Università degli Studi di Ferrara

DOCTORAL COURSE IN ENGINEERING SCIENCE

Cycle XXXIII

Coordinator: Prof. Stefano Trillo

Quantum Communications: State Characterization and System Design

Scientific/Disciplinary Sector ING-INF/03

Candidate:
Dott. Stefano Guerrini

Supervisor:
Prof. Andrea Conti

Years 2017-2021

Sommario

L'informazione quantistica sarà essenziale nello sviluppo delle reti di futura generazione per una vasta gamma di applicazioni che coinvolgono, nel dominio quantistico, il sensing, la crittografia, la computazione, e le reti. La supremazia delle tecnologie quantistiche si basa sull'utilizzo delle proprietà peculiari della meccanica quantistica, tra cui la sovrapposizione di stati, l'entanglement e il principio di indeterminazione. Questo richiede quindi lo sviluppo di sistemi e reti di comunicazione in grado di sfruttare appieno le potenzialità della meccanica quantistica.

La progettazione di sistemi e reti di comunicazione quantistici pone nuove sfide rispetto alla controparte classica. Da un lato, a livello di sistema, è necessario caratterizzare nuove classi di stati non classici non Gaussiani per poter progettare sistemi di comunicazione quantistici innovativi, in grado di raggiungere nuovi livelli di prestazioni. Dall'altro lato, a livello di rete, la fragilità dei sistemi quantistici richiede lo sviluppo di nuove metodologie per l'analisi e la progettazione di reti quantistiche.

Gli obiettivi di questa tesi di dottorato sono: (i) caratterizzare una importante classe di stati non classici non Gaussiani, noti come photon-added coherent states (PACSs); (ii) introdurre l'utilizzo di stati non classici non Gaussiani nei sistemi di comunicazione quantistici; e (iii) sviluppare un framework per analizzare e progettare le reti per la distribuzione di chiavi quantistiche in presenza di relay intermittenti. Nella tesi si dimostra che l'utilizzo di stati non classici non Gaussiani può migliorare significativamente la discriminazione di stati quantistici. Inoltre, si dimostra che un'analisi globale dei protocolli per la distribuzione di chiavi quantistiche porta a definire nuove strategie per il progetto delle reti. I risultati di questa tesi evidenziano l'utilità degli stati non classici non Gaussiani per i sistemi di comunicazione quantistici ed evidenziano la necessità di definire metodi olistici per l'analisi di reti quantistiche.

Abstract

Quantum information science is essential in the development of future-generation networks for a variety of new applications in the quantum domain involving sensing, cryptography, computing, and networking. The supremacy of quantum technologies relies on the exploitation of unique properties in quantum mechanics, such as superposition, entanglement, and indeterminacy. This calls for the design of communication systems and networks able to unleash the full potentialities of quantum mechanics.

The design of quantum communication systems and networks poses new challenges compared to classical ones. On the one side, at system level, the characterization of new classes of non-classical non-Gaussian states is needed for the design of innovative quantum communication systems with unprecedented performance. On the other side, at network level, the fragility of quantum systems requires the development of new methodologies for the analysis and the design of quantum networks.

The main objectives of this thesis are as follows: (i) characterize an important class of non-classical non-Gaussian states, namely photon-added coherent states (PACSs); (ii) establish the use of non-classical non-Gaussian states for quantum communication systems; and (iii) design a framework for the analysis of quantum key distribution (QKD) networks in the presence of a realistic intermittent relaying. It is shown that the use of non-classical non-Gaussian states can significantly improve the performance of quantum state discrimination. Moreover, it is also shown that a comprehensive analysis and the design of a QKD in the presence of intermittent relaying leads to new network design strategies. The findings of this thesis reveal the utility of non-classical non-Gaussian states for quantum communication systems and highlights the need for an holistic analysis of quantum networks.

Contents

List of Acronyms

BB84 Bennett and Brassard (1984)

CECC classical error-correcting code

CPTP completely positive trace-preserving

CV continuous variable

DEP discrimination error probability

DV discrete variable

FTR fully trusted relay

ICT information and communication technologies

IR information reconciliation

LDPC low-density parity-check codes

LEO low-Earth orbit

MDEP minimum discrimination error probability

MSEP minimum symbol error probability

OPA optical parametric amplifier

PA privacy amplification

PE parameter estimation

IR information reconciliation

PAS photon-added state

PACS photon-added coherent state

PADTS photon-added displaced thermal state

PADSTS photon-added displaced squeezed thermal state

PAGS photon-added Gaussian state

PASS photon-added squeezed state

PATS photon-added thermal state

PSS photon-subtracted state

PSGS photon-subtracted Gaussian state

PSSS photon-subtracted squeezed state

POVM positive operator-valued measure

QCF quantum characteristic function

QN quantum network

QSD quantum state discrimination

QKD quantum key distribution

QOOK quantum on-off keying

QPPM quantum pulse position modulation

SEP symbol error probability

SRM square root measurement

STR simplified trusted relay

Chapter 1

Introduction

1.1 Big picture

Quantum mechanics is a key enabler for next-generation information and communication technologies (ICT). In particular, the possibility to actively employ and engineer the properties of quantum mechanical systems is an essential aspect of the undergoing second quantum revolution [1–3] allowing, on one side, the development of new technologies and applications, including quantum communications [4–9], quantum cryptography [10–13], quantum computing [14–18] and quantum networks [19–23]. On the other side, the use of quantum mechanics allows unprecedented improvements on existing technologies such as high precision sensing and metrology [24–28].

A technology is considered to be quantum if it is based on at least one of the peculiar and unique aspects of quantum mechanics [2]:

- Quantum superposition: the possibility, for a quantum system, to be in a superposition of states (e.g., the Schrodinger cat that is "simultaneously" dead and alive);
- Quantum entanglement: the non-local correlation between two or more spatially separated quantum systems that allows one system to instantaneously affect the other system; and
- Quantum uncertainty: the intrinsic impossibility to simultaneously know all of the properties of a quantum system.

Quantum technologies can be classified into two categories: discrete variables (DVs) [14–17], and continuous variables (CVs) [29–33] DV technologies are based on discrete quantum states, such as qubits and qutrits. DVs are the quantum equivalent of digital signals and they are a natural framework for the development of quantum protocols.

The use of DVs allows on one side, to exploit a simple theory of quantum information; and, on the other side, allows a simpler description of the quantum impairments. However, DVs systems are more difficult to prepare, manage and control, as they are typically embedded in a complex system [14]. Conversely, CVs technologies are based on continuous quantum states, such as coherent states and Gaussian states. CVs are the quantum equivalent of analog signals and they are a natural framework to describe optical and radio quantum signals and thus quantum communication systems. The use of CVs offers, on one side, the possibility to re-use the existing classical network infrastructure by just adapting the apparatuses in the network nodes; and, on the other side, CVs states are more easy to generate and manage with respect to DV states as they have a natural physical description. However, the analysis and the design of protocol in the CV domain is more difficult than in the DV domain.

Recently, DVs and CVs quantum systems have been considered to be merged in a unified framework that exploits the benefits of both the approaches for the development of hybrid powerful technologies [34].

Quantum communications

Quantum communication is the task of transferring classical or quantum information from one place to another by using a quantum carrier, a quantum-capable system. The use of a quantum carrier to transfer information allows to: (i) overcome the performance limits of classical communication systems [4–7]; and (ii) provide an information-theoretical secret communication channel [10–12]. However, the design and the analysis of a quantum communication system is challenging as the symbol error probability (SEP) in the quantum domain requires solving a quantum state discrimination (QSD) problem. This is a difficult task, especially in the presence of thermal noise: the discrimination error probability (DEP) of the QSD problem depends on the set of quantum states and the measurement used to discriminate among them.

When used to transmit classical information, quantum modulations such as quantum on-off keying (QOOK) and quantum pulse position modulation (QPPM) can provide higher reliability than classical ones [4]. Nevertheless, the analysis and the design of a quantum communication system is more difficult than in the classical domain: the error probability depends on the quantum states employed in the constellation, and the design of a quantum receiver that minimizes the error probability is challenging, especially in the presence of noise. In the literature, particular attention has been devoted to the analysis of quantum communication systems that employ Gaussian states [35–46]. In contrast, quantum communication systems with non-Gaussian states has received

less attention except for attempts made on the use of number states [47–49].

Photon-added coherent states (PACSs) and photon-added squeezed states (PASSs) [50–55] are two important classes of non-Gaussian states that can exhibit a non-classical behavior and that can be generated by using linear and non-linear optical devices together with conditional measurements on a coherent state state [56–58].PACSs and PASSs have been considered for use in quantum technologies [59–62] but a characterization of quantum communication systems with PACSs and PASSs is still missing. Determining the effects of thermal noise on quantum communication systems requires a mathematical characterization of the quantum states, which is still missing for these states.

When used to transmit quantum information, quantum systems can be exploited to distribute a information-theoretically secret cryptographic key via a quantum key distribution (QKD) protcol [63–65]. QKD is one of the most mature quantum communication technologies, with several commercial implementations available on the market. However, the distribution of secret keys across long distances is still a challenge with current technologies, due to noise and attenuations in quantum channels [64]. The most promising techniques for long-distance QKD involve the usage of low attenuation optical fibers [66–68] for metropolitan distances and low-Earth orbit (LEO) satellites [69–71] for long-range communications. However, a direct and efficient distribution of secret keys over long distances is a challenging task with current technologies, calling for the implementation of quantum networks to allow a global-scale QKD.

Quantum networks

A quantum network (QN) [19–23] is an ensemble of spatially distributed and physically interconnected nodes that are able to manage and transmit quantum information. Indeed, in analogy with the classical world, the quantum technologies running in a point-to-point scenario can be interconnected with each other to form a QN. QNs exploit the unique features of quantum mechanics to enable new communication and computing applications, including the distribution of cryptographically secret keys (these networks are referred to as QKD networks). However, the analysis and the design of quantum networks present several critical issues that are related to the quantum nature of the systems. First of all, quantum systems, such as the quantum bits, are much more fragile with respect to classical systems, making them more sensible to impairments during the propagation [14]. Furthermore, quantum systems cannot be cloned [72]: as such, it is difficult to apply the store-and-forward paradigm of classical networks. There are two possible solutions to these problems: (i) use quantum repeaters, which are specifi-

cally designed to regenerate a quantum signal and acting transparently with respect to the quantum protocol running on the QN and thus preserving all of its characteristics (e.g., the secrecy of the information in QKD networks); (ii) use trusted nodes, which regenerate the quantum signal by reading it and regenerating a new quantum signal to mitigate the effect of noise impairments, thus requiring the intermediate nodes to be trusted.

In almost all theoretical studies, the efficiency of a QKD protocol is evaluated in terms of the secret key rate (or secret fraction), i.e., the number of secret key bits per raw key bit. This rate is the most important figure of merit in the design of a QKD link, as it gives an estimate of the speed that the QKD system can achieve. However, in a QKD network, it may happen that one or more of the relays are not always available to their neighbours, as in the case of LEO satellites. Moreover, the end nodes may be able to communicate between them using an existing communication network (e.g., Internet), even in the absence of the relay. This is the case of the recent satellite-relayed QKD network established through the Chinese satellite named Micius [71]. In this scenario, the design and the analysis of a QKD protocol is more subtle, and it should take into account these limitations to improve the overall secret key throughput of the network, i.e., the total amount of exchanged secret key bits in the time frame during which the relay is visible to the end nodes.

1.2 Objectives

The goals of this thesis is to establish the use of non-Gaussian states for quantum technologies and provide new methodologies for the analysis of quantum networks.

The key contributions of the thesis are as follows:

- characterization of PACSs in terms of Fock representation and quasi-probability distributions;
- put forth the idea of using PACSs for QSD and quantum communication systems;
- characterization of QSD with noisy PACSs in terms of DEP;
- characterization of QOOK and QPPM system operating with noisy PACSs in terms of SEP;
- analysis of the decoherence and losses effects on the system performance for both QOOK and QPPM systems;

- evaluation of the source generation efficiency and its impact on the data rate for both QOOK and QPPM systems.
- definition of a new metric for the comparison of QKD network protocols with intermittent relaying; and
- analysis of the secret key throughput for protocols operating in an intermittent-relay scenario.

The remainder of the thesis is organized as in the Following.

Chapter 2 reviews the fundamentals of quantum mechanics and presents the mathematical preliminaries to describe DVs and CVs quantum systems.

Chapter 3 provides a characterization for the class of PACSs in terms of Fock representation, Wigner W-function, Glauber–Sudarshan P-function, and Husimi–Kano Q-function.

Chapter 4 characterizes QSD with PACSs in terms of DEP with and without noise in state preparation.

Chapter 5 characterizes the performance of QOOK and QPPM systems employing PACSs and PASSs in the presence of noise in state preparation. Morevover, the effect of decoherence and noise impairments is analyzed for these systems.

Chapter 6 analyses the performance of a QKD networks in the presence of intermittent trusted relays and defines a new performance metric for QNs operating in this scenario referred to as secret key throughput. This metric is then applied to analyze the performance of different protocols in a realistic scenario involving a LEO satellite.

The results presented in this thesis have been published in the proceedings of international conferences and journals [5–7, 13].

1.3 Notation

Random variables are displayed in sans serif, upright fonts; their realizations in serif, italic fonts. Vectors are denoted by bold lowercase letters. Operators and matrices are denoted by uppercase letters. For example, a random variable and its realization are denoted by x and x; a random vector and its realization are denoted by $\mathbf{x}$ and $\boldsymbol{x}$; a random matrix/operator and its realization are denoted by $\mathbf{X}$ and $\boldsymbol{X}$, respectively. Sets are denoted by upright sans serif. The m-by-m identity matrix is denoted by $\boldsymbol{I}_m$: the subscript is removed when the dimension of the matrix is clear from the context.

The sets of complex numbers and of positive integer numbers are denoted by $\mathbb{C}$ and $\mathbb{N}$, respectively. For $z \in \mathbb{C}$: $|z|$ and $\arg(z)$ denote the absolute value and the

phase, respectively; $\mathrm{Re}\{z\} = z_\mathrm{r}$ and $\mathrm{Im}\{z\} = z_\mathrm{i}$ denote the real part and the imaginary part, respectively; z^* is the complex conjugate; $\check{\boldsymbol{z}} = [z \;\; z^*]^T$ is the augmented vector associated to z; and $\imath = \sqrt{-1}$. The trace and the adjoint of an operator are denoted by $\mathrm{tr}\{\cdot\}$ and $(\cdot)^\dagger$, respectively. The trace norm of an operator is represented by $\|\cdot\|_1$. For a matrix $\boldsymbol{M} \in \mathbb{C}^{n\times m}$: $\boldsymbol{M}^\mathrm{T}$ denotes the transpose; $\boldsymbol{M}^\mathrm{H}$ denotes the transpose conjugate. For a quantum system: $\mathcal{H}$ denotes the Hilbert space of states; $\mathcal{D}(\mathcal{H})$ denotes the set of densities operators on $\mathcal{H}$, i.e., $\mathcal{D}(\mathcal{H}) = \{\boldsymbol{\Xi} : \mathcal{H} \to \mathcal{H} \,|\, \boldsymbol{\Xi} = \boldsymbol{\Xi}^\dagger \text{ and } \mathrm{tr}\{\boldsymbol{\Xi}\} = 1\}$. For two operators $\boldsymbol{X}$ and $\boldsymbol{Y}$, the commutator is denoted by $[\boldsymbol{X}, \boldsymbol{Y}] = \boldsymbol{X}\boldsymbol{Y} - \boldsymbol{Y}\boldsymbol{X}$. For a quantum state $\boldsymbol{\Xi}$, the expectation value of an observable $\boldsymbol{A}$ is $\langle \boldsymbol{A} \rangle = \mathrm{tr}\{\boldsymbol{\Xi}\boldsymbol{A}\}$.

Chapter 2

Quantum information

Quantum information is the discipline that underpins the second quantum revolution. It considers the creation, the manipulation, and the transmission of quantum or classical information via a quantum system. There are two complementary approaches to quantum information: CV, and DV. A CV system is the quantum equivalent of an analog signal, and it is well-suited to describe the low-level protocols of a quantum network such as the quantum communication systems. In these systems, the information is encoded in a quantum system having a degree of freedom with a continuous spectrum. A DV system is the quantum equivalent of a digital signal, and it is well-suited to describe high-level applications and protocols, such as quantum computing and quantum cryptography. In these systems, the information is encoded in a quantum system having a degree of freedom with a finite spectrum.

This section reviews the fundamentals of quantum mechanics and presents the mathematical preliminaries on CVs and DVs systems.

2.1 Fundamentals of quantum mechanics

2.1.1 Postulates

This section reviews the postulate of quantum mechanics in the form of Dirac and von Neumann [73, 74].

Postulate 1 (States)**.** The state space of an isolated physical system is a separable complex Hilbert space $\mathcal{H}$. The system is completely described by its state vector $|\psi\rangle$, which is a unit vector in the space $\mathcal{H}$.

Postulate 2 (Observables)**.** Every observable is associated with a linear, self-adjoint operator $\boldsymbol{M}$ on the space $\mathcal{H}$. The possibile outcomes for m are the eigenvalues of $\boldsymbol{M}$.

If the system is in the state $|\psi\rangle$, the probability to get the outcome m is equal to $\mathbb{P}\{\mathsf{m} = m\} = \langle\psi| \boldsymbol{E}_m |\psi\rangle$ where $\boldsymbol{E}_m$ is the projector onto the eigenspace corresponding to m. For the outcome m, the state of the system after the measurement is $\boldsymbol{E}_m |\psi\rangle$.

Postulate 3 (Evolution)**.** The evolution of a closed quantum system is described by a unitary operator $\boldsymbol{U}$ in $\mathcal{H}$. Let the system be in the state $|\psi(t_0)\rangle$ at the time instant t_0. Then, the state of the system $|\psi(t)\rangle$ at the time istant t is:

$$|\psi(t)\rangle = \boldsymbol{U}(t, t_0) |\psi(t_0)\rangle \ . \tag{2.1}$$

Postulate 4 (Composite systems)**.** The space state $\mathcal{H}$ of a system composed by two subsystems, $\mathcal{H}_1$ and $\mathcal{H}_2$, is given by the tensor product $\mathcal{H} = \mathcal{H}_1 \otimes \mathcal{H}_2$.

2.1.2 Quantum noise

This section gives a description of quantum systems, channels and measurement in the presence of noise. In practice, the noise can be interpreted as the interaction of a quantum system with its surrounding.

Noisy states

In the most general framework which comprehends the possibility for a quantum state to be affected by noise, the definition for a quantum state is given as follows.

Definition 2.1.1. The state of a quantum system is determined by a linear operator, called density operator, $\boldsymbol{\Xi} : \mathcal{H} \to \mathcal{H}$ such that $\boldsymbol{\Xi} = \boldsymbol{\Xi}^\dagger$ and $\mathrm{tr}\{\boldsymbol{\Xi}\} = 1$.

According to this definition, the postulates can be reformulated as follows.

Measurement. If the system is in the state $\boldsymbol{\Xi}$, the probability to get the outcome m with the observable $\boldsymbol{M}$ is $\mathbb{P}\{\mathsf{m} = m\} = \mathrm{tr}\{\boldsymbol{\Xi}\boldsymbol{E}_m\}$ and the state after the measurement, given the outcome m, is given by $\boldsymbol{E}_m\boldsymbol{\Xi}\boldsymbol{E}_m^\dagger / \mathrm{tr}\{\boldsymbol{E}_m\boldsymbol{\Xi}\boldsymbol{E}_m^\dagger\}$, where $\boldsymbol{E}_m$ is the projector into the eigenspace corresponding to the eigenvalue m of $\boldsymbol{M}$.

Evolution. If the system is in the state $\boldsymbol{\Xi}$, the state after the evolution described by the unitary operator $\boldsymbol{U}$ is given by $\boldsymbol{U}\boldsymbol{\Xi}\boldsymbol{U}^\dagger$.

Quantum channels

The description of the evolution for a quantum system given in Postulate 3 is not sufficiently general to describe all of the possible evolution. In particular, it does not

consider the possibility for a quantum system $\boldsymbol{\Xi}_S$ to interact with an ancilla in the state $\boldsymbol{\Xi}_A$ using a unitary evolution $\boldsymbol{U}_{SA}$, and then perform a joint measurement $\boldsymbol{M}_{SA}$ on the two systems. The ancilla is then discarded after the measurement. In this case, the state of the system after the interaction is given by

$$\mathrm{tr}_B \left\{ \sum_m \frac{\boldsymbol{E}_m \boldsymbol{U}_{SA} \boldsymbol{\Xi}_S \otimes \boldsymbol{\Xi}_A \boldsymbol{U}_{SA}^\dagger \boldsymbol{E}_m^\dagger}{\mathrm{tr}\{\boldsymbol{E}_m \boldsymbol{U}_{SA} \boldsymbol{\Xi}_S \otimes \boldsymbol{\Xi}_A \boldsymbol{U}_{SA}^\dagger \boldsymbol{E}_m^\dagger\}} \right\}$$

It can be shown that this definition is equivalent to the following.

Definition 2.1.2. A quantum channel is described by a linear completely positive trace-preserving (CPTP) mapping $\boldsymbol{C} : \mathcal{D}(\mathcal{H}) \to \mathcal{D}(\mathcal{H})$ such that the state $\boldsymbol{\Xi}$ at the end of the quantum channel is $\boldsymbol{C}(\boldsymbol{\Xi})$.

Generalized measurements

The description of a quantum measurement given in Postulate 2 is not sufficiently general to describe all of the observations which can be performed in the real world. In particular, it does not consider the possibility for a quantum system $\boldsymbol{\Xi}_S$ to interact with an ancilla in the state $\boldsymbol{\Xi}_A$ and then perform a joint measurement $\boldsymbol{M}_{SA}$ on the two systems. In this case, the state of the quantum system after the measurement with outcome m is given by

$$\frac{\mathrm{tr}_B\{\boldsymbol{E}_m \boldsymbol{U}_{SA} \boldsymbol{\Xi}_S \otimes \boldsymbol{\Xi}_A \boldsymbol{U}_{SA}^\dagger \boldsymbol{E}_m^\dagger\}}{P_m}$$

where $\boldsymbol{E}_m$ is the projector onto the eigenspace of $\boldsymbol{M}_{SA}$ associated to m, and $P_m = \mathrm{tr}\{\boldsymbol{E}_m \boldsymbol{U}_{SA} \boldsymbol{\Xi}_S \otimes \boldsymbol{\Xi}_A \boldsymbol{U}_{SA}^\dagger \boldsymbol{E}_m^\dagger\}$ is the probability to get the outcome m.

If the state after the measurement is not of importance, then this is equivalent to the following definition.

Definition 2.1.3. A positive operator-valued measure (POVM) is described by a set of operators $\mathcal{P} = \{\boldsymbol{\Pi}_0, \boldsymbol{\Pi}_1, ..., \boldsymbol{\Pi}_{M-1}\}$ such that $\boldsymbol{\Pi}_i \succcurlyeq 0$ for $i = 0, 1, ..., M-1$, and $\sum_i \boldsymbol{\Pi}_i = \boldsymbol{I}$. The probability to get the i-th outcome for a given state $\boldsymbol{\Xi}$ is $\mathrm{tr}\{\boldsymbol{\Xi}\boldsymbol{\Pi}_i\}$.

2.1.3 Relevant properties

In this section, we report two noticeable results which are fundamental for quantum cryptography.

Uncertainty

The Heisenberg uncertainty principle is one of the oldest results in quantum mechanics. It formally states that it is not possible to have, at the same time, a perfect knowledge of two observable quantities which belong to operators that do not commute.

Theorem 2.1.4 (Robertson-Heisenberg)**.** Let $|\psi\rangle \in \mathcal{H}$ be a quantum state. For any two observables $\boldsymbol{A}$, $\boldsymbol{B}$:

$$\Delta \boldsymbol{A} \Delta \boldsymbol{B} \geq \frac{1}{2} |\langle \psi | \left[\boldsymbol{A}, \boldsymbol{B} \right] | \psi \rangle| \,. \tag{2.2}$$

where $(\Delta \boldsymbol{A})^2 = \langle \psi | \, \boldsymbol{A}^2 \, | \psi \rangle - \langle \psi | \, \boldsymbol{A} \, | \psi \rangle^2$ and $(\Delta \boldsymbol{B})^2 = \langle \psi | \, \boldsymbol{B}^2 \, | \psi \rangle - \langle \psi | \, \boldsymbol{B} \, | \psi \rangle^2$.

No-cloning

One of the most simple results of quantum mechanics is the no-cloning Theorem. Despite its simplicity, it was discovered only in 1982 by Wooters and Zurek [72] and has profound implications in quantum information.

Theorem 2.1.5. It is not possible to create a copy of an unknown quantum state.

Proof. Let's suppose that such a system exists. If the state space is the Hilbert space $\mathcal{H}$, it means that there exist a unitary operator $\boldsymbol{U}$ in $\mathcal{H} \otimes \mathcal{H}$ such that for all source states $|\psi\rangle, |\phi\rangle \in \mathcal{H}$ it is able to to build a copy of the state, independently from the state $|s\rangle$ of the target system. Thus, $\forall \, |s\rangle \in \mathcal{H}$:

$$\boldsymbol{U}\big(\, |\psi\rangle \otimes |s\rangle \, \big) = |\psi\rangle \otimes |\psi\rangle$$

$$\boldsymbol{U}\big(\, |\phi\rangle \otimes |s\rangle \, \big) = |\phi\rangle \otimes |\phi\rangle \ .$$

It follows that:

$$\langle \phi | \, \langle s | \, \boldsymbol{U}^\dagger \boldsymbol{U} \, | \psi \rangle \, | s \rangle = \left[\langle \phi | \psi \rangle \right]^2 = \langle \phi | \psi \rangle \ .$$

Where the last equality follows from the unitarity of $\boldsymbol{U}$. However, the last relation can hold if and only if $\langle \phi | \psi \rangle$ is equal to 0 or 1. This means that a cloning operator can only work correctly if the input states are orthogonal. Therefore, a general cloning device can not exist.

□

2.2 Quantum information with continuous variables

The CV framework is related to the study of quantum systems with an infinite-dimensional Hilbert space. The CV framework is used to describe the quantized elec-

tromagnetic field, that is the best-known example of CV quantum system. Indeed, the electromagnetic field inside a conductive cavity can be represented as a superposition of modes which behave as independent harmonic oscillators. For these reasons, hereafter, the term CV system will be used to indicate a system behaving like a set of harmonic oscillator.

2.2.1 Classical electromagnetic field

Consider an electromagnetic cavity with perfectly conducting walls delimited by the volume $\mathcal{V} \subset \mathbb{R}^3$. The electric field $\boldsymbol{e}(\boldsymbol{r}, t)$ inside the cavity is determined by Maxwell's equations and can be written as a superposition of the cavity modes [75–77]

$$\boldsymbol{e}(\boldsymbol{r}, t) = -\sum_n p_n(t)\boldsymbol{u}_n(\boldsymbol{r}) \tag{2.3}$$

where $p_n(t)$ and $\boldsymbol{u}_n(\boldsymbol{r})$ describe the temporal evolution and the shape of each cavity mode, respectively, and are determined by the initial conditions of the field and the shape of the cavity [75–77]. For a cubical cavity of side L, it can be shown that

$$\boldsymbol{u}_n(\boldsymbol{r}) = \frac{1}{\sqrt{L^3}} \exp\{\imath \boldsymbol{k}_n \cdot \boldsymbol{r}\}$$

where $\boldsymbol{k}_n$ is the propagation vector that defines the allowed frequencies $\omega_n = c|\boldsymbol{k}_n|^2$. Correspondingly, the magnetic field $\boldsymbol{h}(\boldsymbol{r}, t)$ is given by

$$\boldsymbol{h}(\boldsymbol{r}, t) = \sum_n q_n(t)\nabla \times \boldsymbol{u}_n(\boldsymbol{r}) \tag{2.4}$$

where $q_n(t)$ is related to $p_n(t)$ by the relation

$$p_n(t) = \frac{\mathrm{d}q_n(t)}{\mathrm{d}t}\,. \tag{2.5}$$

The total energy H of the electromagnetic field is given by

$$H = \frac{1}{2}\int_{\mathcal{V}} \epsilon_0 \boldsymbol{e}^2(\boldsymbol{r}, t) + \mu_0 \boldsymbol{h}^2(\boldsymbol{r}, t)\,\mathrm{d}\boldsymbol{r} \tag{2.6}$$

and, by using (2.3)-(2.4), it can be expressed as

$$H = \sum_n H_n \tag{2.7}$$

where H_n is the energy associated to the mode n, and it is given by

$$H_n = \frac{1}{2}\left[p_n^2(t) + \omega_n^2 q_n^2(t)\right] . \tag{2.8}$$

Therefore, the electromagnetic field inside an ideal cavity is formally equivalent to an infinite ensemble of uncoupled harmonic oscillators. The harmonic oscillator can be equivalently described by introducing the complex variable $a_n(t)$ defined as

$$a_n(t) = \frac{\omega_n q_n(t) + \imath p_n(t)}{\sqrt{2\hbar\omega_n}} . \tag{2.9}$$

By using (2.9) in (2.8), the energy of every harmonic oscillator can be expressed as

$$H_n = \hbar\omega_n |\alpha_n(t)|^2 \tag{2.10}$$

and thus the total energy in terms of $\alpha_n(t)$ is given by

$$H = \sum_{n=-\infty}^{\infty} \hbar\omega_n |\alpha_n(t)|^2 . \tag{2.11}$$

2.2.2 Quantized electromagnetic field

The quantization of the electromagnetic field is obtained by associating two time-varying Hermitian operators $\boldsymbol{Q}_n(t), \boldsymbol{P}_n(t) \in \mathcal{L}(\mathcal{H}_n)$ to the two dynamical variables $q_n(t)$ and $p_n(t)$ of the classical harmonic oscillator, for every n.[1] Note that, by construction, the Hilbert space $\mathcal{H}_n$ associated to the n-th mode of the cavity is infinite dimensional as the physical observables $\boldsymbol{Q}_n(t)$ and $\boldsymbol{P}_n(t)$ are allowed to assume numerical values in a continuous interval. Therefore, the Hilbert space $\mathcal{H}$ associated to the quantized electromagnetic field is given by $\mathcal{H} = \otimes_n \mathcal{H}_n$.

The quantization is obtained by imposing the following set of commutation relations for every n, m

$$[\boldsymbol{Q}_n, \boldsymbol{P}_m] = \imath\hbar\delta_{n,m}\boldsymbol{I} \tag{2.12}$$

$$[\boldsymbol{Q}_n, \boldsymbol{Q}_m] = 0 \tag{2.13}$$

$$[\boldsymbol{P}_n, \boldsymbol{P}_m] = 0 . \tag{2.14}$$

The quantum harmonic oscillator can be equivalently described by introducing the

[1] In the following, unless otherwise specified, the temporal dependence of the operators will not be considered.

annihilation operator defined as

$$\boldsymbol{A}_n = \frac{\omega_n \boldsymbol{Q}_n + \imath \boldsymbol{P}_n}{\sqrt{2\hbar\omega_n}}\,. \tag{2.15}$$

Notice that $\boldsymbol{A}_n$ is not self-adjoint and thus it is not an observable. The adjoint of $\boldsymbol{A}_n$ is called creation operator and it is given by

$$\boldsymbol{A}_n^\dagger = \frac{\omega_n \boldsymbol{Q}_n - \imath \boldsymbol{P}_n}{\sqrt{2\hbar\omega_n}}\,. \tag{2.16}$$

From (2.7), the Hamiltonian of the quantum system is

$$\boldsymbol{H} = \sum_n \boldsymbol{H}_n \tag{2.17}$$

where

$$\boldsymbol{H}_n = \frac{1}{2}\left[\boldsymbol{P}_n^2 + \omega_n^2 \boldsymbol{Q}_n^2\right] \tag{2.18}$$

is the Hamiltonian operator associated to the n-th cavity mode. Equivalently, from (2.10), the Hamiltonian can be expressed in terms of $\boldsymbol{A}_n^\dagger$ and $\boldsymbol{A}_n$ as

$$\boldsymbol{H}_n = \hbar\omega_n \boldsymbol{A}_n^\dagger \boldsymbol{A}_n\,. \tag{2.19}$$

Single-mode cavity

In several cases of practical interest, it is useful to consider a single-mode cavity for which the Hilbert space $\mathcal{H}$ corresponds to the Hilbert space of a single quantum Harmonic oscillator, and thus the Hamiltonian reduces to

$$\boldsymbol{H} = \hbar\omega \boldsymbol{A}^\dagger \boldsymbol{A} \tag{2.20}$$

where $\boldsymbol{A}$ and $\boldsymbol{A}^\dagger$ are the bosonic field operators associated to the single mode of the quantum field. In this case the number operator is $\boldsymbol{N} = \boldsymbol{A}^\dagger \boldsymbol{A}$.

