UNIVERSITÀ DEGLI STUDI DI MILANO

Scuola di Dottorato in Fisica, Astrofisica e Fisica Applicata
Dipartimento di Fisica

Corso di Dottorato in Fisica, Astrofisica e Fisica Applicata
Ciclo XXXVII

Quantum communications in continuous variable systems

Settore Scientifico Disciplinare FIS/03

Supervisore: Prof. Stefano OLIVARES

Coordinatore: Prof. Aniello MENNELLA

Tesi di Dottorato di:
Michele N. NOTARNICOLA

Anno Accademico 2023/2024

Commission of the final examination:

External Referees:

Prof. Radim FILIP (Palacký University Olomouc, Czech Republic)
Dr. Marco GENOVESE (INRiM–Istituto Nazionale di Ricerca Metrologica, Torino, Italy)

External Members:

Prof. Virginia D'AURIA (Institut de Physique de Nice, Université Côte d'Azur, Nice, France)
Dr. Marco GENOVESE (INRiM–Istituto Nazionale di Ricerca Metrologica, Torino, Italy)
Prof. Lorenzo MACCONE (Università degli Studi di Pavia, Italy)

Final examination:

Date: December 2nd, 2024

Dipartimento di Fisica"Aldo Pontremoli"
Università degli Studi di Milano
Via Celoria 16, 20133 Milano, Italy

Non ti disunire, Schisa.
Non ti disunire mai.

- Antonio Capuano, *È stata la mano di dio*
(directed by Paolo Sorrentino)

To my family
and my best friends

Cover illustration:

Generated with the graphic artificial intelligence DALL-E 2

Internal illustrations:

Michele N. NOTARNICOLA

MIUR subjects:

FIS/03

PACS:

02.50.Le
03.67.-a
03.67.Hk
03.67.Dd
42.50.-p
42.79.Sz

Contents

List of Publications

As of November 7, 2024

Material discussed in this thesis

Publications in peer-reviewed journals

1. M. N. Notarnicola, M. G. A. Paris, and S. Olivares, "Hybrid near-optimum binary receiver with realistic photon-number-resolving detectors", J. Opt. Soc. Am. B **40**, 705–714 (2023), presented in Sec.s 4.4 and 4.5.

2. M. N. Notarnicola and S. Olivares, "Long-distance continuous-variable quantum key distribution with feasible physical noiseless linear amplifiers", Phys. Rev. A **108**, 022404 (2023), presented in Sec. 8.4.

3. M. N. Notarnicola, M. Jarzyna, S. Olivares, and K. Banaszek, "Optimizing state-discrimination receivers for continuous-variable quantum key distribution over a wiretap channel", New J. Phys. **25**, 103014 (2023), presented in Sec.s 5.2.1 and 5.3.1.2, and Chapter 9.

4. M. N. Notarnicola and S. Olivares, "Beating the standard quantum limit for binary phase-shift-keying discrimination with a realistic hybrid feed-forward receiver", Phys. Rev. A **108**, 042619 (2023), presented in Sec.s 4.4 and 4.5.

5. M. N. Notarnicola, S. Olivares, E. Forestieri, E. Parente, L. Potì, and M. Secondini, "Probabilistic amplitude shaping for continuous-variable quantum key distribution with discrete modulation over a wiretap channel", IEEE Trans. Commun. **72**, 375–386 (2024), presented in Sec.s 6.5.2 and 7.2.

6. M. N. Notarnicola, F. Cieciuch, and M. Jarzyna, "Continuous-variable quantum key distribution over multispan links employing phase-insensitive and phase-sensitive amplifiers", New J. Phys. **26**, 043015 (2024), presented in Sec. 8.3.

7. M. N. Notarnicola and S. Olivares, "A robust hybrid receiver for binary phase-shift keying discrimination in the presence of phase noise", Int. J. Quantum Inf. **22**, 2450008 (2024), presented in Sec. 4.6.

Papers in preparation

1. M. N. Notarnicola and S. Olivares, "Optimality of Gaussian attacks in continuous-variable quantum key distribution with discrete modulation under the trusted-device scenario", *t.b.a.*, presented in Sec. 7.1.

2. E. Parente, M. N. Notarnicola, S. Olivares, E. Forestieri, L. Potí, and M. Secondini, "Unconditional security of continuous-variable quantum key distribution employing quadrature amplitude modulation", *t.b.a.*, presented in Sec. 6.5.

Other material

Publications in peer-reviewed journals

1. A. Morea, M. N. Notarnicola, and S. Olivares, "Entanglement recovery in noisy binary quantum information protocols via three-qubit quantum error correction codes", Int. J. Quantum Inf. **21**, 2340002 (2023).

2. M. N. Notarnicola, S. Olivares, and M. G. A. Paris, "Joint estimation of noise and nonlinearity in Kerr systems", APL Quantum **1**, 036118 (2024).

3. A. Sanvito, S. Cassina, M. Lamperti, M. N. Notarnicola, S. Olivares, and A. Allevi, "Assessing a binary quantum channel exploiting a silicon photomultiplier based hybrid receiver ", Opt. Express **32**, 39846-39859 (2024).

Papers under review

1. M. N. Notarnicola and S. Olivares, "Employing weak-field homodyne detection for quantum communications", arXiv:2405.14310 [quant-ph] (2024), submitted to IEEE J. Sel. Areas Commun.

Publications in conference proceedings

1. E. Parente, M. N. Notarnicola, S. Olivares, E. Forestieri, L. Potì, and M. Secondini, "Exploring The Potential of Probabilistic Shaping Technique in Quantum Key Distribution Systems", in *CLEO 2024*, Technical Digest Series (Optica Publishing Group, 2024), paper FM3K.5.

Outreach publications

1. S. Altilia, M. N. Notarnicola, and S. Olivares, "La distribuzione quantistica di chiave", Ihaca: Viaggio nella Scienza **XXII**, 91–104 (2023), in Italian.

Acknowledgments

The latest three years as a PhD student have been really dense of experience and novelties, therefore I want to thank all the people that contributed to make them special.

First of all, I have to thank my Supervisor, Stefano, who has been much more than a boss for me. Our collaboration dates back to my Master Thesis and, since then, we shared great moments, both inside and outside the University: we had many stimulating discussions, and also had a lot of fun with the students and the other members of our group. I am really grateful to him, as, throughout these years, he gave me complete freedom and trust to pursue our research, which made me become more confident and independent. He has always been close to me, with his help and support, and I am sure that our relationship will be maintained also in the future.

Secondly, I am also thankful to the Supervisors of my visiting period in Warsaw, Konrad and Marcin, that brought my mind and knowledge to new and interesting topics. I also have to thank Matteo Paris, not only for the time spent together in our research activity, but also for all the support and advice he gave me in the latest months, when decisions for my future career had to be taken. Furthermore, I thank all the members of our group, starting from the "lunch break company", namely Claudia, Fabrizio, Dario, and Nicola, up to Andrea, Marco, and Matteo Bina, with whom I shared many nice moments, and, finally, Bassano, and Alessandro Ferraro.

Of course, I have to make a special acknowledgment to all the other comrades encountered in these years in the offices and corridors of Via Celoria, with some of which we have also become friends: Alessandro Candeloro, Paolo, Davide, Daniele, Massimo, Samuele, Edoardo, Francesco, Tin, Shoukang, Eoin, and Alessandra. In particular, a special thank to Alessandro for both being a close friend, and for having drawn me inspiration with his own PhD thesis on how to write this work.

Beside, I cannot fail to express my gratitude to all my other friends outside University, starting from my lifelong friends (Riccardo, Angelo, Gennaro, Cosimo; Gianvito, Felice, Marco; Clemente, Felice, Laura), without which I would have not become the person that I am. Further thanks to the other guys later encountered (Giuseppe, Francesco, Antonio); the friends from Trieste (Domenico, Alessandro, Edoardo, Gianluca, Fabiano, Sara), that are always close as we had never been apart; those from Warsaw (Julia, Manfredi, Ray, Varun, Moein, Marcin, Klaudia, Marco, Karol, Antoni), with whom I spent few but irreplaceable months, and, last but not least, those from Milan (Michele, Giacomo, Viviana), with which we survived the pandemic period. Moreover, a special thank to Riccardo and Domenico, for being present in every single moment of my life: your constant presence and support is always essential to me. A further acknowledgment to Riccardo and

Cosimo for indirectly inspiring me how to prove the optimality of Gaussian attacks in the trusted-device scenario. A part of this Thesis is due to you.

Finally, I have to really thank my family, who has always done everything for me. Even if it is tough to live far apart, in you I always find the protection and strength to go on.

