatrix} \hat{q} \\ \hat{p} \\ \hat{Q} \\ \hat{P}_1 \end{pmatrix}, \tag{A.4}$$

where S is the symplectic transformation corresponding to the Hamiltonian $\hat{H}(t) = \delta(t - t_1)\hat{q}\hat{P}_1$. However, this method gets a little complicated for the modified Arthurs-Kelly scheme, where the Hamiltonian is $H = \delta(t - t_1)\left(\hat{q}\hat{P}_1 - \hat{p}\hat{Q}_2 + \frac{\kappa}{2}\hat{P}_1\hat{Q}_2\right)$. Alternatively, we can take another approach where such complicated calculations can be performed easily.

A.2 Exponentiation of generators of $Sp(2n, \mathcal{R})$

Let J be the generator of the symplectic group $Sp(2n, \mathcal{R})$, *i.e.*, J is an element of the Lie algebra of $Sp(2n, \mathcal{R})$ group. The corresponding symplectic group element S can be obtained by exponentiating J as follows:

$$S = \exp(J). \tag{A.5}$$

We can associate a quadratic function of quadrature operators with every J, which is Hermitian, as follows:

$$H(J) = \frac{1}{2}\hat{\xi}^T(\Omega J)\hat{\xi}, \tag{A.6}$$

where $\hat{\xi}$ is the column of quadrature operators and Ω is the symplectic form. Since the generators of the symplectic group and quadratic functions of the quadrature operators are in one-to-one correspondence at Lie algebra level, we can exponentiate $H(J)$ to obtain infinite-dimensional unitary representation of $S = \exp(J)$. Thus, in our case, we can first determine the generator J from the given Hamiltonian and evaluate the corresponding symplectic transformation by exponentiation. We illustrate this procedure with the help of the Hamiltonian $\hat{H}(t) = \delta(t - t_1)\hat{q}\hat{P}_1$, whose corresponding infinite dimensional unitary representation is $\mathrm{e}^{-i\hat{q}\hat{P}_1}$. We can write

$$-i\hat{q}\hat{P}_1 = \frac{1}{2}\hat{\xi}^T(\Omega J)\hat{\xi}, \tag{A.7}$$

where $\hat{\xi} = (\hat{q},\, \hat{p},\, \hat{Q}_1,\, \hat{P}_1)^T$ and

$$\Omega J = - \begin{pmatrix} 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 \end{pmatrix}. \tag{A.8}$$

Consequently, the generator J becomes

$$J = \begin{pmatrix} 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & -1 \\ 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \end{pmatrix}. \tag{A.9}$$

Thus, the sympletic matrix corresponding to the generator J is

$$S = \exp(J) = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & -1 \\ 1 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}, \tag{A.10}$$

which is the same as the symplectic transformation matrix obtained using the B-C-H formula in the previous section.

A. Calculation of the symplectic transformation matrix for a given Hamiltonian

Appendix B

Wigner characteristic function approach

This section provides alternate method to compute the probability and the covariance matrix of k photon subtraction on one mode of the two-mode squeezed coherent (TMSC) state using the Wigner characteristic function.

B.0.1 Wigner characteristic function of the TMSC state

The Wigner characteristic function of an n-mode system is given by

$$\chi(\Lambda) = \text{Tr}[\hat{\rho}\, exp(-i\Lambda^T \Omega \hat{\xi})], \tag{B.1}$$

where $\xi = (\hat{q_1}, \hat{p_1}, \ldots \hat{q_n}, \hat{p_n})^T$, $\Lambda = (\tau_1, \sigma_1, \ldots \tau_n, \sigma_n)^T$ ($[\hat{q_i}, \hat{p_i}] = i\delta_{ij}, i, j \in \{1, 2, \ldots n\}$), and

$$\Omega = \bigoplus_{k=1}^{n} \omega, \quad \omega = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}. \tag{B.2}$$

States with Gaussian characteristic function takes the following simple form [15, 42]:

$$\chi(\Lambda) = \exp[-\frac{1}{2}\Lambda^T(\Omega V \Omega^T)\Lambda - i(\Omega - \overline{\xi})\Lambda], \tag{B.3}$$

where V is the covariance matrix of the state and $\overline{\xi}$ represents the displacement of the Gaussian state. Thus, the Wigner characteristic function for two-mode coherent state is the product of two single-mode coherent state:

$$\chi(\tau_1, \sigma_1, \tau_2, \sigma_2) = e^{-(1/4)\left(\tau_1^2+\sigma_1^2\right) - i(\tau_1 d_2 - \sigma_1 d_1)} e^{-(1/4)\left(\tau_2^2+\sigma_2^2\right) - i(\tau_2 d_2 - \sigma_2 d_1)}, \tag{B.4}$$

where $\overline{\xi} = (d_1, d_2, d_1, d_2)$ is the displacement of two-mode coherent state. Now, the two-mode coherent state (B.4) is sent through a two-mode squeezer given by S_{12} (1.93), and thus the Wigner characteristic function transforms as $\chi(\Lambda) \to \chi(S_{12}^{-1}\Lambda)$. The Wigner characteristic function of the TMSC state becomes ($d_1 = d, d_2 = 0$)

$$\begin{aligned}\chi_{A_1A_2}(\tau_1, \sigma_1, \tau_2, \sigma_2) = &\exp\left[-\frac{1}{4}\cosh 2r\left(\tau_1^2 + \sigma_1^2 + \tau_2^2 + \sigma_2^2\right)\cosh(2r)\right] \\ &\times \exp\left[\frac{\tau_1\tau_2 - \sigma_1\sigma_2}{2}\sinh 2r + i(\sigma_1 + \sigma_2)de^r\right].\end{aligned} \tag{B.5}$$

The Wigner characteristic function of the Fock state $|k\rangle$ is given by

$$\chi(\tau, \sigma)_{|k\rangle} = \exp\left(-\frac{\tau^2}{4} - \frac{\sigma^2}{4}\right)L_k\left(\frac{\tau^2}{2} + \frac{\sigma^2}{2}\right). \tag{B.6}$$

B.0.2 Probability of k-photon detection

In the next step, Fred mixes the vacuum mode F_0 with the mode A_2 of the TMSC state, obtained from Alice, using a beam splitter of transmittivty τ represented by the transformation matrix $B(\tau)$ (1.89). The Wigner characteristic function transforms as $\chi(\Lambda) \to \chi(B(\tau)^{-1}\Lambda)$, which yields a three mode entangled state described by the following Wigner characteristic function:

$$\chi_{A_1A_2'F_1}(\Lambda) = \chi'_{A_1A_2}(\tau_1, \sigma_1, \tau_2, \sigma_2)\chi'(\tau_3, \sigma_3)_{|0\rangle}. \tag{B.7}$$

After a successful photon subtraction, *i.e.*, when the POVM element $\Pi_k = |k\rangle\langle k|$ clicks, the unnormalized characteristic function of the k-PSTMSC state can be written using Eq. (1.112) as

$$\chi^k_{A_1A_2'}(\tau_1, \sigma_1, \tau_2, \sigma_2) = \frac{1}{2\pi}\int d\tau_3 d\sigma_3 \underbrace{\chi'_{A_1A_2}(\tau_1, \sigma_1, \tau_2, \sigma_2)\chi'_{|0\rangle}(\tau_3, \sigma_3)}_{\text{Three mode entangled state}} \underbrace{\chi_{|k\rangle}(\tau_3, \sigma_3)}_{\text{Projection on } |k\rangle\langle k|}. \tag{B.8}$$

To integrate Eq. (B.8), we use the following substitution for the Laguerre polynomial appearing in $\chi_{|k\rangle}(\tau_3, \sigma_3)$:

$$\partial_s^k\partial_t^k \exp\left[st + s\frac{\tau + i\sigma}{\sqrt{2}} - t\frac{\tau - i\sigma}{\sqrt{2}}\right]\Bigg|_{s=t=0} = k!L_k\left(\frac{\tau^2}{2} + \frac{\sigma^2}{2}\right), \tag{B.9}$$

This substitution turns the integrand into a Gaussian integral, which can be easily evaluated. The final expression of the unnormalized characteristic function of the k-PSTMSC state can be written in the following succinct form:

$$\chi^k_{A_1A_2'}(\Lambda) = \frac{A^k}{1 + \alpha^2(1 - \tau)}\exp\left[-\Lambda^T M\Lambda + N\Lambda + O\right]L_k(C), \tag{B.10}$$

where

$$M = \begin{pmatrix} x & 0 & -y & 0 \\ 0 & x & 0 & y \\ -y & 0 & x & 0 \\ 0 & y & 0 & x \end{pmatrix}, \quad N = \begin{pmatrix} 0 \\ z_1 \\ 0 \\ z_2 \end{pmatrix}, \tag{B.11}$$

where $x = \frac{1+\alpha^2(1+\tau)}{4(1+\alpha^2(1-\tau))}$, $y = \frac{\alpha\beta\sqrt{\tau}}{2(1+\alpha^2(1-\tau))}$, $z_1 = \frac{id(\beta+\alpha\tau)}{1+\alpha^2(1-\tau)}$, $z_2 = \frac{id(\alpha+\beta)\sqrt{\tau}}{1+\alpha^2(1-\tau)}$,
$O = -\frac{d^2\left(1+2\alpha(\alpha+\sqrt{1+\alpha^2})\right)(1-\tau)}{2(1+\alpha^2(1-\tau))}$, $\alpha = \sinh r$, $\beta = \sqrt{1+\alpha^2}$, $A = \frac{\alpha^2(1-\tau)}{1+\alpha^2(1-\tau)}$, and
$C = \frac{[d(\alpha+\beta)+\alpha(\tau_1+i\sigma_1)\beta-(\tau_2-i\sigma_2)\alpha\sqrt{\tau}][-d(\alpha+\beta)+\alpha(\tau_1-i\sigma_1)\beta-(\tau_2+i\sigma_2)\alpha\sqrt{\tau}]}{2\alpha^2(1+\alpha^2(1-\tau))}$.