Fock states

The operator $\boldsymbol{N}_n = \boldsymbol{A}_n^\dagger \boldsymbol{A}_n$ is called the number operator of the n-th mode and it can be shown that its spectrum is discrete, i.e.,

$$\boldsymbol{N}_n \left|n_n\right\rangle = n_n \left|n_n\right\rangle \tag{2.21}$$

with $n_n \in \mathbb{N}$. Hence, by (2.19), the energy of a quantum harmonic oscillator is quantized and the measurement operator $\boldsymbol{N}_n$ determines the number of "quanta" in the mode n. In particular, from (2.19) and the definition of $\boldsymbol{N}_n$, the Hamiltonian is

$$\boldsymbol{H} = \sum_n \hbar\, \omega_n \boldsymbol{N}_n \tag{2.22}$$

and, from (2.21) and (2.22) the eigenvalues of $\boldsymbol{H}$ are

$$E_{\boldsymbol{n}} = \sum_n \hbar\, \omega_n n_n \tag{2.23}$$

where $\boldsymbol{n} = \{n_n\}_n$ is the vector containing the number of "quanta" of each mode. It is thus possible to introduce the operator $\boldsymbol{N}$ which quantifies the total number of "quanta" in the quantized electromagnetic field, and it is given by

$$\boldsymbol{N} = \sum_n \boldsymbol{A}_n^\dagger \boldsymbol{A}_n \,. \tag{2.24}$$

The spectrum of $\boldsymbol{N}$ is discrete and it is given by

$$\boldsymbol{N} \left|\boldsymbol{n}\right\rangle = n \left|\boldsymbol{n}\right\rangle \tag{2.25}$$

where the eigenvalue n (i.e., the number of quanta) is

$$n = \sum_n \boldsymbol{n}_n \tag{2.26}$$

and the eigenvector $|\boldsymbol{n}\rangle$ is

$$\left|\boldsymbol{n}\right\rangle = \bigotimes_n \left|n_n\right\rangle \,. \tag{2.27}$$

The state $|\boldsymbol{n}\rangle$ is referred to as multi-mode Fock state. The state $|\boldsymbol{0}\rangle$ is associated to the lowest energy level of the system and thus it is also referred to as ground state. It is important to note that the set of all Fock states forms an orthonormal basis for the Hilbert space $\mathcal{H}$. Therefore, every state $\boldsymbol{\Xi} \in \mathcal{D}(\mathcal{H})$ can be represented as

$$\boldsymbol{\Xi} = \sum_{\boldsymbol{n}} \sum_{\boldsymbol{m}} c_{\boldsymbol{n},\boldsymbol{m}} \left|\boldsymbol{n}\right\rangle\!\left\langle\boldsymbol{m}\right| \tag{2.28}$$

where

$$c_{\boldsymbol{n},\boldsymbol{m}} = \left\langle\boldsymbol{n}\right| \boldsymbol{\Xi} \left|\boldsymbol{m}\right\rangle \,. \tag{2.29}$$

Single-mode Fock states

In a single mode cavity the number operator is given by $\boldsymbol{N} = \boldsymbol{A}^\dagger \boldsymbol{A}$. Therefore, the set of the single-mode Fock states is determined by the eigenvalue equation

$$\boldsymbol{N} \left|n\right\rangle = n \left|n\right\rangle \ .$$

It can be proven that [73] the action of the annihilation operator on a Fock state decreases the number of photons by one, i.e.,

$$\boldsymbol{A} \left|n\right\rangle = \sqrt{n} \left|n-1\right\rangle \ . \tag{2.30}$$

Conversely, the action of the creation operator on a Fock state increases the number of photons by one, i.e.,

$$\boldsymbol{A}^\dagger \left|n\right\rangle = \sqrt{n+1} \left|n+1\right\rangle \ . \tag{2.31}$$

Finally, observe that by using Equations (2.28)-(2.29) every single-mode state $\boldsymbol{\Xi}$ can be represented using the (single-mode) Fock representation

$$\boldsymbol{\Xi} = \sum_n \left\langle n\right| \boldsymbol{\Xi} \left|m\right\rangle \left|n\right\rangle\!\left\langle m\right| \ . \tag{2.32}$$

Thermal state

Consider an electromagnetic cavity in thermal equilibrium with its surrounding. In this case, the probability that the system is in a state with a given energy E is given by the Boltzmann distribution, and it is proportional to $\exp\{-E/(k_{\mathrm{B}}T)\}$. Recall that the energy levels for the quantized electromagnetic fields are given by (2.23) and therefore, the state of the system in thermal equilibrium is

$$\boldsymbol{\Xi} = \frac{1}{Z} \sum_{\boldsymbol{n}} \exp\left\{-\frac{E_{\boldsymbol{n}}}{k_{\mathrm{B}}T}\right\} \left|\boldsymbol{n}\right\rangle\!\left\langle \boldsymbol{n}\right|$$

where Z is a normalization constant, called partition function, that ensures $\mathrm{tr}\{\boldsymbol{\Xi}\} = 1$. It can be shown that [77] $Z = \prod_n Z_n$ with

$$Z_n = \left(1 - \exp\left\{-\frac{\hbar\omega_n}{k_{\mathrm{B}}T}\right\}\right)^{-1} .$$

Furthermore the state $\boldsymbol{\Xi}$ is a product of independent states for each mode, i.e.,

$$\boldsymbol{\Xi} = \bigotimes_n \boldsymbol{\Xi}_n$$

where $\boldsymbol{\Xi}_n = \boldsymbol{\Xi}_{\text{th}}$, with

$$\boldsymbol{\Xi}_{\text{th}} = \sum_{n=0}^{\infty} \frac{\bar{n}^n}{(\bar{n}+1)^{n+1}} |n\rangle\langle n| \tag{2.33}$$

and

$$\bar{n} = \left(\exp\left\{ -\frac{\hbar\omega}{k_{\text{B}}T} \right\} - 1 \right)^{-1} \tag{2.34}$$

in which, for each mode, $n = n_n$ and $\omega = \omega_n$. Notice that Equation (2.34) is the famous Planck distribution. In the following, the state (2.33) will be referred to as thermal state. Equation (2.33) can be conveniently rewritten as [4]

$$\boldsymbol{\Xi}_{\text{th}} = (1-v) \sum_{n=0}^{\infty} v^n |n\rangle\langle n| \tag{2.35}$$

where

$$v = \frac{\bar{n}}{\bar{n}+1} \,. \tag{2.36}$$

2.2.3 Quantum transformations

This section presents some important transformations that can be applied to a single-mode or a two-mode CV system by using physical devices.

Displacement

The first important evolution operator for a single-mode CV system is the displacement operator defined as

$$\boldsymbol{D}_{\xi} = \exp\{\xi \boldsymbol{A}^{\dagger} - \xi^* \boldsymbol{A}\} \,. \tag{2.37}$$

In the Heisenberg picture, the annihilation and creation operators $\boldsymbol{A}$ and $\boldsymbol{A}^{\dagger}$, are transformed by the linear transformation

$$\begin{bmatrix} \boldsymbol{A} \\ \boldsymbol{A}^{\dagger} \end{bmatrix} \rightarrow \begin{bmatrix} \boldsymbol{A} \\ \boldsymbol{A}^{\dagger} \end{bmatrix} + \begin{bmatrix} \alpha \\ \alpha^* \end{bmatrix} \boldsymbol{I} \,. \tag{2.38}$$

The displacement operator can be implemented by using a beam splitter together with a strong laser beam [78].

Rotation

The second important evolution operator for a single-mode CV system is the rotation operator defined as

$$\boldsymbol{R}_{\phi} = \exp\{\imath\phi \boldsymbol{A}^{\dagger}\boldsymbol{A}\} \,. \tag{2.39}$$

In the Heisenberg picture, the annihilation and creation operators $\boldsymbol{A}$ and $\boldsymbol{A}^\dagger$, are transformed by the linear transformation

$$\begin{bmatrix} \boldsymbol{A} \\ \boldsymbol{A}^\dagger \end{bmatrix} \rightarrow \begin{bmatrix} e^{\imath\theta} & 0 \\ 0 & e^{-\imath\theta} \end{bmatrix} \begin{bmatrix} \boldsymbol{A} \\ \boldsymbol{A}^\dagger \end{bmatrix} . \tag{2.40}$$

The rotation operator can be implemented by increasing the optical length of the electromagnetic beam by using, for example, a transparent material with a different refractive index [31].

Squeezing

The last important evolution operator for a single-mode CV system is the squeezing operator defined as

$$\boldsymbol{S}_\zeta = \exp\{\frac{1}{2}(\zeta(\boldsymbol{A}^\dagger)^2 + \zeta^*\boldsymbol{A}^2)\} . \tag{2.41}$$

In the Heisenberg picture, the annihilation and creation operators $\boldsymbol{A}$ and $\boldsymbol{A}^\dagger$, are transformed by the linear transformation

$$\begin{bmatrix} \boldsymbol{A} \\ \boldsymbol{A}^\dagger \end{bmatrix} \rightarrow \begin{bmatrix} \cosh(r) & -\sinh(r)e^{-\imath\phi} \\ -\sinh(r)e^{\imath\phi} & \cosh(r) \end{bmatrix} \begin{bmatrix} \boldsymbol{A} \\ \boldsymbol{A}^\dagger \end{bmatrix} . \tag{2.42}$$

The single-mode squeezing operator can be implemented by using a degenerate parametric amplifier [79].

Beam splitter

The first important evolution operator for a two-mode CV system is the beam splitter defined as

$$\boldsymbol{B}_\theta = \exp\{\theta(\boldsymbol{A}_1^\dagger\boldsymbol{A}_2 - \boldsymbol{A}_1\boldsymbol{A}_2^\dagger)\} . \tag{2.43}$$

In the Heisenberg picture, the annihilation and creation operators $\boldsymbol{A}_1$, $\boldsymbol{A}_2$, and $\boldsymbol{A}_1^\dagger$, $\boldsymbol{A}_2^\dagger$ for the two modes are transformed by the linear transformation

$$\begin{bmatrix} \boldsymbol{A}_1 \\ \boldsymbol{A}_1^\dagger \\ \boldsymbol{A}_2 \\ \boldsymbol{A}_2^\dagger \end{bmatrix} \rightarrow \begin{bmatrix} \sqrt{\tau}\boldsymbol{I}_2 & \sqrt{1-\tau}\boldsymbol{I}_2 \\ -\sqrt{1-\tau}\boldsymbol{I}_2 & \sqrt{\tau}\boldsymbol{I}_2 \end{bmatrix} \begin{bmatrix} \boldsymbol{A}_1 \\ \boldsymbol{A}_1^\dagger \\ \boldsymbol{A}_2 \\ \boldsymbol{A}_2^\dagger \end{bmatrix} . \tag{2.44}$$

The beam splitter is a four-port device that can be implemented using a mirror [77].

Two-mode squeezing

The last important evolution operator for a two-mode CV system is the two-mode squeezing operator defined as

$$\boldsymbol{S}_{\zeta}^{(2)} = \exp\{\zeta \boldsymbol{A}_1^{\dagger}\boldsymbol{A}_2^{\dagger} + \zeta^{*}\boldsymbol{A}_1\boldsymbol{A}_2\}\,. \tag{2.45}$$

In the Heisenberg picture, the annihilation and creation operators $\boldsymbol{A}_1$, $\boldsymbol{A}_2$, and $\boldsymbol{A}_1^{\dagger}$, $\boldsymbol{A}_2^{\dagger}$ for the two modes are transformed by the linear transformation

$$\begin{bmatrix} \boldsymbol{A}_1 \\ \boldsymbol{A}_1^{\dagger} \\ \boldsymbol{A}_2 \\ \boldsymbol{A}_2^{\dagger} \end{bmatrix} \rightarrow \begin{bmatrix} \cosh(2r)\boldsymbol{I}_2 & -\sinh(2r)\boldsymbol{I}_2 \\ -\sinh(2r)\boldsymbol{I}_2 & \cosh(2r)\boldsymbol{I}_2 \end{bmatrix} \begin{bmatrix} \boldsymbol{A}_1 \\ \boldsymbol{A}_1^{\dagger} \\ \boldsymbol{A}_2 \\ \boldsymbol{A}_2^{\dagger} \end{bmatrix}\,. \tag{2.46}$$

The two-mode squeezing operator can be implemented by using a non-degenerate parametric amplifier [31].

2.2.4 Phase-space description

The state of a CV quantum system is described by an infinite-dimensional density operator $\boldsymbol{\Xi}$. The phase-space description of a CV quantum system provides an alternative and convenient representation for the quantum state $\boldsymbol{\Xi}$ via a complex function called quasi-probability distribution. This tool was introduced by Wigner [80] and further investigated in [81, 82] and [83–85]. For simplicity, we consider here only the case of a single-mode bosonic system. The extension to the multidimensional case is trivial and can be found in other works [29–33, 45].

Characteristic function

In analogy with classical probability theory [86], the state of a quantum system can be expressed in terms of a complex-valued function called quantum characteristic function, which is the Fourier-Weyl transform of the density operator associated to the state.

Definition 2.2.1 (Quantum characteristic function)**.** The s–ordered characteristic function $\chi(\xi, s)$, with $\xi, s \in \mathbb{C}$, associated to the quantum state $\boldsymbol{\Xi}$ is

$$\chi(\xi, s) = \exp\left\{\frac{s}{2}|\xi|^2\right\} \mathrm{tr}\{\boldsymbol{\Xi}\boldsymbol{D}_{\xi}\}\,. \tag{2.47}$$

Notice that, in contrast to classical probability theory, there is an infinite number of quantum characteristic functions, indexed by the parameter $s \in \mathbb{C}$, representing

the same quantum state. This can be attributed to the non-commutativity of the annihilation and creation operators for which the parameter s identifies the ordering of the product. Indeed notice that, by using the Baker–Campbell–Hausdorff formula [87, 88]

$$\boldsymbol{D}_{\xi} = e^{\xi \boldsymbol{A}^{\dagger} - \xi^{*} \boldsymbol{A}} = e^{\xi \boldsymbol{A}^{\dagger}} e^{-\xi^{*} \boldsymbol{A}} e^{-\frac{1}{2}|\xi|^{2}} = e^{-\xi^{*} \boldsymbol{A}} e^{\xi \boldsymbol{A}^{\dagger}} e^{\frac{1}{2}|\xi|^{2}} . \tag{2.48}$$

Notice that, in the second equality, all of the creation operators are on the left and all the annihilation operators are on the right (normal ordering), and, in the third equality all of the creation operators are on the right and all the annihilation operators are on the left (anti-normal ordering). The ordering in the first equality is the so called symmetric ordering. Therefore, it is possible to define an s-ordered displacement operator as

$$\boldsymbol{D}_{\xi,s} = \boldsymbol{D}_{\xi} \exp\left\{ \frac{s}{2} |\xi|^{2} \right\} \tag{2.49}$$

which comprehends the normal ordering ($s = 1$), the anti-normal ordering ($s = -1$) and the symmetric ordering ($s = 0$).

In analogy with the classical characteristic function, the quantum characteristic function can be used to compute the moments of the s–ordered product, hereafter referred with $\{(\boldsymbol{A}^{\dagger})^{n} \boldsymbol{A}^{m}\}_{s}$, as follows

$$\left\langle \{(\boldsymbol{A}^{\dagger})^{n} \boldsymbol{A}^{m}\}_{s} \right\rangle = \mathrm{tr}\{\boldsymbol{\Xi} \{(\boldsymbol{A}^{\dagger})^{n} \boldsymbol{A}^{m}\}_{s}\} = (-1)^{m} \frac{\partial^{m+n}}{\partial \xi \partial \xi^{*}} \chi(\xi, s) \Big|_{\xi=0} . \tag{2.50}$$

The s-ordered quantum characteristic function $\chi(\xi, s)$ associated to the quantum state $\boldsymbol{\Xi}$ is unique [89]. Therefore, the state $\boldsymbol{\Xi}$ can be obtained from $\chi(\xi, s)$ by using the inversion formula [81, Eq. (5.16)], as given in the following.

Theorem 2.2.2 (Representation)**.** Let $\chi(\xi, s)$ be the s-ordered characteristic function associated to $\boldsymbol{\Xi}$. Then

$$\boldsymbol{\Xi} = \frac{1}{\pi^{2}} \int_{\mathbb{R}^{2}} \chi(\xi, s) \boldsymbol{D}^{\dagger}_{\xi,-s} \, \mathrm{d}^{2}\xi \ . \tag{2.51}$$

Quasi-probability distribution

The state of a quantum system can be equivalently described by using the inverse Fourier transform of the characteristic function, called quasi-probability distribution.

Definition 2.2.3 (Quasi-probability distribution)**.** The s-ordered quasi-probability distribution $W(\alpha, s)$, with $s \in \mathbb{C}$, associated to the quantum state $\boldsymbol{\Xi}$ is

$$W(\alpha, s) = \frac{1}{\pi^{2}} \int_{\mathbb{R}^{2}} \chi(\xi, s) e^{\alpha \xi^{*} - \alpha^{*} \xi} \, \mathrm{d}^{2}\xi \tag{2.52}$$

where $\chi(\xi, s)$ is the s-ordered characteristic function associated to $\boldsymbol{\Xi}$ as in (2.47).

Remark. Recall that, in classical probability theory, the inverse Fourier transform of the quantum characteristic function (QCF) associated to a random variable is the probability density function of the random variable itself. In quantum mechanics, the quasi-probability distribution must not be interpreted as the probability density function for $\boldsymbol{\alpha}$. Indeed, for a non-classical state, the quasi-probability distribution may assume negative values.

For $s = 0$, the function $W(\alpha) = W(\alpha, 0)$ is the Wigner W-function [80]; for $s = -1$ the function $Q(\alpha) = W(\alpha, -1)$ is the Husimi–Kano Q-function [90, 91]; and for $s = 1$ the function $P(\alpha) = W(\alpha, 1)$ is the Glauber–Sudarshan P-function [87, 88, 92].

The Glauber–Sudarshan P-function has the remarkable property to represent the quantum state in terms of coherent states as

$$\boldsymbol{\Xi} = \int P(\alpha) \, |\alpha\rangle\langle\alpha| \, \mathrm{d}^2\alpha \ . \tag{2.53}$$

Therefore, the Fock representation of $\boldsymbol{\Xi}$ can be expressed from (2.53) in terms of the P-function as

$$\langle m| \, \boldsymbol{\Xi} \, |n\rangle = \frac{1}{\sqrt{n!m!}} \int P(\alpha) e^{-|\alpha|^2} (\alpha^*)^n \alpha^m \, \mathrm{d}^2\alpha \ . \tag{2.54}$$

Notice that, for every quantum state $\boldsymbol{\Xi} \in \mathcal{D}(\mathcal{H})$, the characteristic function $\chi(\xi, s)$ defined in (2.47) satisfies the following bound [82, Eq. (6.25)]

$$|\chi(\xi, s)| \leq \exp\left\{ \frac{1}{2} \, \mathrm{Re}(s) |\xi|^2 \right\} . \tag{2.55}$$

Therefore, since $|\chi(\xi, s)| \leq 1$ for every $s \in \mathbb{C}$ such that $\mathrm{Re}(s) \leq 0$, the quasi-probability distributions $W(\alpha, s)$ always exists for every $s \in \mathbb{C}$ such that $\mathrm{Re}(s) \leq 0$. Therefore, the Wigner W-function and the Husimi Q-function always exists, while the Glauber–Sudarshan P-function may not exist. If the s–ordered quasi-probability distribution $W(\alpha, s)$ exists, then the corresponding quantum characteristic function can be obtained by using the Fourier inversion formula.

Theorem 2.2.4. Let $W(\alpha, s)$ be the s-ordered quasi-probability quasi-probability distribution associated to $\boldsymbol{\Xi}$. Then

$$\chi(\xi, s) = \frac{1}{\pi^2} \int_{\mathbb{R}^2} W(\alpha, s) e^{\alpha^* \xi - \alpha \xi^*} \, \mathrm{d}^2\alpha \ . \tag{2.56}$$

2.2.5 Gaussian states

Gaussian states [29–33] is a broad class of quantum states that plays a central role in CV quantum information, and can be defined as follows.

Definition 2.2.5. A quantum state $\boldsymbol{\Xi}_{\mathrm{G}}$ is Gaussian iff its Wigner function $W_{\mathrm{G}}(\alpha)$ is Gaussian, i.e.,

$$W_{\mathrm{G}}(\alpha) = \frac{1}{\pi\sqrt{\det \check{\boldsymbol{C}}_0}} \exp\left\{-\frac{1}{2}(\check{\boldsymbol{\alpha}} - \check{\boldsymbol{\mu}})^{\mathrm{H}} \check{\boldsymbol{C}}_0^{-1} (\check{\boldsymbol{\alpha}} - \check{\boldsymbol{\mu}})\right\} \tag{2.57}$$

where $\check{\boldsymbol{\mu}}$ is the augmented displacement vector, and $\check{\boldsymbol{C}}_0$ is the augmented covariance matrix.

The symmetrically-ordered characteristic function $\chi_{\mathrm{G}}(\xi)$ of a Gaussian state $\boldsymbol{\Xi}$ can be obtained by using Equation (2.57) in (2.56) to get

$$\chi_{\mathrm{G}}(\xi) = \exp\left\{-\frac{1}{2}\check{\boldsymbol{\xi}}^{\mathrm{H}} \boldsymbol{Z} \check{\boldsymbol{C}}_0 \boldsymbol{Z}^{\mathrm{H}} \check{\boldsymbol{\xi}} + (\boldsymbol{Z}\check{\boldsymbol{\mu}})^{\mathrm{H}} \check{\boldsymbol{\xi}}\right\}. \tag{2.58}$$

Remark. Notice that, in the literature, the definition of Gaussian states is given with respect to the Wigner function defined on $\mathbb{R}^2$ instead of $\mathbb{C}$, i.e.,

$$W(\boldsymbol{x}) = \frac{1}{\pi\sqrt{\det \boldsymbol{V}}} \exp\left\{-\frac{1}{2}(\boldsymbol{x} - \bar{\boldsymbol{x}})^{\mathrm{T}} \boldsymbol{V}^{-1} (\boldsymbol{x} - \bar{\boldsymbol{x}})\right\} \tag{2.59}$$

where $\bar{\boldsymbol{x}} \in \mathbb{R}^2$ is the displacement vector and $\boldsymbol{V}$ is the covariance matrix. Expression (2.57) is obtained from (2.59) by using the following transformations [93–97]

$$\check{\boldsymbol{\mu}} = \frac{1}{\sqrt{2}} \boldsymbol{J} \bar{\boldsymbol{x}} \tag{2.60}$$

$$\check{\boldsymbol{C}}_0 = \frac{1}{2} \boldsymbol{J} \boldsymbol{V} \boldsymbol{J}^{\mathrm{H}} \tag{2.61}$$

where

$$\boldsymbol{J} = \begin{bmatrix} 1 & \imath \\ 1 & -\imath \end{bmatrix}. \tag{2.62}$$

Using (2.47) it also follows that the s-ordered characteristic function $\chi_{\mathrm{G}}(\xi, s)$ of a Gaussian state $\boldsymbol{\Xi}$ is given by

$$\chi_{\mathrm{G}}(\xi, s) = \exp\left\{-\frac{1}{2}\check{\boldsymbol{\xi}}^{\mathrm{H}} \boldsymbol{Z} \check{\boldsymbol{C}}_s \boldsymbol{Z}^{\mathrm{H}} \check{\boldsymbol{\xi}} + (\boldsymbol{Z}\check{\boldsymbol{\mu}})^{\mathrm{H}} \check{\boldsymbol{\xi}}\right\}. \tag{2.63}$$

where

$$\check{\boldsymbol{C}}_s = \check{\boldsymbol{C}}_0 - \frac{s}{2}\boldsymbol{I}\,. \tag{2.64}$$

Therefore, if $\check{\boldsymbol{C}}_s$ is invertible, the s-ordered quasi probability distribution is given by the Fourier transform of (2.63), i.e.,

$$W_{\mathrm{G}}(\alpha, s) = \frac{1}{\pi\sqrt{\det \check{\boldsymbol{C}}_s}} \exp\left\{ -\frac{1}{2}(\check{\boldsymbol{\alpha}} - \check{\boldsymbol{\mu}})^{\mathrm{H}} \check{\boldsymbol{C}}_s^{-1} (\check{\boldsymbol{\alpha}} - \check{\boldsymbol{\mu}}) \right\}. \tag{2.65}$$

There are some important sub-classes of Gaussian states, as detailed in the following.

Coherent states

A coherent state [87, 88] with amplitude $\mu \in \mathbb{C}$ is defined as the eigenstate $|\mu\rangle$ of the annihilation operator $\boldsymbol{A}$ associated to the eigenvalue μ, i.e.,

$$\boldsymbol{A}\,|\mu\rangle = \mu\,|\mu\rangle\ . \tag{2.66}$$

The state can be obtained from the ground state by using the displacement operator

$$|\mu\rangle = \boldsymbol{D}_{\mu}\,|0\rangle\ . \tag{2.67}$$

A coherent state with amplitude $\mu \in \mathbb{C}$ can be proven to be a Gaussian state with augmented mean $\check{\boldsymbol{\mu}} = [\mu \quad \mu^*]^{\mathrm{T}}$ and augmented covariance matrix

$$\check{\boldsymbol{C}}_0 = \frac{1}{2}\boldsymbol{I}\,. \tag{2.68}$$

Therefore, the Wigner W-function, the Glauber–Sudarshan P-function, and the Husimi–Kano Q-function associated with $\boldsymbol{\Xi}_{\mathrm{th}}(\mu)$ are respectively given by [98]

$$W_{\mathrm{c}}(\alpha) = \frac{2}{\pi}\,\exp\left\{-2|\alpha-\mu|^2\right\} \tag{2.69}$$

$$P_{\mathrm{c}}(\alpha) = \delta^2(\alpha-\mu) \tag{2.70}$$

$$Q_{\mathrm{c}}(\alpha) = \frac{1}{\pi}\,\exp\left\{-|\alpha-\mu|^2\right\}. \tag{2.71}$$

The Fock representation of a coherent state is given by

$$|\alpha\rangle = e^{-\frac{|\alpha|^2}{2}} \sum_{n=0}^{\infty} \frac{\alpha^n}{\sqrt{n}}\,|n\rangle\ . \tag{2.72}$$

Noisy coherent states

A noisy coherent state with amplitude $\mu \in \mathbb{C}$ is defined to be a coherent state affected by thermal noise in state preparation, and it is defined as follows

$$\boldsymbol{\Xi}_{\mathrm{th}}(\mu) = \boldsymbol{D}_{\mu} \boldsymbol{\Xi}_{\mathrm{th}} \boldsymbol{D}_{\mu}^{\dagger} \tag{2.73}$$

where $\boldsymbol{\Xi}_{\mathrm{th}}$ is a thermal state with mean number of thermal photons $\bar{n}$, as defined in (2.33). A noisy coherent state is a Gaussian state with augmented mean $\check{\boldsymbol{\mu}} = [\mu \quad \mu^*]^{\mathrm{T}}$ and augmented covariance matrix

$$\check{\boldsymbol{C}}_0 = \Big(\bar{n} + \frac{1}{2}\Big) \boldsymbol{I} \,. \tag{2.74}$$

The Fock representation of a noisy coherent state $\boldsymbol{\Xi}_{\mathrm{th}}(\mu)$ is given by [4]

$$\langle n| \, \boldsymbol{\Xi}_{\mathrm{th}}(\mu) \, |m\rangle = (1-v) \, e^{-(1-v)|\mu|^2} \sqrt{\frac{n!}{m!}} \, v^n \big[(1-v)\mu^*\big]^{m-n} \, L_n^{m-n}\Big(\frac{-(1-v)^2|\mu|^2}{v}\Big) \tag{2.75}$$

where $v = \bar{n}/(\bar{n}+1)$. The Wigner W-function, the Glauber–Sudarshan P-function, and the Husimi–Kano Q-function associated with $\boldsymbol{\Xi}_{\mathrm{th}}(\mu)$ are respectively given by [98]

$$W_{\mathrm{th}}(\alpha) = \frac{1}{\pi(\bar{n}+\frac{1}{2})} \, \exp\Big\{ - \frac{|\alpha-\mu|^2}{\bar{n}+\frac{1}{2}} \Big\} \tag{2.76}$$

$$P_{\mathrm{th}}(\alpha) = \frac{1}{\pi\bar{n}} \, \exp\Big\{ - \frac{|\alpha-\mu|^2}{\bar{n}} \Big\} \tag{2.77}$$

$$Q_{\mathrm{th}}(\alpha) = \frac{1}{\pi(\bar{n}+1)} \, \exp\Big\{ - \frac{|\alpha-\mu|^2}{\bar{n}+1} \Big\} . \tag{2.78}$$

Squeezed states

A squeezed state [99, 100] with amplitude $\mu \in \mathbb{C}$ and squeezing parameter $\zeta \in \mathbb{C}$ is defined as follows

$$|\mu, \zeta\rangle = \boldsymbol{D}_{\mu} \boldsymbol{S}_{\zeta} \, |0\rangle \ . \tag{2.79}$$

A squeezed state with amplitude $\mu \in \mathbb{C}$ and squeezing parameter $\zeta \in \mathbb{C}$ can be proven to be a Gaussian state with augmented mean $\check{\boldsymbol{\mu}} = [\mu \quad \mu^*]^{\mathrm{T}}$ and augmented covariance matrix

$$\check{\boldsymbol{C}}_0 = \frac{1}{2} \begin{bmatrix} \cosh(2r) & \sinh(2r) e^{-\imath\phi} \\ \sinh(2r) e^{\imath\phi} & \cosh(2r) \end{bmatrix} . \tag{2.80}$$

Therefore, a squeezed state is represented by a Gaussian Wigner function that is not circularly symmetric, i.e., the uncertainty of one quadrature is reduced at the expense

of the uncertainty for the other. Indeed, by using (2.80) into Eq. (2.65), the Wigner function of a squeezed state with $\zeta = re^{-\imath\phi}$ is found to be [98]

$$W_{\mathrm{s}}(\alpha) = \frac{2}{\pi} \exp\left\{|(\alpha-\mu)\cosh(r) - (\alpha-\mu)^* \sinh(r) e^{-\imath\phi}|^2\right\}. \tag{2.81}$$

Noisy squeezed states

A noisy squeezed state with amplitude $\mu \in \mathbb{C}$ and squeezing parameter $\zeta \in \mathbb{C}$ is defined to be a squeezed state affected by thermal noise in state preparation, and it is defined as follows

$$\boldsymbol{\Xi}_{\mathrm{th}}(\mu,\zeta) = \boldsymbol{D}_{\mu}\boldsymbol{S}_{\zeta}\boldsymbol{\Xi}_{\mathrm{th}}\boldsymbol{S}_{\zeta}^{\dagger}\boldsymbol{D}_{\mu}^{\dagger} \tag{2.82}$$

where $\boldsymbol{\Xi}_{\mathrm{th}}$ is a thermal state with mean number of thermal photons $\bar{n}$, as defined in (2.33). A noisy squeezed state is found to be a Gaussian state with augmented mean $\check{\boldsymbol{\mu}} = [\mu \quad \mu^*]^{\mathrm{T}}$ and augmented covariance matrix

$$\check{\boldsymbol{C}}_0 = \left(\bar{n} + \frac{1}{2}\right) \begin{bmatrix} \cosh(2r) & \sinh(2r)e^{-\imath\phi} \\ \sinh(2r)e^{\imath\phi} & \cosh(2r) \end{bmatrix}. \tag{2.83}$$

Note that, for a noisy squeezed state, by using (2.83) in (2.64)

$$\det \check{\boldsymbol{C}}_s = \left(\bar{n} + \frac{1-s}{2}\right)^2 - s(2\bar{n}+1)\sinh^2(r). \tag{2.84}$$

Therefore, the s-ordered quasi-probability distribution in the form of (2.65) exists only for $s < s_{\mathrm{th}}$, with $s_{\mathrm{th}} = (2\bar{n}+1)e^{-r}$ to guarantee that $\det \check{\boldsymbol{C}}_s > 0$ [98,101].[2] By assuming $\det \check{\boldsymbol{C}}_s \neq 0$ it can be shown that

$$\check{\boldsymbol{C}}_s^{-1} = \frac{1}{\det \check{\boldsymbol{C}}_s}\left(\boldsymbol{Z}\check{\boldsymbol{C}}_0\boldsymbol{Z}^{\mathrm{H}} - \frac{s}{2}\boldsymbol{I}\right). \tag{2.85}$$

It can be proven that every Gaussian state can be expressed as a noisy squeezed state with displacement parameter $\mu \in \mathbb{C}$ noise parameter $\bar{n} \in \mathbb{R}$ and squeezing factor $\zeta \in \mathbb{C}$ [31]. Therefore, a Gaussian quantum state is uniquely identified by the augmented mean $\check{\boldsymbol{\mu}}$ and an augmented covariance matrix $\check{\boldsymbol{C}}_0$ in the form of (2.83).

[2] In the following, we will assume the existence of $W_{\mathrm{G}}(\alpha, s)$ and thus the invertibility of $\check{\boldsymbol{C}}_s$.

2.2.6 Quantum channels

The devices presented in Section 2.2.3 are unitary transformation on a CV system and, as such, they can be inverted. In practice, a quantum system can interact with the environment, drifting the quantum state $\boldsymbol{\Xi}$ to $\boldsymbol{\Upsilon}$ after the interaction. In this section we present some popular noise models for CV systems.

Thermal noise

In this noise model, a classical Gaussian noise is superimposed to the quantum state $\boldsymbol{\Xi}$, for which the output state $\boldsymbol{\Upsilon}$ is given by

$$\boldsymbol{\Upsilon} = \int_{\mathbb{R}^2} \frac{1}{\pi\bar{n}} \exp\Big\{-\frac{|\alpha|^2}{\bar{n}}\Big\} \boldsymbol{D}_\alpha \boldsymbol{\Xi} \boldsymbol{D}_\alpha^\dagger \, \mathrm{d}^2\alpha \ . \tag{2.86}$$

This noise model describes the presence of thermal noise in the state preparation, and it can be physically interpreted as follows. The quantum state $\boldsymbol{\Xi}$ enters the first port of a beam splitter with high transmissivity η. The second port of the beam splitter is fed with a highly noisy thermal state with mean number of thermal photons N. Then, in the limit of $\eta \to 1$ and $N \to \infty$, with $(1-\eta)N \to \bar{n}$, the thermal noise channel is obtained.