Introduction

Tu saresti capace di piantare tutto e ricominciare la vita da capo?
Di scegliere una cosa, una cosa sola, ed essere fedele a quella,
riuscire a farla diventare la ragione della tua vita,
una cosa che raccolga tutto e che diventi tutto
proprio perché è la tua fedeltà che la fa diventare infinita. Ne saresti capace? [...]
No, questo tipo no, non è capace.
Questo vuole prendere tutto, arraffare tutto, non sa rinunciare a niente.
Cambia strada ogni giorno perché ha paura di perdere quella giusta,
e sta morendo, come dissanguato ...

Motivation

The appearance of quantum mechanics in the mid 1920's yielded a milestone progress in modern science, providing a fundamental theory to describe natural phenomena at the microscopic and sub-microscopic scale, being untenable within the framework of classical physics. However, if on the one hand it establishes a consistent description of highly non-classical phenomena, involving atoms and molecules, semi- and superconductors, ...; on the other hand, in time, physicists questioned themselves about the non-intuitive aspects of the theory, namely, non-commutativity of observables, the Einstein-Podolsky-Rosen paradox, quantum non-locality and the von Neumann reduction induced by quantum measurements [1]. Starting from the 1950's, the perspective changed, and the emerging results in the quantum mechanics foundations gave birth to a new field: *quantum information science*. While quantum mechanics limits itself to explain the natural phenomena at the microscopic level, quantum information science starts from the Landauer's observation that information is a physical entity, being dependent of the physical laws used to store and processes it [2–4], and focuses on its transmission and processing by means of the quantum features of a physical system.

Historically, the first developments of quantum information arose from the field of *quantum communications*. Indeed, in the 1960's, Gordon [5], Stratonovich [6, 7], and Helstrom [8, 9] firstly proposed a formulation of optical communications in the quantum regime, with the intent of establishing the fundamental limits posed by quantum mechanics in the transmission of classical information over optical communication links. In particular, Gordon and Stratonovich addressed the information capacity of optical channels, while Helstrom focused himself on quantifying the error probability in a decision

strategy when a finite set of classical symbols is encoded onto non-orthogonal quantum states of radiation. These results provided the first step for all the subsequent investigations, assessing the ultimate limits of quantum protocols and operations ranging from channel parameter estimation [10], information capacity [11], optical amplification [12], and so on. Moreover, thanks to the recent technological progresses, these limits not only provide useful theoretical results, but have also been experimentally demonstrated and, nowadays, are commonly encountered in several contexts, from near- and deep-space communications to loss mitigation of realistic metropolitan fiber channels.

On the other hand, the 1980's brought a remarkable change in perspective. Instead of merely considering quantum properties as *passive* features that pose limitations on the performance of classical protocols, scientists realized that they could be exploited as *active* resources to design completely new protocols and paradigms that outperform the existing classical schemes. In other words, since information is physical, we can employ quantum mechanical effects, e.g. Heisenberg's uncertainty, superposition, ..., to transmit it in novel and more powerful fashion. The main result in this direction has been achieved by quantum key distribution (QKD), firstly introduced by Bennett and Brassard in 1984 [13], that allows two distant parties to distill a random key via the exchange of quantum states, with unconditional security guaranteed by the quantum mechanics laws. In time, QKD has become one of the milestone aspects of quantum information, and its application has been extended from discrete variable to continuous variable systems [14]. Following this philosophy, in more recent years, a big enhancement has been obtained also regarding the information transmission over quantum channels, by addressing the transmission of genuine quantum information, i.e. quantum states (possibly entangled), instead of the simple encoding of classical symbols onto a quantum optical carrier field [15].

Thesis overview

Given the motivations described above, nowadays quantum communications provide a vast field of research in rapid expansion, with a huge potential impact on the future developments of quantum technologies. The scope of this Thesis is then to address some relevant aspects of the field, and provide innovative results being also experimentally oriented. In particular, here we focus on two relevant paradigms, namely quantum state discrimination and continuous variable (CV) QKD, with particular reference to optical platforms. In the former case, we design new hybrid receivers for discrimination of phase-shift-keyed coherent states, obtaining a quantum advantage over conventional detection schemes. In the latter scenario, we proceed in two different directions. On the one hand, we design new CVQKD protocols employing discrete modulation of coherent states, being a more feasible solution compatible with the state of the art in optical communications technologies; on the other hand, we address the more fundamental problem of performing channel losses mitigation to enhance the key generation rate (KGR), by considering both feasible conventional optical amplifiers and more sophisticated schemes like probabilistic noiseless linear amplifiers. Finally, we make a first step towards a fully non-Gaussian CVQKD scheme by proposing, for the first time, the adoption of an optimized state discrimination receiver, commonly adopted for quantum decision theory, within the context of CVQKD, obtaining a genuine quantum enhancement over conventional protocols in particular ranges of transmission distance.

Here below, the structure and the main original results of the Thesis are summarized in more detail.

Organizational note

The present PhD Thesis consists of three Parts, followed by Conclusions and a list of Appendices, for a total of ten Chapters. In particular, Part I provides a preliminary part that introduces the notation and the fundamental tools employed throughout the rest of the Thesis, and it is divided into three Chapters. Part II is devoted to quantum state discrimination theory, presenting a comprehensive analysis of binary and M-ary discrimination protocols, and it is composed of two Chapters. Finally, Part III deals with QKD in continuous variable systems, addressing the different existing approaches to assess security, and it consists of four Chapters.

- In Chapter 1, we summarize the modern tools of quantum mechanics, presenting the postulates of the theory regarding quantum states, quantum evolution and quantum measurements.
- In Chapter 2, we present the basic elements of quantum optics, with relevant examples of quantum states of radiation, quantum maps and quantum measurements. In particular, we give a detailed presentation of the Gaussian state formalism, that will be widely exploited in the main Parts of the Thesis.
- In Chapter 3, we introduce the main aspects of realistic quantum communication systems and information theory, highlighting the difference between the classical and quantum description.
- In Chapter 4, we outline the framework of quantum state discrimination theory: we introduce the decision error probability as the main figure of merit, and address the fundamental case of binary discrimination of quantum states. In particular, we focus on coherent-state discrimination and present a comprehensive analysis of the quantum receivers proposed in literature, assessing their performance also in the presence of realistic inefficiencies, e.g. non-unit quantum efficiency, dark counts, visibility reduction and phase noise. Results have been published in [16–18].
- In Chapter 5, we extend the analysis to multiple-state discrimination. We present a deep review of all the fundamental theoretical results of the theory and, eventually, specialize it to quadrature phase-shift-keying discrimination of coherent states, discussing the functioning and the limits of the most relevant quantum receivers. Results have been published in [19].
- In Chapter 6, we address QKD: at first, we provide a basic overview of its main aspects and, thereafter, we focus on CVQKD, where coherent states are employed as information carrier. We present three different approaches to assess the security of the protocols, namely unconditional security, trusted-device scenario and wiretap channel assumption, and introduce the KGR as the fundamental figure of merit. Subsequently, we focus on the unconditional scenario and provide security proofs by the "optimality of Gaussian attacks" theorem. Then, we apply the obtained theoretical results to both Gaussian modulation and discrete modulation protocols. Results have been published in [20].
- In Chapter 7, we study the two other security frameworks previously introduced, that represent examples of restricted eavesdropping. At first, we address the trusted-

device scenario and extend the validity of the optimality of Gaussian attacks, accounting also for the limitations of the eavesdropper. Thereafter, we study the security of a wiretap channel, in which the eavesdropping attack is assumed to be known, comparing the resulting KGR with the unconditional security case. Results have been published in [20].

- In Chapter 8, we discuss the potentiality of optical amplifiers to perform mitigation of the transmission losses and enhance CVQKD. We address the problem of optical amplification at the quantum limit, introducing both conventional amplifiers, i.e. phase-insensitive and phase-sensitive amplifiers, and probabilistic noiseless linear amplifiers. Then, we study their application in CVQKD schemes, providing security analysis under different security frameworks. Results have been published in [21, 22].

- In Chapter 9, we proceed beyond the standard CVQKD protocols, employing Gaussian measurements, and investigate the potentiality of non-Gaussian detection schemes to increase the KGR. In particular, we resort to M-ary quantum state discrimination theory, discussed in Chapter 5, and design an optimized quantum receiver maximizing the KGR, comparing its performance with respect to standard Gaussian receivers under the wiretap channel assumption. Results have been published in [19].