The probability of k-photon subtraction can be computed from Eq. (B.10) as following:

$$P_{PS}^{(k)} = \chi^k_{A_1A_2'}(\tau_1,\sigma_1,\tau_2,\sigma_2)\Big|_{\tau_1=\sigma_1=\tau_2=\sigma_2=0} = \frac{A^k}{1+\alpha^2(1-\tau)}\exp(O)L_k(D), \tag{B.12}$$

with $D = -\frac{d^2\left(\alpha+\beta\right)^2}{2\alpha^2(1+\alpha^2(1-\tau))}$.

B.0.3 Covariance matrix of the k-PSTMSC state

The normalized Wigner characteristic function $\widetilde{\chi}$ of the k-PSTMSC state is obtained as

$$\widetilde{\chi}^k_{A_1A_2'}(\Lambda) = \left(P_{PS}^{(k)}\right)^{-1}\chi^k_{A_1A_2'}(\Lambda) = \exp\left[-\Lambda^T M\Lambda + N\Lambda\right]\frac{L_k(C)}{L_k(D)}. \tag{B.13}$$

We can evaluate the averages of symmetrically ordered operators by differentiating Wigner characteristic function of the k-PSTMSC state with respect to τ and σ parameters as shown in Sec. 1.5. In our case, the averages of symmetrically ordered operator of the form $\{\hat{q_1}^{r_1}\hat{p_1}^{s_1}\hat{q_2}^{r_2}\hat{p_2}^{s_2}\}_{\text{sym}}$ can be evaluated by differentiating Wigner characteristic function of the k-PSTMSC state (B.13):

$$\begin{aligned}\langle\{\hat{q_1}^{r_1}\hat{p_1}^{s_1}\hat{q_2}^{r_2}\hat{p_2}^{s_2}\}_{\text{sym}}\rangle = &\left(\frac{1}{i}\right)^{r_1+r_2}\left(\frac{1}{-i}\right)^{s_1+s_2} \\ &\times \frac{\partial^{r_1+s_1}}{\partial\sigma_1^{r_1}\partial\tau_1^{s_1}}\frac{\partial^{r_2+s_2}}{\partial\sigma_2^{r_2}\partial\tau_2^{s_2}}\widetilde{\chi}^k_{A_1A_2'}(\tau_1,\sigma_1,\tau_2,\sigma_2)\Big|_{\tau_1=\sigma_1=\tau_2=\sigma_2=0}.\end{aligned} \tag{B.14}$$

By suitably choosing the values of r_1, s_1, r_2, s_2 in Eq. (B.14), all the elements of the covariance matrix can be calculated. To convert all the results of $[\hat{q},\hat{p}] = i$ (natural units) to $[\hat{q},\hat{p}] = 2i$ (shot noise unit), one needs to replace $d \to d/\sqrt{2}$. Here, we

directly write the averages of all the quantities appearing in the covariance matrix in shot noise unit:

$$
\begin{aligned}
\langle \hat{x_1} \rangle =& \frac{d(\beta+\alpha\tau)}{1+\alpha^2(1-\tau)} + \frac{d(1+\alpha(\alpha+\beta))}{\alpha(1+\alpha^2(1-\tau))}\frac{L_{n-1}^1(D)}{L_n(D)},\\
\langle \hat{x_2} \rangle =& \frac{d(\alpha+\beta)\sqrt{\tau}}{1+\alpha^2(1-\tau)}\left(1+\frac{L_{n-1}^1(D)}{L_n(D)}\right),\\
\langle \hat{x_1}^2 \rangle =& \frac{d^2-\alpha^2}{\alpha^2} + \frac{d^2\beta^2\left(1+2\alpha\left(\alpha+\beta\right)\right)}{\alpha^2(1+\alpha^2(1-\tau))^2}\left(1+2\frac{L_{n-1}^1(D)}{L_n(D)}+\frac{L_{n-2}^2(D)}{L_n(D)}\right),\\
& \frac{2\alpha^2\beta^2-2d^2\left(1+\alpha\left(\alpha+\beta\right)\right)}{\alpha^2(1+\alpha^2(1-\tau))}\left(1+\frac{L_{n-1}^1(D)}{L_n(D)}\right),\\
\langle \hat{x_2}^2 \rangle =& -1 + \frac{d^2\beta^2\left(1+2\alpha\left(\alpha+\beta\right)\right)}{\alpha^2(1+\alpha^2(1-\tau))^2}\left(1+\frac{L_{n-1}^1(D)}{L_n(D)}+\frac{\alpha^2\tau}{\beta^2}\frac{L_{n-2}^2(D)}{L_n(D)}\right),\\
& \frac{2\alpha^2\beta^2-2d^2\left(1+\alpha\left(\alpha+\beta\right)\right)}{\alpha^2(1+\alpha^2(1-\tau))}\left(1+\frac{L_{n-1}^1(D)}{L_n(D)}\right),\\
\langle \hat{p_1}^2 \rangle =& \frac{1+\alpha^2(1+\tau)}{1+\alpha^2(1-\tau)} + \frac{2(1+\alpha^2)}{1+\alpha^2(1-\tau)}\frac{L_{n-1}^1(D)}{L_n(D)},\\
\langle \hat{p_2}^2 \rangle =& \frac{1+\alpha^2(1+\tau)}{1+\alpha^2(1-\tau)} + \frac{2\alpha^2\tau}{1+\alpha^2(1-\tau)}\frac{L_{n-1}^1(D)}{L_n(D)},\\
\langle \hat{x_1}\hat{x_2} \rangle =& \frac{d^2(\beta+2\alpha(1+\alpha(\alpha+\beta)))\sqrt{\tau}}{\alpha(1+\alpha^2(1-\tau))^2}\left(1+2\frac{L_{n-1}^1(D)}{L_n(D)}+\frac{L_{n-2}^2(D)}{L_n(D)}\right),\\
& + \frac{(2\alpha^2\beta-d^2(\alpha+\beta))\sqrt{\tau}}{\alpha(1+\alpha^2(1-\tau))}\left(1+\frac{L_{n-1}^1(D)}{L_n(D)}\right),\\
\langle \hat{p_1}\hat{p_2} \rangle =& -\frac{2\alpha\beta\sqrt{\tau}}{1+\alpha^2(1-\tau)}\left(1+\frac{L_{n-1}^1(D)}{L_n(D)}\right),\\
\langle \hat{p_1} \rangle =& \langle \hat{p_2} \rangle = \langle \{\hat{x_1}\hat{p_1}\}_{\text{sym}} \rangle = \langle \{\hat{x_2}\hat{p_2}\}_{\text{sym}} \rangle = \langle \hat{x_1}\hat{p_2} \rangle = \langle \hat{p_1}\hat{x_2} \rangle = 0,
\end{aligned}
\tag{B.15}
$$

with $\beta = \sqrt{1+\alpha^2}$. Thus, the covariance matrix takes the following form:

$$
\Sigma_{A_1A_2'} = ((\Sigma_{A_1A_2'})_{ij}) \equiv \begin{pmatrix} \gamma_A^x & 0 & \gamma_C^x & 0 \\ 0 & \gamma_A^p & 0 & \gamma_C^p \\ \gamma_C^x & 0 & \gamma_B^x & 0 \\ 0 & \gamma_C^p & 0 & \gamma_B^p \end{pmatrix}, \tag{B.16}
$$

where $(\Sigma_{A_1A_2'})_{ij} = \frac{1}{2}\langle\{\hat{\xi}_i, \hat{\xi}_j\}\rangle - \langle\hat{\xi}_i\rangle\langle\hat{\xi}_j\rangle$.