Phase diffusion

The phase diffusion model [98] is a purely quantum mechanical model that has no classical counterparts and can be used to model different phenomena (e.g., the random scattering of photons in a waveguide) and, in particular, the loss of quantum coherence without energy loss. In the presence of phase diffusion, the quantum state $\boldsymbol{\Xi}$ becomes $\boldsymbol{\Upsilon}$ such that

$$\boldsymbol{\Upsilon} = \int_{-\infty}^{\infty} \frac{1}{\sqrt{2\pi\sigma^2}} \exp\Big\{-\frac{\phi^2}{2\sigma^2}\Big\} \boldsymbol{R}_\phi \boldsymbol{\Xi} \boldsymbol{R}_\phi \, \mathrm{d}\phi \tag{2.87}$$

where σ is the phase diffusion parameter. Notice that the effect of a phase diffusion channel can be evaluated in the Fock representation as

$$\langle n| \boldsymbol{\Upsilon} |m\rangle = e^{-(n-m)^2\sigma^2} \langle n| \boldsymbol{\Xi} |m\rangle \ .$$

Therefore, the effect of phase diffusion is the exponential damping of the off-diagonal elements in the Fock representation. Note that this model can be used to describe the reception of a state with unknown phase. For example, when the phase of a state is

unknown, a uniform random model is used [29] and the state $\boldsymbol{\Upsilon}$ results in

$$\boldsymbol{\Upsilon} = \int_0^{2\pi} \frac{1}{2\pi} \boldsymbol{R}_\phi \boldsymbol{\Xi} \boldsymbol{R}_\phi^\dagger d\phi \,.$$

In such a case, $\langle n| \boldsymbol{\Upsilon} |m\rangle = \delta_{n,m} \langle n| \rho |m\rangle$, which resembles to the phase diffusion model with large σ (high-phase diffusion), for which $\boldsymbol{\Upsilon}$ reduces to a purely classical state.

Photon loss

The photon loss model [39] describes the energy loss of a CV quantum state, and it can be used to model different phenomena (e.g., the free-space propagation). The loss of energy can be modeled by a beam splitter of transmissivity η, as described in Section 2.2.3. In the presence of photon loss, the P-function $P_{\boldsymbol{\Upsilon}}(\alpha)$ of the output state $\boldsymbol{\Upsilon}$ is related to the $P_{\boldsymbol{\Upsilon}}(\alpha)$ is given by

$$P_{\boldsymbol{\Upsilon}}(\alpha) = \frac{1}{\eta^2} P_{\boldsymbol{\Xi}} \left(\frac{\alpha}{\eta} \right) . \tag{2.88}$$

2.3 Quantum information with discrete variables

The DV framework is related to the study of quantum systems with a finite-dimensional Hilbert space. The DV framework allows the description of several quantum systems of practical interest in quantum information, such as the qubit.

2.3.1 Quantum bit

A qubit is a two-level quantum system, i.e., the Hilbert space $\mathcal{H} = \mathcal{H}_2$ associated to the system has dimension two. The two orthogonal states of the basis are conventionally written as $|0\rangle$ and $|1\rangle$. Therefore, every state $|\psi\rangle \in \mathcal{H}_2$ can be written as

$$|\psi\rangle = \alpha |0\rangle + \beta |1\rangle \,.$$

where $\alpha, \beta \in \mathbb{C}$ such that $|\alpha|^2 + |\beta|^2 = 1$. The normalization condition $|\alpha|^2 + |\beta|^2 = 1$ is satisfied by any couple of points $|\alpha|, |\beta|$ on the unitary circle in the Cartesian plane. Therefore, by defining

$$|\alpha| = \cos\left(\frac{\theta}{2}\right) \quad ; \quad |\beta| = \sin\left(\frac{\theta}{2}\right) \quad \theta \in [0, \pi]$$

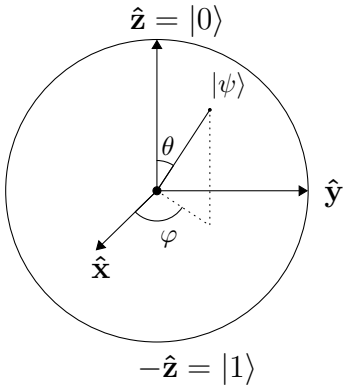


Figure 2.1: Block sphere representation of a qubit.

it follows that

$$|\psi\rangle = \cos\left(\frac{\theta}{2}\right)|0\rangle + \sin\left(\frac{\theta}{2}\right)e^{i\phi}|1\rangle$$

and thus the density matrix is

$$\boldsymbol{\Xi} = |\psi\rangle\langle\psi| = \frac{1}{2}\boldsymbol{I} + \frac{1}{2}\begin{bmatrix} \cos(\theta) & \sin(\theta)e^{i\phi} \\ \sin(\theta)e^{-i\phi} & -\cos(\theta) \end{bmatrix}.$$

By defining $\vec{n} = (\sin\theta\cos\phi, \sin\theta\sin\phi, \cos\theta)$, with $|\vec{n}| = 1$, it follows from (2.3.1) that any pure qubit can be geometrically represented as a unit vector $\vec{n}$ on the unit sphere (see Figure 2.1), referred to as Bloch sphere. Analogously, a mixed (noisy) qubit can be represented as a non unitary vector $\vec{n}$ with $|\vec{n}| < 1$ inside the Block sphere.

2.3.2 Qubit transformations

In this section, we presents the most important transformations that can be applied to a quantum bit, useful for DV applications.

Hadamard gate

The Hadamard gate $\boldsymbol{H}$ is an operator that acts on a single qubit and it performs a rotation of $\pi/2$ radians around the z axis in the Bloch representation. This gate is represented by a 2×2 Hadamard matrix

$$\boldsymbol{H} = \frac{1}{\sqrt{2}}\begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix}.$$

The Hadamard gate is an elementary circuit to generate a non-classical state in the DV domain. Indeed the basis vectors $|0\rangle$ and $|1\rangle$ are transformed as follows

$$\boldsymbol{H}\,|0\rangle = \frac{|0\rangle + |1\rangle}{\sqrt{2}} \tag{2.89}$$

$$\boldsymbol{H}\,|1\rangle = \frac{|0\rangle - |1\rangle}{\sqrt{2}}\,. \tag{2.90}$$

Pauli matrices

The Pauli gates $\boldsymbol{X}$, $\boldsymbol{Y}$ and $\boldsymbol{Z}$ are operators acting on a single qubit and they perform a rotation of π radians around the x, y, and z axis of the Bloch sphere. These gates are respectively represented by the Pauli matrices

$$\boldsymbol{X} = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} \tag{2.91}$$

$$\boldsymbol{Y} = \begin{bmatrix} 0 & -i \\ i & 0 \end{bmatrix} \tag{2.92}$$

$$\boldsymbol{Z} = \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}\,. \tag{2.93}$$

Controlled NOT

The controlled NOT gate acts on a pair of qubits, the first of which is called source and the second one target. It is described by the matrix

$$\boldsymbol{C}_{\mathrm{X}} = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{bmatrix}\,.$$

The controlled NOT gate can be used, together with the Hadamard gate and the Pauli gates to generate an entangled state in the DV domain, indeed

$$\begin{aligned}
\boldsymbol{C}_{\mathrm{X}}\boldsymbol{H}_A\,|00\rangle_{AB} &= \frac{|00\rangle_{AB} + |11\rangle_{AB}}{\sqrt{2}} \\
\boldsymbol{Z}_B\boldsymbol{C}_{\mathrm{X}}\boldsymbol{H}_A\,|00\rangle_{AB} &= \frac{|00\rangle_{AB} - |11\rangle_{AB}}{\sqrt{2}} \\
\boldsymbol{Y}_B\boldsymbol{C}_{\mathrm{X}}\boldsymbol{H}_A\,|00\rangle_{AB} &= \frac{|01\rangle_{AB} - |10\rangle_{AB}}{\sqrt{2}} \\
\boldsymbol{X}_B\boldsymbol{C}_{\mathrm{X}}\boldsymbol{H}_A\,|00\rangle_{AB} &= \frac{|01\rangle_{AB} + |10\rangle_{AB}}{\sqrt{2}}\,.
\end{aligned}$$

2.3.3 Qubit physical implementations

The physical realization of quantum bits requires the ability to represent and manage a two-level quantum system. Alternatively, a two-level quantum system can be embedded into a multi-level quantum system such as a quantum harmonic oscillator. There are different technological implementations as detailed in the following.

Linear optics

In linear optical quantum computing, the qubit is physically represented by an optical photon [102–104]. Therefore, the qubit is embedded in a two-dimensional Hilbert subspace of a quantum harmonic oscillator, such as the space spanned by the ground state $|0\rangle$ and the single Fock state $|1\rangle$. The main advantages of this architecture are: (i) the possibility to use off-the-shelf optical components; and (ii) the weak effect of thermal noise at optical frequencies. This framework has been used for proving the quantum supremacy in solving the boson sampling problem [105]. The principal drawback of this architecture is the difficulty in coupling different quantum systems.

Superconducting circuits

In superconducting quantum computing, the qubit is physically represented by the state of a superconducting electronic circuit [106–108]. In particular, the qubit is embedded in the two-dimensional Hilbert space spanned by the two lowest energy levels of an anharmonic oscillator. Conversely to the linear optical approach, the anharmonicity is needed to avoid unintentional excitation of the highest energy levels. The main advantages of this architecture are: (i) the possibility to engineer and dynamically configure the circuit parameters; and (ii) the scalability of the architecture. The superconducting architecture is the actually predominant architecture for the realization of a universal quantum computer [109]. The main drawback is the need for these circuits to operate at near-zero temperatures to avoid decoherence.

Ion traps

In the ion trap quantum computing, the qubit is represented by the spin of an atom confined into an electromagnetic trap [110–112]. Conversely to the two previous technologies, in this case the qubit is physically represented with a discrete-level quantum systems. The main advantages of this architecture are: (i) the stability of the quantum system at room temperatures; and (ii) the low error rates. The main drawback is that trapped ions quantum computers are difficult to scale.

Chapter 3

Non-Gaussian quantum states

Non-classical states are key enablers for quantum-enhanced technologies such as quantum communications [5], quantum metrology [113], quantum computation [114], and quantum cryptography [115], in both the optical [116–118] and microwave [119–121] spectrum. In particular, squeezed coherent states have been used thoroughly in applied quantum information as the principal source of non-classicality in CV systems [29–33]. However, despite their great success, Gaussian states present several limitations when used as the only source of non-classicality [32], motivating a growing interest for non-Gaussian states.

Photon-added states (PASs) [50–53] and photon-subtracted states (PSSs) [122–126] are two important classes of non-Gaussian states that can exhibit a non-classical behavior and that can be generated by using conventional devices and conditional measurements [56–58, 127–129]. The quantum states obtained by photon-addition or photon-subtraction on a Gaussian state are called photon-added Gaussian states (PAGSs) and photon-subtracted Gaussian states (PSGSs), respectively. The utility of PAGSs and PSGSs has been shown for several applications including quantum communications [6, 7, 130], quantum key distribution [59, 60, 62], and quantum sensing [131–133]. In particular, the use of PACSs [50–52], i.e., the class of quantum states generated by photon addition on a coherent state, is beneficial for QSD applications [5], including quantum communication systems [6,7], quantum key distribution [60,62], and quantum sensing [61, 131].

Nevertheless, in real world scenarios, the preparation of quantum states will always be affected by noise impairments, such as thermal noise. Hereafter, we refer to these classes of states as noisy states. The characterization of PACSs in the presence of thermal noise in state preparation is crucial for the design and the analysis of quantum-enhanced applications, such as quantum communication systems, in a real-world scenario. While significant progress has been made in the literature [53–55], a

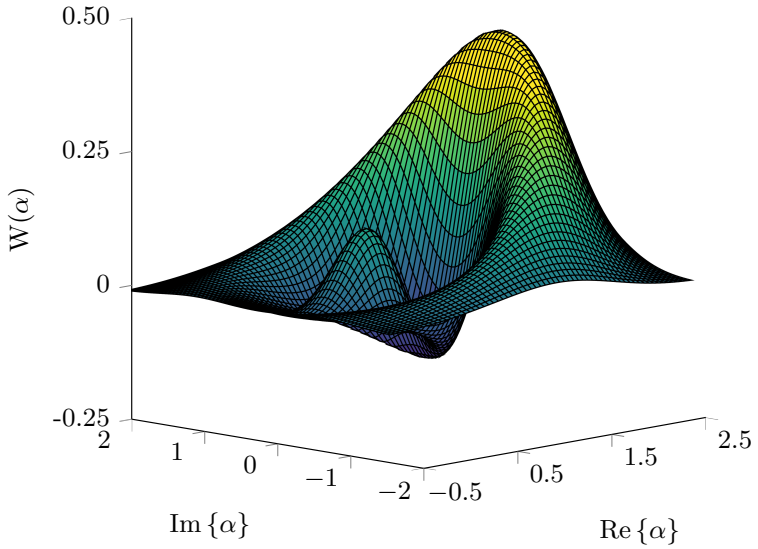


Figure 3.1: Wigner W-function of a PACS highlighting its non-Gaussian shape and exhibiting a non-classical signature evident in terms of negativity.

complete characterization of PACSs in the presence of thermal noise is still missing.

This thesis advocates the use of non-Gaussian quantum states in various applications of quantum systems and networks. In particular, it is shown that PACSs is a class of non-Gaussian states that can be used for providing non-classicality to quantum systems, even in the presence of thermal noise in state preparation. The goal of this chapter is to provide a characterization of noisy PACSs in presence of thermal noise in state preparation. The key contributions of this chapter are as follows:

- characterization of noisy PACSs in terms of Fock representation, Wigner W-function, Glauber–Sudarshan P-function, and Husimi–Kano Q-function;

- observation of the non-classical properties for noisy PACSs in terms of Wigner function negativity.

Notation

This section relies on the Wirtinger calculus discussed in Appendix A. For a complex-valued function $g(z) : \mathbb{C} \to \mathbb{C}$, the symbols $\frac{\partial g(z)}{\partial z}$ and $\frac{\partial g(z)}{\partial z^*}$ indicate the Wirtinger derivatives of $g(z)$ with respect to z and z^*, respectively, as defined in (A.1). For a complex number $z \in \mathbb{C}$: $L_k(z)$ and $L_k^{(\alpha)}(z)$ denote the associated and generalized Laguerre polynomials, respectively.

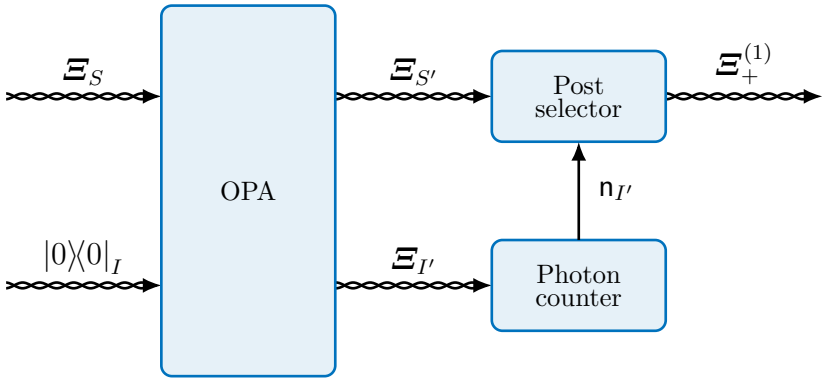


Figure 3.2: Block scheme for the generation of a photon-added state $\boldsymbol{\Xi}_+^{(k)}$ with $k = 1$, from the state $\boldsymbol{\Xi}$ using a low-gain OPA.

3.1 Photon-added states

Consider an arbitrary quantum state $|\psi\rangle$. The corresponding PAS $|\psi_+^{(k)}\rangle$ is defined as

$$|\psi_+^{(k)}\rangle = \frac{(\boldsymbol{A}^\dagger)^k |\psi\rangle}{\sqrt{\langle\psi| \boldsymbol{A}^k (\boldsymbol{A}^\dagger)^k |\psi\rangle}} \tag{3.1}$$

where $k \in \mathbb{N}$ is the number of addition operations. It is important to notice that, despite the name, the operation of photon-addition should not be interpreted in a deterministic sense: if the mean number of photons in $\boldsymbol{\Xi}$ is n, the mean number of photons in $\boldsymbol{\Xi}_+^{(k)}$ is not given by $n + k$, in general. This slight abuse of terminology comes out from the fact that photon-addition on the Fock state $|n\rangle$ produces the state $|n + k\rangle$, as given by Eq. (2.31), i.e., it effectively adds k photons.

3.1.1 Physical implementation

There are different architectures to generate a PAS. Consider the scheme of Figure 3.2 and assume without loss of generality, that the state $\boldsymbol{\Xi} = |\phi\rangle\langle\phi|$ enters the signal port of an optical parametric amplifier (OPA), while the vacuum state enters the idler port of the OPA. Therefore, the input state of the OPA is $|\psi\rangle_{SI} = |\phi\rangle_S |0\rangle_I$. The output state $|\psi\rangle_{S'I'}$ of the OPA is given by the two-mode squeezing transformation (2.45)

$$|\psi\rangle_{S'I'} = \boldsymbol{S}_\zeta^{(2)} \; |\psi\rangle_{SI}$$

where, for a small amount of squeezing (i.e., for a small amount of the OPA gain), the operator $\boldsymbol{S}_\zeta^{(2)}$ can be approximated as

$$\boldsymbol{S}_\zeta^{(2)} \simeq \boldsymbol{I} + \zeta \boldsymbol{A}_S^\dagger \boldsymbol{A}_I^\dagger - \zeta^* \boldsymbol{A}_S \boldsymbol{A}_I$$

and thus

$$|\psi\rangle_{S'I'} \simeq |\phi\rangle_S |0\rangle_I + \zeta \boldsymbol{A}_S^\dagger |\phi\rangle_S |1\rangle_I \ . \tag{3.2}$$

Therefore, the state of the output signal S' conditioned on the result $n_I = 1$ of a photon number measurement n_I on the idler output is

$$|\phi\rangle_{S'} = \frac{1}{\sqrt{\langle\phi|_S \boldsymbol{A}_S \boldsymbol{A}_S^\dagger |\phi\rangle_S}} \boldsymbol{A}_S^\dagger |\phi\rangle_S \ .$$

Notice that, for a generic input state $\boldsymbol{\Xi} = \sum_n p_n |\phi_n\rangle\langle\phi_n|$, the joint signal-idler state at the output of the OPA can be written as $\boldsymbol{\Xi}_{S'I'} = \sum_n p_n |\psi_n\rangle\langle\psi_n|_{S'I'}$ where $|\psi_n\rangle$ is given by Equation (3.2)

$$|\psi_n\rangle_{S'I'} \simeq |\phi_n\rangle_S |0\rangle_I + \zeta \boldsymbol{A}_S^\dagger |\phi_n\rangle_S |1\rangle_I$$

and therefore, for a generic state $\boldsymbol{\Xi}$, the state of the output signal S' conditioned on the result $n_{I'} = 1$ of a photon number measurement $\mathsf{n}_{I'}$ on the idler output is given by

$$\boldsymbol{\Xi}_+^{(1)} = \frac{\boldsymbol{A}^\dagger \boldsymbol{\Xi} \boldsymbol{A}}{\mathrm{tr}\{\boldsymbol{A}^\dagger \boldsymbol{\Xi} \boldsymbol{A}\}} \ .$$

3.1.2 Photon-added coherent states

Let $|\psi\rangle$ be a coherent state, i.e., $|\psi\rangle = |\mu\rangle$ with $\mu \in \mathbb{C}$ as in Eq. (2.66). The corresponding PAS is given by

$$\left|\mu^{(k)}\right\rangle = \frac{(\boldsymbol{A}^\dagger)^k |\mu\rangle}{\sqrt{\langle\mu| \boldsymbol{A}^k (\boldsymbol{A}^\dagger)^k |\mu\rangle}} \ . \tag{3.3}$$

The state $\left|\mu^{(k)}\right\rangle$ is called PACS. The Wigner function of a PACS is given by [50]

$$W_+^{(k)}(\alpha) = B_+^{(k)}(\alpha)\, W_{\mathrm{c}}(\alpha) \tag{3.4}$$

where $W_{\mathrm{c}}(\alpha)$ is the Wigner function of the coherent state $|\mu\rangle$ as given by Eq (2.69) and

$$B_+^{(k)}(\alpha) = (-1)^k \frac{2L_k(|2\alpha - \mu|^2)}{\pi L_k(-|\mu|^2)} \ . \tag{3.5}$$

Notice that the Wigner function of a PACS is given by the product of the Gaussian function W_{c} and a non-Gaussian function $B_+^{(k)}(\alpha)$. Also notice that the non-Gaussian term also admits negative values, due to the presence of a Laguerre polynomial, thus highlighting the non-classical nature of this class of states.

In this thesis, we will focus on the class of PACSs for several reason: (i) PACSs are generated from a quasiclassical Gaussian state, i.e., the initial state can be generated straightforwardly; (ii) PACSs have a simple mathematical characterization; and (iii) PACSs turns out to be useful to improve the performance of quantum communication systems, such as QOOK and QPPM systems. In the following, we will derive a model for describing PACSs in the presence of thermal noise in state preparation.

3.1.3 Photon-added squeezed states

If $|\psi\rangle$ is a squeezed state, i.e., $|\psi\rangle = |\mu, \zeta\rangle$ with $\mu, \zeta \in \mathbb{C}$ as in Eq. (2.79), the corresponding PAS is called PASS. The Wigner function of a PASS is shown to be

$$W_{+}^{(k)}(\alpha) = B_{+}^{(k)}(\alpha)\, W_{\mathrm{s}}(\alpha) \tag{3.6}$$

where $W_{\mathrm{s}}(\alpha)$ is the Wigner function of a squeezed state as given by Eq. (2.81) and $B_{+}^{(k)}(\alpha)$ is the non-Gaussian factor that depends on μ and ζ. The expression of $B_{+}^{(k)}(\alpha)$ is rather cumbersome [53] and it will not be reported here for brevity. Notice that, by comparing Eq. (3.4) and Eq. (3.6) both PACSs and PASSs have a similar structure for the Wigner function. However, note that a PASS is more difficult to generate than a PACS as a squeezed state is needed as a initial state to generate a PASS.

3.2 Photon-subtracted states

Let $|\psi\rangle$ be an arbitrary quantum state. The corresponding PSS $|\psi_{-}\rangle$ is defined as

$$|\psi_{-}\rangle = \frac{\boldsymbol{A}^{k}\,|\psi\rangle}{\sqrt{\langle\psi|\,(\boldsymbol{A}^{\dagger})^{k}\boldsymbol{A}^{k}\,|\psi\rangle}} \tag{3.7}$$

where $k \in \mathbb{N}$ is the number of subtraction operations. As for the case of photon-addition, it is important to notice that the photon-subtraction operation should not be interpreted in a deterministic sense. This slight abuse of terminology comes out from the fact that photon-subtraction on the Fock state $|n\rangle$ produces the state $|n-k\rangle$, as given by Eq. (2.30), i.e., it effectively annihilates k photons. Also notice that, if $|\psi\rangle$ is a coherent state, i.e., $|\psi\rangle = |\mu\rangle$ with $\mu \in \mathbb{C}$ as in Eq. (2.66), the corresponding PSS $|\psi_{+}\rangle = |\mu\rangle$, i.e., photon-subtraction has no effect on a coherent state. This is due to the fact that a coherent state is an eigenstate of the annihilation operator. Therefore, photon-subtraction requires a squeezed state as input to produce a non-trivial state as output.

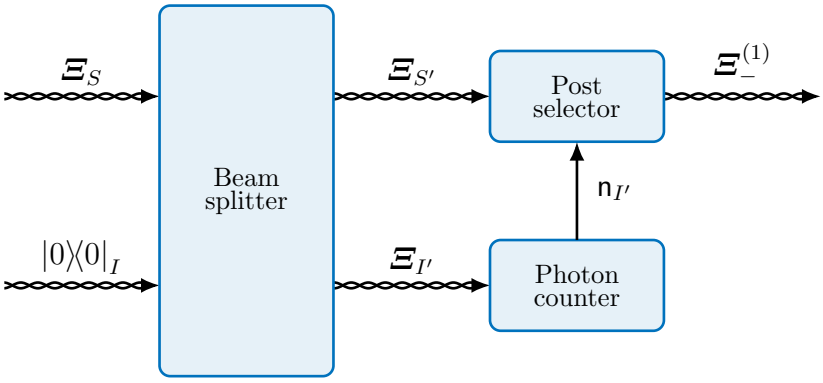


Figure 3.3: Block scheme for the generation of a PSS $\boldsymbol{\Xi}_-^{(k)}$ with $k = 1$, from the state $\boldsymbol{\Xi}$ using a low-reflectivity beam splitter.

3.2.1 Physical implementation

Consider the scheme of Figure 3.3 and assume without loss of generality, that the state $\boldsymbol{\Xi} = |\phi\rangle\langle\phi|$ enters the first port of a beam splitter, while the vacuum state enters the second port. Therefore the input state of the beam splitter is $|\psi\rangle_{SI} = |\phi\rangle_S |0\rangle_I$. The output state $|\psi\rangle_{S'I'}$ of the beam splitter is given by

$$|\psi\rangle_{S'I'} = \boldsymbol{B}_\theta |\psi\rangle_{SI}$$

where, for small reflectivity, the operator $\boldsymbol{B}_\theta$ can be approximated as

$$\boldsymbol{B}_\theta \simeq \boldsymbol{I} + \imath\theta(\boldsymbol{A}^\dagger \boldsymbol{B} + \boldsymbol{A}\boldsymbol{B}^\dagger)$$

and thus

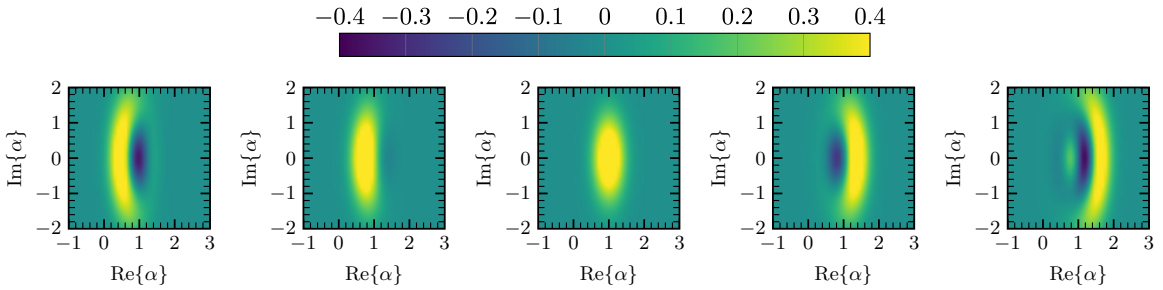
$$|\psi\rangle_{S'I'} \simeq |\phi\rangle_S |0\rangle_I + \imath\theta \boldsymbol{A} |\phi\rangle_S |1\rangle_I \ .$$

Therefore, the state of the system S conditioned on the result $n_{I'} = 1$ of a photon number measurement $\mathsf{n}_{I'}$ on the system i is

$$|\phi\rangle_{S'} = \frac{1}{\langle\phi|_S \boldsymbol{A}^\dagger \boldsymbol{A} |\phi\rangle_S} \boldsymbol{A} |\phi\rangle_S \ .$$

Analogously to PAS it is possible to show that, for a generic input state $\boldsymbol{\Xi} = \sum_n p_n |\phi_n\rangle\langle\phi_n|$ the output signal S' conditioned on the result $n_{I'} = 1$ of a photon number measurement $\mathsf{n}_{I'}$ on the system I is given by

$$\boldsymbol{\Xi}_-^{(1)} = \frac{\boldsymbol{A}\boldsymbol{\Xi}\boldsymbol{A}^\dagger}{\mathrm{tr}\{\boldsymbol{A}\boldsymbol{\Xi}\boldsymbol{A}^\dagger\}} \ .$$



(a) PSSS with $k = 2$ (b) PSSS with $k = 1$ (c) Initial state (d) PASS with $k = 1$ (e) PASS with $k = 2$

Figure 3.4: Wigner W-function $W_+^{(k)}(\alpha)$ of a PASS and a PSSS for different values of k with $\mu = 1$ and $\zeta = -0.5$.

3.2.2 Photon-subtracted squeezed states

If $|\psi\rangle$ is a squeezed state, i.e., $|\psi\rangle = |\mu, \zeta\rangle$ with $\mu, \zeta \in \mathbb{C}$ as in Eq. (2.79), the corresponding PAS is called photon-subtracted squeezed state (PSSS). The Wigner function of a PASS is shown to be

$$W_-^{(k)}(\alpha) = B_-^{(k)}(\alpha)\, W_{\rm s}(\alpha) \tag{3.8}$$

where $W_{\rm s}(\alpha)$ is the Wigner function of a squeezed state as given by Eq.(2.81) and $B_-^{(k)}(\alpha)$ is a non-Gaussian function that depends on μ and ζ. The expression of $B_-^{(k)}(\alpha)$ is rather cumbersome [134] and it will not be reported here for brevity. Notice that, by comparing Eq. (3.4) and Eq. (3.8) both PASSs and PSSSs have a similar structure for the Wigner function even if the corresponding states are obtained with rather different operations. Also notice that, in general, the generation of a PSSS is simpler than that of a PASS because, as shown in the previous section, the generation of a PSSS does not require active devices such as an OPA.

3.3 Noisy photon-added coherent states

In this section, we derive a complete characterization for PACSs affected by thermal noise in state preparation. This model will be of particular importance in the analysis and the design of quantum communication systems with non-Gaussian states.

Let $\boldsymbol{\Xi}$ be a coherent state affected by thermal noise. Then, the corresponding photon-added state $\boldsymbol{\Xi}_+$ is referred to as noisy PACS.[1] Therefore, a noisy PACS is

[1]This definition of noisy PACS is in accordance with that of photon-added displaced thermal state (PADTS) in [54], a special case of a photon-added displaced squeezed thermal state (PADSTS) [53,55] with no squeezing. We then provide new results, all in closed form, for PADTS.

defined as

$$\boldsymbol{\Xi}(\mu,k)=\frac{(\boldsymbol{A}^\dagger)^k\boldsymbol{\Xi}_{\mathrm{th}}(\mu)\boldsymbol{A}^k}{N_k(\mu,\bar{n})} \tag{3.9}$$

where $k\in\mathbb{N}$ represents the number of addition operations, and $N_k(\mu,\bar{n})$ is the normalization constant given by $N_k(\mu,\bar{n})=\mathrm{tr}\{(\boldsymbol{A}^\dagger)^k\boldsymbol{\Xi}_{\mathrm{th}}(\mu)\boldsymbol{A}^k\}$. From [82, eq. (7.16)], we obtain[2]

$$N_k(\mu,\bar{n})=k!(\bar{n}+1)^k L_k\Big(-\frac{|\mu|^2}{\bar{n}+1}\Big)\,. \tag{3.10}$$

Note that a noisy PACS is uniquely determined by the parameters k, μ, and $\bar{n}$; such dependencies will not be explicated unless strictly needed. The mean number of photons $n_{\mathrm{p}}(\mu,\bar{n})$ in a noisy PACS is given by $\langle\boldsymbol{A}^\dagger\boldsymbol{A}\rangle$. Since

$$\langle\boldsymbol{A}^\dagger\boldsymbol{A}\rangle=\mathrm{tr}\{\boldsymbol{\Xi}(\mu,k)\boldsymbol{A}^\dagger\boldsymbol{A}\}=\mathrm{tr}\{\boldsymbol{\Xi}(\mu,k)\boldsymbol{A}\boldsymbol{A}^\dagger\}-1$$

we find

$$n_{\mathrm{p}}(\mu,\bar{n})=\frac{N_{k+1}(\mu,\bar{n})}{N_k(\mu,\bar{n})}-1\,. \tag{3.11}$$

For a given noise level $\bar{n}$, the $n_{\mathrm{p}}(\mu,\bar{n})$ has a minimum at $\mu=0$. From (3.11) and (3.10) such a minimum is given by

$$n_{\mathrm{p}}(0,\bar{n})=(k+1)(\bar{n}+1)-1\,. \tag{3.12}$$

In the following, the Fock representation, the Wigner W-function, the Glauber–Sudarshan P-function, and the Husimi–Kano Q-function are given for noisy PACS.

Theorem 3.3.1 (*Fock representation).* The Fock representation of a noisy PACS $\boldsymbol{\Xi}(\mu,k)$ is found to be

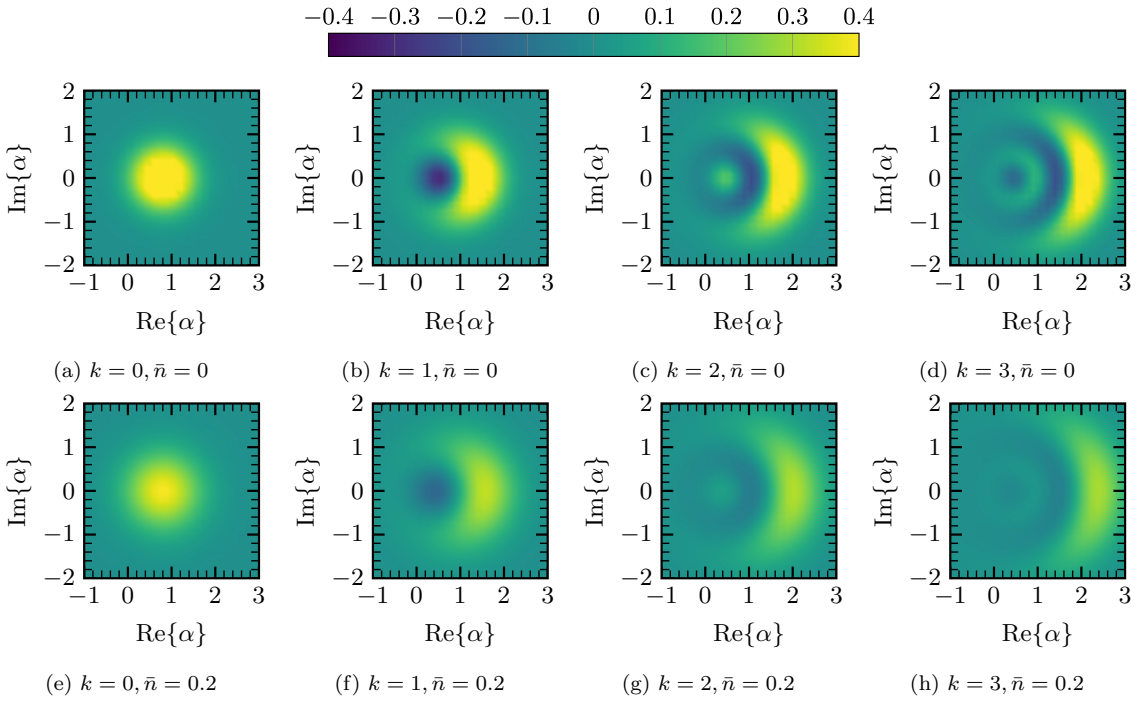
$$\langle n|\,\boldsymbol{\Xi}(\mu,k)\,|m\rangle=\begin{cases}c_{n,m}^{(k)} & \text{for both } n,m\geq k\\ 0 & \text{otherwise}\end{cases} \tag{3.13}$$

where $k\in\mathbb{N}$, and

$$\begin{aligned}c_{n,m}^{(k)}=\frac{(1-v)^{k+1}e^{-(1-v)|\mu|^2}}{v^k}\sqrt{\frac{n!}{m!}}\binom{m}{k}v^n\big[(1-v)\mu^*\big]^{m-n}\\ \times\frac{L_{n-k}^{m-n}\Big(\frac{-(1-v)^2|\mu|^2}{v}\Big)}{L_k\big(-|\mu|^2(1-v)\big)}\,.\end{aligned} \tag{3.14}$$

Proof. See Section 3.4.1. □

[2] This result is in accordance with [54, eq. (7)] for $V=2\bar{n}+1$.