Main results

Binary discrimination of coherent states (see Sec.s 4.4, 4.5, and 4.6): Starting from the state-of-the-art quantum receivers, namely the homodyne and displacement receivers (e.g. the Kennedy one), we propose a new hybrid scheme, the hybrid near-optimum receiver (HYNORE), that combines both the homodyne-like and displacement-photon counting setups via feed-forward operations to obtain an enhanced discrimination strategy. The receiver not only outperforms the Kennedy, but also provide a fascinating proposal for experimental implementations, as it only relies on photon-number-resolving (PNR) detectors and electro-optic modulators (EOMs) to implement conditional displacements. Thereafter, we also extend the scheme to a multi-copy receiver, to design a second hybrid receiver, the hybrid feed-forward receiver (HFFRE), where further reduction of the decision error probability is obtained by splitting the encoded signal into many rescaled copies and performing subsequent feed-forward operations. Finally, we detailedly address the robustness of the two proposed hybrid receivers against the typical experimental imperfections, that is non-unit quantum efficiency, dark counts, reduced interference visibility, and phase diffusion noise.

M-ary state discrimination (see Sec.s 5.2.1 and 5.3.1.2): The problem of the optimal decision becomes highly nontrivial in the presence of a constellation of $M > 2$ quantum states. Unlike the binary case, where Helstrom's theory provides an explicit derivation of the optimum receiver and the corresponding minimum error probability, for M-ary state discrimination, the decision problem is recast into a convex optimization problem. The optimum receiver is only indirectly characterized by Yuen's theorem, presenting necessary and sufficient conditions to be fulfilled, while, in general, calculation of the corresponding positive-operator valued measure (POVM) and decision error probability should be handled numerically. Given this limitation, suboptimal POVMs with simpler construction have been proposed, among which

the paradigmatic example is provided by the pretty good measurement (PGM), being proved to yield the optimum receiver in the particular case of pure-state constellations satisfying the geometrically uniform symmetry (GUS). In this Thesis, we present a new and simpler derivation of the optimum receiver in this latter scenario. In particular, we prove that, in the presence of GUS, every pure-state discrimination receiver is ultimately identified by a set of $M-1$ phases, which may be properly chosen to minimize the decision error probability, thus transforming a convex functional optimization into optimization of a real function with $M-1$ real variables. Remarkably, this result provide a huge simplification, and leads to straightforward construction of the optimum receiver that does not refer to suboptimal methods, obtained by setting all the free phases equal to 0.

CVQKD with discrete modulation (see Sec. 6.5.2): Given the practical difficulty to implement Gaussian modulation of coherent states in the current CVQKD demonstrations, we propose a new CVQKD protocol employing quadrature amplitude modulation (QAM) of the coherent pulses, assisted by probabilistic amplitude shaping to obtain a non-uniform sampling probability distribution that approximates a Gaussian distribution. We prove QAM to both outperform the conventional discrete modulation formats based on phase-shift keying (PSK), and to close the gap with respect to Gaussian modulation, thus providing a solution to achieve high values of KGR with a feasible experimental setup.

Security of CVQKD in the trusted-device scenario (see Sec. 7.1): Usual security proofs for CVQKD are obtained in the unconditional security framework, where the whole channel connecting sender and receiver is considered to be untrusted, thus assuming the presence of an omnipotent eavesdropper. However, this represent an excessive assumption, that can be relaxed in practical conditions. To this aim, we consider the trusted-device scenario, in which some of the channel components (e.g. detection losses and noise) are trusted. We provide for the first time a security proof for discrete modulation protocols, by extending the "optimality of Gaussian attacks" theorem, commonly adopted in the unconditional framework, to this scenario, providing a general tool to assess security also in the presence of restricted eavesdropping.

Long-distance CVQKD with optical amplifiers (see Sec.s 8.3 and 8.4): We address the problem of channel losses mitigation in CVQKD by adopting different kinds of optical amplifiers. At first, we consider conventional amplifiers, namely phase-insensitive (PIAs) and phase-sensitive amplifiers (PSAs), arranged in a multi-span configuration, where the quantum channel is composed of many regenerative stations interspersed with lossy links. We address security under both the unconditional and the trust-device frameworks. In the former case, we prove that the KGR is improved with respect to the standard no-amplifier protocol only for PSA links where the de-amplified quadrature is measured. In the latter, we assume all amplifiers and spans except one are trusted, and show that the position of the untrusted span greatly affects the potential enhancement offered by amplification. Thereafter, we study CVQKD assisted by heralded noiseless linear amplifiers (NLAs), being probabilistic operations that amplify signals without additional noise, provided that a particular outcome is retrieved from the measurement of some ancillary modes. For the sake of simplicity, we only address unconditional security, and prove that, remarkably, it is possible to distill a secure key at arbitrary large distances if the amplifier gain is properly optimized.

CVQKD with state-discrimination receivers (see Chapter 9): Ultimately, we make

a first step towards the design of fully non-Gaussian CVQKD protocols. By drawing inspiration on our original results for M-ary quantum state discrimination, we propose an innovative optimized state-discrimination receiver for the quadrature PSK (QPSK) protocol, referred to as the key-rate optimized receiver (KOR). For the sake of simplicity, we analyze security under a pure-loss wiretap channel, and obtain an enhancement with respect to the conventional QPSK protocol in the metropolitan-network distance regime. We also consider the performance of a feasible displacement feed-forward receiver, in which case we have an increase in the KGR with respect to Gaussian detection for short transmission distances.

As a final remark, we underline that all the materials presented in the Thesis are either original or adapted from the author's published articles listed at the beginning of the Thesis, with the intent of providing a coherent and consistent picture of the research conducted during the PhD activity.

. . . Ma che cos'è questo lampo di felicità che mi fa tremare, mi ridà forza, vita?
Vi domando scusa, dolcissime creature; non avevo capito, non sapevo.
Com'è giusto accettarvi, amarci. E come è semplice!
Luisa, mi sento come liberato: tutto mi sembra buono, tutto ha un senso, tutto è vero.
Ah, come vorrei sapermi spiegare. Ma non so dire. . .
Ecco, tutto ritorna come prima, tutto è di nuovo confuso.
Ma questa confusione sono io, io come sono, non come vorrei essere adesso.
E non mi fa più paura dire la verità, quello che non so, che cerco, che non ho ancora trovato.
Solo così mi sento vivo, e posso guardare i tuoi occhi fedeli senza vergogna.
È una festa la vita: viviamola insieme! Non so dirti altro, Luisa, né a te né agli altri:
accettami così come sono, se puoi. È l'unico modo per tentare di trovarci.

- Guido Anselmi, *8½*
(directed by Federico Fellini)

Part I

Preliminaries

CHAPTER 1

Mathematical tools of quantum mechanics

This thesis deals with the analysis of communication protocol at the quantum limit; therefore this preliminary Part is devoted to a basic introduction to the main features that will be exploited throughout the work.

To begin with, this Chapter presents the fundamental tools of quantum mechanics from a modern perspective, by following a quantum information approach [23]. The Chapter is organized as follows. In Sec. 1.1, we first introduce the standard prescriptions to establish a statistical theory, i.e. states, evolution and measurements. Then, we address the case of quantum mechanics, presenting the postulates of the theory in the standard fashion. Finally, we proceed beyond and generalize the postulates, accounting for the presence of an open quantum system. In particular, in Sec. 1.1.1 we present the generalized description of quantum states in terms of statistical operators, in Sec. 1.1.2 we introduce the concept of quantum completely positive maps as an extension of the usual unitary dynamics, and in Sec. 1.1.3 we define positive-operator-valued measures, providing the most general description for quantum measurements.

1.1 Mathematical tools of quantum mechanics

Generally speaking, any physical theory that provide a complete description of a physical system[1] should be structured by a minimum set of prescriptions, establishing the connection between the observed phenomena and the adopted mathematical framework. The typical fundamental building blocks are three. Firstly, we identify what is the *state* of the system, that is the mathematical object describing its preparation. Secondly, we introduce the *dynamics*, that is the evolution law of a physical state of the system. Finally, we define *measurements*, specifying the objects that describe observables. As an example, in the case of classical mechanics, the state of a system is identified by a set of canonical variables, i.e. positions and momenta $\{x_j, p_j\}_j$, the evolution is provided by a suitable differential equation in the canonical variables, namely the Hamilton equation, while probability measures determine the rule that predicts the measurement outcomes.

Beside, in the case of quantum mechanics, these three prescriptions are defined through the postulates of the theory, representing the minimal requirements to describe the behaviour of a system in the presence of genuine quantum effects. In their original formulation, the standard postulates of quantum mechanics can be summarized as follows [23, 24].