References

[1] W. Heisenberg, Über den anschaulichen Inhalt der quantentheoretischen Kinematik und Mechanik, Zeitschrift für Physik **43**(3), 172–198 (Mar 1927). 1

[2] E. H. Kennard, Zur Quantenmechanik einfacher Bewegungstypen, Zeitschrift für Physik **44**(4), 326–352 (Apr 1927). 1

[3] H. Weyl, Gruppentheorie und Quantenmechanik, S. Hirzel, Leipzig, Germany, second edition, 1931. 1

[4] D. Bohm, A Suggested Interpretation of the Quantum Theory in Terms of "Hidden" Variables. I, Phys. Rev. **85**, 166–179 (Jan 1952). 1

[5] D. Bohm, A Suggested Interpretation of the Quantum Theory in Terms of "Hidden" Variables. II, Phys. Rev. **85**, 180–193 (Jan 1952). 1

[6] H. Everett, "Relative State" Formulation of Quantum Mechanics, Rev. Mod. Phys. **29**, 454–462 (Jul 1957). 1

[7] G. C. Ghirardi, A. Rimini, and T. Weber, Unified dynamics for microscopic and macroscopic systems, Phys. Rev. D **34**, 470–491 (Jul 1986). 1

[8] A. Einstein, B. Podolsky, and N. Rosen, Can Quantum-Mechanical Description of Physical Reality Be Considered Complete?, Phys. Rev. **47**, 777–780 (May 1935). 1, 33, 83

[9] E. Schrödinger, Discussion of Probability Relations between Separated Systems, Mathematical Proceedings of the Cambridge Philosophical Society **31**(4), 555–563 (1935). 2, 83

[10] E. Schrödinger, Probability relations between separated systems, Mathematical Proceedings of the Cambridge Philosophical Society **32**(3), 446–452 (1936). 2, 83

[11] J. S. Bell, On the Einstein Podolsky Rosen paradox, Physics **1**(3), 195–200 (1964). 2, 83

[12] M. A. Nielsen and I. L. Chuang, Quantum Computation and Quantum Information: 10th Anniversary Edition, Cambridge University Press, New York, NY, USA, 10th edition, 2011. 2, 4, 83

[13] C. H. Bennett and G. Brassard, Quantum Cryptography: Public Key Distribution and Coin Tossing, in Proceedings of the IEEE International Conference on Computers, Systems and Signal Processing, pages 175–179, New York, 1984, IEEE Press. 2, 103

[14] G. Adesso, S. Ragy, and A. R. Lee, Continuous Variable Quantum Information: Gaussian States and Beyond, Open Systems & Information Dynamics **21**(01n02), 1440001 (2014). 2, 7, 43

[15] 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**, 621–669 (May 2012). 2, 7, 17, 31, 39, 65, 95, 149

[16] N. Schuch, J. I. Cirac, and M. M. Wolf, Quantum States on Harmonic Lattices, Communications in Mathematical Physics **267**(1), 65–92 (Oct 2006). 3

[17] J. Eisert, S. Scheel, and M. B. Plenio, Distilling Gaussian States with Gaussian Operations is Impossible, Phys. Rev. Lett. **89**, 137903 (Sep 2002). 3

[18] J. Niset, J. Fiurášek, and N. J. Cerf, No-Go Theorem for Gaussian Quantum Error Correction, Phys. Rev. Lett. **102**, 120501 (Mar 2009). 3

[19] S. Lloyd and S. L. Braunstein, Quantum Computation over Continuous Variables, Phys. Rev. Lett. **82**, 1784–1787 (Feb 1999). 3

[20] A. Gilchrist, P. Deuar, and M. D. Reid, Contradiction of Quantum Mechanics with Local Hidden Variables for Quadrature Phase Amplitude Measurements, Phys. Rev. Lett. **80**, 3169–3172 (Apr 1998). 3

[21] R. García-Patrón, J. Fiurášek, N. J. Cerf, J. Wenger, R. Tualle-Brouri, and P. Grangier, Proposal for a Loophole-Free Bell Test Using Homodyne Detection, Phys. Rev. Lett. **93**, 130409 (Sep 2004). 3

[22] A. Ourjoumtsev, A. Dantan, R. Tualle-Brouri, and P. Grangier, Increasing Entanglement between Gaussian States by Coherent Photon Subtraction, Phys. Rev. Lett. **98**, 030502 (Jan 2007). 3, 104

[23] S.-Y. Lee, S.-W. Ji, H.-J. Kim, and H. Nha, Enhancing quantum entanglement for continuous variables by a coherent superposition of photon subtraction and addition, Phys. Rev. A **84**, 012302 (Jul 2011). 3, 104

[24] L. Hu, Z. Liao, and M. S. Zubairy, Continuous-variable entanglement via multiphoton catalysis, Phys. Rev. A **95**, 012310 (Jan 2017). 3, 104

[25] C. Navarrete-Benlloch, R. García-Patrón, J. H. Shapiro, and N. J. Cerf, Enhancing quantum entanglement by photon addition and subtraction, Phys. Rev. A **86**, 012328 (Jul 2012). 3, 104

[26] K. Thapliyal, N. L. Samantray, J. Banerji, and A. Pathak, Comparison of lower- and higher-order nonclassicality in photon added and subtracted squeezed coherent states, Physics Letters A **381**(37), 3178 – 3187 (2017). 3

[27] S. Bose and M. S. Kumar, Quantitative study of beam-splitter-generated entanglement from input states with multiple nonclassicality-inducing operations, Phys. Rev. A **95**, 012330 (Jan 2017). 3, 104

[28] C. Sudheesh, S. Lakshmibala, and V. Balakrishnan, Squeezing and higher-order squeezing of photon-added coherent states propagating in a Kerr-like medium, Journal of Optics B: Quantum and Semiclassical Optics **7**(12), S728–S735 (nov 2005). 3

[29] A. R. Usha Devi, R. Prabhu, and M. S. Uma, Non-classicality of photon added coherent and thermal radiations, The European Physical Journal D - Atomic, Molecular, Optical and Plasma Physics **40**(1), 133–138 (Oct 2006). 3

[30] T. Opatrný, G. Kurizki, and D.-G. Welsch, Improvement on teleportation of continuous variables by photon subtraction via conditional measurement, Phys. Rev. A **61**, 032302 (Feb 2000). 3

[31] S. Wang, L.-L. Hou, X.-F. Chen, and X.-F. Xu, Continuous-variable quantum teleportation with non-Gaussian entangled states generated via multiple-photon subtraction and addition, Phys. Rev. A **91**, 063832 (Jun 2015). 3

[32] H.-X. Ma, P. Huang, D.-Y. Bai, S.-Y. Wang, W.-S. Bao, and G.-H. Zeng, Continuous-variable measurement-device-independent quantum key distribution with photon subtraction, Phys. Rev. A **97**, 042329 (Apr 2018). 3, 104, 113, 114, 117

[33] Y. Guo, W. Ye, H. Zhong, and Q. Liao, Continuous-variable quantum key distribution with non-Gaussian quantum catalysis, Phys. Rev. A **99**, 032327 (Mar 2019). 3, 104

[34] G. Harder, T. J. Bartley, A. E. Lita, S. W. Nam, T. Gerrits, and C. Silberhorn, Single-Mode Parametric-Down-Conversion States with 50 Photons as a Source for Mesoscopic Quantum Optics, Phys. Rev. Lett. **116**, 143601 (Apr 2016). 3, 63

[35] J. Hloušek, M. Dudka, I. Straka, and M. Ježek, Accurate Detection of Arbitrary Photon Statistics, Phys. Rev. Lett. **123**, 153604 (Oct 2019). 3, 63

[36] J. Sakurai, Modern Quantum Mechanics, Addison-Wesley, USA, 1994. 4, 5

[37] R. F. Werner, Quantum states with Einstein-Podolsky-Rosen correlations admitting a hidden-variable model, Phys. Rev. A **40**, 4277–4281 (Oct 1989). 6, 83

[38] R. Horodecki, P. Horodecki, M. Horodecki, and K. Horodecki, Quantum entanglement, Rev. Mod. Phys. **81**, 865–942 (Jun 2009). 6

[39] Arvind, B. Dutta, N. Mukunda, and R. Simon, The real symplectic groups in quantum mechanics and optics, Pramana **45**(6), 471–497 (1995). 7, 28, 32, 35, 36

[40] S. L. Braunstein and P. van Loock, Quantum information with continuous variables, Rev. Mod. Phys. **77**, 513–577 (Jun 2005). 7, 39

[41] G. Adesso and F. Illuminati, Entanglement in continuous-variable systems: recent advances and current perspectives, Journal of Physics A: Mathematical and Theoretical **40**(28), 7821–7880 (jun 2007). 7

[42] S. Olivares, Quantum optics in the phase space, The European Physical Journal Special Topics **203**(1), 3–24 (Apr 2012). 7, 29, 31, 43, 149