(a) $k = 0, \bar{n} = 0$ (b) $k = 1, \bar{n} = 0$ (c) $k = 2, \bar{n} = 0$ (d) $k = 3, \bar{n} = 0$

(e) $k = 0, \bar{n} = 0.2$ (f) $k = 1, \bar{n} = 0.2$ (g) $k = 2, \bar{n} = 0.2$ (h) $k = 3, \bar{n} = 0.2$

Figure 3.5: Wigner W-function $W(\alpha)$ of a noisy PACS for different values of k and $\bar{n}$ with $\mu = 0.8$.

The probability distribution for the number of photons n in a PACS $\boldsymbol{\Xi}(\mu, k)$ is obtained using Theorem 3.3.1 as

$$\mathbb{P}\mathsf{n} = n = \langle n| \boldsymbol{\Xi}(\mu, k) |n\rangle = \begin{cases} p_n^{(k)}, & \text{for } n \geq k \\ 0 & \text{otherwise} \end{cases} \tag{3.15}$$

where $p_n^{(k)} = c_{n,n}^{(k)}$ is obtained from (3.14) with $m = n$. The following Theorems 3.3.2–3.3.4 provide a characterization of noisy PACS in terms of Wigner W-function, Glauber–Sudarshan P-function, and Husimi–Kano Q-function, respectively.

Theorem 3.3.2 (*W-function*)**.** The Wigner W-function of a noisy PACS $\boldsymbol{\Xi}(\mu, k)$ is found to be

$$W(\alpha) = \frac{(-1)^k}{(2\bar{n}+1)^k} \frac{L_k\left(\frac{|2\alpha(\bar{n}+1)-\mu|^2}{(2\bar{n}+1)(\bar{n}+1)}\right)}{L_k\left(-\frac{|\mu|^2}{\bar{n}+1}\right)} W_{\text{th}}(\alpha) \tag{3.16}$$

where $k \in \mathbb{N}$ and $W_{\text{th}}(\alpha)$ is the Wigner W-function of a noisy coherent state given by (2.76).

Proof. See Section 3.4.2. □

Fig. 3.5 shows $W(\alpha)$ for different values of k and $\bar{n}$. Notice that the Wigner function gets stretched and looses its negativity as $\bar{n}$ increases. Recalling that the negativity of

the Wigner function is an indicator of non-classicality of the state [135], this behavior shows that the quantum state decoheres as the thermal noise increases.

Theorem 3.3.3 (*P-function).* The Glauber–Sudarshan P-function of a noisy PACS $\boldsymbol{\Xi}(\mu, k)$ is found to be

$$P(\alpha) = \frac{(-1)^k}{\bar{n}^k} \frac{L_k\big(\frac{|\alpha(\bar{n}+1)-\mu|^2}{\bar{n}(\bar{n}+1)}\big)}{L_k\big(-\frac{|\mu|^2}{\bar{n}+1}\big)} P_{\text{th}}(\alpha) \tag{3.17}$$

where $k \in \mathbb{N}$ and $P_{\text{th}}(\alpha)$ is the Glauber–Sudarshan P-function of a noisy coherent state given by (2.77).

Proof. See Section 3.4.3. □

Theorem 3.3.4 (*Q-function).* The Husimi–Kano Q-function of a noisy PACS $\boldsymbol{\Xi}(\mu, k)$ is found to be

$$Q(\alpha) = \frac{|\alpha|^{2k}}{k!(\bar{n}+1)^k L_k\big(-\frac{|\mu|^2}{\bar{n}+1}\big)} Q_{\text{th}}(\alpha)\,. \tag{3.18}$$

where $k \in \mathbb{N}$ and $Q_{\text{th}}(\alpha)$ is the Husimi–Kano Q-function of a noisy coherent state given by (2.78).

Proof. See Section 3.4.4. □

It is worth noting that this characterization of a noisy PACS has relevant special cases. First, in case of no photon addition (i.e., $k = 0$) the characterization of a noisy PACS reduces to that of a noisy coherent state, as described in Section 2.2.5. Moreover, in the absence of noise (i.e., $\bar{n} = 0$), the characterization of a noisy PACS reduces to that of a noiseless PACS presented in [50]. Furthermore, in the absence of displacement (i.e., $\mu = 0$), the characterization of a noisy PACS reduces to that of a photon-added thermal state (PATS) presented in [51]. Finally, in the absence of both noise and displacement (i.e., $\bar{n} = \mu = 0$), the characterization of a noisy PACS reduces to that of a Fock state shown in [98].

3.4 Proof of the Results

3.4.1 Proof of Theorem 3.3.1

The coherent-state representation of a noisy PACS $\boldsymbol{\Xi}(\mu, k)$, defined as [88, eq. (6.1)], can be written as

$$R(\alpha^*, \beta) = e^{\frac{1}{2}(|\alpha|^2+|\beta|^2)} \langle\alpha|\, \boldsymbol{\Xi}(\mu, k)\, |\beta\rangle\ .$$

From (3.9),

$$R(\alpha^*,\beta) = \frac{e^{\frac{1}{2}(|\alpha|^2+|\beta|^2)}}{N_k} \langle\alpha|\,(\boldsymbol{A}^\dagger)^k \boldsymbol{D}_\mu \boldsymbol{\Xi}_{\mathrm{th}} \boldsymbol{D}_\mu^\dagger \boldsymbol{A}^k\,|\beta\rangle$$
$$= \frac{(\alpha^*\beta)^k}{N_k}\, e^{\frac{1}{2}(|\alpha|^2+|\beta|^2)} \langle\alpha|\,\boldsymbol{D}_\mu \boldsymbol{\Xi}_{\mathrm{th}} \boldsymbol{D}_\mu^\dagger\,|\beta\rangle \tag{3.19}$$

where the first equality is from (3.9) and (2.73), and the second equality follows from the fact that a coherent state is an eigenvector of $\boldsymbol{A}$. From the coherent-state representation of a displaced thermal state [4, eq. (4.15)] together with (3.10) and (2.35), the (3.19) becomes

$$R(\alpha^*,\beta) = \frac{(\alpha^*\beta)^k(1-v)^{k+1}}{k!L_k\big(-|\mu|^2(1-v)\big)} \exp\big\{-(1-v)|\mu|^2\big\}$$
$$\times \exp\big\{v\alpha^*\beta + (1-v)(\alpha^*\mu + \beta\mu^*)\big\}\,. \tag{3.20}$$

From the Mollow–Glauber double generating function for the associated Laguerre polynomials [136, eqs. (A1) and (A6)] and by applying some simple algebra, the (3.20) results in

$$R(\alpha^*,\beta) = \sum_{n=k}^{\infty}\sum_{m=k}^{\infty} \frac{(\alpha^*)^n\beta^m}{\sqrt{n!m!}} \frac{(1-v)^{k+1}}{L_k\big(-|\mu|^2(1-v)\big)v^k}$$
$$\times \exp\big\{-(1-v)|\mu|^2\big\}\sqrt{\frac{n!}{m!}}\binom{m}{k}v^n$$
$$\times [(1-v)\mu^*]^{m-n}\, L_{n-k}^{m-n}\Big(-\frac{(1-v)^2|\mu|^2}{v}\Big)\,. \tag{3.21}$$

From the relationship between coherent-state representation (3.21) and Fock representation [88, eq. (6.2)], the (3.13) is obtained. □

3.4.2 Proof of Theorem 3.3.2

The Wigner W-function of a noisy PACS $\boldsymbol{\Xi}(\mu,k)$, defined according to [50, eq. (3.5)], can be written as

$$W(\alpha) = \frac{2\,e^{2|\alpha|^2}}{\pi^2}\iint \langle-\beta|\,\boldsymbol{\Xi}(\mu,k)\,|\beta\rangle\, e^{2(\beta^*\alpha-\beta\alpha^*)} d\beta_{\mathrm{r}} d\beta_{\mathrm{i}}\,. \tag{3.22}$$

From (3.19),

$$\langle-\beta|\,\boldsymbol{\Xi}(\mu,k)\,|\beta\rangle = R(-\beta^*,\beta)e^{-|\beta|^2} \tag{3.23}$$

and by using it together with (3.20) in (3.22), it follows that

$$W(\alpha) = \frac{2(1-v)^{k+1} e^{2|\alpha|^2-(1-v)|\mu|^2}}{\pi^2 k!\, L_k\big(-|\mu|^2(1-v)\big)} \times \iint (-\beta^*\beta)^k\, e^{-(1+v)|\beta|^2+\beta^*(2\alpha-(1-v)\mu)-\beta(2\alpha-(1-v)\mu)^*} d\beta_{\mathrm{r}} d\beta_{\mathrm{i}}\,. \tag{3.24}$$

Then, by applying a double change of variable

$$\gamma = \beta\sqrt{1+v} \tag{3.25a}$$

$$\xi = \frac{2\alpha-(1-v)\mu}{\sqrt{1+v}} \tag{3.25b}$$

we obtain

$$W(\alpha) = \frac{2(1-v)^{k+1} e^{2|\alpha|^2-(1-v)|\mu|^2}}{\pi k!\, L_k\big(-|\mu|^2(1-v)\big)(1+v)^{k+1}}\, I^{(k)}(\xi) \tag{3.26}$$

where

$$I^{(k)}(\xi) = \frac{1}{\pi} \iint (-\gamma^*\gamma)^k\, e^{-|\gamma|^2+\gamma^*\xi-\gamma\xi^*} d\gamma_{\mathrm{r}} d\gamma_{\mathrm{i}}\,.$$

Using [137, eq. (A.28)] and the Wirtinger derivatives,

$$I^{(k)}(\xi) = \frac{\partial^{2k}}{\partial\xi^{*k}\,\partial\xi^k} e^{-|\xi|^2}$$

and, from the definition of Laguerre polynomials,

$$I^{(k)}(\xi) = (-1)^k k!\, e^{-|\xi|^2} L_k\big(|\xi|^2\big)\,. \tag{3.27}$$

From (3.27), the (3.26) can be rewritten as

$$W(\alpha) = \frac{(v-1)^k L_k\big(|\xi|^2\big) 2(1-v)\, e^{-|\xi|^2} e^{2|\alpha|^2-(1-v)|\mu|^2}}{(1+v)^k L_k\big(-|\mu|^2(1-v)\big)\pi(1+v)}\,. \tag{3.28}$$

From (3.25b) together with (2.36) and (2.76), the (3.28) results in (3.16). □

3.4.3 Proof of Theorem 3.3.3

The Glauber–Sudarshan P-function of a noisy PACS $\boldsymbol{\Xi}(\mu,k)$, defined according to [138, eq. (6)], can be written as

$$P(\alpha) = \frac{e^{|\alpha|^2}}{\pi^2} \iint \langle -\beta|\, \boldsymbol{\Xi}(\mu,k)\, |\beta\rangle\, e^{|\beta|^2} e^{\beta^*\alpha-\beta\alpha^*} d\beta_{\mathrm{r}} d\beta_{\mathrm{i}}\,. \tag{3.29}$$

Using (3.20) and (3.23) in (3.29), it follows that

$$P(\alpha) = \frac{(1-v)^{k+1} e^{|\alpha|^2-(1-v)|\mu|^2}}{\pi^2 k!\, L_k\big(-|\mu|^2(1-v)\big)} \iint (-\beta^*\beta)^k\, e^{-v|\beta|^2+\beta^*(\alpha-(1-v)\mu)-\beta(\alpha-(1-v)\mu)^*} d\beta_{\mathrm{r}} d\beta_{\mathrm{i}}\,. \tag{3.30}$$

Then, by applying a double change of variable

$$\gamma = \sqrt{v}\beta \tag{3.31a}$$

$$\xi = \frac{\alpha-(1-v)\mu}{\sqrt{v}} \tag{3.31b}$$

we obtain

$$P(\alpha) = \frac{(1-v)^{k+1} e^{|\alpha|^2-(1-v)|\mu|^2}}{\pi^2 k!\, L_k\big(-|\mu|^2(1-v)\big) v^{k+1}}\, I^{(k)}(\xi)\,. \tag{3.32}$$

From (3.27), (3.32) can be written as

$$P(\alpha) = \frac{(v-1)^k L_k(|\xi|^2)(1-v)\, e^{-|\xi|^2} e^{|\alpha|^2-(1-v)|\mu|^2}}{v^k L_k\big(-|\mu|^2(1-v)\big)\pi v}\,. \tag{3.33}$$

From (3.31b) together with (2.36) and (2.77), the (3.33) results in (3.17). □

3.4.4 Proof of Theorem 3.3.4

The Husimi–Kano Q-function of a noisy PACS $\boldsymbol{\Xi}(\mu, k)$, defined according to [139, eq. (12.7)], can be written as

$$Q(\alpha) = \frac{1}{\pi} \langle\alpha|\, \boldsymbol{\Xi}(\mu,k)\, |\alpha\rangle\ . \tag{3.34}$$

From (3.19),

$$Q(\alpha) = \frac{e^{-|\alpha|^2}}{\pi} R(\alpha^*, \alpha)\,. \tag{3.35}$$

From (3.20) together with (2.36) and (2.78), the (3.35) results in (3.18). □

Chapter 4

Quantum discrimination of non-Gaussian states

Quantum state discrimination (QSD) addresses the problem of identifying an unknown state among a set of quantum states [4, 38, 140]. QSD enables several applications including quantum communications [37, 45, 141], quantum sensing [25–27], quantum illumination [117, 142, 143], quantum cryptography [11–13], quantum networks [19, 21, 23], and quantum computing [14–16]. The DEP depends on the set of quantum states and the measurement used to discriminate among them. Determining the DEP and identifying the quantum measurement that minimizes the DEP are difficult tasks, especially for states prepared in the presence of thermal noise (hereafter referred to as noisy states).

Understanding how the choice of quantum states impacts the discrimination performance plays an important role in QSD applications. In particular, CV quantum states have been considered in quantum optics as they supply a quantum description of the electromagnetic field and can be efficiently prepared, manipulated, and measured [9, 29, 31, 144–147]. Previous works on CV-QSD have devoted particular attention to the analysis of discrimination between coherent states [35, 36, 42, 148–150], largely motivated by the success of the Glauber theory [81, 82, 87, 88].

In contrast, QSD with non-coherent states has received less attention except for attempts made on the use of squeezed states [46, 151, 152] and number states [47–49]. PACSs is an important class of non-coherent quantum states that can be generated in a laboratory [50, 56, 57], which have been characterized in the previous section. PACSs have been considered for quantum illumination [133] and quantum cryptography [153] but a characterization of QSD with PACSs is still missing.

This thesis envisions the use of non-Gaussian quantum states for QSD (see Fig-

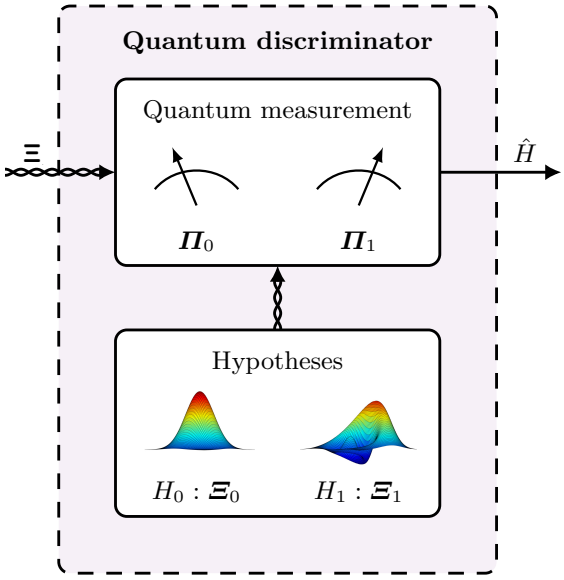


Figure 4.1: Illustration of binary QSD with non-Gaussian states: hypotheses are described by the Wigner functions corresponding to the quantum states.

ure 4.1). In particular, PACSs is an important class of non-Gaussian states that can provide significant benefits to QSD and pave the way for innovative applications in quantum sensing and networking. The goal is to establish the use of PACSs to improve QSD. The key contributions of this chapter are as follows:

- put forth the idea of using non-Gaussian states for QSD applications;
- characterization of QSD with noisy PACSs in terms of DEP.

4.1 General framework

Consider a quantum system with Hilbert space $\mathcal{H}$ and let $\mathcal{A} = \{\boldsymbol{\Xi}_i\}_{i=0}^{M-1} \subseteq \mathcal{D}(\mathcal{H})$ be the set of possible states for the quantum system. If the state of the system is unknown, there are M hypotheses about the state $\boldsymbol{\Xi}$ of the quantum system given by

$$H_j : \quad \boldsymbol{\Xi} = \boldsymbol{\Xi}_j \quad \text{for } j = 0, ..., M-1\,. \tag{4.1}$$

The decision among the M hypotheses, as depicted in Figure 5.1 for a binary scenario ($M = 2$), is done by mean of a quantum measurement described by the POVM $\mathcal{P} = \{\boldsymbol{\Pi}_0, \boldsymbol{\Pi}_1, ..., \boldsymbol{\Pi}_{M-1}\}$ so that the probability that the hypothesis H_j is choosen when H_k is true is given by

$$\mathbb{P}\{H_j|H_k\} = \mathrm{tr}\{\boldsymbol{\Xi}_k \boldsymbol{\Pi}_j\}\,. \tag{4.2}$$

By denoting with p_i the prior probabilities of H_i for $i = 0, 1, ..., M-1$, the DEP, i.e., the probability of choosing the wrong hypothesis is

$$P_{\mathrm{e}} = 1 - \sum_{i=0}^{M-1} p_i \operatorname{tr}\{\boldsymbol{\Xi}_i \boldsymbol{\Pi}_i\} . \tag{4.3}$$

The DEP determined by Equation (4.3) depends on the set $\mathcal{A}$ of the possible quantum states, and on the POVM $\mathcal{P}$ used to discriminate among them.

4.1.1 Optimal discrimination

Among several QSD strategies, of particular interest are those aiming to design the quantum measurement that minimizes the DEP, i.e., determine the POVM $\mathcal{P}$ that is a solution of the following semi-definite optimization problem

$$\begin{aligned} \min \quad & 1 - \sum_{i=1}^{M} p_i \operatorname{Tr}\{\boldsymbol{\Xi}_i \boldsymbol{\Pi}_i\} \\ \text{s.t.} \quad & \mathbf{0} \preccurlyeq \boldsymbol{\Pi}_i \preccurlyeq \boldsymbol{I} \qquad \text{for } i = 1, ..., M \\ & \sum_{i=1}^{M} \boldsymbol{\Pi}_i = \boldsymbol{I} \end{aligned} \tag{4.4}$$

This problem has been extensively studied in [4, 38, 140]. Determining the DEP and identifying the quantum measurement that minimizes the DEP are difficult tasks.

4.1.2 Optimal binary discrimination

Consider a binary QSD problem ($M = 2$) for which the hypotheses (4.1) are given by

$$\begin{aligned} H_0 &: \boldsymbol{\Xi} = \boldsymbol{\Xi}_0 \\ H_1 &: \boldsymbol{\Xi} = \boldsymbol{\Xi}_1 . \end{aligned} \tag{4.5}$$

The quantum states $\boldsymbol{\Xi}_0$ and $\boldsymbol{\Xi}_1$ have prior probability p_0 and p_1, respectively. Under these premises, the DEP is

$$P_{\mathrm{e}} = p_0 \operatorname{tr}\{\boldsymbol{\Xi}_0 \boldsymbol{\Pi}_1\} + p_1 \operatorname{tr}\{\boldsymbol{\Xi}_1 \boldsymbol{\Pi}_0\} . \tag{4.6}$$

In the binary case ($M = 2$), the minimum discrimination error probability (MDEP) is given in closed form by the Helstrom bound

$$\breve{P}_{\mathrm{e}} = \frac{1}{2}\left(1 - \|p_1\boldsymbol{\Xi}_1 - p_0\boldsymbol{\Xi}_0\|_1\right) . \tag{4.7}$$

The elements of the optimal POVM that achieves the Helstrom bound are given by

$$\breve{\boldsymbol{\Pi}}_0 = \sum_{\substack{i \\ \lambda_i<0}} |\lambda_i\rangle\langle\lambda_i| \tag{4.8a}$$

$$\breve{\boldsymbol{\Pi}}_1 = 1 - \breve{\boldsymbol{\Pi}}_0 = \sum_{\substack{i \\ \lambda_i\geq 0}} |\lambda_i\rangle\langle\lambda_i| \tag{4.8b}$$

where $|\lambda_i\rangle$ is the eigenvector of $p_1\boldsymbol{\Xi}_1 - p_0\boldsymbol{\Xi}_0$ associated with the eigenvalue λ_i. For pure states, i.e., $\boldsymbol{\Xi}_0 = |\psi_0\rangle\langle\psi_0|$ and $\boldsymbol{\Xi}_1 = |\psi_1\rangle\langle\psi_1|$, the MDEP is given by

$$\breve{P}_{\mathrm{e}} = \frac{1}{2}\Big(1 - \sqrt{1 - 4p_0p_1|\langle\psi_0|\psi_1\rangle|^2}\Big) . \tag{4.9}$$

Note that, in this case, the MDEP is zero when the two states are orthogonal, i.e., $\langle\psi_0|\psi_1\rangle = 0$. In the case of mixed states, the MDEP is zero when the density operators $\boldsymbol{\Xi}_0$ and $\boldsymbol{\Xi}_1$ have support on orthogonal subspaces [154].

4.2 Discrimination of PACSs

An important application of the QSD techniques described in the previous section is the discrimination of two photon-added coherent states, described in Section 3.3. This is an important application of the QSD techniques that will guide the design of quantum communication systems with non-Gaussian states.

4.2.1 Noiseless PACSs

Consider the discrimination of two PACS in a noiseless scenario, i.e., the states associated with the hypotheses in (4.5) are given by $\boldsymbol{\Xi}_0 = |\xi^{(h)}\rangle\langle\xi^{(h)}|$ and $\boldsymbol{\Xi}_1 = |\mu^{(k)}\rangle\langle\mu^{(k)}|$. Since the states are pure, the MDEP is determined by (4.9) with $|\psi_0\rangle = |\xi^{(h)}\rangle$ and $|\psi_1\rangle = |\mu^{(k)}\rangle$, and its dependence on the quantum states is manifested by the following Lemma.

Lemma 4.2.1. Consider two PACSs $|\xi^{(h)}\rangle$ and $|\mu^{(k)}\rangle$ according to (3.3). Without loss

of generality, let $h \leq k$. It is

$$\langle \xi^{(h)} | \mu^{(k)} \rangle = \frac{(\xi^*)^{k-h} L_h^{k-h}(-\mu\xi^*) e^{-\frac{1}{2}(|\mu|^2+|\xi|^2-2\mu\xi^*)}}{\sqrt{\frac{k!}{h!} L_k(-|\mu|^2) L_h(-|\xi|^2)}} \,. \tag{4.10}$$

Proof. See Section 4.3.1. □

The MDEP is found by using (4.10) in (4.9). Note that the scalar product between the two states, and thus the MDEP, is zero if one of the following orthogonality conditions holds

$$\text{(i)} \quad \xi = 0 \text{ and } h \neq k \tag{4.11a}$$

$$\text{(ii)} \quad L_h^{k-h}(-\mu\xi^*) = 0 \,. \tag{4.11b}$$

The orthogonality condition (4.11a) is of particular interest because $|\xi^{(h)}\rangle$ with $\xi = 0$ corresponds to the Fock state $|h\rangle$. This orthogonality condition is related to the fact that the photon-addition operation on $|\mu\rangle$ generates a state $|\mu^{(k)}\rangle$ orthogonal to the span of the set $\{|n\rangle : n \leq h\}$. If both $\xi = 0$ and $h = 0$, then $|\xi^{(h)}\rangle$ corresponds to the ground state, and therefore the QSD reduces to the discrimination between a PACS and the ground state. The orthogonality condition (4.11b) represents the situation in which there are canceling cross-terms in the scalar product of the two states. It can also be observed that the exponential factor in (4.10) makes the DEP vanish as $|\mu - \xi|$ increases. It is thus important to notice that, in the absence of noise it is possible to choose two PACSs such that the DEP is zero. Therefore, in the absence of noise, the use of PACSs can provide an optimal solution to the QSD problem.

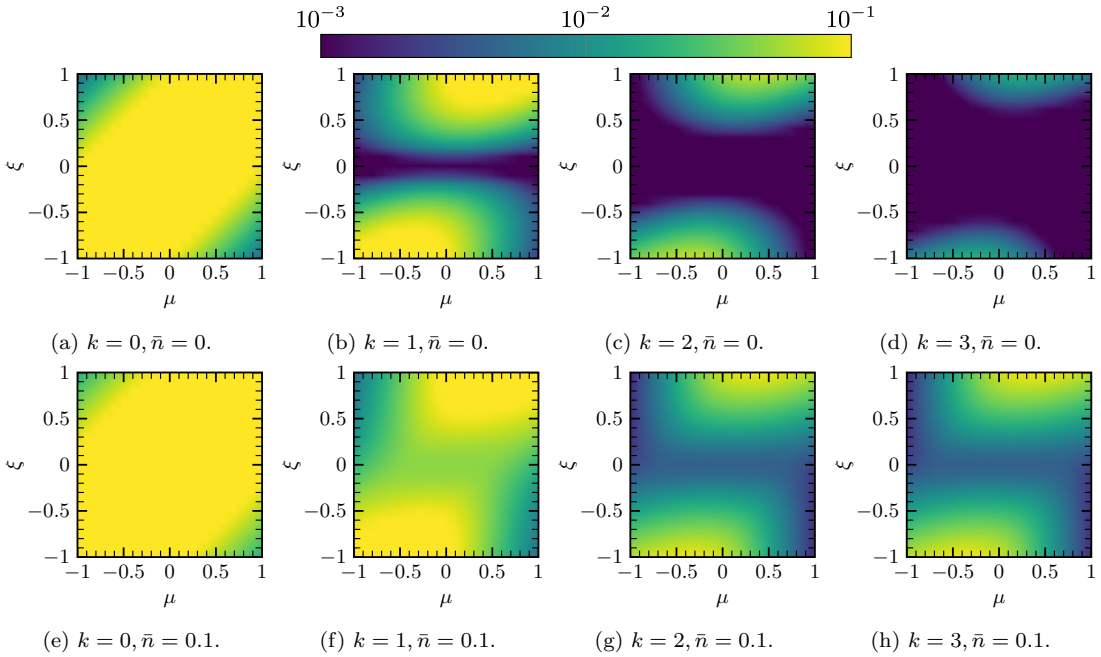
In the following, it is shown that the presence of thermal noise during state preparation increases the DEP. Since a noise component is unavoidable in quantum systems, it is essential to represent the noisy quantum states and characterize the QSD that accounts for thermal noise in state preparation.

4.2.2 Noisy PACSs

This section characterizes the binary QSD with noisy PACSs using the characterization given in Section 3.3. In particular, the quantum states associated with the binary hypotheses in (4.5) are

$$\boldsymbol{\Xi}_0 = \boldsymbol{\Xi}(\xi, h) \tag{4.12a}$$

$$\boldsymbol{\Xi}_1 = \boldsymbol{\Xi}(\mu, k) \,. \tag{4.12b}$$



(a) $k = 0, \bar{n} = 0.$ (b) $k = 1, \bar{n} = 0.$ (c) $k = 2, \bar{n} = 0.$ (d) $k = 3, \bar{n} = 0.$

(e) $k = 0, \bar{n} = 0.1.$ (f) $k = 1, \bar{n} = 0.1.$ (g) $k = 2, \bar{n} = 0.1.$ (h) $k = 3, \bar{n} = 0.1.$

Figure 4.2: MDEP for discrimination between a noisy PACS and a noisy coherent state as a function of μ and ξ, with $p_0 = p_1 = 1/2$.

Recall that, according to the Helstrom bound (4.7), the MDEP for a binary QSD depends on $\|\boldsymbol{\Delta}\|_1$ with $\boldsymbol{\Delta} = p_1\boldsymbol{\Xi}_1 - p_0\boldsymbol{\Xi}_0$. The following lemma shows that the MDEP for a binary QSD with quantum states as in (4.12) does not depend on the individual phases of ξ and μ, but only on the phase difference.

Lemma 4.2.2. Consider the PACSs $\boldsymbol{\Xi}_0 = \boldsymbol{\Xi}(\xi, h)$, $\boldsymbol{\Xi}_1 = \boldsymbol{\Xi}(\mu, k)$, $\boldsymbol{\Xi}_0^{(\theta)} = \boldsymbol{\Xi}(\xi e^{\imath\theta}, h)$, and $\boldsymbol{\Xi}_1^{(\phi)} = \boldsymbol{\Xi}(\mu e^{\imath\phi}, k)$ with $\theta, \phi \in \mathbb{R}$, defined as in (3.9). Then,

$$\|p_1\boldsymbol{\Xi}_1^{(\phi)} - p_0\boldsymbol{\Xi}_0^{(\theta)}\|_1 = \|p_1\boldsymbol{\Xi}_1 - p_0\boldsymbol{\Xi}_0^{(\theta-\phi)}\|_1 . \tag{4.13}$$

Proof. See Section 4.3.2. □

This result simplifies the QSD characterization, especially when one of the states is the thermal state for which the phase is irrelevant, as shown in the following corollary.

Corollary 4.2.3. Consider the PACSs of Lemma 4.2.2 with $\xi = h = 0$, for which $\boldsymbol{\Xi}_0 = \boldsymbol{\Xi}_{\text{th}}$. Then,

$$\|p_1\boldsymbol{\Xi}_1^{(\phi)} - p_0\boldsymbol{\Xi}_0^{(\theta)}\|_1 = \|p_1\boldsymbol{\Xi}_1 - p_0\boldsymbol{\Xi}_{\text{th}}\|_1 . \tag{4.14}$$

Proof. From $\boldsymbol{\Xi}_0^{(\theta-\phi)} = \boldsymbol{R}_{\theta-\phi}\boldsymbol{\Xi}_{\text{th}}\boldsymbol{R}_{\theta-\phi}^\dagger$ and rotational invariance of $\boldsymbol{\Xi}_{\text{th}}$, the (4.13) reduces to (4.14). □

The operator $\boldsymbol{\Delta}$ has an infinite number of eigenvalues that have no closed-form expression. This is a long standing problem [4] and a tractable approximation of $\boldsymbol{\Delta}$ is

needed to compute the MDEP. A simple way to approximate $\boldsymbol{\Delta}$ is to use an operator $\tilde{\boldsymbol{\Delta}}_N$, of finite dimension N, in the Fock representation. In particular, $\boldsymbol{\Delta} \simeq \tilde{\boldsymbol{\Delta}}_N$ where

$$\tilde{\boldsymbol{\Delta}}_N = \sum_{n=0}^{N-1} \sum_{m=0}^{N-1} \langle n| \boldsymbol{\Delta} |m\rangle \, |n\rangle\langle m|$$

with entries $\langle n| \boldsymbol{\Delta} |m\rangle$ obtained using (3.13). The accuracy of MDEP approximation using $\tilde{\boldsymbol{\Delta}}_N$ depends on N.[1]

To quantify the noise effects on QSD, the following case study will be considered: $\boldsymbol{\Xi}_0$ is assumed to be a noisy coherent state and $\boldsymbol{\Xi}_1$ a noisy PACS. Therefore, the quantum states associated with the binary hypotheses in (4.5) are

$$\begin{aligned} \boldsymbol{\Xi}_0 &= \boldsymbol{\Xi}(\xi, 0) \\ \boldsymbol{\Xi}_1 &= \boldsymbol{\Xi}(\mu, k)\,. \end{aligned}$$

Recall from (4.7) and Lemma 4.2.1 that, since $h = 0$, the MDEP only depends on $\bar{n}$, k, $|\xi|$, $|\mu|$, and $\arg(\xi) - \arg(\mu)$.

Figure 4.2 shows the MDEP as a function of μ and ξ, for different values of k and $\bar{n}$.[2] Note that, for $\bar{n} \neq 0$, the MDEP is always greater than zero and, differently from (4.11a) in the noiseless case, $\xi = 0$ is no longer an optimal solution.

4.3 Proof of the Results

4.3.1 Proof of Lemma 4.2.1

From (3.3) and the normalization in [50],

$$\langle \xi^{(h)} | \mu^{(k)} \rangle = \frac{\langle \xi| \boldsymbol{A}^h (\boldsymbol{A}^\dagger)^k |\mu\rangle}{\sqrt{h!k! L_k(-|\mu|^2) L_h(-|\xi|^2)}}\,. \tag{4.15}$$

[1] $N = 30$ will be used in the remainder.

[2] While ξ and μ are complex in general, here they are plotted for real values.