- **Postulate 1. (States)** The quantum state of a system is described by a normalized vector of a separable Hilbert space $\mathcal{H}$, $|\psi\rangle \in \mathcal{H}$, $\langle\psi|\psi\rangle = 1$. For multipartite systems,

[1] With the term physical system we refer to a single given degree of freedom, e.g. position, spin, polarization, angular momentum,...

the global Hilbert space is the tensor product of the Hilbert spaces associated with each subsystem. Given this vector space description, the superposition principle holds: if $|\psi_1\rangle$ and $|\psi_2\rangle$ are two physical states, then every (normalized) linear combination $\alpha|\psi_1\rangle + \beta|\psi_2\rangle$, $\alpha, \beta \in \mathbb{C}$, $|\alpha|^2 + |\beta|^2 = 1$, is also a possible physical state of the system.

- **Postulate 2. (Dynamics)** Given the initial state $|\psi_0\rangle$ at time t_0, its time evolution is obtained through a unitary operator $U(t, t_0)$, that is $U^\dagger(t, t_0)U(t, t_0) = \mathbb{1}$, $\mathbb{1}$ being the identity operator over $\mathcal{H}$. The state at time t then reads $|\psi(t)\rangle = U(t, t_0)|\psi_0\rangle$.

- **Postulate 3. (Measurements)** Observables are Hermitian operators acting on the Hilbert space $\mathcal{H}$, $X \in \mathcal{B}(\mathcal{H})$. By the spectral theorem, $X = \sum_x x\mathbb{P}_x$, where $x \in \mathbb{R}$ and $\mathbb{P}_x = |x\rangle\langle x|$ are a complete set of orthogonal projectors $\mathbb{P}_x\mathbb{P}_{x'} = \delta_{xx'}\mathbb{P}_x$. The eigenvalues of X represent all possible outcomes of the measurement, and the probability of retrieving x given state $|\psi\rangle$ is provided by the Born rule:

$$p_x = |\langle x|\psi\rangle|^2 . \tag{1.1}$$

Finally, when the measurement brings the value x, the conditional state of the system after detection is the (normalized) projection of the probed state onto the eigenspace associated with x, namely

$$|\psi_x\rangle = \frac{1}{\sqrt{p_x}}\mathbb{P}_x|\psi\rangle , \tag{1.2}$$

referred to as Von Neumann reduction.

Actually, all these postulates presuppose a "Postulate 0", that is to consider a *closed and isolated system*. On the other hand, in practical situations we mostly deal with systems interacting with the rest of the universe, either during their dynamical evolution, or when subjected to measurement. In turn, in the following we develop a suitable modification of the three prescriptions, referred to as the generalized postulates, that hold also in the presence of open quantum systems.

1.1.1 Postulate 1: Quantum states

The first generalized postulate takes into account that the preparation of a quantum system, in general, may not be completely under control. Thus, a probabilistic description must be considered, in terms of a given statistical ensemble $\{p_k, |\psi_k\rangle\}_k$, meaning that state $|\psi_k\rangle$ is prepared with probability p_k. In this case, the description of the system is obtained by the statistical (density) operator $\rho = \sum_k p_k|\psi_k\rangle\langle\psi_k|$. By suitably characterizing this mathematical object, we rephrase Postulate 1 as follows.

Postulate 1. (States) *The quantum state of a system is described by a statistical operator, that is a positive operator of unit trace, $\rho \in \mathcal{L}(\mathcal{H})$, $\rho \geq 0$, $\mathrm{Tr}[\rho] = 1$.*

In the former expression, $\mathcal{L}(\mathcal{H})$ refers to the set of all linear operator acting on he Hilbert space $\mathcal{H}$. As a consequence, given state ρ, if we consider a traditional Hermitian observable X, the Born rule and the von Neumann reduction become:

$$p_x = \mathrm{Tr}[\rho\,\mathbb{P}_x] \qquad \text{and} \qquad \rho_x = \frac{1}{p_x}\,\mathbb{P}_x\rho\,\mathbb{P}_x , \tag{1.3}$$

respectively. In the presence of a pure state $|\psi\rangle \in \mathcal{H}$, we have a 1-rank density operator $\rho = |\psi\rangle\langle\psi|$, while, in the more general case, we have $1 \leq \mathrm{rank}(\rho) \leq d$, with $d = \dim(\mathcal{H})$, and the state is said to be mixed.

The new generalized postulate can be reconciled with the standard Postulate 1 by observing that, for an isolated bipartite system AB, described by the vector state $|\psi\rangle\!\rangle_{AB}$, the state describing only subsystem A is obtained as the partial trace of the global state:

$$\rho_A = \mathrm{Tr}_B \left[|\psi\rangle\!\rangle_{AB} \langle\!\langle \psi| \right], \tag{1.4}$$

and the same undergoes for ρ_B. Conversely, any density operator on $\mathcal{H}$ can be viewed as the partial trace of a state vector on a larger Hilbert space. In fact, given a quantum state ρ it is also possible to construct its *purification* as follows. We start from the spectral decomposition $\rho = \sum_k \lambda_k |\phi_k\rangle\langle\phi_k|$; now, we introduce another Hilbert space $\mathcal{K}$ with dimension $\dim(\mathcal{K}) \geq \mathrm{rank}(\rho)$ and an orthonormal basis $\{|\theta_k\rangle\}_k$ in $\mathcal{K}$. Then, the vector $|\Psi\rangle\!\rangle \in \mathcal{H} \otimes \mathcal{K}$, equal to:

$$|\Psi\rangle\!\rangle = \sum_k \sqrt{\lambda_k}\, |\phi_k\rangle |\theta_k\rangle\,, \tag{1.5}$$

provides a purification of ρ, namely a pure state such that $\mathrm{Tr}_{\mathcal{K}}[|\Psi\rangle\!\rangle\langle\!\langle\Psi|] = \rho$. We also note that the expression (1.5) represents the Schmidt decomposition of $|\Psi\rangle\!\rangle$ [25, 26]. Given this argument, we underline that there exist infinitely many purifications of a density operator. However, thanks to the "freedom-in-purifications theorem" [27], all purifications are unitarily equivalent. That is, if $|\Psi_1\rangle\!\rangle \in \mathcal{H} \otimes \mathcal{K}_1$ and $|\Psi_2\rangle\!\rangle \in \mathcal{H} \otimes \mathcal{K}_2$ are two purifications of ρ, there exists a unitary operation $U : \mathcal{K}_1 \to \mathcal{K}_2$ which transforms $|\Psi_1\rangle\!\rangle$ into $|\Psi_2\rangle\!\rangle$, namely:

$$|\Psi_2\rangle\!\rangle = \left(\hat{\mathbb{1}}_{\mathcal{H}} \otimes U\right) |\Psi_1\rangle\!\rangle\,. \tag{1.6}$$

Finally, to quantify the degree of mixedness of a quantum state ρ, that is how far a density operator is from a pure state, we introduce two typical measures:

- the *purity*, defined as the trace of the square density operator:

$$\mu[\rho] = \mathrm{Tr}[\rho^2]\,, \tag{1.7}$$

  such that $1/d \leq \mu[\rho] \leq 1$, d being the dimension of the Hilbert space. Pure states, satisfying $\rho^2 = \rho$, have $\mu = 1$, while for any $\mu < 1$ we have a mixed state;

- the *von Neumann entropy*:

$$\mathsf{S}[\rho] = -\,\mathrm{Tr}[\rho \log \rho] = -\sum_n \lambda_n \log \lambda_n\,, \tag{1.8}$$

  where $\{\lambda_n\}_n$ are the eigenvalues of ρ, and the logarithm is typically taken in basis 2. The von Neumann entropy captures the intuitive idea that, if a system is prepared in a pure state, we have the maximum possible information, and $\mathsf{S}[\rho] = 0$; while mixed states are obtaining by tracing out some degrees of freedom of a larger system, thus ignoring the information encoded in the correlations between the portion under investigation and the rest of the universe. In this latter case, we have $0 < \mathsf{S}[\rho] \leq \log d$.

1.1.2 Postulate 2: Quantum dynamics

The second generalized postulate characterizes the dynamics of quantum states in the presence of open systems, in which case the unitary description is untenable. Within this framework, the evolution of system is described in terms of a map $\mathcal{E} : \mathcal{L}(\mathcal{H}) \to \mathcal{L}(\mathcal{H})$ that transforms a quantum state ρ into another quantum state $\mathcal{E}(\rho)$. The fundamental requirements that should be fulfilled by $\mathcal{E}$ to describe a physical operation are the following [23]:

(a) The map $\mathcal{E}$ is *positive and trace preserving*: if $\rho \geq 0$, then $\mathcal{E}(\rho) \geq 0$ and $\mathrm{Tr}[\mathcal{E}(\rho)] = \mathrm{Tr}[\rho]$, guaranteeing that the output state is a genuine quantum state satisfying Postulate 1.