[43] E. C. G. Sudarshan, Equivalence of Semiclassical and Quantum Mechanical Descriptions of Statistical Light Beams, Phys. Rev. Lett. **10**, 277–279 (Apr 1963). 14, 19, 35, 84

[44] K. E. Cahill and R. J. Glauber, Density Operators and Quasiprobability Distributions, Phys. Rev. **177**, 1882–1902 (Jan 1969). 15

[45] K. E. Cahill and R. J. Glauber, Ordered Expansions in Boson Amplitude Operators, Phys. Rev. **177**, 1857–1881 (Jan 1969). 15

[46] G. S. Agarwal and E. Wolf, Calculus for Functions of Noncommuting Operators and General Phase-Space Methods in Quantum Mechanics. I. Mapping Theorems and Ordering of Functions of Noncommuting Operators, Phys. Rev. D **2**, 2161–2186 (Nov 1970). 15

[47] G. S. Agarwal and E. Wolf, Calculus for Functions of Noncommuting Operators and General Phase-Space Methods in Quantum Mechanics. II. Quantum Mechanics in Phase Space, Phys. Rev. D **2**, 2187–2205 (Nov 1970). 15

[48] R. J. Glauber, Coherent and Incoherent States of the Radiation Field, Phys. Rev. **131**, 2766–2788 (Sep 1963). 19, 35, 84

[49] C. Gerry and P. Knight, Introductory Quantum Optics, Cambridge University Press, 2004. 22

[50] T. Tyc and B. C. Sanders, Operational formulation of homodyne detection, Journal of Physics A: Mathematical and General **37**(29), 7341–7357 (jul 2004). 25

[51] C. Gerry and P. Knight, Introductory Quantum Optics, Cambridge University Press, 2004. 25

[52] J. Williamson, On the Algebraic Problem Concerning the Normal Forms of Linear Dynamical Systems, American Journal of Mathematics **58**(1), 141–163 (1936). 28

[53] W. B. Case, Wigner functions and Weyl transforms for pedestrians, American Journal of Physics **76**(10), 937–946 (2008). 29

[54] J. F. Clauser, M. A. Horne, A. Shimony, and R. A. Holt, Proposed Experiment to Test Local Hidden-Variable Theories, Phys. Rev. Lett. **23**, 880–884 (Oct 1969). 33, 83

[55] J. S. Bell and A. Aspect, Speakable and Unspeakable in Quantum Mechanics: Collected Papers on Quantum Philosophy, Cambridge University Press, 2 edition, 2004. 33, 83

[56] A. Peres, Quantum theory concepts and methods, Kluwer Academic Publishers, 2002. 34

[57] L. Masanes, Y.-C. Liang, and A. C. Doherty, All Bipartite Entangled States Display Some Hidden Nonlocality, Phys. Rev. Lett. **100**, 090403 (Mar 2008). 34

[58] M. Navascués and T. Vértesi, Activation of Nonlocal Quantum Resources, Phys. Rev. Lett. **106**, 060403 (Feb 2011). 34

[59] F. Buscemi, All Entangled Quantum States Are Nonlocal, Phys. Rev. Lett. **108**, 200401 (May 2012). 34

[60] J. Kiukas, P. Lahti, and J. Schultz, Position and momentum tomography, Phys. Rev. A **79**, 052119 (May 2009). 34, 37, 41

[61] A. Di Lorenzo, Sequential Measurement of Conjugate Variables as an Alternative Quantum State Tomography, Phys. Rev. Lett. **110**, 010404 (Jan 2013). 34, 37, 38

[62] D. Das and Arvind, Weak measurement-based state estimation of Gaussian states of one-variable quantum systems, Journal of Physics A: Mathematical and Theoretical **50**(14), 145307 (mar 2017). 34, 35, 37, 41

[63] A. Kumari, A. K. Pan, and P. K. Panigrahi, Joint weak value for all order coupling using continuous variable and qubit probe, The European Physical Journal D **71**(11), 275 (Nov 2017). 34

[64] E. Arthurs and J. L. Kelly Jr., On the Simultaneous Measurement of a Pair of Conjugate Observables, Bell System Technical Journal **44**(4), 725–729 (1965). 34, 38

[65] C. R. Müller, C. Peuntinger, T. Dirmeier, I. Khan, U. Vogl, C. Marquardt, G. Leuchs, L. L. Sánchez-Soto, Y. S. Teo, Z. Hradil, and J. Řeháček, Evading Vacuum Noise: Wigner Projections or Husimi Samples?, Phys. Rev. Lett. **117**, 070801 (Aug 2016). 35, 38

[66] M. Lobino, D. Korystov, C. Kupchak, E. Figueroa, B. C. Sanders, and A. I. Lvovsky, Complete characterization of quantum-optical processes, Science **322**(5901), 563–566 (2008). 35, 63, 73

[67] S. Rahimi-Keshari, A. Scherer, A. Mann, A. T. Rezakhani, A. I. Lvovsky, and B. C. Sanders, Quantum process tomography with coherent states, New Journal of Physics **13**(1), 013006 (jan 2011). 35, 63, 73

[68] A. Anis and A. I. Lvovsky, Maximum-likelihood coherent-state quantum process tomography, New Journal of Physics **14**(10), 105021 (oct 2012). 35, 63

[69] M. Ghalaii and A. T. Rezakhani, Scheme for coherent-state quantum process tomography via normally-ordered moments, Phys. Rev. A **95**, 032336 (Mar 2017). 35, 63

[70] A. Ferraro and M. G. A. Paris, Nonclassicality Criteria from Phase-Space Representations and Information-Theoretical Constraints Are Maximally Inequivalent, Phys. Rev. Lett. **108**, 260403 (Jun 2012). 35, 84

[71] M. Brunelli, C. Benedetti, S. Olivares, A. Ferraro, and M. G. A. Paris, Single- and two-mode quantumness at a beam splitter, Phys. Rev. A **91**, 062315 (Jun 2015). 35, 84

[72] A. Leverrier, R. García-Patrón, R. Renner, and N. J. Cerf, Security of Continuous-Variable Quantum Key Distribution Against General Attacks, Phys. Rev. Lett. **110**, 030502 (Jan 2013). 36, 104

[73] P. W. Shor and J. Preskill, Simple Proof of Security of the BB84 Quantum Key Distribution Protocol, Phys. Rev. Lett. **85**, 441–444 (Jul 2000). 36, 103, 104

[74] S. L. Braunstein and S. Pirandola, Side-Channel-Free Quantum Key Distribution, Phys. Rev. Lett. **108**, 130502 (Mar 2012). 36, 104

[75] S. Pirandola, C. Ottaviani, G. Spedalieri, C. Weedbrook, S. L. Braunstein, S. Lloyd, T. Gehring, C. S. Jacobsen, and U. L. Andersen, High-rate measurement-device-independent quantum cryptography, Nature Photonics **9**, 397 (05 2015). 36, 104

[76] S. Chaturvedi and V. Srinivasan, Photon-number distributions for fields with Gaussian Wigner functions, Phys. Rev. A **40**, 6095–6098 (Nov 1989). 36

[77] F. Grosshans, G. Van Assche, J. Wenger, R. Brouri, N. J. Cerf, and P. Grangier, Quantum key distribution using gaussian-modulated coherent states, Nature **421**, 238 EP – (01 2003). 36, 104, 125

[78] D. F. V. James, P. G. Kwiat, W. J. Munro, and A. G. White, Measurement of qubits, Phys. Rev. A **64**, 052312 (Oct 2001). 37

[79] M. Paris and J. Řeháček, editors, Quantum state estimation, volume 649 of Lecture Notes in Physics, Springer-Verlag, Berlin, 2004. 37

[80] A. I. Lvovsky and M. G. Raymer, Continuous-variable optical quantum-state tomography, Rev. Mod. Phys. **81**, 299–332 (Mar 2009). 37

[81] G. Vallone and D. Dequal, Strong Measurements Give a Better Direct Measurement of the Quantum Wave Function, Phys. Rev. Lett. **116**, 040502 (Jan 2016). 37

[82] L. Calderaro, G. Foletto, D. Dequal, P. Villoresi, and G. Vallone, Direct Reconstruction of the Quantum Density Matrix by Strong Measurements, Phys. Rev. Lett. **121**, 230501 (Dec 2018). 37

[83] 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 (Mar 2020). 37, 82

[84] H. P. Yuen and V. W. S. Chan, Noise in homodyne and heterodyne detection, Opt. Lett. **8**(3), 177–179 (Mar 1983). 37

[85] G. L. Abbas, V. W. S. Chan, and T. K. Yee, Local-oscillator excess-noise suppression for homodyne and heterodyne detection, Opt. Lett. **8**(8), 419–421 (Aug 1983). 37