The enumerator of (4.15) can be written as

$$\begin{aligned}\langle\xi|\,\boldsymbol{A}^h(\boldsymbol{A}^\dagger)^k\,|\mu\rangle &= \langle\xi|\mu\rangle\sum_{n=0}^{h} n!\binom{k}{n}\binom{h}{n}\mu^{h-n}(\xi^*)^{k-n}\\ &= \langle\xi|\mu\rangle\, h!(\xi^*)^{k-h}\sum_{n=0}^{h}\binom{k}{h-n}\frac{(\mu\xi^*)^n}{n!}\\ &= \langle\xi|\mu\rangle\, h!(\xi^*)^{k-h}L_h^{k-h}(-\mu\xi^*) \qquad (4.16)\end{aligned}$$

where the first equality is obtained by using [81, eq. (5.12)] to express $\boldsymbol{A}^h(\boldsymbol{A}^\dagger)^k$ in the normal order and noticing that $\boldsymbol{A}\,|\mu\rangle = \mu\,|\mu\rangle$ when $|\mu\rangle$ is a coherent state; the second equality follows from simple algebra; and the third equality follows from the definition of generalized Laguerre polynomials. From (4.16), and [88, eq. (3.32)], (4.15) results in (4.10). □

4.3.2 Proof of Lemma 4.2.2

From (3.9) and (2.73),

$$\boldsymbol{\Xi}_1^{(\phi)} = \frac{1}{N_k}(\boldsymbol{A}^\dagger)^k\boldsymbol{D}_\nu\boldsymbol{\Xi}_{\rm th}\boldsymbol{D}_\nu^\dagger\boldsymbol{A}^k \qquad (4.17)$$

where $\nu = \mu e^{\imath\phi}$. By using the relationships between the operators $\boldsymbol{A}$, $\boldsymbol{A}^\dagger$, $\boldsymbol{D}_\mu$, and $\boldsymbol{R}_\phi$ [155], we obtain

$$\begin{aligned}\boldsymbol{\Xi}_1^{(\phi)} &= \frac{1}{N_k}(\boldsymbol{A}^\dagger)^k\boldsymbol{R}_\phi\boldsymbol{D}_\mu\boldsymbol{\Xi}_{\rm th}\boldsymbol{D}_\mu^\dagger\boldsymbol{R}_\phi^\dagger\boldsymbol{A}^k\\ &= \frac{1}{N_k}\boldsymbol{R}_\phi(\boldsymbol{A}^\dagger)^k\boldsymbol{D}_\mu\boldsymbol{\Xi}_{\rm th}\boldsymbol{D}_\mu^\dagger\boldsymbol{A}^k\boldsymbol{R}_\phi^\dagger\\ &= \boldsymbol{R}_\phi\boldsymbol{\Xi}_1\boldsymbol{R}_\phi^\dagger \qquad (4.18)\end{aligned}$$

where the first equality follows from $\boldsymbol{R}_\phi\boldsymbol{D}_\mu\boldsymbol{R}_\phi^\dagger = \boldsymbol{D}_\nu$ and the rotational invariance of $\boldsymbol{\Xi}_{\rm th}$, for which $\boldsymbol{R}_\phi^\dagger\boldsymbol{\Xi}_{\rm th}\boldsymbol{R}_\phi = \boldsymbol{\Xi}_{\rm th}$; the second equality follows from $\boldsymbol{R}_\phi^\dagger\boldsymbol{A}\boldsymbol{R}_\phi = \boldsymbol{A}e^{-i\phi}$; and the third equality follows from the definition of $\boldsymbol{\Xi}_1$. Therefore, by using (4.18) for both $\boldsymbol{\Xi}_1^{(\phi)}$ and $\boldsymbol{\Xi}_0^{(\theta)}$ in the left-hand side of (4.13),

$$\begin{aligned}\|p_1\boldsymbol{\Xi}_1^{(\phi)} - p_0\boldsymbol{\Xi}_0^{(\theta)}\|_1 &= \|p_1\boldsymbol{R}_\phi\boldsymbol{\Xi}_1\boldsymbol{R}_\phi^\dagger - p_0\boldsymbol{R}_\theta\boldsymbol{\Xi}_0\boldsymbol{R}_\theta^\dagger\|_1\\ &= \|p_1\boldsymbol{\Xi}_1 - p_0\boldsymbol{R}_{\theta-\phi}\boldsymbol{\Xi}_0\boldsymbol{R}_{\theta-\phi}^\dagger\|_1 \qquad (4.19)\end{aligned}$$

where the last equality follows from the isometric invariance of the trace norm [154], and $\boldsymbol{R}_\phi^\dagger = \boldsymbol{R}_{-\phi}$. From the definition of $\boldsymbol{\Xi}_0^{(\theta-\phi)}$, (4.19) results in (4.13). □

Chapter 5

Quantum communications with non-Gaussian states

Quantum state discrimination [4,5,38,140] is a key enabler for next-generation information and communication technologies, including quantum sensing [26,27,156], quantum networking [13, 19–21, 157], and quantum communications [8, 37, 141, 158]. In particular, the use of quantum properties is beneficial for conveying classical information via a quantum communication system [35, 36, 39–41, 45]. However, the design and the analysis of a quantum communication system is challenging as the error probability in the quantum domain requires solving a QSD problem. This is a difficult task, especially in the presence of noisy quantum states.

In the literature, attention has been devoted to the analysis of quantum communication systems employing constellations with coherent states [4, 36–38, 43–45], which can be easily generated by a laser and have been extensively characterized from a theoretical viewpoint. The possibility to use a different set of states in the communication system has received scarce attention. This is in part due to the fact that the preparation of non-classical states of light is a difficult task that should be taken into account for a fair comparison between different systems. However, the few attempts made in this direction with squeezed states [46, 151, 152] and number states [47, 48], showed an improvement of the system performance.

The possibility of using other classes of non-Gaussian states in a quantum communication system was envisioned in [5], which proved the utility of PACSs in QSD. However, despite this preliminar work proving the utility of PACSs in QSD applications, the possibility of using non-Gaussian states in quantum communication systems has not been investigated yet.

This thesis envisions the use of non-Gaussian quantum states for quantum commu-

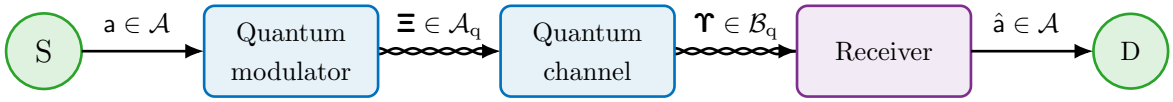


Figure 5.1: Block scheme of a quantum communication systems.

nication systems. In particular, it is shown that PACSs and PASSs are two important classes of non-Gaussian states that can provide significant benefits to quantum communication systems. The goal is to establish the use of non-Gaussian states in quantum communication systems systems. The key contributions are as follows:

- put forth the idea of using non-Gaussian states for quantum communication systems, including QOOK and QPPM;
- characterization of QOOK and QPPM systems with noisy PACSs and PASSs in terms of error probability; and
- quantification of the effects of state preparation and decoherence on the system performance.

5.1 Quantum communication systems

In an M-ary quantum communication system (see Figure 5.1), a classical symbol $\mathsf{a} \in \mathcal{A} = \{a_0, a_1, \ldots, a_{M-1}\}$ is conveyed to the destination by a quantum state chosen from a set $\mathcal{A}_{\mathrm{q}} = \{\boldsymbol{\Xi}_0, \boldsymbol{\Xi}_1, \ldots, \boldsymbol{\Xi}_{M-1}\} \subseteq \mathcal{D}(\mathcal{H}_{\mathrm{q}})$, referred to as quantum constellation [44].

Therefore, a quantum modulator, described by a map $a_i \mapsto \boldsymbol{\Xi}_i$ for $i = 0, 1, \ldots, M-1$, associates a classical symbol to a quantum state. The probability that the symbol a_i with $i = 0, 1, \ldots, M-1$ is chosen is given by p_i, i.e., $p_i = \mathbb{P}\{\mathsf{a} = a_i\}$. The Hilbert space $\mathcal{H}_{\mathrm{q}}$ associated to the quantum constellation is assumed to be the Hilbert space of a CV system, as described in Section 2.2.

In the propagation from source to destination, the quantum state may decohere due to the noise present in the quantum channel. A quantum channel is described by a completely positive trace-preserving mapping $\boldsymbol{\Xi}_i \mapsto \boldsymbol{\Upsilon}_i$ for $i = 0, 1, \ldots, M-1$. In this section, the phase-diffusion and the photon-loss channels described in Section 2.2.6 will be considered.

The receiver consists of a quantum measurement that provides an estimator $\hat{\mathsf{a}}$ of the transmitted symbol. The quantum measurement has M outcomes and it is described by an M-ary POVM $\mathcal{P} = \{\boldsymbol{\Pi}_0, \boldsymbol{\Pi}_1, \ldots, \boldsymbol{\Pi}_{M-1}\}$. Since the transmitted symbol is unknown, the design of the receiver can be formulated as an hypothesis testing problem

in which there are M hypotheses about the state $\boldsymbol{\Xi}$ as given by (4.1). The set of states defining the hypotheses corresponds to the quantum constellation $\mathcal{A}_{\mathrm{q}}$, and thus it depends on the modulation employed. The SEP is defined as the probability that the estimate symbol $\hat{a}$ is different from the transmitted symbol, and it is given by the DEP of the corresponding hypothesis testing problem.

This section characterizes the modulators and the different receivers for QOOK and QPPM systems.

5.1.1 Quantum modulator

This section defines two different quantum modulations, i.e., two different choices for the quantum constellation $\mathcal{A}_{\mathrm{q}}$.

Quantum on-off keying

The QOOK modulation is a binary modulation ($M = 2$) in a single mode CV system, i.e., the Hilbert space of the quantum system is $\mathcal{H}_{\mathrm{q}} = \mathcal{H}$ where $\mathcal{H}$ is the Hilbert space of a single-mode CV system described in Section 2.2. The quantum states associated with the binary hypotheses in (4.1) are

$$\begin{aligned} \boldsymbol{\Xi}_0 &= \boldsymbol{\Xi}^{(0)} \\ \boldsymbol{\Xi}_1 &= \boldsymbol{\Xi}^{(1)} \end{aligned} \tag{5.1}$$

where the density operator $\boldsymbol{\Xi}^{(0)}$ describes the state of the quantum system when no signal is transmitted, i.e., the ground state (2.32) in the absence of preparation noise or the thermal state (2.33) in the presence of noise, and $\boldsymbol{\Xi}^{(1)}$ describes the state of the quantum system in the presence of a signal. The choice of $\boldsymbol{\Xi}^{(1)}$ is purely arbitrary. In a conventional QOOK system, $\boldsymbol{\Xi}^{(1)}$ is a coherent state as in (2.66), in the absence of noise, or a noisy coherent state as in (2.73), in the presence of thermal noise in state preparation. Notice that the state $\boldsymbol{\Xi}^{(1)}$ affects the system performance and thus it can be engineered together with the system receiver, to maximize the system performance, as detailed in the following.

Quantum pulse position modulation

In an M-ary QPPM the information is encoded in the temporal position of a known signal called pulse. Therefore, the modulation is encoded in an ensemble of M single-mode CV systems, i.e., the Hilbert space of the quantum system is $\mathcal{H}_{\mathrm{q}} = \mathcal{H}^{\otimes M}$ where $\mathcal{H}$ is the Hilbert space of a single-mode CV system described in Section 2.2.

In particular, the quantum states associated with the M hypotheses in (4.1) are

$$\boldsymbol{\Xi}_i = \bigotimes_{j=0}^{M-1} \boldsymbol{\Psi}_{i,j} \quad \text{for} \quad i = 0, \ldots, M-1 \tag{5.2}$$

where $\boldsymbol{\Psi}_{i,j} = \boldsymbol{\Xi}^{(1)}$ for $j = i$ and $\boldsymbol{\Psi}_{i,j} = \boldsymbol{\Xi}^{(0)}$ for $j \neq i$. As for the QOOK modulation, the density operator $\boldsymbol{\Xi}^{(0)}$ describes the state of the quantum system when no signal is transmitted (i.e., a ground state or thermal state), and $\boldsymbol{\Xi}^{(1)}$ describes the state of the quantum system in the presence of a signal, for which its choice is arbitrary. In particular, for a conventional QPPM system, in the presence of thermal noise in state preparation, $\boldsymbol{\Xi}^{(1)}$ is a noisy coherent state as in (2.73). As for QOOK, the state can be engineered together with the system receiver, to maximize the system performance, as detailed in the following.

As an example, in a 4-QPPM system the states of the quantum constellation (5.2) are given by

$$\begin{aligned}
\boldsymbol{\Xi}_0 &= \boldsymbol{\Xi}^{(1)} \otimes \boldsymbol{\Xi}^{(0)} \otimes \boldsymbol{\Xi}^{(0)} \otimes \boldsymbol{\Xi}^{(0)} \\
\boldsymbol{\Xi}_1 &= \boldsymbol{\Xi}^{(0)} \otimes \boldsymbol{\Xi}^{(1)} \otimes \boldsymbol{\Xi}^{(0)} \otimes \boldsymbol{\Xi}^{(0)} \\
\boldsymbol{\Xi}_2 &= \boldsymbol{\Xi}^{(0)} \otimes \boldsymbol{\Xi}^{(0)} \otimes \boldsymbol{\Xi}^{(1)} \otimes \boldsymbol{\Xi}^{(0)} \\
\boldsymbol{\Xi}_3 &= \boldsymbol{\Xi}^{(0)} \otimes \boldsymbol{\Xi}^{(0)} \otimes \boldsymbol{\Xi}^{(0)} \otimes \boldsymbol{\Xi}^{(1)} .
\end{aligned}$$

5.1.2 Quantum and classical receivers

This section descrjbes three different quantum receivers, i.e., three different choices of the POVM $\mathcal{P}$. The choice of $\mathcal{P}$ affects the SEP, that is given by Eq. (4.3), i.e.,

$$P_{\mathrm{e}} = \mathbb{P}\{\hat{\mathsf{a}} \neq \mathsf{a}\} = 1 - \sum_{i=0}^{M-1} p_i \operatorname{tr}\{\boldsymbol{\Upsilon}_i \boldsymbol{\Pi}_i\} . \tag{5.3}$$

Minimum SEP receiver

The optimal receiver is the receiver that minimizes the SEP, given by Eq. (5.3). The optimal receiver can be determined by solving the optimization problem (4.4), which is in general a difficult task. For the special case of binary modulation ($M = 2$) the elements of the POVM are given by Eqs. (4.8a)-(4.8b), and the minimum symbol error probability (MSEP) is given by Eq. (4.7), i.e.,

$$\breve{P}_{\mathrm{e}} = \frac{1}{2} \left(1 - \| p_1 \boldsymbol{\Upsilon}_1 - p_0 \boldsymbol{\Upsilon}_0 \|_1\right) . \tag{5.4}$$

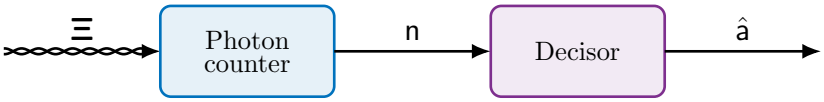


Figure 5.2: Counting receiver for QOOK.

Square root measurement receiver

The square root measurement (SRM) receiver is a suboptimal receiver that can be used to overcome the difficulties in the design of the MSEP receiver. It has been first introduced in [159], and then studied in [160–162]. In the SRM receiver the POVM can be determined directly from the set of states to be discriminated, without solving the optimization problem (4.4). In particular, the elements of the POVM are given by

$$\boldsymbol{\Pi}_i = \boldsymbol{\Upsilon}^{-1/2} p_i \boldsymbol{\Upsilon}_i \boldsymbol{\Upsilon}^{-1/2} \quad \text{for} \quad i = 0, \dots, M-1 \tag{5.5}$$

where

$$\boldsymbol{\Upsilon} = \sum_{i=0}^{M-1} \boldsymbol{\Upsilon}_i \,. \tag{5.6}$$

The SRM is a good approximation of the MSEP receiver and it has the advantage to be easily found directly from the quantum states by using an algebraic equation (5.5) instead of solving the semi-definite problem to find the MSEP receiver.

Counting receiver

The counting receiver counts the number of photons in the received quantum states, and takes a decision based on the measurement result. The decision policy depends on the modulation. The counting receiver is more feasible to realize than the MDEP receiver and admits a purely classical description [41].

Counting receiver for QOOK modulation. For a QOOK modulation the counting receiver (see Figure 5.2) simply counts the number of photons n (or, equivalently, the energy as given in (2.7)) in the received state $\boldsymbol{\Xi}$ and compares with a threshold $\lambda \in \mathbb{N}$. If the number of counted photons is greater than λ, then H_1 is chosen, otherwise H_0 is chosen. Therefore, the POVM is given by

$$\begin{aligned} \boldsymbol{\Pi}_0 &= \sum_{n<\lambda} |n\rangle\langle n| \\ \boldsymbol{\Pi}_1 &= \sum_{n\geq\lambda} |n\rangle\langle n| \,. \end{aligned} \tag{5.7}$$

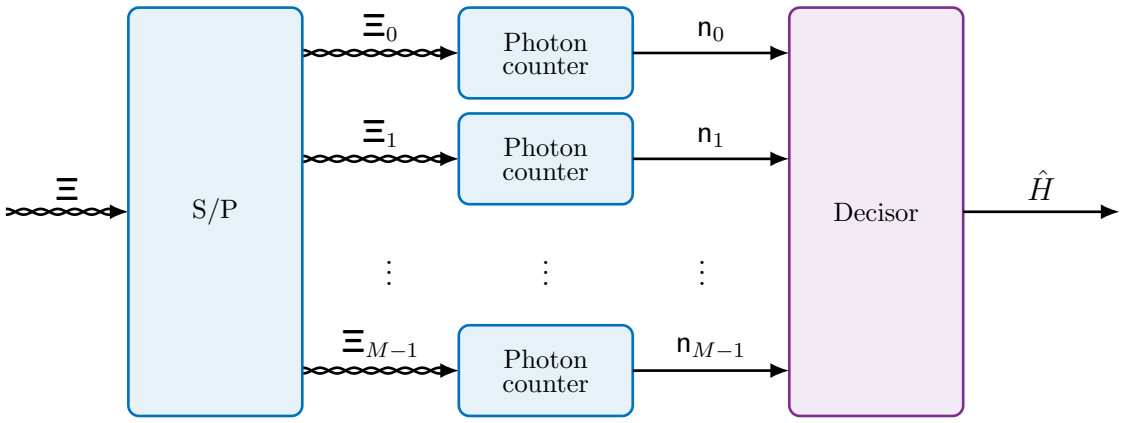


Figure 5.3: Counting receiver for QPPM.

The SEP is given by using the POVM definition (5.7) into Eq. (4.6) for the DEP in a binary QSD, for which

$$P_{\mathrm{e}}(\lambda) = p_0 v^{\lambda} + p_1 \sum_{n<\lambda} \langle n| \boldsymbol{\Xi}^{(1)} |n\rangle \ . \tag{5.8}$$

Since the quantum measurement is fixed, the measurement statistic is determined and thus the choice of the threshold λ is guided by the classical detection theory [163]. In particular, the hypothesis H_1 is chosen if the following condition is satisfied

$$\frac{q_1(n)}{q_0(n)} > \frac{p_0}{p_1} \tag{5.9}$$

where

$$q_j(n) = \langle n| \boldsymbol{\Xi}_j |n\rangle \quad \text{for } j = 0, 1 \, . \tag{5.10}$$

Therefore, there exists an optimal threshold λ^* such that $P_{\mathrm{e}} = P_{\mathrm{e}}(\lambda^*) = \min_{\lambda} P_{\mathrm{e}}(\lambda)$.

Counting receiver for QPPM modulation. For a M-QPPM modulation the counting receiver (see Figure 5.3) counts the number of photons n_j in each mode j of the received state $\boldsymbol{\Xi}$ and decides the hypothesis H_j with the highest n_j.[1] If a number g of modes have an equal number of photons, then one of these modes is chosen at random with probability $1/g$. Therefore, the POVM is given by

$$\boldsymbol{\Pi}_i = \sum_{\boldsymbol{n}\in\mathcal{D}_i} |\boldsymbol{n}\rangle\langle\boldsymbol{n}| + \sum_{g=2}^{M} \frac{1}{g} \sum_{\boldsymbol{n}\in\mathcal{G}_i^{(g)}} |\boldsymbol{n}\rangle\langle\boldsymbol{n}| \quad \text{for} \quad i = 0, \ldots, M-1 \tag{5.11}$$

[1] Recall that $\boldsymbol{\Xi} \in \mathcal{D}(\mathcal{H}^{\otimes M})$

where

$$\mathcal{D}_i = \{\boldsymbol{n} \in \mathbb{N}^M : n_i > n_j \text{ for } j \neq i\} \tag{5.12}$$

is the decision region for the mode i, and

$$\mathcal{G}_i^{(g)} = \{\boldsymbol{n} \in \mathbb{N}^M : n_i = n_j \text{ for } j \in \mathcal{K}, \text{with } \mathcal{K} \in {}_g\mathcal{C}_M\} \tag{5.13}$$

is the "confusion" regions in which g of the M modes have the same number of photons. The probability for a correct detection $P_\mathrm{c} = 1 - P_\mathrm{e}$ has been derived by Helstrom [4, Eq. (A.7) p. 194] and it is given by

$$P_\mathrm{c} = \frac{1}{M(1-v)}\,\mathbb{E}_{\mathsf{n}}\left\{\sum_{h=1}^{M}(-1)^h\binom{M}{h}(v^h-1)v^{\mathsf{n}(h-1)}\right\} \tag{5.14}$$

where the expected value is taken over to the number of photons n in the state $\boldsymbol{\Xi}^{(1)}$.

5.2 Quantum on-off keying with non-Gaussian states

This section defines and characterizes a QOOK system with a PACS. The use of a PACS in QPPM communication systems can reduce the SEP with respect to the use of coherent states, as shown in the following.

5.2.1 System model

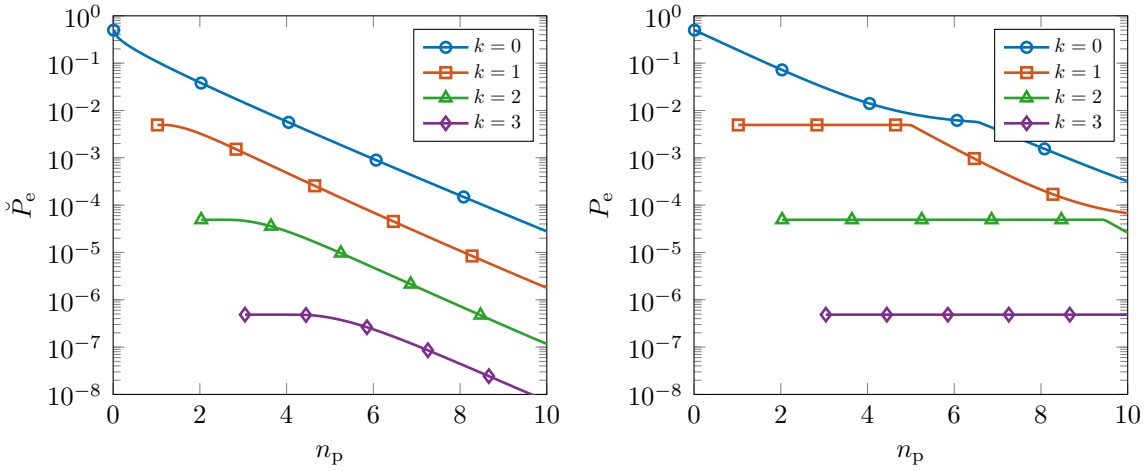
The quantum constellation of an QOOK using a PACS is given by (5.1) with $\boldsymbol{\Xi}_1 = \boldsymbol{\Xi}(\mu, k)$, where $\boldsymbol{\Xi}(\mu, k)$ is a PACS as defined in (3.9), and $\boldsymbol{\Xi}_0 = \boldsymbol{\Xi}_\mathrm{th}$.

5.2.2 Performance evaluation in absence of noise

Performance evaluation with optimal receiver

The MSEP for this binary system is determined according to the Helstrom bound (4.7) and depends on $\|\boldsymbol{\Delta}\|_1$, with $\boldsymbol{\Delta} = p_1\boldsymbol{\Upsilon}_1 - p_0\boldsymbol{\Upsilon}_0$. However, in this case, the eigenvalues of the operator $\boldsymbol{\Delta}$ have no closed form expression and thus a tractable approximation of $\boldsymbol{\Delta}$ is needed to compute the MSEP. The operator $\boldsymbol{\Delta}$ can be approximated with a finite dimensional operator $\tilde{\boldsymbol{\Delta}}_N$ defined as in Section 4.2.2. Here, the minimum symbol error probability is approximated using $\|\boldsymbol{\Delta}\|_1 \simeq \|\tilde{\boldsymbol{\Delta}}_{30}\|_1$.

Figure 5.4a shows the MSEP as a function of the mean number n_p of photons in $\boldsymbol{\Xi}_1$, for different values of k. Note that the use of a PACS improves the system performance



(a) Optimal receiver (quantum).

(b) Counting receiver (classical).

Figure 5.4: Performance of QOOK as a function of n_p, with $\bar{n} = 10^{-2}$ and $p_0 = p_1 = 1/2$.

compared to the use of a coherent state ($k = 0$). Moreover, the performance improves with the number of photon addition operations, which is inversely proportional to the state generation efficiency. Therefore, there is a trade-off between the MSEP and the state generation rate. Furthermore, the minimum value of n_p is given by (3.12).

Notice that the performance analysis of this section does not consider the state preparation efficiency. Indeed, as shown in Sec. 3.1.1, PAS are typically prepared by means of a non-deterministic procedure, with a low probability of successfully generate a PAS. Moreover, the probability decreases as the number of addition operation k increases. We will consider this effect in the performance analysis of a quantum communication system in Sec. 5.3.4.

Performance evaluation with counting receiver

The performance of a QOOK system using a PACS and employing a counting receiver can be easily determined by using (5.8) together with the Fock representation of a PACS given in (3.13).

Figure 5.4b shows the SEP of a counting receiver as a function of the mean number n_p of photons in $\boldsymbol{\Xi}_1$, for different values of k. In comparison to Figure 5.4a, it can be observed that the SEP with a counting receiver is higher than that of the optimal quantum receiver (i.e., the MSEP), as expected. Note that the use of a PACS improves the QSD performance compared to the use of a coherent state ($k = 0$), even for the counting receiver. Note also that the SEP of a counting receiver approaches the MSEP for low values of n_p. This can be attributed to the fact that, when n_p is low, the

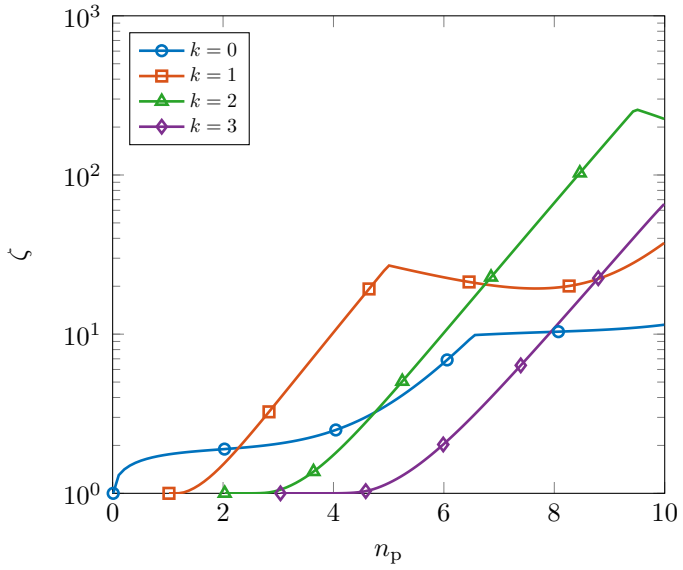


Figure 5.5: Quantum gain ζ as a function of n_p, with $\bar{n} = 10^{-2}$, and $p_0 = p_1 = 1/2$.

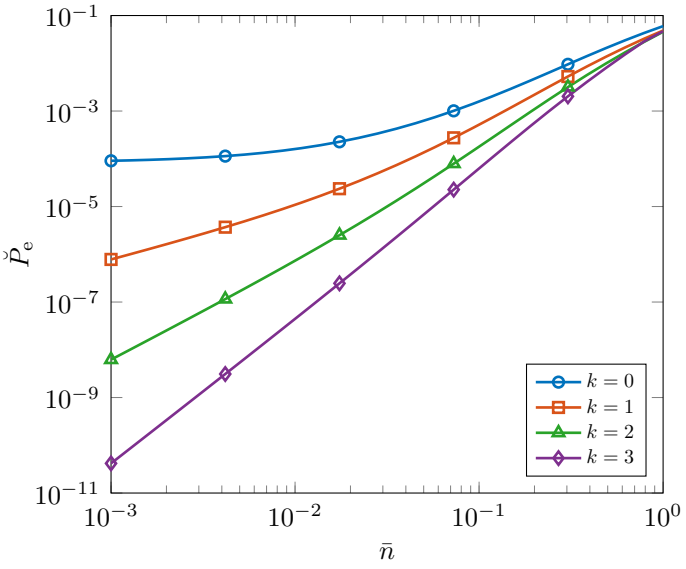


Figure 5.6: MSEP of a QOOK system using a PACS as a function of $\bar{n}$, with $n_\mathrm{p} = 8$, and $p_0 = p_1 = 1/2$.

off-diagonal terms in the Fock representation vanish, hence the quantum advantage of in using PACSs is reduced.

Figure 5.5 shows the quantum gain ζ, the ratio between the SEP with a counting receiver and the MSEP with the optimal receiver, as a function of n_p, for different values of k. Note that the use of the optimal quantum receiver always allows for improvement of the performance with respect to a classical receiver.

Figure 5.6 shows the MSEP as a function of the mean number $\bar{n}$ of thermal photons, for different values of k and for fixed $n_\mathrm{p} = 8$. Note that the use of a PACS improves

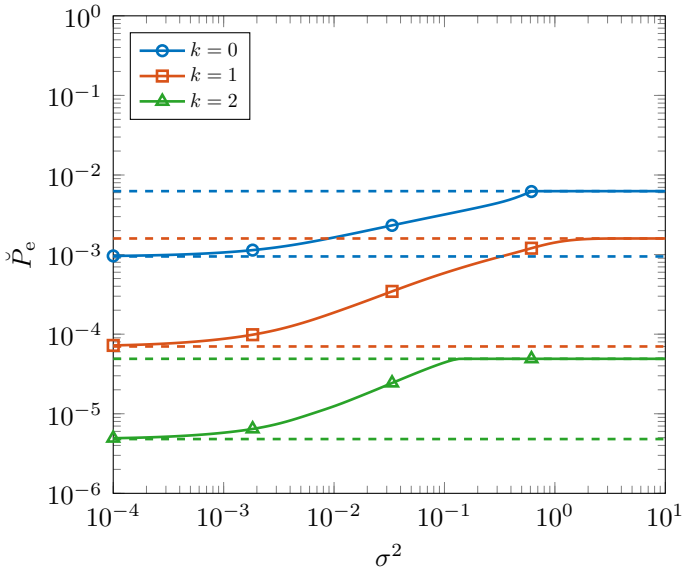


Figure 5.7: MSEP of a QOOK system using a PACS affected by phase diffusion as a function of σ^2, with $n_\mathrm{p} = 6$, $\bar{n} = 10^{-2}$, and $p_0 = p_1 = 1/2$. The two dashed lines for each k represent the MSEP without phase noise (bottom) and the SEP of a counting receiver (top).

the system performance compared to the use of a coherent state ($k = 0$), especially for small $\bar{n}$. Therefore, PACSs are particularly valuable in situations when thermal noise is low.

5.2.3 Performance evaluation in presence of noise

Phase diffusion

We now quantify the effects of phase diffusion on the MSEP. Figure 5.7 shows the MSEP as a function of σ^2 for different values of k. Note that the use of a PACS improves the system performance compared to the use of a coherent state ($k = 0$). It can be observed that, for small σ, MSEP with phase diffusion approaches to that without phase diffusion. It can also be observed that, for large σ, the MSEP with the optimal receiver approaches the SEP with a counting receiver as the off-diagonal terms vanish. Therefore, in the presence of a strong phase diffusion, the counting receiver is asymptotically optimal. This can be attributed to the fact that the off-diagonal terms in the Fock representation vanish as the diffusion parameter increases.

Photon loss

We now quantify the effects of photon loss on the MSEP.Figure 5.8 shows the MSEP as a function of η for different values of k. Note that the use of a PACS improves

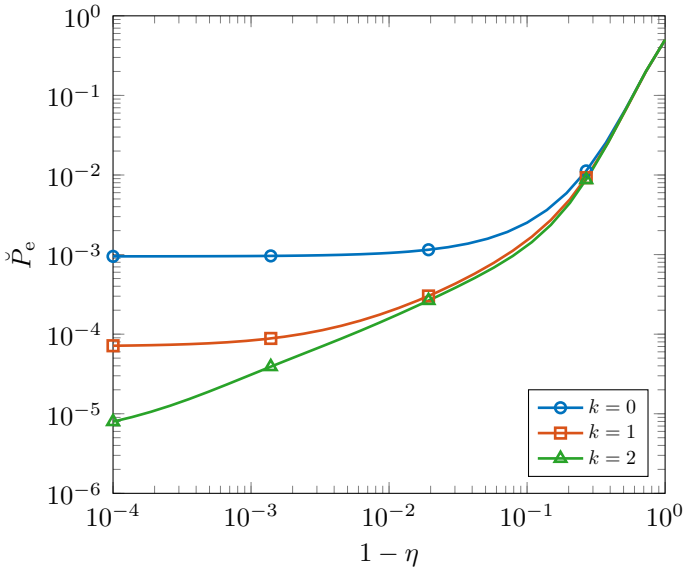


Figure 5.8: MSEP of a QOOK system using a PACS affected by photon loss as a function of η, with $n_{\mathrm{p}} = 6$, $\bar{n} = 10^{-2}$, and $p_0 = p_1 = 1/2$.

the QSD performance compared to the use of a coherent state ($k = 0$), especially for high η. Note also that, in the high-loss regime (i.e., when $\eta \approx 0$), MSEP with a PACS approaches to that with a coherent state for all k. Therefore, PACSs are particularly valuable in situations when the loss is low. This can be attributed to the fact that the quantum state loses its non-classical properties rapidly as η decreases [164–166].