(b) The map $\mathcal{E}$ is *linear*: $\mathcal{E}\left(\sum_k p_k \rho_k\right) = \sum_k p_k \mathcal{E}(\rho_k)$, such that the state obtained by applying the map to the ensemble $\{p_k, \rho_k\}_k$ is the ensemble $\{p_k, \mathcal{E}(\rho_k)\}_k$.

(c) The map $\mathcal{E}$ is *completely positive* (CP): besides satisfying positivity, the map $\mathcal{E} \otimes \hat{\mathbb{1}}_n : \mathcal{L}(\mathcal{H} \otimes \mathbb{C}^n) \to \mathcal{L}(\mathcal{H} \otimes \mathbb{C}^n)$ is also positive $\forall n \in \mathbb{N}$. This property captures the idea that the map should be preserve its physical meaning when applied to subsystems of a composite system.

Then, we have:

Postulate 2. (Dynamics) *The evolution of a quantum system is described by a map $\mathcal{E} : \mathcal{L}(\mathcal{H}) \to \mathcal{L}(\mathcal{H})$ satisfying $(\mathrm{a}) - (\mathrm{c})$, usually referred to with the terms quantum CP map, quantum operation, or quantum channel.*

The reconciliation with the usual closed system dynamics is guaranteed by Kraus theorem [26, 28].

Theorem 1.1 (Kraus, 1971). *Let $\mathcal{E} : \mathcal{L}(\mathcal{H}) \to \mathcal{L}(\mathcal{H})$ be a linear map. Then, the following are equivalent:*

- *$\mathcal{E}$ is a quantum CP map,*
- *there exists a group of operators $\{M_k\}_k \subset \mathcal{L}(\mathcal{H})$ (named Kraus operators) such that*

$$\mathcal{E}(\rho) = \sum_k M_k \rho M_k^\dagger \,, \qquad \sum_k M_k^\dagger M_k = \hat{\mathbb{1}} \,, \tag{1.9}$$

- *there exist a Hilbert space $\mathcal{H}_B$, a preparation $|\omega\rangle_B \in \mathcal{H}_B$ and a unitary operation $U \in \mathcal{L}(\mathcal{H} \otimes \mathcal{H}_B)$ such that*

$$\mathcal{E}(\rho) = \mathrm{Tr}_B\Big[U\ \rho \otimes |\omega\rangle_B\langle\omega|\ U^\dagger\Big]. \tag{1.10}$$

We note that the theorem yields two equivalent representations for the map $\mathcal{E}$. Eq. 1.9 constitutes a "local representation", the so-called Kraus representation, providing the generalization of unitary evolution in terms of a set of Kraus operators. In this framework, unitary maps are retrieved as CP maps associated with a single Kraus operator M_k. On the contrary, Eq. 1.10 is a "microscopic representation", that constructs a *unitary dilation* of $\mathcal{E}$ as the partial trace of a unitary evolution on a larger system. In particular, this construction follows from the Stinespring dilation theorem [26, 29].

1.1.3 Postulate 3: Quantum measurements

Finally, we deal with quantum measurements. As introduced before, a quantum measurement in a closed and isolated system is characterized by a complete set of orthogonal projectors $\{\mathbb{P}_x\}_x$ associated with the self-adjoint operator $X = \sum_x x\mathbb{P}_x$. Analogously to quantum maps, we now relax these requirements and highlight the minimum prescriptions that should be satisfied by quantum observables, leading to the definition of generalized measurements. In fact, we note that the Born rule in (1.3) can be rewritten as:

$$p_x = \mathrm{Tr}[\rho\,\mathbb{P}_x] = \mathrm{Tr}[\rho\,\mathbb{P}_x^2]\,. \tag{1.11}$$

In turn, the only request to let p_x be a faithful probability distribution is that $\mathbb{P}_x^2$ should be a positive operator $\Pi_x \geq 0$, satisfying the normalization condition $\sum_x \Pi_x = \hat{\mathbb{1}}$. This condition defines a generalized quantum measurement as a *positive operator-valued measure* (POVM) $\{\Pi_x\}_x$, such that $\Pi_x \geq 0$ for all x, and $\sum_x \Pi_x = \hat{\mathbb{1}}$. Moreover, due to positivity, the POVM elements Π_x can be expressed in terms of *detection operators* M_x as $\Pi_x = M_x^\dagger M_x$ [23]. In summary:

Postulate 3. (Measurements) *A generalized quantum measurement is described by a POVM, i.e. a collection $\{\Pi_x\}_x$ of positive operators $\Pi_x = M_x^\dagger M_x \geq 0$, such that $\sum_x \Pi_x = \hat{\mathbb{1}}$. Then, the Born rule and the Von Neumann reduction become:*

$$p_x = \mathrm{Tr}[\rho\,\Pi_x] \qquad \textit{and} \qquad \rho_x = \frac{1}{p_x} M_x \rho M_x^\dagger\,, \tag{1.12}$$

respectively.

Formally, the detection operators are obtained as $M_x = \sqrt{\Pi_x}$, thus representing the counterpart of the projectors $\mathbb{P}_x$ in the conventional projection-valued measures (PVMs). However, unlike PVMs, the orthogonality condition between the $\{M_x\}_x$ is not required, therefore the number of the POVM elements need not to coincide with the dimension of the Hilbert space, and can also be larger.

Similarly to Kraus theorem, one can prove that any POVM $\{\Pi_x\}$ can be brought back to a suitable PVM performed on a larger Hilbert space. This provides conciliation with the standard postulate, guaranteed by Naimark theorem [26, 30].

Theorem 1.2 (**Naimark, 1943**). *Given a generalized measurement $\{\Pi_x\}_x$ on a Hilbert space $\mathcal{H}_A$, there exist a Hilbert space $\mathcal{H}_B$, a preparation $|\omega\rangle_B \in \mathcal{H}_B$, a unitary operation $U_{AB} \in \mathcal{L}(\mathcal{H}_A \otimes \mathcal{H}_B)$ and a projective measurement $\{\mathbb{P}_x\}_x$ on $\mathcal{H}_B$ such that:*

$$p_x = \mathrm{Tr}_A[\rho\Pi_x] = \mathrm{Tr}_{AB}\Big[U_{AB}\;\rho \otimes |\omega\rangle_B\langle\omega|\;U_{AB}^\dagger\;(\hat{\mathbb{1}}_A \otimes \mathbb{P}_x)\Big]\,, \tag{1.13a}$$

$$\rho_x = \frac{1}{p_x} M_x \rho M_x^\dagger = \frac{1}{p_x}\mathrm{Tr}_B\Big[U_{AB}\;\rho \otimes |\omega\rangle_B\langle\omega|\;U_{AB}^\dagger\;(\hat{\mathbb{1}}_A \otimes \mathbb{P}_x)\Big]\,. \tag{1.13b}$$

As for the case of quantum maps, Naimark theorem provides a "microscopic representation" of a generalized quantum measurement. In fact, in practical contexts, performing a quantum measurement implies the presence of a detection apparatus, prepared into an ancillary state interacting with the quantum state of the system and, thereafter, being measured. As a matter of fact, within this description, the measured quantity may be always described by a PVM on the global Hilbert space of both the system and

the apparatus. Then, an equivalent description in terms of POVMs is obtained when tracing out the degrees of freedom of the apparatus. Conversely, any conceivable POVM is associated with a *Naimark extension*, providing a physical implementation via ancilla-based standard measurement. We also note that the possible Naimark extensions are infinite, corresponding to the intuitive idea that exists infinitely many apparatuses, with an arbitrary number of ancillary systems, to measure a physical quantity: indeed, for a given POVM element Π_x there are infinite possible detection operators M_x. For this reason, the construction reported in the statement of Naimark theorem is usually referred to as the *canonical extension* of the POVM, which does not necessarily coincide with a feasible actual implementation.

CHAPTER 2

Basics of quantum optics

In this Chapter, we present a general overview of continuous variable systems, with particular attention to quantum optical systems, that will provide the main platform for the quantum communication protocols discussed throughout the thesis. We establish the quantum description of optical electromagnetic fields, both in the Hilbert space and the quantum phase space representations, and, in particular, we focus on the Gaussian state formalism, that describes most of the optical elements being commonly exploited in the state-of-art technologies.