[86] B. L. Schumaker, Noise in homodyne detection, Opt. Lett. **9**(5), 189–191 (May 1984). 37

[87] K. Banaszek and K. Wódkiewicz, Operational theory of homodyne detection, Phys. Rev. A **55**, 3117–3123 (Apr 1997). 37

[88] K. Vogel and H. Risken, Determination of quasiprobability distributions in terms of probability distributions for the rotated quadrature phase, Phys. Rev. A **40**, 2847–2849 (Sep 1989). 37

[89] D. T. Smithey, M. Beck, M. G. Raymer, and A. Faridani, Measurement of the Wigner distribution and the density matrix of a light mode using optical homodyne tomography: Application to squeezed states and the vacuum, Phys. Rev. Lett. **70**, 1244–1247 (Mar 1993). 37

[90] T. Kiesel, W. Vogel, V. Parigi, A. Zavatta, and M. Bellini, Experimental determination of a nonclassical Glauber-Sudarshan P function, Phys. Rev. A **78**, 021804 (Aug 2008). 37

[91] A. Javan, E. A. Ballik, and W. L. Bond, Frequency Characteristics of a Continuous-Wave He–Ne Optical Maser, J. Opt. Soc. Am. **52**(1), 96–98 (Jan 1962). 38

[92] W. S. Read and R. G. Turner, Tracking Heterodyne Detection, Appl. Opt. **4**(12), 1570–1573 (Dec 1965). 38

[93] H. R. Carleton and W. T. Maloney, A Balanced Optical Heterodyne Detector, Appl. Opt. **7**(6), 1241–1243 (Jun 1968). 38

[94] H. Gerhardt, H. Welling, and A. Güttner, Measurements of the laser linewidth due to quantum phase and quantum amplitude noise above and below threshold. I, Zeitschrift für Physik **253**(2), 113–126 (Apr 1972). 38

[95] H. Yuen and J. Shapiro, Optical communication with two-photon coherent states–Part III: Quantum measurements realizable with photoemissive detectors, IEEE Transactions on Information Theory **26**(1), 78–92 (January 1980). 38

[96] H. P. Yuen, Generalized quantum measurements and approximate simultaneous measurements of noncommuting observables, Physics Letters A **91**(3), 101 – 104 (1982). 38

[97] E. Arthurs and M. S. Goodman, Quantum Correlations: A Generalized Heisenberg Uncertainty Relation, Phys. Rev. Lett. **60**, 2447–2449 (Jun 1988). 38

[98] J. Shapiro and S. Wagner, Phase and amplitude uncertainties in heterodyne detection, IEEE Journal of Quantum Electronics **20**(7), 803–813 (July 1984). 38

[99] J. Shapiro, Quantum noise and excess noise in optical homodyne and heterodyne receivers, IEEE Journal of Quantum Electronics **21**(3), 237–250 (March 1985). 38

[100] M. Collett, R. Loudon, and C. Gardiner, Quantum Theory of Optical Homodyne and Heterodyne Detection, Journal of Modern Optics **34**(6-7), 881–902 (1987). 38

[101] H. Martens and W. M. de Muynck, Towards a new uncertainty principle: quantum measurement noise, Physics Letters A **157**(8), 441 – 448 (1991). 38

[102] M. G. Raymer, Uncertainty principle for joint measurement of noncommuting variables, American Journal of Physics **62**(11), 986–993 (1994). 38

[103] J. Rehácek, Y. S. Teo, Z. Hradil, and S. Wallentowitz, Surmounting intrinsic quantum-measurement uncertainties in Gaussian-state tomography with quadrature squeezing, Scientific Reports **5**, 12289 EP – (Jul 2015), Article. 38

[104] Y. S. Teo, C. R. Müller, H. Jeong, Z. Hradil, J. Řeháček, and L. L. Sánchez-Soto, Superiority of heterodyning over homodyning: An assessment with quadrature moments, Phys. Rev. A **95**, 042322 (Apr 2017). 38

[105] S. Wallentowitz and W. Vogel, Unbalanced homodyning for quantum state measurements, Phys. Rev. A **53**, 4528–4533 (Jun 1996). 38

[106] Y. S. Teo, H. Jeong, and L. L. Sánchez-Soto, Progress toward optimal quantum tomography with unbalanced homodyning, Phys. Rev. A **96**, 042333 (Oct 2017). 38

[107] M. Hillery, Quantum cryptography with squeezed states, Phys. Rev. A **61**, 022309 (Jan 2000). 38

[108] N. J. Cerf, M. Lévy, and G. V. Assche, Quantum distribution of Gaussian keys using squeezed states, Phys. Rev. A **63**, 052311 (Apr 2001). 38

[109] F. Grosshans and P. Grangier, Continuous Variable Quantum Cryptography Using Coherent States, Phys. Rev. Lett. **88**, 057902 (Jan 2002). 38, 103, 126, 140

[110] P. Busch, Indeterminacy relations and simultaneous measurements in quantum theory, International Journal of Theoretical Physics **24**(1), 63–92 (Jan 1985). 38, 59

[111] T. J. Bullock and P. Busch, Focusing in Arthurs-Kelly-Type Joint Measurements with Correlated Probes, Phys. Rev. Lett. **113**, 120401 (Sep 2014). 38, 59

[112] Arvind, S. Chaturvedi, and N. Mukunda, Symplectic group methods and the Arthurs Kelly model of measurement in quantum mechanics, Physics Letters A **384**(23), 126543 (2020). 39

[113] Y. Aharonov, D. Z. Albert, and L. Vaidman, How the result of a measurement of a component of the spin of a spin-1/2 particle can turn out to be 100, Phys. Rev. Lett. **60**, 1351–1354 (Apr 1988). 41

[114] I. M. Duck, P. M. Stevenson, and E. C. G. Sudarshan, The sense in which a "weak measurement" of a spin-½ particle's spin component yields a value 100, Phys. Rev. D **40**, 2112–2117 (Sep 1989). 41

[115] S. Kocsis, B. Braverman, S. Ravets, M. J. Stevens, R. P. Mirin, L. K. Shalm, and A. M. Steinberg, Observing the Average Trajectories of Single Photons in a Two-Slit Interferometer, Science **332**(6034), 1170–1173 (2011). 41

[116] N. W. M. Ritchie, J. G. Story, and R. G. Hulet, Realization of a measurement of a "weak value", Phys. Rev. Lett. **66**, 1107–1110 (Mar 1991). 41

[117] A. Steinberg, A. Feizpour, L. Rozema, D. Mahler, and A. Hayat, In praise of weakness, Physics World **26**(03), 35–40 (mar 2013). 41

[118] T. A. Brun, A simple model of quantum trajectories, American Journal of Physics **70**(7), 719–737 (2002). 41

[119] J. S. Lundeen, B. Sutherland, A. Patel, C. Stewart, and C. Bamber, Direct measurement of the quantum wavefunction, Nature **474**, 188 EP – (Jun 2011). 41

[120] R. Simon, Peres-Horodecki Separability Criterion for Continuous Variable Systems, Phys. Rev. Lett. **84**, 2726–2729 (Mar 2000). 60

[121] J. Fiurášek and N. J. Cerf, How to Measure Squeezing and Entanglement of Gaussian States without Homodyning, Phys. Rev. Lett. **93**, 063601 (Aug 2004). 63

[122] J. Wenger, J. Fiurášek, R. Tualle-Brouri, N. J. Cerf, and P. Grangier, Pulsed squeezed vacuum measurements without homodyning, Phys. Rev. A **70**, 053812 (Nov 2004). 63

[123] K. R. Parthasarathy and R. Sengupta, From particle counting to Gaussian tomography, Infin. Dimens. Anal. Quantum Probab. Relat. Top. **18**(4), 1550023, 21 (2015). 63, 64, 66, 74, 76, 77, 82

[124] X.-B. Wang, Z.-W. Yu, J.-Z. Hu, A. Miranowicz, and F. Nori, Efficient tomography of quantum-optical Gaussian processes probed with a few coherent states, Phys. Rev. A **88**, 022101 (Aug 2013). 63, 73

[125] M. Cooper, E. Slade, M. Karpiński, and B. J. Smith, Characterization of conditional state-engineering quantum processes by coherent state quantum process tomography, New Journal of Physics **17**(3), 033041 (mar 2015). 63

[126] C. Kupchak, S. Rind, B. Jordaan, and E. Figueroa, Quantum Process Tomography of an Optically-Controlled Kerr Non-linearity, Scientific Reports **5**(1), 16581 (2015). 63

[127] J. Fiurášek, Continuous-variable quantum process tomography with squeezed-state probes, Phys. Rev. A **92**, 022101 (Aug 2015). 63

[128] L. Ruppert and R. Filip, Estimation of nonclassical independent Gaussian processes by classical interferometry, Scientific Reports **7**(1), 39641 (2017). 63