5.3 Quantum pulse position modulation with non-Gaussian states

This section defines and characterizes a QPPM system with a PASS. The use of a PASS in QPPM communication systems can reduce the SEP with respect to the use of squeezed states and coherent states, as shown in the following.

5.3.1 System model

The quantum constellation of an M-QPPM using a PASS is given by (5.2) with $\boldsymbol{\Xi}^{(1)} = \boldsymbol{\Xi}(\mu, \zeta, k)$, where $\boldsymbol{\Xi}(\mu, \zeta, k)$ is a PASS as defined in the following, and $\boldsymbol{\Xi}^{(0)} = \boldsymbol{\Xi}_{\mathrm{th}}$.

Recall that, the photon-addition operation on a quantum state $\boldsymbol{\Xi}$ produces a new state $\boldsymbol{\Xi}_+$ given by

$$\boldsymbol{\Xi}_+ = \frac{\boldsymbol{A}^\dagger \boldsymbol{\Xi} \boldsymbol{A}}{\mathrm{tr}\{\boldsymbol{A}^\dagger \boldsymbol{\Xi} \boldsymbol{A}\}}.$$

If $\boldsymbol{\Xi}$ is a squeezed state affected by thermal noise [101], then the corresponding photon-added state $\boldsymbol{\Xi}_+$ is referred to as a noisy PASS. Therefore, a noisy PASS is defined as

$$\boldsymbol{\Xi}(\mu,\zeta,k)=\frac{(\boldsymbol{A}^\dagger)^k\boldsymbol{D}_\mu\boldsymbol{S}_\zeta\boldsymbol{\Xi}\boldsymbol{S}_\zeta^\dagger\boldsymbol{D}_\mu^\dagger\boldsymbol{A}^k}{N_+^{(k)}} \tag{5.15}$$

where $k\in\mathbb{N}$ represents the number of addition operations, $\boldsymbol{\Xi}_{\rm th}$ is a thermal state defined in (2.33), and $N_+^{(k)}=\mathrm{tr}\{(\boldsymbol{A}^\dagger)^k\boldsymbol{D}_\mu\boldsymbol{S}_\zeta\boldsymbol{\Xi}_{\rm th}\boldsymbol{S}_\zeta^\dagger\boldsymbol{D}_\mu^\dagger\boldsymbol{A}^k\}$ is the normalization constant.

Note that, in the case of no photon addition (i.e., $k=0$), (5.15) defines a noisy squeezed state as in (2.82). Note also that, in absence of squeezing (i.e., $r=0$), (5.15) defines a noisy PACS as in (3.9). Finally, when both $k=0$ and $r=0$, (5.15) defines a noisy coherent state as in (2.73). This definition allows to study a more general case with respect to the QOOK of the previous section.

Note that the characterization of an M-QPPM system using a PASS depends on the displacement parameter $\mu\in\mathbb{C}$, the squeezing parameter $\zeta\in\mathbb{C}$, and the number of addition operations $k\in\mathbb{N}$. The SEP of such quantum communication system depends on the strategy employed for the design of the receiver.

5.3.2 Performance evaluation in absence of noise

Performance evaluation with optimal receiver

Consider a 2-QPPM system with a PASS according to Sec. 5.1.1, i.e., $\boldsymbol{\Xi}^{(1)}=\boldsymbol{\Xi}(\mu,\zeta,k)$ and $\boldsymbol{\Xi}^{(0)}=\boldsymbol{\Xi}_{\rm th}$. The states of the quantum constellation (5.2) are thus given by $\boldsymbol{\Xi}_0=\boldsymbol{\Xi}(\mu,\zeta,k)\otimes\boldsymbol{\Xi}_{\rm th}$, and $\boldsymbol{\Xi}_1=\boldsymbol{\Xi}_{\rm th}\otimes\boldsymbol{\Xi}(\mu,\zeta,k)$. The MSEP for this binary system is determined according to the Helstrom bound (4.7) and depends on $\|\boldsymbol{\Delta}\|_1$, with $\boldsymbol{\Delta}=p_1\boldsymbol{\Upsilon}_1-p_0\boldsymbol{\Upsilon}_0$. However, in this case, the eigenvalues of the operator $\boldsymbol{\Delta}$ have no closed form expression and thus a tractable approximation of $\boldsymbol{\Delta}$ is needed to compute the MSEP. The operator $\boldsymbol{\Delta}$ can be approximated with a finite dimensional operator $\tilde{\boldsymbol{\Delta}}_N$ defined as in [5]. Here, the minimum symbol error probability is approximated using $\|\boldsymbol{\Delta}\|_1\simeq\|\tilde{\boldsymbol{\Delta}}_{30}\|_1$.

Performance evaluation with counting receiver

The performance of a QPPM system using a PASS and employing a counting receiver can be determined in a closed form as given in the following.

Proposition 5.3.1. The probability of a correct detection for an M-QPPM system with equiprobable symbols ($p_i=1/M$, for $i=0,1,...,M-1$) using a PASS, i.e.,

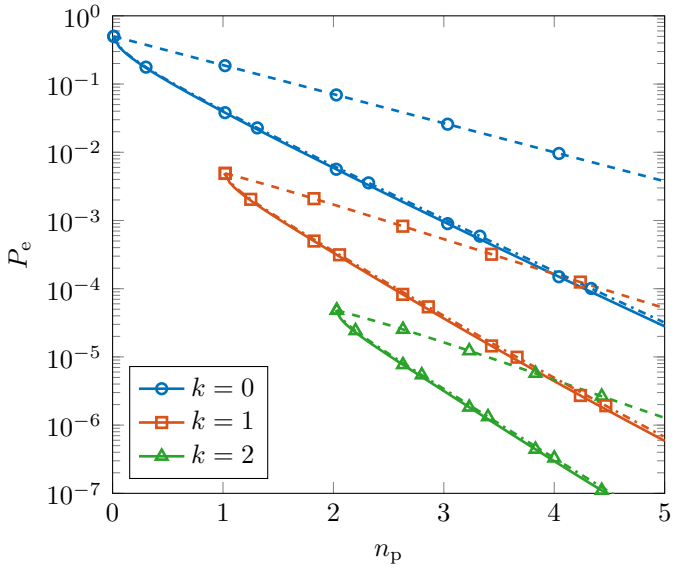


Figure 5.9: Error probability of 2-QPPM systems for SEP receiver (solid line), SRM receiver (dash dotted line), and counting receiver (dashed line) as a function of n_p and $\bar{n} = 10^{-2}$.

$\boldsymbol{\Xi}^{(1)} = \boldsymbol{\Xi}(\mu, \zeta, k)$, is given by

$$P_c = \frac{R}{M(1-v)v^k N_+^{(k)}} \sum_{h=1}^{M} (-1)^h \binom{M}{h} \frac{(v^h-1)v^{kh}}{(1-\tilde{A}v^{h-1})^{k+1}} G\Big(\frac{|\tilde{B}|v^{h-1}}{1-\tilde{A}v^{h-1}}, \frac{\tilde{C}}{\sqrt{2\tilde{B}}}; k\Big) \quad (5.16)$$

where R, $\tilde{A}$, $\tilde{B}$, and $\tilde{C}$ are given by (4.4)-(4.7) of [101], respectively, $v = \bar{n}/(1+\bar{n})$, and

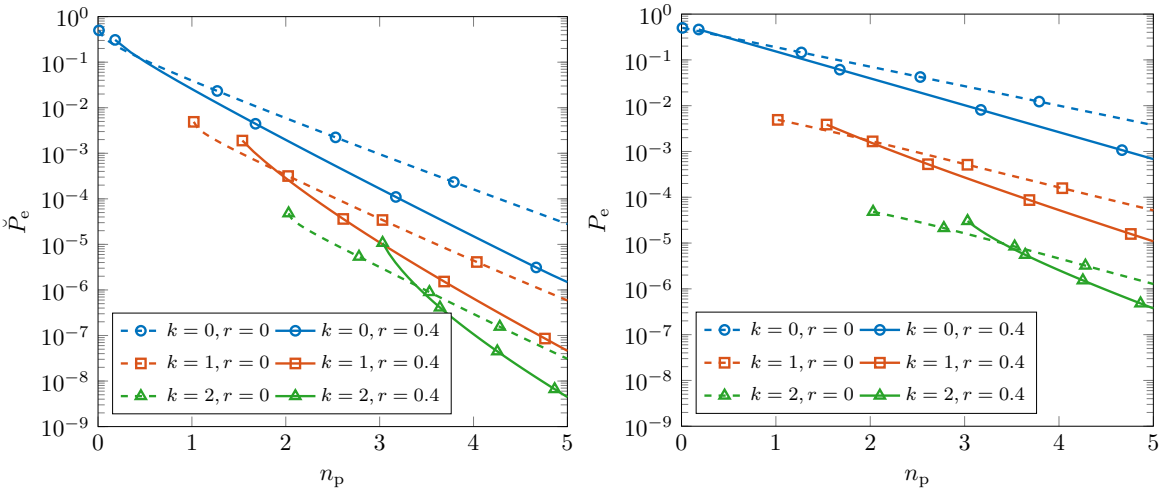
$$G(w, x; k) = \frac{\partial^k}{\partial w^k}\Big[\frac{w^k}{\sqrt{1-w^2}} \exp\Big\{\frac{2|x|^2 w - 2x_r^2 w^2}{1-w^2}\Big\}\Big].$$

Proof. See Section 5.4.1. □

The expression for the probability of a correct detection can be further simplified in the absence of squeezing ($r = 0$) as given in the following.

Proposition 5.3.2. The probability of a correct detection for an M-QPPM system with equiprobable symbols ($p_i = 1/M$, for $i = 0, 1, ..., M-1$) using a PACS, i.e., $\boldsymbol{\Xi}^{(1)} = \boldsymbol{\Xi}(\mu, \zeta, k)$, is given by

$$P_c = \Big[\frac{1-v}{v}\Big]^k \frac{e^{-(1-v)|\mu|^2}}{ML_k(-|\mu|^2(1-v))} \sum_{r=1}^{M} (-1)^r \binom{M}{r} (v^r - 1)\, H\Big(-\frac{(1-v)^2|\mu|^2}{v}, v^r; k\Big) \quad (5.17)$$



(a) Optimal receiver (quantum).

(b) Counting receiver (classical).

Figure 5.10: Performance of 2-QPPM as a function of n_p, with $\bar{n} = 10^{-2}$ and $p_0 = p_1 = 1/2$.

where $v = \bar{n}/(1+\bar{n})$, and

$$H(x, z; k) = \frac{z^k}{k!} \frac{\partial^k}{\partial z^k} \left[\frac{z^k}{1-z} \exp\left\{ -\frac{xz}{1-z} \right\} \right] . \tag{5.18}$$

Proof. See Section 5.4.2. □

Figure 5.9 shows the error probability P_e for a 2-QPPM as a function of n_p, for different receivers and values of k. Notice that the use of PACSs improves the performance of the QPPM system with respect to coherent states ($k = 0$). Notice also that, the performance of the SRM receiver is essentially the same of the SEP. This can be attributed to the fact that the noise parameter is very small and therefore, the SRM is a good approximation to the SEP [45]. For this reason, the performance of the SRM will not be considered anymore.

Figure 5.10a shows the error probability for a 2-QPPM system with the optimal receiver as a function of the mean number n_p of photons in $\boldsymbol{\Xi}^{(1)}$, for different values of k and r. Note that, for a fixed amount of squeezing r, the use of a PASS improves the performance of the optimal receiver compared to the case of squeezed state ($k = 0$) with same n_p and r. Note also that, as n_p increases, the use of a PASS improves the performance of the optimal receiver with respect to the use of a PACS ($r = 0$) with the same n_p and k.

Figure 5.10b shows the error probability for a 2-QPPM system with the counting receiver as a function of the mean number n_p of photons in $\boldsymbol{\Xi}^{(1)}$, for different values of k and r. In comparison to Figure 5.10a, it can be observed that the error probability

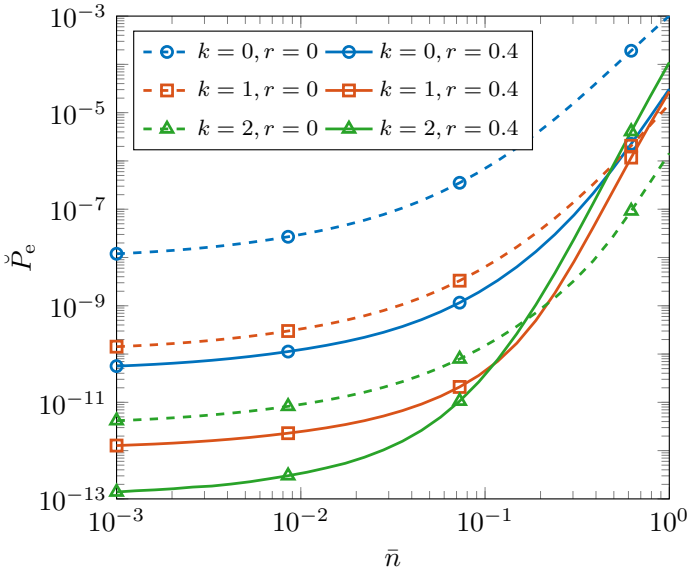


Figure 5.11: MSEP for a 2-QPPM system with the optimal receiver as a function of $\bar{n}$, with $n_\mathrm{p} = 9$, and $p_0 = p_1 = 1/2$.

with the counting receiver is higher than the error probability with the optimal receiver, as expected. Note that the use of a PASS instead of a squeezed state improves the performance of the system even with a sub-optimal receiver. Note also that the use of squeezing is advantageous particularly for sufficiently high values of n_p even with the counting receiver.

Figure 5.11 shows the MSEP for a 2-QPPM system with the optimal receiver as a function of the mean number $\bar{n}$ of thermal photons, for different values of k and r, and $n_\mathrm{p} = 9$. Note that the use of a PASS improves the performance of the MSEP receiver compared to the use of a squeezed state with the same squeezing parameter r, especially for small $\bar{n}$. Note also that, for sufficiently small n_p, the use of a PASS improves the performance of the optimal receiver compared to the use of a PACS.

5.3.3 Performance evaluation in presence of noise

Finally, the impact of decoherence in the quantum channel on the system performance is evaluated. Figure 5.12 shows the error probability for a 2-QPPM system with the optimal receiver as a function of the decoherence parameter σ^2, for different values of k, and $n_\mathrm{p} = 4$. Note that the performance of the optimal receiver approaches that of the counting receiver as σ^2 increases. This can be attributed to the fact that the state loses its quantum phase as the noise parameter increases.

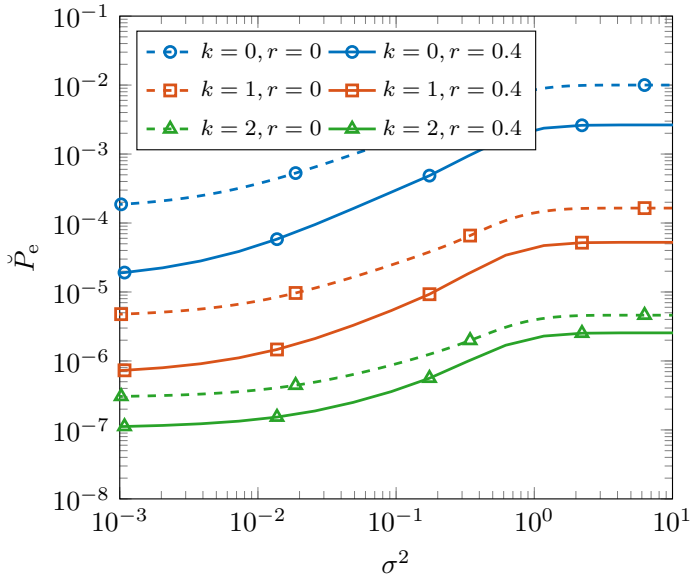


Figure 5.12: Performance of 2-QPPM with optimal receiver as a function of σ^2, with $n_p = 4$, $\bar{n} = 10^{-2}$, and $p_0 = p_1 = 1/2$.

5.3.4 Analysis of state preparation efficiency

Photon-added states are typically prepared by means of a conditional preparation technique [57]. This technique has been used to generate different classes of photon-added states, but is extremely inefficient and slow. Therefore, it is important to compare different quantum communication systems by taking into account the efficiency of the preparation on the effective speed of the system. Denote with $R_M(n_p, \zeta; k)$ the transmission rate for an M-QPPM system, as described in Sec. 5.1.1, for which $R_M(n_p, 0; 0)$ denotes the transmission rate of a M-QPPM system using coherent states [44]. Following the approach in [7], the performance gain $G_M(\zeta, k) = R_M(n_p, \zeta; k)/R_M(n_p, 0; 0)$ is considered to compare the two systems. For an M-QPPM using a PASS, the performance gain is given by

$$G_M(\zeta, k) = \frac{C_M(n_p, \zeta; k)}{C_M(n_p, 0; 0)} \frac{F_k(\zeta) + (M-1)F_0F_k(\zeta)}{1 + (M-1)F_0F_k(\zeta)} \tag{5.19}$$

where F_0 is the ratio between the generation rate of a coherent state and that of a thermal state, $F_k(\zeta)$ is the ratio between the generation rate of a PASS $\boldsymbol{\Xi}(\mu, \zeta, k)$ and that of a coherent state, and $C_M(n_p, \zeta; k)$ is the Shannon capacity of the system. The capacity of the system with a counting receiver is [167]

$$C_M(n_p, \zeta; k) = \log_2(M) - h_2(P_e) - P_e \log_2(M-1) \tag{5.20}$$

M	$F_1 = 1$		$F_1 = 10^{-1}$		$F_1 = 10^{-2}$		$F_1 = 10^{-3}$	
	$r = 0.4$	$r = 0.0$	$r = 0.4$	$r = 0.0$	$r = 0.4$	$r = 0.0$	$r = 0.4$	$r = 0.0$
2	1.560	1.558	0.284	0.283	0.031	0.030	0.003	0.003
16	1.339	1.333	0.857	0.853	0.186	0.185	0.021	0.021
128	1.243	1.220	1.162	1.140	0.701	0.688	0.141	0.138
1024	1.190	1.149	1.179	1.139	1.084	1.048	0.602	0.581

Table 5.1: Performance gain $G_M(\zeta, 1)$ of an M-QPPM system using a PASS with respect to a M-QPPM system using coherent states: counting receiver, $n_{\mathrm{p}} = 2$, $\bar{n} = 10^{-2}$, and $F_0 = 1$.

where $h_2(x) = -x\log_2(x) - (1-x)\log_2(1-x)$ is the binary entropy function and $P_{\mathrm{e}} = 1 - P_{\mathrm{c}}$ with P_{c} given by Eq. (5.16). Table 5.1 shows the gain $G_M(\zeta, 1)$ as function of M, for different values of the squeezing parameter ζ and generation rates ratio F_1. Note that the presence of squeezing increases the gain G_1 with respect to the absence of squeezing. Note also that, when the ratio F_1 is low, the gain increases with M. This can be attributed to the fact that preparation inefficiency is compensated by the constellation size.

5.4 Proof of the Results

5.4.1 Proof of Proposition 5.3.1

The proof of the proposition requires the following Lemma.

Lemma 5.4.1. For $k \in \mathbb{N}$, $x, w \in \mathbb{C}$, it is

$$\sum_{n=0}^{+\infty} \frac{(n+k)!}{(n!)^2} \Big(\frac{w}{2}\Big)^n H_n(x) H_n(x^*) = G(w, x; k) \tag{5.21}$$

where

$$G(w, x; k) = \frac{\partial^k}{\partial w^k} \Big[\frac{w^k}{\sqrt{1-w^2}} \exp\Big\{ \frac{2|x|^2 w - 2x_{\mathrm{r}}^2 w^2}{1-w^2} \Big\} \Big] .$$

Proof. Notice that the left-hand side of (5.21) can be written as

$$2^k \frac{\partial^k}{\partial w^k} \left[\Big(\frac{w}{2}\Big)^k \sum_{n=0}^{+\infty} \frac{1}{q!} H_n(x) H_n(x^*) \Big(\frac{w}{2}\Big)^n \right] . \tag{5.22}$$

Then, (5.21) follows by using Mehler's formula [168] in (5.22). □

Recall that, the probability for a correct dectection is given by Eq. (5.14)

$$P_{\rm c} = \frac{1}{M(1-v)}\,\mathbb{E}_{\mathsf{n}}\Big\{\sum_{h=1}^{M}(-1)^h\binom{M}{h}(v^h-1)v^{\mathsf{n}(h-1)}\Big\}$$

where the expected value is taken over to the number of photons n in the state $\boldsymbol{\Xi}^{(1)}$. Note that the probability of a correct detection depends on the probability generating function of n, $\mathbb{E}_{\mathsf{n}}\{z^{\mathsf{n}}\} = \sum_{n=0}^{+\infty} P_n z^n$, with $z = v^{h-1}$, where $P_n = \mathbb{P}\{\mathsf{n}=n\} = \langle n|\,\boldsymbol{\Xi}^{(1)}\,|n\rangle$. Therefore, by using the Fock representation of a noisy squeezed state [101], and after some algebra we obtain

$$\mathbb{E}_{\mathsf{n}}\{z^{\mathsf{n}}\} = \frac{R}{N^{(k)}(\mu,\zeta)}\sum_{n=k}^{+\infty}\sum_{q=0}^{n-k}\frac{n!z^n\tilde{A}^{n-k}}{(n-k)!q!}\binom{n-k}{q}\Big(\frac{|\tilde{B}|}{2\tilde{A}}\Big)^q H_q(x)H_q(x^*) \tag{5.23}$$

where R, $\tilde{A}$, $\tilde{B}$ and $\tilde{C}$ are given by (4.4)-(4.7) of [101], respectively. By changing the order of the summations, the (5.23) results in

$$\mathbb{E}_{\mathsf{n}}\{z^{\mathsf{n}}\} = \frac{R}{N^{(k)}(\mu,\zeta)}\sum_{q=0}^{+\infty}\frac{1}{q!}\Big(\frac{|\tilde{B}|}{2\tilde{A}}\Big)^q H_q(x)H_q(x^*)\sum_{n=q+k}^{+\infty}\frac{n!z^n\tilde{A}^{n-k}}{(n-k)!}\binom{n-k}{q}. \tag{5.24}$$

Recall that, for $y\in\mathbb{C}$, the following identity holds

$$\sum_{n=h}^{+\infty}\binom{n}{h}\frac{(n+k)!}{n!}y^n = \frac{(h+k)!}{h!(1-y)^{k+1}}\Big(\frac{y}{1-y}\Big)^h. \tag{5.25}$$

Using (5.25), the (5.24) can be written as

$$\mathbb{E}_{\mathsf{n}}\{z^{\mathsf{n}}\} = \frac{Rz^k}{N^{(k)}(\mu,\zeta)(1-\tilde{A}z)^{k+1}}\sum_{q=0}^{+\infty}\frac{(q+k)!}{(q!)^2}\Big[\frac{|\tilde{B}|z}{2(1-\tilde{A}z)}\Big]^q H_q(x)H_q(x^*)\,. \tag{5.26}$$

From (5.21), (5.26) with $z=v^{r-1}$, and (5.14), the (5.16) is obtained. □

5.4.2 Proof of Proposition 5.3.2

The proof of the proposition requires the following Lemma.

Lemma 5.4.2. For $k\in\mathbb{N}$ and $|z|<1$, it is

$$\sum_{n=k}^{\infty}\binom{n}{k}L_{n-k}(x)z^n = \frac{z^k}{k!}\frac{\partial^k}{\partial z^k}\left[G(x,z)z^k\right] = H(x,z;k) \tag{5.27}$$

where

$$G(x,z)=\frac{1}{1-z}\exp\left\{-\frac{xz}{1-z}\right\}.$$

Proof. Consider the generating function of the Laguerre polynomials [168], which can be equivalently written as

$$\sum_{n=k}^{\infty}L_{n-k}(x)z^n=\frac{z^k}{1-z}\exp\left\{-\frac{xz}{1-z}\right\}. \tag{5.28}$$

Relation (5.27) follows from taking the k-th derivative on both sides of (5.28). □

Recall that, the probability for a correct dectection is given by Eq. (5.14)

$$P_{\mathrm{c}}=\frac{1}{M(1-v)}\,\mathbb{E}_{\mathsf{n}}\Big\{\sum_{h=1}^{M}(-1)^h\binom{M}{h}(v^h-1)v^{\mathsf{n}(h-1)}\Big\}$$

where the expected value is taken over to the number of photons n in the state $\boldsymbol{\Xi}^{(1)}$. Note that the probability of a correct detection depends on the probability generating function of n, $\mathbb{E}_{\mathsf{n}}\{z^{\mathsf{n}}\}=\sum_{n=0}^{+\infty}P_nz^n$, with $z=v^{h-1}$, where $P_n=\mathbb{P}\{\mathsf{n}=n\}=\langle n|\,\boldsymbol{\Xi}^{(1)}\,|n\rangle$. Therefore, by using the Fock representation (3.13) of a noisy PACSs , and after some algebra we obtain

$$\mathbb{E}_{\mathsf{n}}\{z^{\mathsf{n}}\}=\frac{(1-v)^{k+1}e^{-(1-v)|\mu|^2}}{L_k(-|\mu|^2(1-v))v^k}H\Big(-\frac{(1-v)^2|\mu|^2}{v},vz;k\Big).$$

Equation (5.17) follows by applying this expression into Equation (5.14) with $z=v^{h-1}$. □

Chapter 6

Quantum key distribution networks

Quantum key distribution is a technology that exploits the peculiarity of quantum mechanics to allow the exchange of cryptographically secure keys between two remote parties [63–65]. It is one of the most mature quantum technologies, with different commercial implementations available on the market. However, the distribution of secure keys across long distances is still a challenge with current technologies, due to noise and attenuations in quantum channels [64]. The most promising techniques for long distance QKD involve the usage of low attenuation fibers [66–68] for metropolitan distances and LEO satellites [69–71] for long-range communications.

The advent of quantum networks will be beneficial for a global diffusion of QKD protocols. Indeed, the use of a quantum network allows to break a long-distance noisy quantum communication into shorter-distance point to point communications. Moreover, the network structure allows the interconnected nodes to exchange secret keys reliably and robustly. However, one of the main challenges is related to the no-cloning Theorem, which states that an unknown quantum system can not be cloned [72]. On one side, this Theorem is beneficial to guarantee information-theoretical secure communications, but on the other side, making it more difficult to apply classical solutions.

A possible enabler for the construction of a quantum network are the quantum repeaters [169]. Such repeaters are specifically designed to regenerate a quantum signal, without perturbing it, by exploiting different kind of quantum effects such as entanglement swapping and entanglement distillation [170, 171]. In this way, two end parties may be connected with a chain of quantum repeaters, which will allow the parties themselves to establish a secure key without requiring the intermediate nodes to be trusted. In the future, quantum repeaters may be used as the fundamental building block for the quantum Internet [22, 23]. As an alternative in the short-term, different protocols have been proposed and implemented to overcome these limitations by

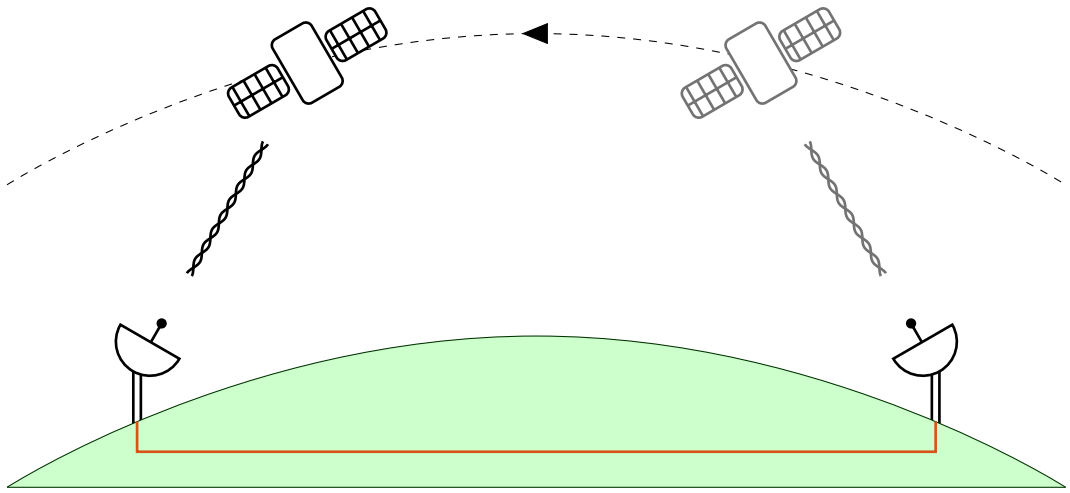


Figure 6.1: Illustration of a simple QKD network with a relay operating in an intermittent availability scenario. In this example, the two end nodes are allowed to exchange quantum information by relying on a trusted LEO satellite, which is visible to one end node at time and only for a short period of time during the day. Conversely, classical information can be exchanged via the classical internet even if the relay is not visible.

relying on the trustiness of the intermediate nodes [64, 67, 68, 71, 172, 173].

Independently from the implementation, the QKD may work in a complex scenario. For example, it may happen that one or more of the (trusted or not) relays are not always available to their neighbours, as in the case of LEO satellites. This is the case of the recent satellite-relayed QKD network established through the Micius satellite [71]. In this scenario (see Figure 6.1), the design of a QKD protocol is more subtle, and it should take into account these limitations to improve the overall secret key throughput of the network, i.e., the total amount of exchanged secret key bits in the time frame during which the relay is visible to the end nodes.

This thesis envisions the possibility to use properly tuned QKD protocols to improve the throughput of QKD networks in the intermittent-relay scenario. In particular, it is shown that under certain conditions, apparently slower QKD protocols may perform better than state-of-the-art protocols, when they operate in an intermittent-relay scenario. The goal is to establish new techniques for performance evaluation of trusted-relay intermittent QKD networks. The key contributions are as follows:

- analysis of secret key throughput for QKD networks with intermittent trusted relays; and
- definition of a new performance metric for QKD networks with intermittent trusted relays.

6.1 Quantum key distribution

The security of classical public-key cryptosystems relies on the computational hardness of some algorithms, and therefore they are not based information theoretically secure [174]. In an ideal situation, with an infinite amount of processing power, and with the capability to intercept the communications between the legitimate users, an evil agent (also referred to as eavesdropper) would be able to intercept and decipher the messages exchanged by the users, without leaving any trace of his actions. This is a well known problem in modern cryptography and it is considered an Achille's heel for the future of secure communications. The no-cloning theorem, together with the Heisenberg uncertainty principle, turns out to be a fundamental tool for cryptographic applications, which can overcome the limitation of classical cryptographic systems.

6.1.1 QKD protocols

QKD protocols can be divided into two categories: (i) prepare-and-measure protocols which are essentially based on the superposition and undeterminancy principle; and (ii) entanglement-based protocols which are based on the properties of bipartite entagled systems. A wide class of these QKD protocols can be described as follows [175].

1. **Quantum communication:** The two legitimate parties Alice and Bob use a quantum channel to share a set of N bipartite quantum states among them.

2. **Parameter estimation (PE):** Alice and Bob sacrifice a subset of the m subsystems to estimate the error rate ϵ due to the presence of impairments or eavesdroppers in the quantum channel. If the error rate ϵ is too high, which may be a signature for the presence of an eavesdropper, then the two parties may agree to abort the protocol. Otherwise, the protocol proceeds by throwing away the systems used for PE.

3. **Measurement:** If the protocol has not been aborted, the two parties apply a local quantum measurement on their remaining subsystems to obtain a pair of raw keys (i.e., a classical string of bits) of length $N - m$.

4. **Block-wise processing:** Alice and Bob apply a classical post-processing procedure to increase their correlation, by sacrifying a subset of their classical bits, to obtain a set n of bits.

5. **Information reconciliation (IR):** To counteract the effect of the noise in the quantum channel, Alice and Bob share some error correcting information for

the set of n classical bits. In state of the art implementations [67, 68, 71, 176], low-density parity-check codes (LDPC) codes are used to correct errors.

6. **Privacy amplification (PA):** To reduce the information that may have been acquired by a non-legitimate third party in the previous step of the protocol, the legitimate parties Alice and Bob apply a classical protocol to transform their strings of n bits into secret keys of length l. In general, Alice and Bob apply a $l \times k$ Toeplitz matrix $\boldsymbol{T}$ as a 2-universal hash function [177]. If $\boldsymbol{r}$ is the string of bits after IR, then $\boldsymbol{k} = \boldsymbol{T}\boldsymbol{r}$ is the string of secure key bits after PA.

The secret key rate, which quantifies the efficiency of a QKD protocol to generate a secret key is defined as in the following.

Definition 6.1.1. The key rate C_r of a QKD protocol is defined as the ratio between the number l of secret key bits obtained at the end of the protocol, and the number n of bits used for the computation of the key, i.e.,

$$C_r = \frac{l}{n}\,.$$

6.1.2 Security of a QKD protocol

Consider a QKD protocol with two legitimate parties, Alice and Bob, together with a malicious attacker, referred to as Eve. The peculiarities of QKD protocols is the possibility to prove that they are not based on the complexity of a mathematical problem, but they use the peculiarities of quantum mechanics to satisfy an information-theoretical security criterion.

The security analysis for a QKD protocol is performed by assuming that the quantum channel connecting Alice and Bob is under full control of Eve. This is a pessimistic assumption, but it allows to derive an upper bound on the performance of the QKD protocol. The strongest security criterion is formulated as follows [175, 178].