The structure of the Chapter is the following. In Sec. 2.1 we introduce continuous variable systems, namely physical systems described by position- and momentum-like operators that obey the canonical commutation rule. Then, Sec. 2.2 specializes the analysis to quantum optical fields, presenting the description of quantum states in both the Hilbert space and the quantum phase space. Thereafter, Gaussian states are introduced and characterized, and some relevant examples are reported. Instead, in Sec. 2.3 we discuss the quantum evolution of quantum optical states, focusing on the case of Gaussian dynamics, transforming input Gaussian states into output Gaussian states. Finally, in Sec. 2.4, we study quantum measurements of optical systems. At first, we provide a complete description of Gaussian measurement, yielding Gaussian statistics and Gaussian conditional states when performed on a Gaussian probe. Then, we present some relevant examples of non-Gaussian measurements that will be discussed in the rest of the thesis, i.e. photon-number resolving detection and weak-field homodyne detection.

2.1 Introduction to continuous variable systems

In this thesis, we deal with continuous variable systems. With this terminology, we refer to a non-relativistic degrees of freedom, each one being quantized by a pair of Hermitian position-like and momentum-like operators q and p that satisfy the canonical commutation relation (CCR):

$$[q, p] = 2i\sigma_0^2 \,, \tag{2.1}$$

where $\sigma_0 \geq 0$ is a proper multiplicative constant, whose physical meaning will be discussed thereafter. These systems require the adoption of an infinite dimensional Hilbert space, hence the terminology "quantum continuous variables". In fact, operators q and p have continuous spectrum, $q = \int_{\mathbb{R}} q \, |q\rangle\langle q|$ and $p = \int_{\mathbb{R}} p \, |p\rangle\langle p|$, with eigenvalues over the whole real line, and improper eigenstates $\{|q\rangle\}$ and $\{|p\rangle\}$ such that $\langle q_1|q_2\rangle = \delta(q_1 - q_2)$, $\langle p_1|p_2\rangle = \delta(p_1 - p_2)$, and $\langle q|p\rangle = \exp(iqp)/\sqrt{2\pi}$ [31].

Equivalently, for bosonic systems we also introduce the creation and annihilation operators:

$$a = \frac{q + ip}{2\sigma_0} \qquad \text{and} \qquad a^\dagger = \frac{q - ip}{2\sigma_0}\,, \tag{2.2}$$

effecting the creation and annihilation of energy quanta, e.g. photons, phonons, ..., of an harmonic oscillator, that obey $[a, a^\dagger] = 1$ [32]. Furthermore, the extension of the CCR to n pairs of canonical variables $\{q_j, p_j\}$, $j = 1, \ldots, n$, is straightforward, and reads $[q_j, p_k] = 2i\sigma_0^2\delta_{jk}$, or, equivalently, $[a_j, a_k] = [a_j^\dagger, a_k^\dagger] = 0$ and $[a_j, a_k^\dagger] = \delta_{jk}$, δ_{jk} being the Kronecker delta. To get a more compact notation, it is useful to introduce a vector representation of the canonical operators:

$$\hat{\mathbf{r}} = (q_1, p_1, ..., q_n, p_n)^\mathsf{T}\,, \tag{2.3}$$

and re-express the CCRs as:

$$[\hat{\mathbf{r}}, \hat{\mathbf{r}}^\mathsf{T}] = 2i\sigma_0^2\,\Omega^{(n)}\,, \tag{2.4}$$

where $[\mathbf{A}, \mathbf{B}] = \mathbf{AB} - (\mathbf{AB})^\mathsf{T}$ and $\Omega^{(n)} = \oplus_{j=1}^n \Omega$ is the n-mode symplectic form, with

$$\Omega = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}\,, \tag{2.5}$$

and $\oplus$ denoting direct sum.

2.2 Quantum states of radiation

The previous description provides theoretical modeling of a wide range of physical bosonic platforms, such as mechanical harmonic oscillators, electromagnetic field, trapped ions, ... For the purposes of this thesis, we will only focus on quantum optical platforms, in which case the canonical operators q and p represent the quantized *quadratures* of a single mode optical field at given angular frequency ω, associated with the Hamiltonian:

$$H = \hbar\omega\left(\hat{n} + \frac{1}{2}\right)\,, \tag{2.6}$$

where $\hbar$ is the reduced Planck's constant and $\hat{n} = a^\dagger a$ is the photon-number operator, revealing the number of excitation quanta (photons) of a given quantum state [31–33]. Moreover, the corresponding electric field operator $\hat{\mathbf{E}}(\mathbf{r})$ at position $\mathbf{r}$, is obtained as:

$$\hat{\mathbf{E}}(\mathbf{r}) = \mathscr{E}_0\left[a\, e^{i\mathbf{k}\cdot\mathbf{r}} + a^\dagger\, e^{-i\mathbf{k}\cdot\mathbf{r}}\right] = \frac{\mathscr{E}_0}{\sigma_0}\Big[q\,\cos(\mathbf{k}\cdot\mathbf{r}) - p\,\sin(\mathbf{k}\cdot\mathbf{r})\Big]\,, \tag{2.7}$$

where $\mathbf{k}$ is the wave-vector associated with the carrier frequency, with modulus $k = |\mathbf{k}| = \omega/c$, and $\mathscr{E}_0 = \sqrt{\hbar\omega/(2\epsilon_0 V)}$ is the so-called electric field "per single photon", in which c, ϵ_0 and V are the speed of light, the vacuum electric permittivity, and the quantization volume, respectively. If the number of modes of the field is $n > 1$, the Hamiltonian becomes $H = \sum_{j=1}^n \hbar\omega_j(\hat{n}_j + 1/2)$, $\hat{n}_j$ being the photon-number operator associated with the bosonic mode a_j [32].

Given these considerations, we present some paradigmatic examples of quantum states for optical fields.

Fock states. They are the eigenstates of the Hamiltonian (2.6), corresponding to the eigenstates of the number operator, $\{|n\rangle\}$, $n \in \mathbb{N}$, such that $\hat{n}|n\rangle = n|n\rangle$. By the spectral theorem, they form a complete orthonormal system. In particular, among Fock states, we find the *vacuum state* $|0\rangle$ such that $\hat{n}|0\rangle = 0$, for which the quadrature mean values and variances read:

$$\langle q\rangle = \langle p\rangle = 0 \qquad \text{and} \qquad \Delta^2 q = \Delta^2 p = \sigma_0^2\,, \tag{2.8}$$

revealing the physical meaning of constant σ_0^2 introduced in (2.1), namely the *zero-point fluctuations* of the field quadratures, also referred to as *vacuum fluctuations* or *shot noise variance*. In turn, the shot noise σ_0^2 provides a measurement scale to evaluate the quadrature variances of all quantum states; thus, in principle, its value can be arbitrarily chosen. Typically, there are two conventional choices: either fixing $\sigma_0^2 = 1/2$, the so-called canonical representation, or $\sigma_0^2 = 1$, corresponding to shot-noise units (SNU).

Coherent states. They are the eigenstates of the annihilation operator a, that is $a|\alpha\rangle = \alpha|\alpha\rangle$, $\alpha \in \mathbb{C}$, expanded in the Fock basis as:

$$|\alpha\rangle = e^{-\frac{|\alpha|^2}{2}} \sum_{\mathrm{n}=0}^{\infty} \frac{\alpha^n}{\sqrt{n!}}|n\rangle = D(\alpha)|0\rangle\,, \tag{2.9}$$

where $D(\alpha) = \exp(\alpha a^\dagger - \alpha^* a)$ is the *displacement operator*. Coherent states are not orthogonal with one another, since eigenstates of a non-Hermitian operator,

$$\langle\beta|\alpha\rangle = e^{-|\alpha-\beta|^2/2} e^{(\alpha\beta^* - \alpha^*\beta)/2}\,, \quad \alpha,\beta \in \mathbb{C}\,, \tag{2.10}$$

but, nevertheless, they form an overcomplete set, as:

$$\int_{\mathbb{C}} \frac{d^2\alpha}{\pi}|\alpha\rangle\langle\alpha| = \hat{\mathbb{1}}\,. \tag{2.11}$$

Moreover, these states are usually considered as *quasi* classical states, namely the quantum states that describe classical optical fields in the absence of noise. Indeed, given a coherent state with amplitude $\alpha = |\alpha|e^{i\phi}$, $0 \le \phi < 2\pi$, the expectations values of quadratures read $\langle q\rangle = 2\sigma_0|\alpha|\cos\phi$ and $\langle p\rangle = 2\sigma_0|\alpha|\sin\phi$, reproducing the behaviour of a classical harmonic oscillator, albeit exhibiting shot noise fluctuations $\Delta^2 q = \Delta^2 p = \sigma_0^2$, that become negligible in the classical limit of high-intensity fields, $|\alpha|^2 \gg \sigma_0^2$.