[129] K. V. Jacob, A. E. Mirasola, S. Adhikari, and J. P. Dowling, Direct characterization of linear and quadratically nonlinear optical systems, Phys. Rev. A **98**, 052327 (Nov 2018). 63

[130] T. Heinosaari, A. S. Holevo, and M. M. Wolf, The semigroup sturucture of Gaussian channels, Quantum Information & Computation **10**(7&8), 619–635 (2010). 64, 73

[131] A. S. Holevo, Quantum systems, channels, information, a mathematical introduction, volume 16 of De Gruyter Studies in Mathematical Physics, De Gruyter, Berlin, 2012. 64, 73

[132] K. R. Parthasarathy, Symplectic dilations, Gaussian states and Gaussian channels, Indian J. Pure Appl. Math. **46**(4), 419–439 (2015). 64, 73

[133] D. B. S. Soh, C. Brif, P. J. Coles, N. Lütkenhaus, R. M. Camacho, J. Urayama, and M. Sarovar, Self-Referenced Continuous-Variable Quantum Key Distribution Protocol, Phys. Rev. X **5**, 041010 (Oct 2015). 64, 143

[134] B. Qi, P. Lougovski, R. Pooser, W. Grice, and M. Bobrek, Generating the Local Oscillator "Locally" in Continuous-Variable Quantum Key Distribution Based on Coherent Detection, Phys. Rev. X **5**, 041009 (Oct 2015). 64, 143

[135] V. V. Dodonov, O. V. Man'ko, and V. I. Man'ko, Multidimensional Hermite polynomials and photon distribution for polymode mixed light, Phys. Rev. A **50**, 813–817 (Jul 1994). 66, 77

[136] G. Vallone, G. Cariolaro, and G. Pierobon, Means and covariances of photon numbers in multimode Gaussian states, Phys. Rev. A **99**, 023817 (Feb 2019). 77

[137] A. Allevi, M. Bina, S. Olivares, and M. Bondani, Homodyne-like detection scheme based on photon-number-resolving detectors, International Journal of Quantum Information **15**(08), 1740016 (2017). 82

[138] P. P. Rohde and T. C. Ralph, Modelling photo-detectors in quantum optics, Journal of Modern Optics **53**(11), 1589–1603 (2006). 82

[139] R. Horodecki, P. Horodecki, M. Horodecki, and K. Horodecki, Quantum entanglement, Rev. Mod. Phys. **81**, 865–942 (Jun 2009). 83

[140] N. Brunner, D. Cavalcanti, S. Pironio, V. Scarani, and S. Wehner, Bell nonlocality, Rev. Mod. Phys. **86**, 419–478 (Apr 2014). 83

[141] J. Barrett, L. Hardy, and A. Kent, No Signaling and Quantum Key Distribution, Phys. Rev. Lett. **95**, 010503 (Jun 2005). 83

[142] A. Acín, N. Brunner, N. Gisin, S. Massar, S. Pironio, and V. Scarani, Device-Independent Security of Quantum Cryptography against Collective Attacks, Phys. Rev. Lett. **98**, 230501 (Jun 2007). 83

[143] L. Masanes, Universally Composable Privacy Amplification from Causality Constraints, Phys. Rev. Lett. **102**, 140501 (Apr 2009). 83

[144] N. Gisin, G. Ribordy, W. Tittel, and H. Zbinden, Quantum cryptography, Rev. Mod. Phys. **74**, 145–195 (Mar 2002). 83, 103

[145] J. Singh, K. Bharti, and Arvind, Quantum key distribution protocol based on contextuality monogamy, Phys. Rev. A **95**, 062333 (Jun 2017). 83, 103

[146] N. D. Mermin, Extreme quantum entanglement in a superposition of macroscopically distinct states, Phys. Rev. Lett. **65**, 1838–1840 (Oct 1990). 83

[147] G. Svetlichny, Distinguishing three-body from two-body nonseparability by a Bell-type inequality, Phys. Rev. D **35**, 3066–3069 (May 1987). 83

[148] D. Collins, N. Gisin, S. Popescu, D. Roberts, and V. Scarani, Bell-Type Inequalities to Detect True n-Body Nonseparability, Phys. Rev. Lett. **88**, 170405 (Apr 2002). 83

[149] Z. Zhao, T. Yang, Y.-A. Chen, A.-N. Zhang, M. Żukowski, and J.-W. Pan, Experimental Violation of Local Realism by Four-Photon Greenberger-Horne-Zeilinger Entanglement, Phys. Rev. Lett. **91**, 180401 (Oct 2003). 83

[150] J.-D. Bancal, J. Barrett, N. Gisin, and S. Pironio, Definitions of multipartite nonlocality, Phys. Rev. A **88**, 014102 (Jul 2013). 83

[151] D. Klyshko, The Bell and GHZ theorems: a possible three-photon interference experiment and the question of nonlocality, Physics Letters A **172**(6), 399 – 403 (1993). 83

[152] J.-L. Chen, D.-L. Deng, H.-Y. Su, C. Wu, and C. H. Oh, Detecting full N-particle entanglement in arbitrarily-high-dimensional systems with Bell-type inequalities, Phys. Rev. A **83**, 022316 (Feb 2011). 83

[153] J.-D. Bancal, N. Brunner, N. Gisin, and Y.-C. Liang, Detecting Genuine Multipartite Quantum Nonlocality: A Simple Approach and Generalization to Arbitrary Dimensions, Phys. Rev. Lett. **106**, 020405 (Jan 2011). 83

[154] Arvind and N. Mukunda, Bell's inequalities, multiphoton states and phase space distributions, Physics Letters A **259**(6), 421 – 426 (1999). 84

[155] K. Banaszek and K. Wódkiewicz, Testing Quantum Nonlocality in Phase Space, Phys. Rev. Lett. **82**, 2009–2013 (Mar 1999). 84

[156] Z.-B. Chen, J.-W. Pan, G. Hou, and Y.-D. Zhang, Maximal Violation of Bell's Inequalities for Continuous Variable Systems, Phys. Rev. Lett. 88, 040406 (January 2002). 84

[157] W. Son, C. Brukner, and M. S. Kim, Test of Nonlocality for a Continuous-Variable State Based on an Arbitrary Number of Measurement Outcomes, Phys. Rev. Lett. **97**, 110401 (Sep 2006). 84

[158] E. G. Cavalcanti, C. J. Foster, M. D. Reid, and P. D. Drummond, Bell Inequalities for Continuous-Variable Correlations, Phys. Rev. Lett. **99**, 210405 (Nov 2007). 84

[159] G. Adesso and S. Piano, Theory of Genuine Tripartite Nonlocality of Gaussian States, Phys. Rev. Lett. **112**, 010401 (Jan 2014). 84

[160] B. Xu, T. Tufarelli, and G. Adesso, Genuine multipartite nonlocality of permutationally invariant Gaussian states, Phys. Rev. A **95**, 012124 (Jan 2017). 84

[161] Y. Xiang, B. Xu, L. Mišta, T. Tufarelli, Q. He, and G. Adesso, Investigating Einstein-Podolsky-Rosen steering of continuous-variable bipartite states by non-Gaussian pseudospin measurements, Phys. Rev. A **96**, 042326 (Oct 2017). 84

[162] S. Olivares and M. G. A. Paris, Enhancement of nonlocality in phase space, Phys. Rev. A **70**, 032112 (Sep 2004). 84

[163] H. Jeong, Testing Bell inequalities with photon-subtracted Gaussian states, Phys. Rev. A **78**, 042101 (Oct 2008). 84

[164] H.-J. Kim, J. Kim, and H. Nha, Enhanced multipartite quantum correlation by non-Gaussian operations, Phys. Rev. A **88**, 032109 (Sep 2013). 84

[165] M. G. A. Paris, Entanglement and visibility at the output of a Mach-Zehnder interferometer, Phys. Rev. A **59**, 1615–1621 (Feb 1999). 84

[166] M. S. Kim, W. Son, V. Bužek, and P. L. Knight, Entanglement by a beam splitter: Nonclassicality as a prerequisite for entanglement, Phys. Rev. A **65**, 032323 (Feb 2002). 84

[167] J. S. Ivan, S. Chaturvedi, E. Ercolessi, G. Marmo, G. Morandi, N. Mukunda, and R. Simon, Entanglement and nonclassicality for multimode radiation-field states, Phys. Rev. A **83**, 032118 (Mar 2011). 84

[168] I. I. Arkhipov, J. Peřina, J. Peřina, and A. Miranowicz, Interplay of nonclassicality and entanglement of two-mode Gaussian fields generated in optical parametric processes, Phys. Rev. A **94**, 013807 (Jul 2016). 84

[169] H. Gholipour and F. Shahandeh, Entanglement and nonclassicality: A mutual impression, Phys. Rev. A **93**, 062318 (Jun 2016). 84