Let $\boldsymbol{\Xi}_{ABE} \in \mathcal{H}_A^{\otimes n} \otimes \mathcal{H}_B^{\otimes n} \otimes \mathcal{H}_E$ be the quantum state shared by Alice, Bob, and Eve at the end of protocol, provided that the protocol has not been aborted. Then, the protocol is said to be ε-secure

$$\frac{1}{2}\|\boldsymbol{\Xi}_{ABE} - \boldsymbol{\Xi}_{UU} \otimes \boldsymbol{\Xi}_E\|_1 \leq \varepsilon$$

where $\rho_{UU} = 1/|\mathcal{S}| \sum_{s\in\mathcal{S}} |s\rangle\langle s|$ is the fully mixed state in $\mathcal{H}_A^{\otimes n} \otimes \mathcal{H}_B^{\otimes n}$, $\mathcal{S}$ is the set of possible values for the key.

Notice that, in the asymptotic limit $n \to \infty$ the security definition stated above can be applied for every $\varepsilon > 0$. Therefore, the definition is equivalent to say that a

protocol is secure if the state shared between Alice and Bob (i.e., the key) at the end of the protocol is indistinguishable from the fully mixed state. In other words, this means that, if the protocol succeed, the two legitimate parties are ensured that, independently from the attack chosen by eavesdropper, no information is leaked. Indeed, it can be proven that a secure protocol according to the above definition, which produces a secret key K, satisfies the following inequality for every $\epsilon > 0$

$$\max_{W} I(K;W) \leq \epsilon$$

where the maximum is taken with respect to over all possible measurements W of the eavesdropper, and $I(K;W)$ is the mutual information between K and W.

The security definition gives important restrictions on the performance of a QKD protocol. In particular, For every QKD protocol it is possible to prove that [175], in the asymptotic limit $n \to \infty$, the protocol is secure if and only if

$$C_r = \frac{l}{n} \leq C$$

where C is a constant that depends on the protocol and on the error rate, and it is referred to as the secret key rate. The secret key rate plays a role analogue to the channel capacity in classical information theory [179]: it measures the mean amount of secret key bits that can be generated from one raw key bit, i.e., the efficiency of the QKD protocol. In the following, it is assumed that the QKD protocols work ideally, i.e., $C_r = C$.

6.1.3 BB84 protocol

The first but still widely used QKD protocol is the Bennett and Brassard (1984) (BB84) [63]. The protocol is described as follows.

1. **Quantum communication:** Alice generates two random strings **a** and **b** of $N = 4n$ classical bits. The two strings are then used to prepare a string $|\psi\rangle$ of $4n$ qubits according to the BB84 rules [63], defined as follows.

$$|\psi\rangle = \bigotimes_{i=1}^{4n} |\phi_{a_i b_i}\rangle \tag{6.1}$$

where a_i denotes the information bit, b_i denotes the qubit basis used for prepare

the quantum bits, and $|\phi_{a_i b_i}\rangle$ is prepared according to the following

$$
\begin{aligned}
|\phi_{00}\rangle &= |0\rangle \\
|\phi_{10}\rangle &= |1\rangle \\
|\phi_{01}\rangle &= \frac{|0\rangle + |1\rangle}{\sqrt{2}} \\
|\phi_{11}\rangle &= \frac{|0\rangle - |1\rangle}{\sqrt{2}} \,.
\end{aligned}
$$

2. **Quantum measurement:** Bob measures the received qubits in a randomly chosen basis, to get a string of $4n$ bits. This does not require any communication.

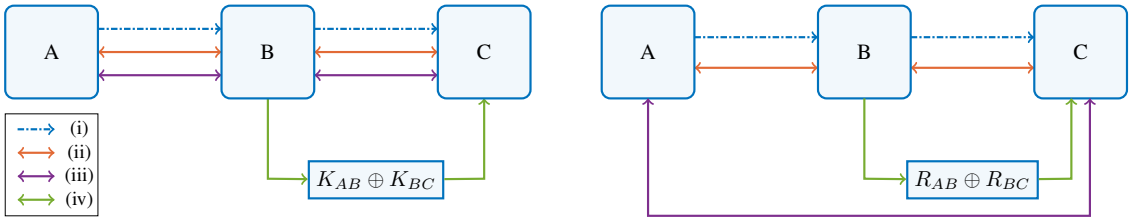
3. **Key sifting:** Alice and Bob publicly announce their choice of basis for each qubit, and they discard the qubits for which their choices differ. The expected number of remaining bits after sifting is $2n$. Since the choices are independent, the Shannon source coding theory [180] can be used to show that both parties have to publish $4n$ classical bits, for a total of $8n$ classical bits.

4. **PE:** Alice and Bob publicly compare a randomly chosen set of half of their remaining bits to guess the error rates ε_{b} and ε_{p} of the channel in the two bases, respectively. In a first approximation, Alice needs $2n$ qubits to tell Bob the set of bits to compare.[1] Then both parties announce the value of such bits, using n classical bits each one. Therefore, this step requires approximately $4n$ bits to be sent on the classical channel.

5. **IR**: Alice and Bob use a classical error-correcting code (CECC) to correct the errors of the quantum channel, as described in the previous section. Assuming that the classical channel is error-free, than Alice needs to send bob only some $n - k$ parity bits to let Bob produce an error-free string of $k < n$ classical bits. Assuming that the parity-check matrix is known in advance, this step requires Alice to send $n - k$ parity bits on the classical channel.

6. **PA**: Alice uses an $l \times k$ Toeplitz matrix $\boldsymbol{T}$ as a 2-universal hash function, with $l < k$, to eliminate the side information, as described in the previous section.The Toeplitz matrix is completely described by a binary vector of length $k + l - 1$, which is sent through the classical channel. The parameter l, which determines

[1] In theory, Alice can use a smaller amount of bits, given by $\log_2 \binom{2n}{n} \approx 2n - \log_2(\sqrt{\pi n})$, which follows from Stirling's approximation. However, $\log_2 \binom{2n}{n} \approx 2n$ for large n.



(a) fully trusted relay (FTR) protocol.

(b) simplified trusted relay (STR) protocol.

Figure 6.2: Illustration of the two trusted-relay protocol architectures: (i) represents the exchange of quantum states over the quantum channel; (ii) indicates the presence of a classical communication to perform the sifting procedure; (iii) represents the post processing procedure; and (iv) points out the publication of trusted-relay information.

the secure key rate, depends on the information leaked during the error correction procedure. When l is sufficiently high, the amount of classical information emitted by Alice is approximately equal to $k + l$ (neglecting -1).

The secret key rate of the BB84 protocol is given by the Shor-Preskill formula [181]

$$C_{\text{BB84}} = \max\{1 - h_2(\varepsilon_{\text{b}}) - h_2(\varepsilon_{\text{p}}), 0\} \tag{6.2}$$

where $h_2(x) = -x \log_2(x) - (1 - x) \log_2(1 - x)$ is the binary entropy function. If the attack is symmetric in the two basis, i.e., $\varepsilon_{\text{b}} = \varepsilon_{\text{p}} = \varepsilon$, then

$$C_{\text{BB84}} = \max\{1 - 2h_2(\varepsilon), 0\}\,. \tag{6.3}$$

From (6.3) it follows that $C = 0$ for $\varepsilon > \tilde{\varepsilon} \approx 0.11$. Therefore, no secret key can be established between Alice and Bob if the error rate affects more than 11% of the control qubits.

6.2 QKD networks with trusted-relay

This section introduces two QKD protocols that can be used in a trusted-relay QKD network. To keep the concepts as simple as possible, consider a simple three-node network in which the two end parties Alice (A) and Charlie (C) want to agree on a secret key by relying on the trusted third party Bob (B). The topology of the network is showed in Figure 6.2.

6.2.1 Fully trusted-relay BB84

The most simple trusted-relay protocol, which has been proposed and used in almost all available QKD networks [67,68,71], uses the intermediate node as a full QKD relay.

In particular, Alice exchanges a secure key K_{AB} with Bob. Bob does the same with Charlie, by establishing a secure key K_{BC} with him. Then, Bob sends Charlie the key K_{AB} using K_{BC} as a one-time pad $K_{AB} \oplus K_{BC}$, which Charlie uses to reconstruct K_{AB}. In this sense, Bob acts as a complete relay between Alice and Charlie who now both know the key K_{AB}. Such protocol is referred to as fully trusted relay (FTR). This idea can be easily generalized to an arbitrary number of nodes. The pictorial representation of this protocol is reported in Figure 6.2a.

$$C_{\text{ftr}} = \max\{1 - 2h_2(\varepsilon), 0\}\,. \tag{6.4}$$

6.2.2 Simplified trusted-relay BB84

Let us now consider the STR protocol, proposed in [173]. The principal idea of this protocol is to demand the classical post-processing procedure to the end users, thus involving the trusted relay only in the quantum state distribution and sifting procedure. The protocol proceeds as follows:

1. Alice prepares a string of $4n$ quantum bits as in the BB84 protocol, and she sends it to Bob using the link $A - B$.

2. Bob measures the received qubits in a random basis. He then performs the sifting procedure to produce the raw key R_{AB}.

3. The steps 1 and 2 are repeated by Bob and Charlie on the link $B - C$ to produce the raw key R_{BC}.

4. Bob announces $P = R_{AB} \oplus R_{BC}$ and its role ends here. Charlie uses his raw key R_{BC} to recover Alice's raw key R_{AB}.

5. **End-to-end PE:** Alice and Charlie publicly determine the error rate for each basis combination, including the choice of Bob. If the error rate is too high, they abort the protocol.

6. **End-to-end IR and PA:** Alice and Charlie perform the usual information reconciliation and privacy amplification procedure to produce the secure key.

A pictorial representation of this protocol is shown in Figure 6.2b. In this case, the trusted relay is involved only in the quantum state preparation and in the sifting procedure; it is not concerned in the post-processing operations. This simplification comes at the expenses of the key rate, which, in this case, is given by [173]

$$C_{\text{str}} = \max\{1 - 2h_2\big(2\varepsilon(1-\varepsilon)\big), 0\}\,. \tag{6.5}$$

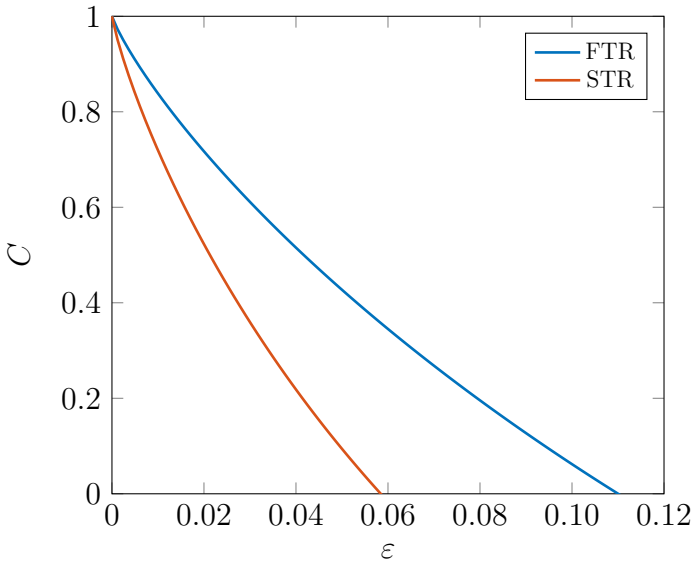


Figure 6.3: Secret key rate C of the FTR and the STR protcols as a function of the error rate ε.

6.2.3 Performance evaluation

If the network nodes are always available, the performance of a QKD protocol operating in an end-to-end link, as in the scenario depicted above, can be evaluated via the secret key rate, which quantifies the amount of secret key generated per channel use. Figure 6.3 shows the secret key rate for the FTR and STR protcols, given by Equations (6.4) and (6.5), as a function of the error rate ε. Note that, the secret key rate of the STR protocol is lower than the one of the FTR protocol. Therfore, according to this analysis, the STR protocol, despite being of simpler implementation, has worse performance than the FTR protocol.

6.3 QKD with intermittent trusted-relay

In the analysis of the previous section, the efficiency of a QKD protocol is evaluated in term of the secret key rate, i.e., the number of secret key bits per raw key bit. This rate is the most important figure of merit in the design of a QKD link, as it gives an estimate of the efficiency of the QKD system. However, in a QKD network, it may happen that one or more of the trusted relays are not always available to their neighbours, as in the case of LEO satellites. Moreover, the end nodes may be able to communicate between them using an existing communication network (e.g., Internet), even in the absence of the relay.

6.3.1 Scenario description

Consider the simple network introduced in the previous section and shown in Figure 6.1, and consider the relay to be operating intermittently. These conditions can be imposed by the assumptions (i)-(v) reported in the following.

(i) The trusted node B is visible to the end nodes only for a certain amount of time t_{v}, after which it remains hidden for a certain amount of time t_{i}, which is supposed to be much greater than t_{v} (e.g., LEO satellites). The time frame during which it is available to A may not overlap to the one of C;

(ii) the quantum transmission rate R_{q} and the classical transmission rate R_{c} are the same for each link, and they remain constant during the whole transmission;

(iii) the quantum channels are identical and independent one from the other;

(iv) the computation times are negligible;

(v) the error correction and privacy amplification procedures work at their theoretical limits, i.e., the effective key rate is equal to the theoretical one.

Note that the first two assumptions are reasonable, according to the experimental data obtained by recent studies with the Micius satellite [69–71]. Anyway, a time-dependent transmission rate does not affect the results of our analysis, as it can be assumed to be piecewise constant. The third assumption is reasonable too, especially if the communication between the source node and the destination node happens during disjoint time slices, as in Micius experiments. Finally, the last two assumptions seem to be optimistic as the computational time may not be negligible with respect to the time slice t_{v}. Furthermore, the IR and PA procedures cannot work at the theoretical limits. This does not affect our analysis since no protocols, except the FTR, rely on the intermediate relay for the post-processing phase. This would thus give us a pessimistic analysis.

6.3.2 Secret key throughput

Fully trusted relay protocol

The performance analysis is simple. Each of the two links runs a complete BB84 protocol during the time slice of length t_{v}. Thus, using the expressions of the previous section

$$t_{\mathrm{v}} = \frac{4n}{R_{\mathrm{q}}} + \frac{8n}{R_{\mathrm{c}}} + \frac{4n}{R_{\mathrm{c}}} + \frac{n-k}{R_{\mathrm{c}}} + \frac{k+l}{R_{\mathrm{c}}} = l\frac{4R_{\mathrm{c}} + (13+C)R_{\mathrm{q}}}{CR_{\mathrm{c}}R_{\mathrm{q}}}$$

where C is the key rate of the standard BB84 protocol, which is given by the well known expression [181]: $C = 1 - 2H_2(\varepsilon)$ where $H_2(x) = -x\log_2(x) - (1-x)\log_2(1-x)$ is the binary entropy function and ε is the error rate as measured in the IR phase. It follows that the amount of exchanged bits, for a single BB84 link during the time slice t_{v}, is given by

$$l = t_{\mathrm{v}}\frac{CR_{\mathrm{c}}R_{\mathrm{q}}}{4R_{\mathrm{c}} + (13+C)R_{\mathrm{q}}}\,.$$

However, to complete the key exchange, the trusted relay needs further classical communication to publish the one-time pad message $K_{AB} \oplus K_{BC}$. This happens just before the end of the second time slice (the one between Bob and Charlie). Therefore,

$$t_{\mathrm{p}} = 2t_{\mathrm{v}} = 2l\frac{4R_{\mathrm{c}} + (13+C)R_{\mathrm{q}}}{CR_{\mathrm{c}}R_{\mathrm{q}}} + \frac{l}{R_{\mathrm{c}}}$$

and

$$l_{\mathrm{ftr}} = \frac{1}{2}t_{\mathrm{p}}\frac{C_{\mathrm{ftr}}R_{\mathrm{c}}R_{\mathrm{q}}}{8R_{\mathrm{c}} + (26+3C_{\mathrm{ftr}})R_{\mathrm{q}}} \tag{6.6}$$

where $C_{\mathrm{ftr}} = C$. Notice that the term one half, which has been added in front of the previous expression, takes into account that the key K_{BC}, which has been exchanged between Bob and Charlie, is discarded after the end of the protocol. It is also worth noticing that, in some works [70], the quantum transmission rate R_{q} is implicitly replaced with the sifted transmission rate R_{s}. Anyway, it is possible to derive one from the other. Indeed, the amount of time needed for quantum state distribution and sifting is given by

$$t_{\mathrm{s}} = \frac{4n}{R_{\mathrm{q}}} + \frac{8n}{R_{\mathrm{c}}} = 2n\left[\frac{2R_{\mathrm{c}} + 4R_{\mathrm{q}}}{R_{\mathrm{c}}R_{\mathrm{q}}}\right]\,.$$

Since the number of bits after the sifting step is equal to $2n$, it follows that the sifted rate is given by

$$R_{\mathrm{s}} = \frac{R_{\mathrm{c}}R_{\mathrm{q}}}{2R_{\mathrm{c}} + 4R_{\mathrm{q}}}\,. \tag{6.7}$$

Simplified trusted relay protocol

In this protocol, the trusted relay is involved only in the quantum state preparation and in the sifting procedure; it is not concerned in the post-processing operations that are executed by the end nodes. This simplification comes at the expenses of the key

rate, as described in the previous section. Therefore, it is

$$t_{\mathrm{p}} = 2\left[\frac{4n}{R_{\mathrm{q}}} + \frac{8n}{R_{\mathrm{c}}}\right] + \frac{2n}{R_{\mathrm{c}}} = l\frac{8R_{\mathrm{c}} + 18R_{\mathrm{q}}}{R_{\mathrm{c}}R_{\mathrm{q}}C_{\mathrm{str}}}\,.$$

The last term in the first expression is due to the public announcement of the trusted relay. From this expression, it follows that

$$l_{\mathrm{str}} = \frac{1}{2}t_{\mathrm{p}}\frac{R_{\mathrm{c}}R_{\mathrm{q}}C_{\mathrm{str}}}{8R_{\mathrm{c}} + 18R_{\mathrm{q}}}\,. \tag{6.8}$$

The term one half has been added for the same reason explained in the previous section.

It is important to note that, according to the standard key-rate analysis, the STR protocol is less efficient than the FTR as $C_{\mathrm{str}} < C_{\mathrm{ftr}}$ for all the significant ε.

6.3.3 Performance evaluation

A performance evaluation of the two protocols presented in the previous section is now given. The FTR protocol is used as the reference protocol, since it represents the state of the art. We define the secret key throughput gain of a protocol p, with respect to the FTR protocol, as

$$G_{\mathrm{p}} = G_{\mathrm{p}}(R_{\mathrm{q}}, R_{\mathrm{c}}, \varepsilon) = \frac{l_{\mathrm{p}}}{l_{\mathrm{ftr}}}$$

where l_{p} represents the amount of bits exchanged in the time slice t_{v} using the protocol p. Since both l_{p} and l_{ftr} linearly depend on t_{v}, G_{p} is a function only of the communication rates R_{q} and R_{c}, and of the error rate of the channel. The throughput gain is a figure of merit in the intermittent-relay scenario. Indeed, if $G_{\mathrm{p}} > 1$, it means that the protocol p has a longer secure key (with respect to the FTR protocol) when the visibility time of the trusted relay is the same, and viceversa for $G_{\mathrm{p}} < 1$.

For the STR protocol, using expressions (6.6) and (6.8), it is

$$G_{\mathrm{str}} = \frac{C_{\mathrm{str}}}{C_{\mathrm{ftr}}}\frac{8 + (26 + 3C_{\mathrm{ftr}})R}{8 + 18R}$$

where we have implicitly defined the quantum-over-classical communication rate ratio parameter R as

$$R = \frac{R_{\mathrm{q}}}{R_{\mathrm{c}}}\,.$$

Note that G_{str} depends only on the parameter R and the error rate ε, i.e., $G_{\mathrm{str}} = G_{\mathrm{str}}(R, \varepsilon)$.

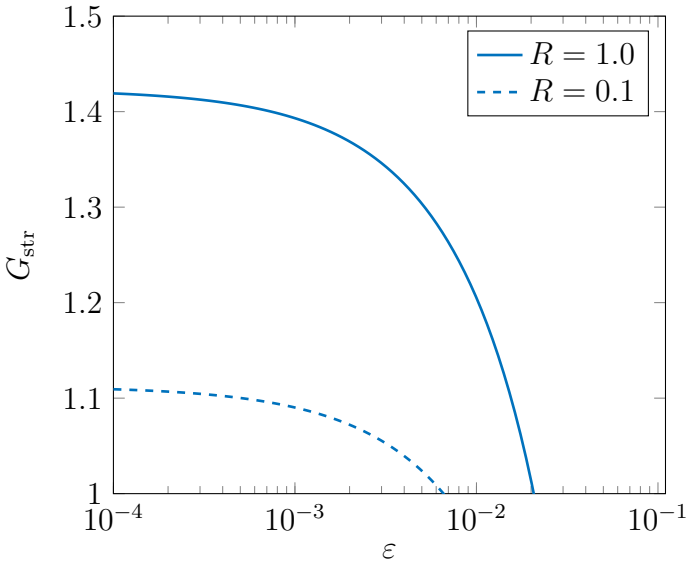


Figure 6.4: Throughput gain of the STR with respect to the FTR protocol as a function of the error rate e.

It is also possible, with similar calculations, to express the gain as a function of the sifted-over-classical communication rate

$$R' = \frac{R_{\text{s}}}{R_{\text{c}}}$$

where R_{s} is the equivalent sifted rate of the protocol, as in (6.7) for the FTR protocol. Using expression (6.7), we can derive the relation between R and R'

$$R' = \frac{R}{2 + 4R}\,.$$

Discussion

Figure 6.4 shows the throughput gain of the STR protocol as a function of the error rate in the channel ε, for different values of the parameter R. It can be observed that, at extremely low error rates, the gain given by the STR protocol can go over 40%, depending on the value of R. Notice that the throughput gain has no physical significance when the error rate ε is such that $C_{\text{ftr}}, C_{\text{str}} < 0$.

Comparing the protocols directly using the throughput gain seems to be hard, at least in principle, because the parameter R has to be fixed. To have a synthetic and more concise comparison, we introduced the parameter $\varepsilon_{\text{u}}(R)$ which is the unitary-gain error rate as a function of R, i.e., $G_{\text{str}}(R, \varepsilon_{\text{u}}(R)) = 1$. Since the function G_{str} is monotonically decreasing in ε, when R is fixed, the parameter ε_{u} discriminates two operating regions for the protocol: when $\varepsilon < \varepsilon_{\text{u}}$, using the STR protocol allows the

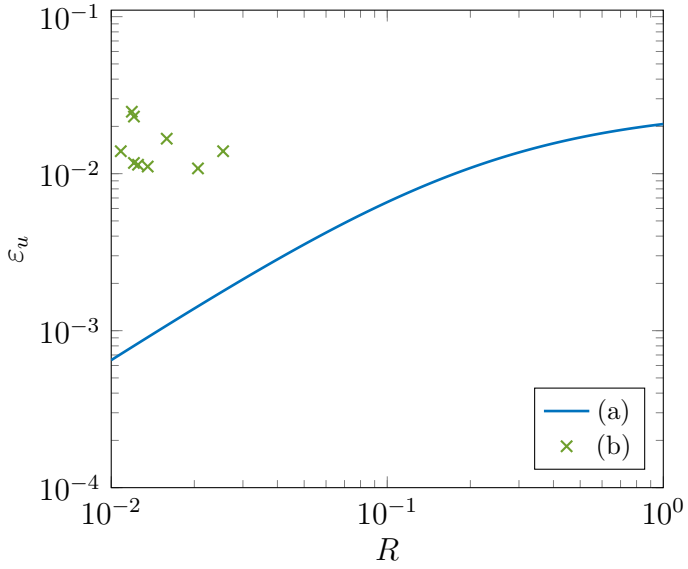


Figure 6.5: Error rate as a function of R: (a) theoretical unitary gain error rate of the STR protocol with respect to the FTR protocol; and (b) experimental mean values as in [70].

network to achieve a greater throughput with respect to the FTR protocol, otherwise the opposite is true.

Figure 6.5 shows the unitary gain error rate for the STR protocol as a function of the ratio R. It is interesting to note that the gain of the STR protocol has a smooth trend in R, and the unitary error-rate function divides the plane into two regions: the one under the curve is the advantageous region for the STR protocol, the other is the advantageous region for the FTR. This means that, under certain conditions on ε and R, the STR protocol is more efficient than FTR, even if it is slower according to a simple key rate analysis. In other words, the secret key rate is not the best figure of merit to analyze QKD system in this scenario. The crosses in the figure are explained hereafter.

Technological considerations

The theoretical study of the last section can be used to design a QKD network when the relay is available only for a limited amount of time. As a toy example, we perform a first analysis of trusted relay protocols on an existing infrastructure, using the experimental data obtained with a state of the art LEO satellite [70], which relies on the FTR protocol to perform relay assisted QKD [71]. In this case, the observed sifted key rate is in the range from 1 to 40 KHz, depending on the environmental conditions, and the classical communication speed is around 1 Mbps. The ratio R' is thus in

the order of 10^{-2}. The measured quantum bit error rates are in the order of 10^{-2}. The experimental data, obtained for different runs of the BB84 protocol using a LEO satellite [70], are Figure 6.5 crosses. This means that according to the above analysis, we can not improve the network throughput with the STR protocol by using current technologies. However, recall that in the assumptions of our analysis we have neglected the computational times needed to perform the relay operations, and the inefficiency of IR and PA operations. Generally, the computational resources of a lightweight satellite are very limited with respect to ground nodes. For this reason, our unitary-gain error curves may be interpreted as a lower bound for real systems, which can perform better than predicted by our analysis. This means that even if current technologies can not still reach the unitary gain error curve (delimiting the advantageous working region for the STR protocol) next generation technologies are very likely to do so in the near future.

Chapter 7

Conclusion

This thesis introduces new methodologies for the design and analysis of quantum systems and networks. In particular, the use of non-classical non-Gaussian states, such as photon-added coherent states (PACSs) and photon-added squeezed states (PASSs), is established for applications relying on quantum state discrimination (QSD). Moreover, a new framework for the characterization of quantum key distribution (QKD) networks in the presence of intermittent relaying is derived.

A characterization for PACSs affected by thermal noise in state preparation is derived in terms of Fock representation, Wigner W-function, Glauber–Sudarshan P-function, and Husimi–Kano Q-function. Then, a characterization of QSD with noisy PACSs is given in terms of discrimination error probability (DEP) for both optimal and sub-optimal quantum measurements. It is shown that the use of PACSs instead of coherent states can significantly reduce the error probability in QSD. These findings are then used for establishing the use of non-Gaussian states for quantum communication systems. In particular, the results on QSD with PACS are used to analyze and design quantum communication systems with quantum on-off keying (QOOK) and quantum pulse position modulation (QPPM) modulations with PACS and PASS. It is shown that the use of PACSs and PASSs is beneficial for the QSD performance and can significantly reduce the error probability with respect to the use of Gaussian states with the same energy, even when a classical receiver is used. The impact of thermal noise, phase diffusion, and photon loss on the system performance is also evaluated.

The characterization of QKD networks is also determined in the presence of intermittent relays such as low-Earth orbit satellites. In this scenario, the design and the analysis of a QKD protocol accounts for all the limitations and network's working conditions to maximize the performance of the network. A new metric for the analysis of QKD networks in presence of intermittent relaying, referred to as secret key throughput, is also introduced. It is shown that the conventional metric to quantify

the efficiency of a QKD protocol, i.e., the secret key rate, may not be accurate to analyze the network performance in the presence of limiting conditions. In particular, the performance of different QKD protocols are evaluated in a realistic scenario, showing that apparently slower protocols, provide an higher secret key throughput.

This thesis (i) establishes the use of non-classical non-Gaussian states for improving QSD, and (ii) develops a framework for design and analysis of QKD in networks with intermittent relays. The findings of this thesis pave the way for the analysis and the design of innovative quantum systems and networks relying on non-classical non-Gaussian states.

Appendix A

Wirtinger calculus

In the phase-space formulation of quantum mechanics it is useful to regard a function (e.g., the quasi-probability distribution) defined on $\mathbb{R}^2$ as a function defined on $\mathbb{C}$. In particular, it is possible to formally replace the two real variables x and y in the real-valued function $f(x, y)$ with one complex variable $z = x + \imath y$ so that $f(x, y)$ becomes a function of z, i.e., $f(x, y) = g(z)$. However, this formal substitution introduces some mathematical issues for the differential calculus due to the structure of the complex space. In particular, even if $f(x, y)$ is differentiable, the function $g(z)$ is differentiable in the complex domain if and only if the Cauchy-Riemann conditions hold [182].

The key idea of the Wirtinger calculus is to introduce a generalized complex derivative with respect to z (or z^*), that considers z^* (or z) as a constant. The theory behind this mathematical framework was initially developed by Wirtinger [183] and then rediscovered recently in the engineer literature [93–97, 184].

Definition A.0.1. Let $g(z) : \mathbb{C} \to \mathbb{C}$ be a complex function and let $\tilde{g}(z, w) : \mathbb{C}^2 \to \mathbb{C}$ be a complex function such that $\tilde{g}(z, z^*) = g(z)$. The Wirtinger derivatives of $g(z)$ are

$$\frac{\partial g(z)}{\partial z} \triangleq \frac{\partial \tilde{g}(z, w)}{\partial z}\bigg|_{w=z^*} \tag{A.1a}$$

$$\frac{\partial g(z)}{\partial z^*} \triangleq \frac{\partial \tilde{g}(z, w)}{\partial w}\bigg|_{w=z^*}. \tag{A.1b}$$

Remark 1. Notice that a complex valued function $g(z) : \mathbb{C} \to \mathbb{C}$ may not be differentiable in the complex domain, but the Wirtinger derivatives may exist. Consider, for example, the function $g(z) = |z|^2 = zz^*$, which is not differentiable in $\mathbb{C}$, but its

Wirtinger derivatives are

$$\frac{\partial g(z)}{\partial z} = z^*$$
$$\frac{\partial g(z)}{\partial z^*} = z\,.$$

Theorem A.0.2 (Adapted from [184])**.** Let $g(z) : \mathbb{C} \to \mathbb{C}$ be a complex function and let $\tilde{g}(z, w) : \mathbb{C}^2 \to \mathbb{C}$ be a complex function such that $g(z) = \tilde{g}(z, z^*)$. If $g(z)$ is differentiable in $\mathbb{R}^2$ and if $\tilde{g}(z, w)$ is analytic, then

$$\frac{\partial g(z)}{\partial z} = \frac{1}{2}\Big(\frac{\partial g(z)}{\partial z_\mathrm{r}} - \imath\frac{\partial g(z)}{\partial z_\mathrm{i}}\Big)$$
$$\frac{\partial g(z)}{\partial z^*} = \frac{1}{2}\Big(\frac{\partial g(z)}{\partial z_\mathrm{r}} + \imath\frac{\partial g(z)}{\partial z_\mathrm{i}}\Big)\,.$$

Corollary A.0.3 (Adapted from [97])**.** If $g(z)$ is holomorphic, then

$$\frac{\partial g(z)}{\partial z} = \frac{\mathrm{d}g(z)}{\mathrm{d}z}\,. \tag{A.2}$$

Remark 2. Brandwood's theorem establishes a connection between the Wirtinger and the conventional derivatives. The corollary highlights the fact that the Wirtinger derivatives are a generalization of the conventional complex derivative. Therefore, an equivalent definition for the Wirtinger derivative can be given as follows.

Definition A.0.4 (Wirtinger [183])**.** For a complex function $g(z) : \mathbb{C} \to \mathbb{C}$ the Wirtinger derivatives are defined as

$$\frac{\partial g(z)}{\partial z} \triangleq \frac{1}{2}\Big(\frac{\partial g(z)}{\partial z_\mathrm{r}} - \imath\frac{\partial g(z)}{\partial z_\mathrm{i}}\Big) \tag{A.3a}$$
$$\frac{\partial g(z)}{\partial z^*} \triangleq \frac{1}{2}\Big(\frac{\partial g(z)}{\partial z_\mathrm{r}} + \imath\frac{\partial g(z)}{\partial z_\mathrm{i}}\Big)\,. \tag{A.3b}$$

Bibliography

[1] J. P. Dowling and G. J. Milburn, "Quantum technology: The second quantum revolution," *Phil. Trans. R. Soc. Lond. A*, vol. 361, no. 1809, pp. 1655–1674, Jun. 2003.

[2] J. P. Dowling, *Schrödinger's Web: Race to Build the Quantum Internet*. Boca Raton, FL: CRC Press, 2020.

[3] J. P. Dowling, *Schrödinger's Killer App: Race to Build the World's First Quantum Computer*. Boca Raton, FL: CRC Press, 2013.

[4] C. W. Helstrom, *Quantum Detection and Estimation Theory*. New York: Academic Press, 1976.

[5] S. Guerrini, M. Z. Win, M. Chiani, and A. Conti, "Quantum discrimination of noisy photon-added coherent states," *IEEE J. Sel. Areas Inf. Theory*, vol. 1, no. 2, pp. 469–479, Aug. 2020, special issue on *Quantum Information Science*.

[6] S. Guerrini, M. Chiani, M. Z. Win, and A. Conti, "Quantum pulse position modulation with photon-added squeezed states," in *Proc. IEEE Workshop on Quantum Commun. and Inf. Technol. (QCIT), Global Telecomm. Conf.*, Taipei, Taiwan, Dec. 2020, pp. 1–5.

[7] S. Guerrini, M. Chiani, M. Z. Win, and A. Conti, "Quantum pulse position modulation with photon-added coherent states," in *Proc. IEEE Workshop on Quantum Commun. and Inf. Technol. (QCIT), Global Telecomm. Conf.*, Waikoloa, HI, USA, Dec. 2019, pp. 1–5.

[8] M. Chiani, A. Conti, and M. Z. Win, "Piggybacking on quantum streams," *Phys. Rev. A*, vol. 102, p. 012410, Jul. 2020.

[9] N. Hosseinidehaj, Z. Babar, R. Malaney, S. X. Ng, and L. Hanzo, "Satellite-based continuous-variable quantum communications: State-of-the-art and a predictive outlook," *IEEE Commun. Surveys Tuts.*, vol. 21, no. 1, pp. 881–919, 2019.

[10] S. Pirandola *et al.*, "Advances in quantum cryptography," *Adv. Opt. Photon.*, vol. 12, no. 4, pp. 1012–1236, Dec. 2020.