Thermal state. It is the mixed state describing radiation emitted by thermal sources, namely:

$$\nu^{\mathrm{th}}(\bar{n}) = \frac{1}{1+\bar{n}} \sum_{\mathrm{n}=0}^{\infty} \left(\frac{\bar{n}}{1+\bar{n}}\right)^n |n\rangle\langle n|\,, \tag{2.12}$$

$\bar{n}$ being the mean number of photons. It has null mean values of quadratures and variances larger than vacuum fluctuations, as $\Delta^2 q = \Delta^2 p = \sigma_0^2(1+2\bar{n})$.

Single-mode squeezed vacuum state. It is the state of radiation obtained from second order interaction of light within a non linear crystal of nonzero second order susceptibility, expressed as:

$$|r\rangle = S(r)|0\rangle\,, \tag{2.13}$$

where $S(r) = \exp[r(a^{\dagger 2} - a^2)/2]$ is the *single-mode squeezing operator*, $r \in \mathbb{C}$. If $r > 0$, we compute the expectation values of quadratures as $\langle q\rangle = \langle p\rangle = 0$ and:

$$\Delta^2 q = e^{2r}\sigma_0^2 \qquad \text{and} \qquad \Delta^2 p = e^{-2r}\sigma_0^2\,. \tag{2.14}$$

The name *squeezing* derives from the fact that fluctuations on p are reduced below the vacuum, at the expense of enlarging those on p above the shot-noise limit. In other words, quadrature p is *squeezed*, i.e. de-amplified, while quadrature q is *anti-squeezed*, that is amplified.

Two-mode squeezed vacuum state (TMSV). It is the paradigmatic example of a two-mode entangled state, defined as:

$$|\mathrm{TMSV}\rangle\rangle = S_2(r)|0\rangle|0\rangle = \sqrt{1-\lambda^2}\sum_{n=0}^{\infty}\lambda^n|n\rangle|n\rangle\,, \tag{2.15}$$

where $S_2(r) = \exp[r(a^\dagger b^\dagger - ab)]$ is the *two-mode squeezing operator*, acting on two modes a and b, $[a,b] = 0$, and $\lambda = \tanh r$. In the previous expression, we assumed $r \geq 0$ for the sake of simplicity. The TMSV represents the maximally entangled state at fixed mean energy, as, after performing partial trace over one mode, we retrieve a thermal state with energy $\bar{n} = \lambda^2/(1-\lambda^2)$ [33].

2.2.1 The quantum phase space description

Beside the Hilbert space description, obtained by expansion over a suitable basis, an equivalent representation of optical quantum states is obtained in the so-called *quantum phase space*. It is introduced as a bijective mapping between n-mode density operators in the Hilbert space and complex scalar function defined in $\mathbb{R}^{2n}$.

Let us consider a n-mode bosonic system, described by the bosonic operators $\mathbf{a} = (a_1, a_2, \ldots, a_n)^\mathsf{T}$, arranged in vector notation. Then, according to Glauber's formula, also referred to as Fourier-Weyl relation, any quantum state ρ can be expressed as [31, 33, 34]:

$$\rho = \int_{\mathbb{C}^n}\frac{d^2\boldsymbol{\alpha}}{\pi^n}\chi(\boldsymbol{\alpha})D_{\mathbf{a}}(\boldsymbol{\alpha})^\dagger\,, \tag{2.16}$$

where $\boldsymbol{\alpha} = (\alpha_1, \alpha_2, \ldots, \alpha_n)^\mathsf{T} \in \mathbb{C}^n$ and

$$D_{\mathbf{a}}(\boldsymbol{\alpha}) = \bigotimes_{k=1}^{n} D_{a_k}(\alpha_k)\,, \tag{2.17}$$

where $D_{a_k}(\alpha_k) = \exp(\alpha_k {a_k}^\dagger - \alpha_k^* a_k)$ is the displacement operator acting on mode a_k. Some useful properties of the displacement operator are reported below:

$$D_{\mathbf{a}}(\boldsymbol{\alpha}_1)D_{\mathbf{a}}(\boldsymbol{\alpha}_2) = D_{\mathbf{a}}(\boldsymbol{\alpha}_1 + \boldsymbol{\alpha}_2)\,, \quad \boldsymbol{\alpha}_1, \boldsymbol{\alpha}_2 \in \mathbb{C}^n\,, \tag{2.18a}$$

$$D_{\xi\mathbf{a}}(\boldsymbol{\alpha}) = D_{\mathbf{a}}(\xi\boldsymbol{\alpha})\,, \quad \xi \in \mathbb{R}\,, \tag{2.18b}$$

$$\mathrm{Tr}\left[D_{\mathbf{a}}(\boldsymbol{\alpha})\right] = \pi^n\delta^{(n)}(\boldsymbol{\alpha})\,, \tag{2.18c}$$

$\delta^{(n)}(\boldsymbol{\alpha})$ being the complex n-mode Dirac delta distribution. Moreover, for any pair of generic operators O_1 and O_2 acting on the Hilbert space $\mathcal{H}$ of n modes the *trace rule* holds:

$$\mathrm{Tr}[O_1 O_2] = \int_{\mathbb{C}^n} \frac{d^2\boldsymbol{\alpha}}{\pi^n} \chi[O_1](\boldsymbol{\alpha})\chi[O_2](-\boldsymbol{\alpha})\,, \tag{2.19}$$

$\chi[O_{1(2)}](\boldsymbol{\alpha})$ being the characteristic function of $O_{1(2)}$, respectively. As an example, for a single radiation mode a, we choose $O_1 = D(\alpha)$, with $\alpha = x + iy$, and $O_2 = q^2 = \sigma_0^2(a + a^\dagger)^2$ and obtain [35]:

$$\mathrm{Tr}\left[D(\alpha)q^2\right] = \sigma_0^2\, e^{-(x^2+y^2)/2}\left[\pi\delta^{(2)}(\alpha) + 2\pi y\delta(x)\frac{d}{dy}\delta(y) - \pi\delta(x)\frac{d^2}{dy^2}\delta(y)\right], \tag{2.20}$$

where $\delta(x)$ is the Dirac delta distribution.

Remarkably, we note that Eq. (2.16) formally represents an expansion on the set of displacement operators, which constitutes a complete basis set on the Hilbert space $\mathcal{L}(\mathcal{H})$ of the linear operators acting on $\mathcal{H}$. In turn, the coefficient:

$$\chi(\boldsymbol{\alpha}) = \mathrm{Tr}\left[\rho D_{\mathbf{a}}(\boldsymbol{\alpha})\right], \tag{2.21}$$

referred to as the *characteristic function* associated with ρ, contains all information about the quantum state. We conclude that, as anticipated before, we can study and analyze the properties of ρ by a function of n complex variables rather than a density operator in the Hilbert space.

Starting from $\chi(\boldsymbol{\alpha})$ we also introduce the generalized characteristic function, or s-ordered characteristic function [31, 33, 34]:

$$\chi_s(\boldsymbol{\alpha}) = \mathrm{Tr}\left[\rho D_{\mathbf{a}}(\boldsymbol{\alpha})\right] e^{s\boldsymbol{\alpha}^\dagger\boldsymbol{\alpha}/2}\,, \tag{2.22}$$

that satisfy the following properties:

i) $\chi_s(\mathbf{0}) = \mathrm{Tr}[\rho] = 1$;

ii) for all $j = 1, \ldots, n$ and $s = -1, 0, 1$, we have:

$$\left(\frac{\partial}{\partial\alpha_j}\right)^m \left(-\frac{\partial}{\partial\alpha_j^*}\right)^k \chi_s(\boldsymbol{\alpha})\bigg|_{\boldsymbol{\alpha}=\mathbf{0}} = \left\langle \left(a_j^\dagger\right)^m a^k \right\rangle_s\,, \tag{2.23}$$

where $\langle\cdot\rangle_s$ is the s-ordered expectation value, corresponding to anti-normal order ($s = -1$), symmetric order ($s = 0$) and normal order ($s = 1$). That is, the generalized characteristic function is the moment generating function for the state ρ.