[170] V. Chille, N. Quinn, C. Peuntinger, C. Croal, L. Mišta, C. Marquardt, G. Leuchs, and N. Korolkova, Quantum nature of Gaussian discord: Experimental evidence and role of system-environment correlations, Phys. Rev. A **91**, 050301 (May 2015). 84

[171] R. Simon and N. Mukunda, Minimal three-component SU(2) gadget for polarization optics, Physics Letters A **143**(4), 165 – 169 (1990). 86

[172] G. W. Stewart, Computing theCS decomposition of a partitioned orthonormal matrix, Numerische Mathematik **40**(3), 297–306 (Oct 1982). 87

[173] I. Dhand and S. K. Goyal, Realization of arbitrary discrete unitary transformations using spatial and internal modes of light, Phys. Rev. A **92**, 043813 (Oct 2015). 87

[174] J. F. Clauser and M. A. Horne, Experimental consequences of objective local theories, Phys. Rev. D **10**, 526–535 (Jul 1974). 89

[175] K. P. Seshadreesan, H. Krovi, and S. Guha, Continuous-variable entanglement distillation over a pure loss channel with multiple quantum scissors, Phys. Rev. A **100**, 022315 (Aug 2019). 95

[176] I. Derkach, V. C. Usenko, and R. Filip, Continuous-variable quantum key distribution with a leakage from state preparation, Phys. Rev. A **96**, 062309 (Dec 2017). 95

[177] G. S. Agarwal, Generation of Pair Coherent States and Squeezing via the Competition of Four-Wave Mixing and Amplified Spontaneous Emission, Phys. Rev. Lett. **57**, 827–830 (Aug 1986). 98

[178] G. S. Agarwal and A. Biswas, Quantitative measures of entanglement in pair-coherent states, Journal of Optics B: Quantum and Semiclassical Optics **7**(11), 350 (2005). 98

[179] G. S. Agarwal, Nonclassical statistics of fields in pair coherent states, J. Opt. Soc. Am. B **5**(9), 1940–1947 (Sep 1988). 98

[180] Arvind, U(2) invariant squeezing properties of pair coherent states, Physics Letters A **299**(5–6), 461 – 468 (2002). 98

[181] A. Gábris and G. S. Agarwal, QUANTUM TELEPORTATION WITH PAIR-COHERENT STATES, International Journal of Quantum Information **05**(01n02), 17–22 (2007). 98

[182] X.-G. Meng, J.-S. Wang, and H.-Y. Fan, Wigner function and tomogram of the pair coherent state, Physics Letters A **363**(1), 12 – 18 (2007). 98

[183] B. C. Sanders, Entangled coherent states, Phys. Rev. A **45**, 6811–6815 (May 1992). 98

[184] S. Pirandola, U. L. Anderson, L. Banchi, M. Berta, D. Bunandar, R. Colbeck, D. Englund, T. Gehring, C. Lupo, C. Ottaviani, J. Pereira, M. Razavi, J. S. Shaari, M. Tomamichel, V. Usenko, G. Vallone, P. Villoresi, and P. Wallden, Advances in Quantum Cryptography, arXiv **1906.01645v1** (June 2019). 103

[185] C. H. Bennett, Quantum cryptography using any two nonorthogonal states, Phys. Rev. Lett. **68**, 3121–3124 (May 1992). 103

[186] C. Branciard, N. Gisin, B. Kraus, and V. Scarani, Security of two quantum cryptography protocols using the same four qubit states, Phys. Rev. A **72**, 032301 (Sep 2005). 103

[187] V. Scarani, H. Bechmann-Pasquinucci, N. J. Cerf, M. Dušek, N. Lütkenhaus, and M. Peev, The security of practical quantum key distribution, Rev. Mod. Phys. **81**, 1301–1350 (Sep 2009). 103

[188] T. C. Ralph, Security of continuous-variable quantum cryptography, Phys. Rev. A **62**, 062306 (Nov 2000). 103

[189] N. Cerf, S. Iblisdir, and G. Van Assche, Cloning and cryptography with quantum continuous variables, The European Physical Journal D - Atomic, Molecular, Optical and Plasma Physics **18**(2), 211–218 (Feb 2002). 103, 127

[190] T. C. Ralph, Continuous variable quantum cryptography, Phys. Rev. A **61**, 010303 (Dec 1999). 103

[191] A. K. Ekert, Quantum cryptography based on Bell's theorem, Phys. Rev. Lett. **67**, 661–663 (Aug 1991). 103

[192] A. Acín, N. Gisin, and L. Masanes, From Bell's Theorem to Secure Quantum Key Distribution, Phys. Rev. Lett. **97**, 120405 (Sep 2006). 103

[193] M. Pawłowski, Security proof for cryptographic protocols based only on the monogamy of Bell's inequality violations, Phys. Rev. A **82**, 032313 (Sep 2010). 103

[194] N. J. Cerf, M. Lévy, and G. V. Assche, Quantum distribution of Gaussian keys using squeezed states, Phys. Rev. A **63**, 052311 (Apr 2001). 103

[195] M. Hillery, Quantum cryptography with squeezed states, Phys. Rev. A **61**, 022309 (Jan 2000). 103

[196] S. Pirandola, C. Ottaviani, G. Spedalieri, C. Weedbrook, S. L. Braunstein, S. Lloyd, T. Gehring, C. S. Jacobsen, and U. L. Andersen, High-rate measurement-device-independent quantum cryptography, Nature Photonics **9**(6), 397–402 (Jun 2015). 104

[197] A. Leverrier, Composable Security Proof for Continuous-Variable Quantum Key Distribution with Coherent States, Phys. Rev. Lett. **114**, 070501 (Feb 2015). 104

[198] A. Leverrier, Security of Continuous-Variable Quantum Key Distribution via a Gaussian de Finetti Reduction, Phys. Rev. Lett. **118**, 200501 (May 2017). 104

[199] R. Renner and J. I. Cirac, de Finetti Representation Theorem for Infinite-Dimensional Quantum Systems and Applications to Quantum Cryptography, Phys. Rev. Lett. **102**, 110504 (Mar 2009). 104

[200] C. H. Bennett, F. Bessette, G. Brassard, L. Salvail, and J. Smolin, Experimental quantum cryptography, Journal of Cryptology **5**(1), 3–28 (Jan 1992). 104

[201] J.-Y. Wang, B. Yang, S.-K. Liao, L. Zhang, Q. Shen, X.-F. Hu, J.-C. Wu, S.-J. Yang, H. Jiang, Y.-L. Tang, B. Zhong, H. Liang, W.-Y. Liu, Y.-H. Hu, Y.-M. Huang, B. Qi, J.-G. Ren, G.-S. Pan, J. Yin, J.-J. Jia, Y.-A. Chen, K. Chen, C.-Z. Peng, and J.-W. Pan, Direct and full-scale experimental verifications towards ground–satellite quantum key distribution, Nature Photonics **7**, 387 EP – (04 2013). 104

[202] A. Acín, N. Brunner, N. Gisin, S. Massar, S. Pironio, and V. Scarani, Device-Independent Security of Quantum Cryptography against Collective Attacks, Phys. Rev. Lett. **98**, 230501 (Jun 2007). 104

[203] H.-K. Lo, M. Curty, and B. Qi, Measurement-Device-Independent Quantum Key Distribution, Phys. Rev. Lett. **108**, 130503 (Mar 2012). 104

[204] M. Curty, F. Xu, W. Cui, C. C. W. Lim, K. Tamaki, and H.-K. Lo, Finite-key analysis for measurement-device-independent quantum key distribution, Nature Communications **5**, 3732 EP – (04 2014). 104

[205] C. Ottaviani, G. Spedalieri, S. L. Braunstein, and S. Pirandola, Continuous-variable quantum cryptography with an untrusted relay: Detailed security analysis of the symmetric configuration, Phys. Rev. A **91**, 022320 (Feb 2015). 104, 113

[206] X.-B. Wang, Three-intensity decoy-state method for device-independent quantum key distribution with basis-dependent errors, Phys. Rev. A **87**, 012320 (Jan 2013). 104

[207] A. Rubenok, J. A. Slater, P. Chan, I. Lucio-Martinez, and W. Tittel, Real-World Two-Photon Interference and Proof-of-Principle Quantum Key Distribution Immune to Detector Attacks, Phys. Rev. Lett. **111**, 130501 (Sep 2013). 104

[208] T. Ferreira da Silva, D. Vitoreti, G. B. Xavier, G. C. do Amaral, G. P. Temporão, and J. P. von der Weid, Proof-of-principle demonstration of measurement-device-independent quantum key distribution using polarization qubits, Phys. Rev. A **88**, 052303 (Nov 2013). 104