[11] N. Gisin, G. Ribordy, W. Tittel, and H. Zbinden, "Quantum cryptography," *Rev. Mod. Phys.*, vol. 74, pp. 145–195, Mar. 2002.

[12] 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.*, vol. 81, pp. 1301–1350, Sep. 2009.

[13] S. Guerrini, M. Chiani, and A. Conti, "Secure key throughput of intermittent trusted-relay QKD protocols," in *Proc. IEEE Workshop on Quantum Commun. and Inf. Technol. (QCIT), Global Telecomm. Conf.*, Abu Dhabi, UAE, Dec. 2018, pp. 1–5.

[14] M. A. Nielsen and I. L. Chuang, *Quantum Computation and Quantum Information*. Cambridge, UK: Cambridge University Press, 2010.

[15] R. Cleve, A. Ekert, C. Macchiavello, and M. Mosca, "Quantum algorithms revisited," *Proc. R. Soc. London, Ser. A*, vol. 454, no. 1969, pp. 339–354, 1998.

[16] J. A. Bergou, U. Herzog, and M. Hillery, "Quantum filtering and discrimination between sets of boolean functions," *Phys. Rev. Lett.*, vol. 90, p. 257901, Jun. 2003.

[17] A. W. Harrow and A. Montanaro, "Quantum computational supremacy," *Nature*, vol. 549, no. 7671, pp. 203–209, Sep. 2017.

[18] D. Bruß and C. Macchiavello, "Multipartite entanglement in quantum algorithms," *Phys. Rev. A*, vol. 83, no. 5, p. 052313, May 2011.

[19] G. Chiribella, G. M. D'Ariano, and P. Perinotti, "Theoretical framework for quantum networks," *Phys. Rev. A*, vol. 80, p. 022339, Aug. 2009.

[20] W. Dai, T. Peng, and M. Z. Win, "Optimal remote entanglement distribution," *IEEE J. Sel. Areas Commun.*, vol. 38, no. 3, pp. 540–556, Mar. 2020, special issue on *Advances in Quantum Communications, Computing, Cryptography and Sensing*.

[21] W. Dai, T. Peng, and M. Z. Win, "Quantum queuing delay," *IEEE J. Sel. Areas Commun.*, vol. 38, no. 3, pp. 605–618, Mar. 2020, special issue on *Advances in Quantum Communications, Computing, Cryptography and Sensing*.

[22] M. Caleffi, A. S. Cacciapuoti, and G. Bianchi, "Quantum Internet: From communication to distributed computing!" in *Proc. of IEEE/ACM NANOCOM*, 2018.

[23] H. Kimble, "The quantum Internet," *Nature*, vol. 453, no. 7198, pp. 1023–1030, 2008.

[24] S. Pirandola, B. R. Bardhan, T. Gehring, C. Weedbrook, and S. Lloyd, "Advances in photonic quantum sensing," *Nat. Photonics*, vol. 12, no. 12, pp. 724–733, Dec. 2018.

[25] C. L. Degen, F. Reinhard, and P. Cappellaro, "Quantum sensing," *Rev. Mod. Phys.*, vol. 89, p. 035002, Jul. 2017.

[26] V. Giovannetti, S. Lloyd, and L. Maccone, "Quantum-enhanced measurements: Beating the standard quantum limit," *Science*, vol. 306, no. 5700, pp. 1330–1336, 2004.

[27] M. Paris, "Quantum estimation for quantum technology," *Int. J. Quantum Inf.*, vol. 7, pp. 125–137, 2009.

[28] U. Khalid, Y. Jeong, and H. Shin, "Measurement-based quantum correlation in mixed-state quantum metrology," *Quantum Inf. Process.*, vol. 17, no. 12, p. 343, Nov. 2018.

[29] S. L. Braunstein and P. van Loock, "Quantum information with continuous variables," *Rev. Mod. Phys.*, vol. 77, pp. 513–577, Jun. 2005.

[30] A. Ferraro, S. Olivares, and M. G. A. Paris, *Gaussian States in Continuous Variable Quantum Information*. Napoli, Italy: Biliopolis, 2005.

[31] 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.*, vol. 84, pp. 621–669, May 2012.

[32] G. Adesso, S. Ragy, and A. R. Lee, "Continuous variable quantum information: Gaussian states and beyond," *Open Syst. Inf. Dyn.*, vol. 21, p. 1440001, 2014.

[33] A. Serafini, *Quantum Continuous Variables: A Primer of Theoretical Methods*. Boca Raton, FL: CRC Press, 2017.

[34] U. L. Andersen, J. S. Neergaard-Nielsen, P. van Loock, and A. Furusawa, "Hybrid discrete- and continuous-variable quantum information," *Nat. Phys.*, vol. 11, no. 9, pp. 713–719, Sep. 2015.

[35] C. W. Helstrom, "Detection theory and quantum mechanics," *Inf. Control*, vol. 10, no. 3, pp. 254–291, 1967.

[36] C. W. Helstrom, "Fundamental limitations on the detectability of electromagnetic signals," *Int. J. Theor. Phys.*, vol. 1, no. 1, pp. 37–50, May 1968.

[37] C. W. Helstrom, J. W. S. Liu, and J. P. Gordon, "Quantum-mechanical communication theory," *Proc. IEEE*, vol. 58, no. 10, pp. 1578–1598, 1970.

[38] H. P. Yuen, R. S. Kennedy, and M. Lax, "Optimum testing of multiple hypotheses in quantum detection theory," *IEEE Trans. Inf. Theory*, vol. 21, no. 2, pp. 125–134, Mar. 1975.

[39] H. Yuen and J. Shapiro, "Optical communication with two-photon coherent states–Part I: Quantum-state propagation and quantum-noise," *IEEE Trans. Inf. Theory*, vol. 24, no. 6, pp. 657–668, Nov. 1978.

[40] J. Shapiro, H. Yuen, and A. Mata, "Optical communication with two-photon coherent states–Part II: Photoemissive detection and structured receiver performance," *IEEE Trans. Inf. Theory*, vol. 25, no. 2, pp. 179–192, Mar. 1979.

[41] H. Yuen and J. Shapiro, "Optical communication with two-photon coherent states–Part III: Quantum measurements realizable with photoemissive detectors," *IEEE Trans. Inf. Theory*, vol. 26, no. 1, pp. 78–92, Jan. 1980.

[42] M. Takeoka and M. Sasaki, "Discrimination of the binary coherent signal: Gaussian-operation limit and simple non-Gaussian near-optimal receivers," *Phys. Rev. A*, vol. 78, p. 022320, Aug. 2008.

[43] G. Cariolaro and G. Pierobon, "Performance of quantum data transmission systems in the presence of thermal noise," *IEEE Trans. Commun.*, vol. 58, no. 2, pp. 623–630, Feb. 2010.

[44] G. Cariolaro and G. Pierobon, "Theory of quantum pulse position modulation and related numerical problems," *IEEE Trans. Commun.*, vol. 58, no. 4, pp. 1213–1222, Apr. 2010.

[45] G. Cariolaro, *Quantum communications*. Heidelberg: Springer, 2015.

[46] G. Chesi, S. Olivares, and M. G. A. Paris, "Squeezing-enhanced phase-shift-keyed binary communication in noisy channels," *Phys. Rev. A*, vol. 97, p. 032315, Mar. 2018.

[47] L. Mandel, "Ideal light source for an optical communication channel," *J. Opt. Soc. Am.*, vol. 66, no. 9, pp. 968–970, Sep. 1976.

[48] C. M. Caves and P. D. Drummond, "Quantum limits on bosonic communication rates," *Rev. Mod. Phys.*, vol. 66, pp. 481–537, Apr. 1994.

[49] A. Vourdas, "Optical signals with thermal noise," *Phys. Rev. A*, vol. 39, pp. 206–213, Jan. 1989.

[50] G. S. Agarwal and K. Tara, "Nonclassical properties of states generated by the excitations on a coherent state," *Phys. Rev. A*, vol. 43, pp. 492–497, Jan. 1991.

[51] G. S. Agarwal and K. Tara, "Nonclassical character of states exhibiting no squeezing or sub-Poissonian statistics," *Phys. Rev. A*, vol. 46, pp. 485–488, Jul. 1992.

[52] G. S. Agarwal, *Quantum Optics*. Cambridge, UK: Cambridge University Press, 2012.

[53] X.-X. Xu, L.-Y. Hu, and H.-Y. Fan, "Photon-added squeezed thermal states: Statistical properties and its decoherence in a photon-loss channel," *Opt. Commun.*, vol. 283, no. 9, pp. 1801–1809, 2010.

[54] R. Zhang, X.-G. Meng, C.-X. Du, and J.-S. Wang, "Nonclassicality of photon-added displaced thermal state via quantum phase-space distributions," *J. Phys. Soc. Jpn.*, vol. 87, no. 2, p. 024001, 2018.

[55] S. Wang and H.-Y. Fan, "Phase-sensitive nonclassical properties of photon-added displaced squeezed thermal states," *J. Opt. Soc. Am. B*, vol. 29, no. 7, pp. 1672–1679, Jul. 2012.

[56] A. Zavatta, S. Viciani, and M. Bellini, "Quantum-to-classical transition with single-photon-added coherent states of light," *Science*, vol. 306, no. 5696, pp. 660–662, 2004.

[57] A. Zavatta, S. Viciani, and M. Bellini, "Single-photon excitation of a coherent state: Catching the elementary step of stimulated light emission," *Phys. Rev. A*, vol. 72, p. 023820, Aug. 2005.

[58] A. Zavatta, V. Parigi, and M. Bellini, "Experimental nonclassicality of single-photon-added thermal light states," *Phys. Rev. A*, vol. 75, p. 052106, May 2007.

[59] P. Huang, G. He, J. Fang, and G. Zeng, "Performance improvement of continuous-variable quantum key distribution via photon subtraction," *Phys. Rev. A*, vol. 87, p. 012317, Jan. 2013.

[60] D. Wang, M. Li, F. Zhu, Z.-Q. Yin, W. Chen, Z.-F. Han, G.-C. Guo, and Q. Wang, "Quantum key distribution with the single-photon-added coherent source," *Phys. Rev. A*, vol. 90, p. 062315, Dec. 2014.

[61] H. Kwon, K. C. Tan, T. Volkoff, and H. Jeong, "Nonclassicality as a quantifiable resource for quantum metrology," *Phys. Rev. Lett.*, vol. 122, p. 040503, Feb. 2019.

[62] S. Srikara, K. Thapliyal, and A. Pathak, "Continuous variable B92 quantum key distribution protocol using single photon added and subtracted coherent states," *Quantum Inf. Process.*, vol. 19, no. 10, p. 371, Oct. 2020.

[63] C. Bennett and G. Brassard, "Quantum cryptography: Public key distribution and coin tossing," *Proc. IEEE Int. Conf. Computers, Systems, and Signal Processing*, pp. 175–179, Dec. 1984.

[64] 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.*, vol. 81, pp. 1301–1350, Sep. 2009.

[65] N. Gisin, G. Ribordy, W. Tittel, and H. Zbinden, "Quantum cryptography," *Rev. Mod. Phys.*, vol. 74, pp. 145–195, Mar. 2002.

[66] H.-L. Yin *et al.*, "Measurement-device-independent quantum key distribution over a 404 km optical fiber," *Phys. Rev. Lett.*, vol. 117, p. 190501, Nov. 2016.

[67] M. Peev *et al.*, "The SECOQC quantum key distribution network in Vienna," *New J. Phys.*, vol. 11, 2009.

[68] M. Sasaki *et al.*, "Field test of quantum key distribution in the Tokyo QKD network," *Opt. Express*, vol. 19, no. 11, pp. 10 387–10 409, 2011.

[69] J. Yin *et al.*, "Satellite-based entanglement distribution over 1200 kilometers," *Science*, vol. 356, no. 6343, pp. 1140–1144, 2017.

[70] S.-K. Liao *et al.*, "Satellite-to-ground quantum key distribution," *Nature*, vol. 549, no. 7670, pp. 43–47, 2017.

[71] S.-K. Liao *et al.*, "Satellite-relayed intercontinental quantum network," *Phys. Rev. Lett.*, vol. 120, p. 030501, Jan. 2018.

[72] W. K. Wootters and W. H. Zurek, "A single quantum cannot be cloned," *Nature*, vol. 299, no. 5886, pp. 802–803, Oct. 1982.

[73] P. A. M. Dirac, *The Principles of Quantum Mechanics*. Oxford University Press, 1981.

[74] J. Von Neumann, *Mathematical foundations of quantum mechanics*. Princeton University Press, 1955.

[75] W. H. Louisell, *Quantum Statistical Properties of Radiation*. New York: Wiley, 1973.

[76] L. Mandel and E. Wolf, *Optical Coherence and Quantum Optics*. New York: Cambridge University Press, 1995.

[77] J. C. Garrison and R. Y. Chiao, *Quantum Optics*. Oxford, UK: Oxford University Press, 2008.

[78] M. G. A. Paris, "Displacement operator by beam splitter," *Phys. Lett. A*, vol. 217, no. 2, pp. 78–80, 1996.

[79] D. F. Walls and G. J. Milburn, *Quantum optics*. Springer Science & Business Media, 2007.

[80] E. Wigner, "On the quantum correction for thermodynamic equilibrium," *Phys. Rev.*, vol. 40, no. 5, p. 749, 1932.

[81] K. E. Cahill and R. J. Glauber, "Ordered expansions in boson amplitude operators," *Phys. Rev.*, vol. 177, pp. 1857–1881, Jan. 1969.

[82] K. E. Cahill and R. J. Glauber, "Density operators and quasiprobability distributions," *Phys. Rev.*, vol. 177, pp. 1882–1902, Jan. 1969.

[83] 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*, vol. 2, pp. 2161–2186, Nov. 1970.

[84] 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*, vol. 2, pp. 2187–2205, Nov. 1970.

[85] G. S. Agarwal and E. Wolf, "Calculus for functions of noncommuting operators and general phase-space methods in quantum mechanics. III. A generalized Wick theorem and multitime mapping," *Phys. Rev. D*, vol. 2, pp. 2206–2225, Nov. 1970.

[86] W. Feller, *An Introduction to Probability Theory and Its Applications.* Wiley, 1971, vol. 2.

[87] R. J. Glauber, "The quantum theory of optical coherence," *Phys. Rev.*, vol. 130, pp. 2529–2539, Jun. 1963.

[88] R. J. Glauber, "Coherent and incoherent states of the radiation field," *Phys. Rev.*, vol. 131, pp. 2766–2788, Sep. 1963.

[89] A. Holevo, *Probabilistic and Statistical Aspects of Quantum Theory.* Pisa, Italy: Edizioni della Normale, 2011.

[90] K. Husimi, "Some formal properties of the density matrix," *Proc. Phys.-Math. Soc. Jpn.*, vol. 22, no. 4, pp. 264–314, 1940.

[91] Y. Kano, "A new phase-space distribution function in the statistical theory of the electromagnetic field," *J. Math. Phys.*, vol. 6, no. 12, pp. 1913–1915, 1965.

[92] E. C. G. Sudarshan, "Equivalence of semiclassical and quantum mechanical descriptions of statistical light beams," *Phys. Rev. Lett.*, vol. 10, pp. 277–279, Apr. 1963.

[93] A. van den Bos, "The multivariate complex normal distribution-a generalization," *IEEE Trans. Inf. Theory*, vol. 41, no. 2, pp. 537–539, Mar. 1995.

[94] B. Picinbono, "Second-order complex random vectors and normal distributions," *IEEE Trans. Signal Process.*, vol. 44, no. 10, pp. 2637–2640, Oct. 1996.

[95] D. P. Mandic and V. S. L. Goh, *Complex Valued Nonlinear Adaptive Filters.* New York: Wiley, 2009.

[96] T. Adali, P. J. Schreier, and L. L. Scharf, "Complex-valued signal processing: The proper way to deal with impropriety," *IEEE Trans. Signal Process.*, vol. 59, no. 11, pp. 5101–5125, Jul. 2011.

[97] P. J. Schreier and L. L. Scharf, *Statistical signal processing of complex-valued data: the theory of improper and noncircular signals.* Cambridge, U.K.: Cambridge University Press, 2010.

[98] C. W. Gardiner and P. Zoller, *Quantum noise*, 3rd ed. Berlin: Springer-Verlag, 2004.

[99] H. P. Yuen, "Two-photon coherent states of the radiation field," *Phys. Rev. A*, vol. 13, pp. 2226–2243, Jun. 1976.

[100] C. M. Caves, "Quantum-mechanical noise in an interferometer," *Phys. Rev. D*, vol. 23, pp. 1693–1708, Apr. 1981.

[101] P. Marian and T. A. Marian, "Squeezed states with thermal noise. I. Photon-number statistics," *Phys. Rev. A*, vol. 47, pp. 4474–4486, May 1993.

[102] E. Knill, R. Laflamme, and G. J. Milburn, "A scheme for efficient quantum computation with linear optics," *Nature*, vol. 409, no. 6816, pp. 46–52, Jan. 2001.

[103] N. C. Menicucci, P. van Loock, M. Gu, C. Weedbrook, T. C. Ralph, and M. A. Nielsen, "Universal quantum computation with continuous-variable cluster states," *Phys. Rev. Lett.*, vol. 97, p. 110501, Sep. 2006.

[104] P. Kok, W. J. Munro, K. Nemoto, T. C. Ralph, J. P. Dowling, and G. J. Milburn, "Linear optical quantum computing with photonic qubits," *Rev. Mod. Phys.*, vol. 79, pp. 135–174, Jan. 2007.

[105] H.-S. Zhong *et al.*, "Quantum computational advantage using photons," *Science*, vol. 370, no. 6523, pp. 1460–1463, 2020.

[106] A. Blais, J. Gambetta, A. Wallraff, D. I. Schuster, S. M. Girvin, M. H. Devoret, and R. J. Schoelkopf, "Quantum-information processing with circuit quantum electrodynamics," *Phys. Rev. A*, vol. 75, p. 032329, Mar. 2007.

[107] J. Clarke and F. K. Wilhelm, "Superconducting quantum bits," *Nature*, vol. 453, no. 7198, pp. 1031–1042, Jun. 2008.

[108] P. Krantz, M. Kjaergaard, F. Yan, T. P. Orlando, S. Gustavsson, and W. D. Oliver, "A quantum engineer's guide to superconducting qubits," *Appl. Phys. Rev.*, vol. 6, no. 2, p. 021318, 2019.

[109] L. DiCarlo *et al.*, "Demonstration of two-qubit algorithms with a superconducting quantum processor," *Nature*, vol. 460, no. 7252, pp. 240–244, Jul. 2009.

[110] J. I. Cirac and P. Zoller, "Quantum computations with cold trapped ions," *Phys. Rev. Lett.*, vol. 74, pp. 4091–4094, May 1995.

[111] A. Steane, "The ion trap quantum information processor," *Appl. Phys. B*, vol. 64, no. 6, pp. 623–643, Jun. 1997.

[112] D. Kielpinski, C. Monroe, and D. J. Wineland, "Architecture for a large-scale ion-trap quantum computer," *Nature*, vol. 417, no. 6890, pp. 709–711, Jun. 2002.

[113] G. Adesso, F. Dell'Anno, S. De Siena, F. Illuminati, and L. A. M. Souza, "Optimal estimation of losses at the ultimate quantum limit with non-Gaussian states," *Phys. Rev. A*, vol. 79, p. 040305, Apr. 2009.

[114] F. Arute *et al.*, "Quantum supremacy using a programmable superconducting processor," *Nature*, vol. 574, no. 7779, pp. 505–510, 2019.

[115] L. Hu, M. Al-amri, Z. Liao, and M. S. Zubairy, "Continuous-variable quantum key distribution with non-Gaussian operations," *Phys. Rev. A*, vol. 102, p. 012608, Jul. 2020.

[116] D. Bouwmeester, J.-W. Pan, K. Mattle, M. Eibl, H. Weinfurter, and A. Zeilinger, "Experimental quantum teleportation," *Nature*, vol. 390, no. 6660, pp. 575–579, Dec. 1997.

[117] E. D. Lopaeva, I. Ruo Berchera, I. P. Degiovanni, S. Olivares, G. Brida, and M. Genovese, "Experimental realization of quantum illumination," *Phys. Rev. Lett.*, vol. 110, p. 153603, Apr. 2013.

[118] J. Etesse, M. Bouillard, B. Kanseri, and R. Tualle-Brouri, "Experimental generation of squeezed cat states with an operation allowing iterative growth," *Phys. Rev. Lett.*, vol. 114, p. 193602, May 2015.

[119] Y. Xia, W. Li, W. Clark, D. Hart, Q. Zhuang, and Z. Zhang, "Demonstration of a reconfigurable entangled radio-frequency photonic sensor network," *Phys. Rev. Lett.*, vol. 124, p. 150502, Apr. 2020.

[120] S. Barzanjeh, S. Pirandola, D. Vitali, and J. M. Fink, "Microwave quantum illumination using a digital receiver," *Sci. Adv.*, vol. 6, no. 19, p. eabb0451, 2020.

[121] A. Houck *et al.*, "Generating single microwave photons in a circuit," *Nature*, vol. 449, no. 7160, pp. 328–331, 2007.

[122] M. Dakna, T. Anhut, T. Opatrný, L. Knöll, and D.-G. Welsch, "Generating schrödinger-cat-like states by means of conditional measurements on a beam splitter," *Phys. Rev. A*, vol. 55, pp. 3184–3194, Apr. 1997.

[123] J. Wenger, R. Tualle-Brouri, and P. Grangier, "Non-Gaussian statistics from individual pulses of squeezed light," *Phys. Rev. Lett.*, vol. 92, p. 153601, Apr. 2004.

[124] M. S. Kim, E. Park, P. L. Knight, and H. Jeong, "Nonclassicality of a photon-subtracted Gaussian field," *Phys. Rev. A*, vol. 71, p. 043805, Apr. 2005.

[125] A. Biswas and G. S. Agarwal, "Nonclassicality and decoherence of photon-subtracted squeezed states," *Phys. Rev. A*, vol. 75, p. 032104, Mar. 2007.

[126] L.-Y. Hu, X.-X. Xu, Z.-S. Wang, and X.-F. Xu, "Photon-subtracted squeezed thermal state: Nonclassicality and decoherence," *Phys. Rev. A*, vol. 82, p. 043842, Oct. 2010.

[127] A. Ourjoumtsev, R. Tualle-Brouri, J. Laurat, and P. Grangier, "Generating optical schrödinger kittens for quantum information processing," *Science*, vol. 312, no. 5770, pp. 83–86, 2006.

[128] A. Ourjoumtsev, A. Dantan, R. Tualle-Brouri, and P. Grangier, "Increasing entanglement between Gaussian states by coherent photon subtraction," *Phys. Rev. Lett.*, vol. 98, p. 030502, Jan. 2007.

[129] N. Namekata, Y. Takahashi, G. Fujii, D. Fukuda, S. Kurimura, and S. Inoue, "Non-Gaussian operation based on photon subtraction using a photon-number-resolving detector at a telecommunications wavelength," *Nat. Photonics*, vol. 4, no. 9, pp. 655–660, Sep. 2010.

[130] T. Opatrný, G. Kurizki, and D.-G. Welsch, "Improvement on teleportation of continuous variables by photon subtraction via conditional measurement," *Phys. Rev. A*, vol. 61, p. 032302, Feb. 2000.

[131] D. Braun, P. Jian, O. Pinel, and N. Treps, "Precision measurements with photon-subtracted or photon-added Gaussian states," *Phys. Rev. A*, vol. 90, p. 013821, Jul. 2014.

[132] H. F. Hofmann, "Generation of a highly-phase-sensitive polarization-squeezed n-photon state by collinear parametric down-conversion and coherent photon subtraction," *Phys. Rev. A*, vol. 74, p. 013808, Jul. 2006.

[133] L. Fan and M. S. Zubairy, "Quantum illumination using non-Gaussian states generated by photon subtraction and photon addition," *Phys. Rev. A*, vol. 98, p. 012319, Jul. 2018.

[134] Z. Wang, X.-G. Meng, and H.-Y. Fan, "Photon-subtracted squeezed coherent state: nonclassicality and decoherence in thermal environment," *J. Opt. Soc. Am. B*, vol. 29, no. 3, pp. 397–406, Mar. 2012.

[135] A. Kenfack and K. Zyczkowski, "Negativity of the Wigner function as an indicator of non-classicality," *J. Opt. B Quantum Semiclassical Opt.*, vol. 6, no. 10, pp. 396–404, Aug. 2004.

[136] B. R. Mollow and R. J. Glauber, "Quantum theory of parametric amplification. I," *Phys. Rev.*, vol. 160, pp. 1076–1096, Aug. 1967.

[137] R. R. Puri, *Mathematical Methods of Quantum Optics*. Berlin: Springer, 2001.

[138] C. L. Mehta, "Diagonal coherent-state representation of quantum operators," *Phys. Rev. Lett.*, vol. 18, pp. 752–754, May 1967.

[139] W. P. Schleich, *Quantum optics in phase space*. Berlin: Wiley-VCH, 2001.

[140] A. S. Holevo, "Statistical decision theory for quantum systems," *J. Math. Phys.*, vol. 3, no. 4, pp. 337–394, 1973.

[141] W. C. Lindsey, "Transmission of classical information over noisy quantum channels–a spectrum approach," *IEEE J. Sel. Areas Commun.*, vol. 38, no. 3, pp. 427–438, Mar. 2020.

[142] S. Lloyd, "Enhanced sensitivity of photodetection via quantum illumination," *Science*, vol. 321, no. 5895, pp. 1463–1465, 2008.

[143] S.-H. Tan, B. I. Erkmen, V. Giovannetti, S. Guha, S. Lloyd, L. Maccone, S. Pirandola, and J. H. Shapiro, "Quantum illumination with Gaussian states," *Phys. Rev. Lett.*, vol. 101, p. 253601, Dec. 2008.

[144] T. C. Ralph, A. Gilchrist, G. J. Milburn, W. J. Munro, and S. Glancy, "Quantum computation with optical coherent states," *Phys. Rev. A*, vol. 68, no. 4, p. 042319, 2003.

[145] H. Yonezawa, T. Aoki, and A. Furusawa, "Demonstration of a quantum teleportation network for continues variables," *Nature*, vol. 431, no. 7007, pp. 430–433, 2004.

[146] P. Jouguet, S. Kunz-Jacques, A. Leverrier, P. Grangier, and E. Diamanti, "Experimental demonstration of long-distance continuous-variable quantum key distribution," *Nat. Photonics*, vol. 7, no. 5, pp. 378–381, 2013.

[147] Y. Xia, W. Li, W. Clark, D. Hart, Q. Zhuang, and Z. Zhang, "Demonstration of a reconfigurable entangled radio-frequency photonic sensor network," *Phys. Rev. Lett.*, vol. 124, p. 150502, Apr. 2020.

[148] R. Yoshitani, "On the detectability limit of coherent optical signals in thermal radiation," *J. Stat. Phys.*, vol. 2, no. 4, pp. 347–378, Dec. 1970.

[149] N. Dalla Pozza and G. Pierobon, "Optimality of square-root measurements in quantum state discrimination," *Phys. Rev. A*, vol. 91, p. 042334, Apr. 2015.

[150] R. Yuan, M. Zhao, S. Han, and J. Cheng, "Kennedy receiver using threshold detection and optimized displacement under thermal noise," *IEEE Commun. Lett.*, vol. 24, no. 6, pp. 1313–1317, Jun. 2020.

[151] R. E. Slusher and B. Yurke, "Squeezed light for coherent communications," *J. Lightwave Technol.*, vol. 8, no. 3, pp. 466–477, Mar. 1990.

[152] G. Cariolaro, R. Corvaja, and G. Pierobon, "Gaussian states and geometrically uniform symmetry," *Phys. Rev. A*, vol. 90, p. 042309, Oct. 2014.

[153] D. Wang, M. Li, F. Zhu, Z.-Q. Yin, W. Chen, Z.-F. Han, G.-C. Guo, and Q. Wang, "Quantum key distribution with the single-photon-added coherent source," *Phys. Rev. A*, vol. 90, p. 062315, Dec. 2014.

[154] M. M. Wilde, *Quantum information theory*, 2nd ed. Cambridge, UK: Cambridge University Press, 2017.

[155] U. Leonhardt, *Measuring the quantum state of light*. Cambridge, UK: Cambridge University Press, 1997.

[156] G. De Palma and J. Borregaard, "Minimum error probability of quantum illumination," *Phys. Rev. A*, vol. 98, p. 012101, Jul. 2018.

[157] A. S. Cacciapuoti, M. Caleffi, F. Tafuri, F. S. Cataliotti, S. Gherardini, and G. Bianchi, "Quantum Internet: Networking challenges in distributed quantum computing," *IEEE Netw.*, vol. 34, no. 1, pp. 137–143, 2020.

[158] A. S. Fletcher, P. W. Shor, and M. Z. Win, "Channel-adapted quantum error correction for the amplitude damping channel," *IEEE Trans. Inf. Theory*, vol. 54, no. 12, pp. 5705–5718, Dec. 2008.

[159] P. Hausladen and W. K. Wootters, "A 'Pretty Good' measurement for distinguishing quantum states," *J. Mod. Opt.*, vol. 41, no. 12, pp. 2385–2390, 1994.

[160] Y. C. Eldar and G. D. Forney, "On quantum detection and the square-root measurement," *IEEE Trans. Inf. Theory*, vol. 47, no. 3, pp. 858–872, Mar. 2001.

[161] Y. C. Eldar, A. Megretski, and G. C. Verghese, "Designing optimal quantum detectors via semidefinite programming," *IEEE Trans. Inf. Theory*, vol. 49, no. 4, pp. 1007–1012, 2003.

[162] Y. C. Eldar, A. Megretski, and G. C. Verghese, "Optimal detection of symmetric mixed quantum states," *IEEE Trans. Inf. Theory*, vol. 50, no. 6, pp. 1198–1207, Jun. 2004.

[163] H. L. Van Trees, *Detection, Estimation, and Modulation Theory.* New York, NY: John Wiley & Sons, Inc., 1968.

[164] C. W. Helstrom, "Nonclassical states in optical communication to a remote receiver," *IEEE Trans. Inf. Theory*, vol. 26, no. 3, pp. 378–382, May 1980.

[165] H. Yuen, "On far-field quantum states in optical communication," *IEEE Trans. Inf. Theory*, vol. 26, no. 3, pp. 382–385, 1980.

[166] C. W. Helstrom, "Comment on "on far-field quantum states in optical communication"," *IEEE Trans. Inf. Theory*, vol. 26, no. 6, pp. 755–757, 1980.

[167] T. M. Cover and J. A. Thomas, *Elements of Information Theory*, 2nd ed. Hoboken, NJ: John Wiley & Sons, Inc., 2006.

[168] A. Erdélyi, W. Magnus, F. Oberhettinger, F. G. Tricomi, and H. Bateman, *Higher transcendental functions.* New York: McGraw-Hill, 1953, vol. 2.

[169] H.-J. Briegel, W. Dür, J. I. Cirac, and P. Zoller, "Quantum repeaters: The role of imperfect local operations in quantum communication," *Phys. Rev. Lett.*, vol. 81, pp. 5932–5935, Dec. 1998.

[170] L. Ruan, W. Dai, and M. Z. Win, "Adaptive recurrence quantum entanglement distillation for two-Kraus-operator channels," *Phys. Rev. A*, vol. 97, no. 5, p. 052332, May 2018.

[171] L. Ruan, W. Dai, and M. Z. Win, "Analysis of efficient recurrence quantum entanglement distillation," in *Proc. IEEE Workshop on Quantum Commun. and Inf. Technol. (QCIT), Global Telecomm. Conf.*, Washington, DC, Dec. 2016, pp. 1–6.

[172] H. Bechmann-Pasquinucci and A. Pasquinucci, "Quantum key distribution with trusted quantum relay," 2005, e-print arXiv:quant-ph/0505089.

[173] W. Stacey, R. Annabestani, X. Ma, and N. Lütkenhaus, "Security of quantum key distribution using a simplified trusted relay," *Phys. Rev. A*, vol. 91, p. 012338, Jan. 2015.

[174] C. E. Shannon, "Communication theory of secrecy systems," *Bell Syst. Tech. J.*, vol. 28, no. 4, pp. 656–715, Oct. 1949.

[175] R. Renner, "Security of quantum key distribution," *Int. J. Quantum Inf.*, vol. 06, no. 01, pp. 1–127, 2008.

[176] C. Elliott *et al.*, "Current status of the DARPA quantum network," in *Quantum Information and Computation III*, vol. 5815. International Society for Optics and Photonics, 2005, pp. 138–150.

[177] J.-P. Bourgoin *et al.*, "Experimental quantum key distribution with simulated ground-to-satellite photon losses and processing limitations," *Phys. Rev. A*, vol. 92, p. 052339, Nov. 2015.

[178] R. König, R. Renner, A. Bariska, and U. Maurer, "Small accessible quantum information does not imply security," *Phys. Rev. Lett.*, vol. 98, p. 140502, Apr. 2007.

[179] R. G. Gallager, *Information Theory and Reliable Communication*, 1st ed. New York, NY, 10158: John Wiley & Sons, Inc., 1968.

[180] C. E. Shannon, "A mathematical theory of communication," *Bell System Technical Journal*, vol. 27, no. 7, pp. 379–423, 1948.

[181] P. W. Shor and J. Preskill, "Simple proof of security of the BB84 quantum key distribution protocol," *Phys. Rev. Lett.*, vol. 85, pp. 441–444, Jul. 2000.

[182] W. Rudin, *Real and Complex Analysis*, 3rd ed. McGraw-Hill, 1987.

[183] W. Wirtinger, "Zur formalen theorie der funktionen von mehr komplexen veränderlichen," *Math. Ann.*, vol. 97, no. 1, pp. 357–375, Dec. 1927.

[184] D. H. Brandwood, "A complex gradient operator and its application in adaptive array theory," *IEE Proceedings H (Microwaves, Optics and Antennas)*, vol. 130, pp. 11–16, Feb. 1983.