[209] Y. Liu, T.-Y. Chen, L.-J. Wang, H. Liang, G.-L. Shentu, J. Wang, K. Cui, H.-L. Yin, N.-L. Liu, L. Li, X. Ma, J. S. Pelc, M. M. Fejer, C.-Z. Peng, Q. Zhang, and J.-W. Pan, Experimental Measurement-Device-Independent Quantum Key Distribution, Phys. Rev. Lett. **111**, 130502 (Sep 2013). 104

[210] Z. Li, Y.-C. Zhang, F. Xu, X. Peng, and H. Guo, Continuous-variable measurement-device-independent quantum key distribution, Phys. Rev. A **89**, 052301 (May 2014). 104, 113, 114

[211] X.-C. Ma, S.-H. Sun, M.-S. Jiang, M. Gui, and L.-M. Liang, Gaussian-modulated coherent-state measurement-device-independent quantum key distribution, Phys. Rev. A **89**, 042335 (Apr 2014). 104

[212] P. Papanastasiou, C. Ottaviani, and S. Pirandola, Finite-size analysis of measurement-device-independent quantum cryptography with continuous variables, Phys. Rev. A **96**, 042332 (Oct 2017). 104

[213] C. Lupo, C. Ottaviani, P. Papanastasiou, and S. Pirandola, Continuous-variable measurement-device-independent quantum key distribution: Composable security against coherent attacks, Phys. Rev. A **97**, 052327 (May 2018). 104

[214] Y. Wang, X. Wang, J. Li, D. Huang, L. Zhang, and Y. Guo, Self-referenced continuous-variable measurement-device-independent quantum key distribution, Physics Letters A **382**(17), 1149 – 1156 (2018). 104

[215] S. L. Zhang and P. van Loock, Distillation of mixed-state continuous-variable entanglement by photon subtraction, Phys. Rev. A **82**, 062316 (Dec 2010). 104

[216] F. Dell'Anno, S. De Siena, L. Albano, and F. Illuminati, Continuous-variable quantum teleportation with non-Gaussian resources, Phys. Rev. A **76**, 022301 (Aug 2007). 104

[217] Y. Yang and F.-L. Li, Entanglement properties of non-Gaussian resources generated via photon subtraction and addition and continuous-variable quantum-teleportation improvement, Phys. Rev. A **80**, 022315 (Aug 2009). 104

[218] Y. Zhao, Y. Zhang, B. Xu, S. Yu, and H. Guo, Continuous-variable measurement-device-independent quantum key distribution with virtual photon subtraction, Phys. Rev. A **97**, 042328 (Apr 2018). 104, 113

[219] R. Birrittella, A. Gura, and C. C. Gerry, Coherently stimulated parametric down-conversion, phase effects, and quantum-optical interferometry, Phys. Rev. A **91**, 053801 (May 2015). 107

[220] P. Huang, G. He, J. Fang, and G. Zeng, Performance improvement of continuous-variable quantum key distribution via photon subtraction, Phys. Rev. A **87**, 012317 (Jan 2013). 113

[221] J.-S. Chen, M.-J. Hu, X.-M. Hu, B.-H. Liu, Y.-F. Huang, C.-F. Li, C.-G. Guo, and Y.-S. Zhang, Experimental realization of sequential weak measurements of non-commuting Pauli observables, Optics Express **27**(5), 6089 (Mar 2019). 113

[222] Z. Li, Y. Zhang, X. Wang, B. Xu, X. Peng, and H. Guo, Non-Gaussian postselection and virtual photon subtraction in continuous-variable quantum key distribution, Phys. Rev. A **93**, 012310 (Jan 2016). 113

[223] F. Grosshans, N. J. Cerf, J. Wenger, R. Tualle-Brouri, and P. Grangier, Virtual Entanglement and Reconciliation Protocols for Quantum Cryptography with Continuous Variables, Quantum Info. Comput. **3**(7), 535–552 (Oct. 2003). 113

[224] S. Pirandola, C. Ottaviani, G. Spedalieri, C. Weedbrook, S. L. Braunstein, S. Lloyd, T. Gehring, C. S. Jacobsen, and U. L. Andersen, High-rate measurement-device-independent quantum cryptography, Nature Photonics **9**, 397 EP – (05 2015). 113

[225] 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**(1), 1800011 (2018). 115

[226] H. Takesue, S. W. Nam, Q. Zhang, R. H. Hadfield, T. Honjo, K. Tamaki, and Y. Yamamoto, Quantum key distribution over a 40-dB channel loss using superconducting single-photon detectors, Nature Photonics **1**, 343 EP – (Jun 2007). 125

[227] A. Fedrizzi, R. Ursin, T. Herbst, M. Nespoli, R. Prevedel, T. Scheidl, F. Tiefenbacher, T. Jennewein, and A. Zeilinger, High-fidelity transmission of entanglement over a high-loss free-space channel, Nature Physics **5**, 389 EP – (May 2009). 125

[228] P. Jouguet, S. Kunz-Jacques, A. Leverrier, P. Grangier, and E. Diamanti, Experimental demonstration of long-distance continuous-variable quantum key distribution, Nature Photonics **7**, 378 EP – (Apr 2013). 125

[229] H. Takenaka, A. Carrasco-Casado, M. Fujiwara, M. Kitamura, M. Sasaki, and M. Toyoshima, Satellite-to-ground quantum-limited communication using a 50-kg-class microsatellite, Nature Photonics **11**, 502 EP – (Jul 2017). 125

[230] A. Joshi, The mesoscopic Josephson junction: a classical quantum-like system, Physics Letters A **270**(5), 249 – 253 (2000). 125

[231] M. J. Everitt, P. Stiffell, T. D. Clark, A. Vourdas, J. F. Ralph, H. Prance, and R. J. Prance, Fully quantum-mechanical model of a SQUID ring coupled to an electromagnetic field, Phys. Rev. B **63**, 144530 (Mar 2001). 125

[232] R. L. Fagaly, Superconducting quantum interference device instruments and applications, Review of Scientific Instruments **77**(10), 101101 (2006). 125

[233] D. Mailly, C. Chapelier, and A. Benoit, Experimental observation of persistent currents in GaAs-AlGaAs single loop, Phys. Rev. Lett. **70**, 2020–2023 (Mar 1993). 125, 141

[234] L. P. Lévy, G. Dolan, J. Dunsmuir, and H. Bouchiat, Magnetization of mesoscopic copper rings: Evidence for persistent currents, Phys. Rev. Lett. **64**, 2074–2077 (Apr 1990). 125, 141

[235] J. R. Friedman, V. Patel, W. Chen, S. K. Tolpygo, and J. E. Lukens, Quantum superposition of distinct macroscopic states, Nature **406**, 43 EP – (Jul 2000). 125

[236] J. Zou and B. Shao, SUPERPOSITIONS OF COHERENT STATES AND SQUEEZING EFFECTS IN A MESOSCOPIC JOSEPHSON JUNCTION, International Journal of Modern Physics B **13**(08), 917–924 (1999). 125, 128, 130

[237] J. Zou and B. Shao, Quantum coherence in a mesoscopic Josephson junction with dissipation, Phys. Rev. B **64**, 024511 (Jun 2001). 125, 128, 130

[238] C. E. Shannon, A Mathematical Theory of Communication, Bell System Technical Journal **27**(3), 379–423 (1948). 127

[239] F. Grosshans and P. Grangier, Quantum cloning and teleportation criteria for continuous quantum variables, Phys. Rev. A **64**, 010301 (Jun 2001). 127, 140

[240] M. J. Everitt, T. D. Clark, P. B. Stiffell, A. Vourdas, J. F. Ralph, R. J. Prance, and H. Prance, Superconducting analogs of quantum optical phenomena: Macroscopic quantum superpositions and squeezing in a superconducting quantum-interference device ring, Phys. Rev. A **69**, 043804 (Apr 2004). 131

[241] J. Banerji, Non-linear wave packet dynamics of coherent states, Pramana **56**(2), 267–280 (Feb 2001). 132

[242] J. Hannay and M. Berry, Quantization of linear maps on a torus-fresnel diffraction by a periodic grating, Physica D: Nonlinear Phenomena **1**(3), 267 – 290 (1980). 132

[243] J. Clarke and F. K. Wilhelm, Superconducting quantum bits, Nature **453**, 1031 EP – (Jun 2008). 141

[244] L. DiCarlo, J. M. Chow, J. M. Gambetta, L. S. Bishop, B. R. Johnson, D. I. Schuster, J. Majer, A. Blais, L. Frunzio, S. M. Girvin, and R. J. Schoelkopf, Demonstration of two-qubit algorithms with a superconducting quantum processor, Nature **460**, 240 EP – (Jun 2009). 141

[245] J. M. Gambetta, J. M. Chow, and M. Steffen, Building logical qubits in a superconducting quantum computing system, npj Quantum Information **3**(1), 2 (2017). 141