Finally, by passing to the Fourier transform, we obtain the *quasi-probability distribution* [31, 33, 34]:

$$W_s(\boldsymbol{\alpha}) = \int_{\mathbb{C}^n} \frac{d^2\boldsymbol{\beta}}{\pi^{2n}}\, e^{(\boldsymbol{\beta}^\dagger\boldsymbol{\alpha} - \boldsymbol{\alpha}^\dagger\boldsymbol{\beta})/2}\, \chi_s(\boldsymbol{\beta})\,, \tag{2.24}$$

such that:

i) $\int_{\mathbb{C}^n} d^2\boldsymbol{\alpha}\, W_s(\boldsymbol{\alpha}) = \chi_s(\mathbf{0}) = 1$;

ii) for all $j = 1, \dots, n$ and $s = -1, 0, 1$, we have:

$$\left(\frac{\partial}{\partial \alpha_j}\right)^m \left(-\frac{\partial}{\partial \alpha_j^*}\right)^k \chi_s(\boldsymbol{\alpha})\Big|_{\boldsymbol{\alpha}=\mathbf{0}} = \int_{\mathbb{C}^n} d^2\boldsymbol{\alpha}\, (\alpha_j^*)^m \alpha_j^k\, W_s(\boldsymbol{\alpha})\,, \tag{2.25}$$

and, by integration, we retrieve all statistical moments of state ρ;

iii) for $s = 0$ the trace rule becomes:

$$\mathrm{Tr}[O_1 O_2] = \pi^n \int_{\mathbb{C}^n} d^2\boldsymbol{\alpha}\, W[O_1](\boldsymbol{\alpha}) W[O_2](\boldsymbol{\alpha})\,, \tag{2.26}$$

where we omitted the pedix 0 for convenience.

We also remark that, by performing a suitable change of variables, we can re-express all the previously introduced functions in terms of $2n$ real variables in the domain $\mathbb{R}^{2n}$, rather than n complex ones in $\mathbb{C}^n$. To this aim, we introduce a set of Cartesian variables $\mathbf{r} = (x_1, y_1; x_2, y_2; \dots; x_n, y_n)^\mathsf{T} = 2\sigma_0(\mathrm{Re}\,\alpha_1, \mathrm{Im}\,\alpha_1; \mathrm{Re}\,\alpha_2, \mathrm{Im}\,\alpha_2; \dots; \mathrm{Re}\,\alpha_n, \mathrm{Im}\,\alpha_n)^\mathsf{T} \in \mathbb{R}^{2n}$ and set:

$$\chi_s(\mathbf{r}) = \chi_s(\boldsymbol{\alpha}(\mathbf{r})) \qquad \text{and} \qquad W_s(\mathbf{r}) = \frac{1}{(4\sigma_0^2)^n} W_s(\boldsymbol{\alpha}(\mathbf{r}))\,, \tag{2.27}$$

where $\boldsymbol{\alpha}(\mathbf{r})$ denotes the re-parametrization of the complex vector $\boldsymbol{\alpha}$ in terms of the new variables, i.e. $\alpha_j = (x_j + i y_j)/2\sigma_0$, $j = 1, \dots, n$, and the pre-factor $1/(4\sigma_0^2)^n$ in the quasi-probability distribution W_s has been introduced to preserve its normalization.

Moreover, quasi-probability distributions provide useful tools to assess some relevant quantum features of the state ρ. In particular, the most common distributions refer to the values $s = -1, 0, 1$ and are presented below for the single mode case, $n = 1$.

***P*-function** ($s = 1$). If $s = 1$, the function $P(\alpha) = W_1(\alpha)$ is called P- function, or Glauber-Sudarshan function, such that for each state ρ we have:

$$\rho = \int_{\mathbb{C}} d^2\alpha\, P(\alpha)\, |\alpha\rangle\langle\alpha|\,, \tag{2.28}$$

$|\alpha\rangle$ being a coherent state. We note that, in general, $P(\alpha)$ is not a regular function. In particular, if we deal with a coherent state $\rho = |\beta\rangle\langle\beta|$, $\beta \in \mathbb{C}$, we have $P(\alpha) = \delta^{(2)}(\alpha - \beta)$; otherwise, if the state cannot be expressed as a statistical mixture of coherent states, the corresponding $P(\alpha)$ is a pathological function, being more singular than a Dirac delta. In turn, the singularity of the P-function provides a sufficient condition to assess non-classicality of quantum states.

Wigner function ($s = 0$). The function $W(\alpha) = W_0(\alpha)$ is called Wigner function, being the Fourier transform of the characteristic function $\chi(\alpha)$. It represents the conventional choice to describe quantum states in the phase space, and can be also computed as [33, 34]:

$$W(\alpha) = \frac{2}{\pi} \sum_{n=0}^{\infty} (-1)^n\, \langle n|D^\dagger(\alpha)\, \rho\, D(\alpha)|n\rangle\,. \tag{2.29}$$

$\{|n\rangle\}_n$ being the Fock basis. Moreover, in the Cartesian notation, performing integration over one of the two variables yields:

$$\int_{\mathbb{R}} dp\, W(q,p) = \langle q|\rho|q\rangle \qquad \text{and} \qquad \int_{\mathbb{R}} dq\, W(q,p) = \langle p|\rho|p\rangle\,, \tag{2.30}$$

where $|q\rangle$ and $|p\rangle$, $q, p \in \mathbb{R}$, are the improper eigenstates of the canonical operators q and p, respectively. Therefore the marginal distributions of the W-function yield the probability distributions associated with quadrature detection [33, 34]. Unlike the P-function, the Wigner function is non-singular, $W(\alpha) < \infty$, but it can get negative values. If so, the width of the Wigner negativity region in the phase space provides a measure of non-classicality [36].

***Q*-function** ($s = -1$). Finally, the function $Q(\alpha) = W_{-1}(\alpha)$ is called Q-function (or Husimi function). Its fundamental property is that:

$$Q(\alpha) = \frac{\langle\alpha|\rho|\alpha\rangle}{\pi} \geq 0\,, \tag{2.31}$$

$|\alpha\rangle$ being a coherent state. In turn, $Q(\alpha)$ is regular for all quantum states.

2.2.2 Gaussian states

Within the phase space representation, a quantum state $\rho_{\rm G}$ is a *Gaussian state* if its associated Wigner function (or, analogously, its characteristic function) is Gaussian, namely:

$$W(\mathbf{r}) = \frac{1}{(2\pi)^n\sqrt{\det(\boldsymbol{\sigma})}}\, \exp\left[-\frac{1}{2}(\mathbf{r}-\mathbf{R})^{\mathsf{T}}\,\boldsymbol{\sigma}^{-1}\,(\mathbf{r}-\mathbf{R})\right] \tag{2.32}$$

where $\mathbf{r} = (x_1, y_1, \ldots, x_n, y_n)^{\mathsf{T}} \in \mathbb{R}^{2n}$, and

$$\mathbf{R} = \mathrm{Tr}[\rho_{\rm G}\,\hat{\mathbf{r}}] \tag{2.33}$$

is the first moment vector (FM) and

$$\begin{aligned}\boldsymbol{\sigma} &= \frac{1}{2}\,\mathrm{Tr}\left[\rho_{\rm G}\left\{(\hat{\mathbf{r}}-\mathbf{R}),(\hat{\mathbf{r}}-\mathbf{R})^{\mathsf{T}}\right\}\right] \\ &= \frac{1}{2}\,\mathrm{Tr}\left[\rho_{\rm G}\left\{\hat{\mathbf{r}},\hat{\mathbf{r}}^{\mathsf{T}}\right\}\right] - \mathbf{R}\mathbf{R}^{\mathsf{T}}\end{aligned} \tag{2.34}$$

is the $2n\times 2n$ covariance matrix (CM), where $\{\mathbf{A},\mathbf{B}\} = \mathbf{AB}+(\mathbf{AB})^{\mathsf{T}}$ is the anti-commutator of $\mathbf{A}$ and $\mathbf{B}$. Thus, a Gaussian state is completely characterized by its FM and its CM. Equivalently, a Gaussian state can be expressed as a Gibbs-state of a (at most) quadratic Hamiltonian $\hat{H} = \hat{\mathbf{r}}^{\mathsf{T}}\mathbb{H}\,\hat{\mathbf{r}}/2 + \mathbf{a}^{\mathsf{T}}\hat{\mathbf{r}}$, where $\mathbb{H}$ is a $2n \times 2n$ symmetric matrix and $\mathbf{a} \in \mathbb{R}^{2n}$ is a "displacement" vector. That is:

$$\rho_{\rm G} = \frac{e^{-\beta\hat{H}}}{\mathcal{Z}}\,, \tag{2.35}$$

$\mathcal{Z} = \mathrm{Tr}[e^{-\beta\hat{H}}]$, where β is a free parameter.

The expansion of a Gaussian state $\rho_{\rm G}$ onto the Fock basis has been recently derived in [37]. To this aim, we first re-express Eq. (2.32) as:

$$W(\boldsymbol{\alpha}) = \frac{1}{\pi^n \sqrt{\det(\widetilde{\boldsymbol{\sigma}})}} \exp\left[-\frac{1}{2}(\boldsymbol{\alpha}-\boldsymbol{\beta})^\dagger\, \widetilde{\boldsymbol{\sigma}}^{-1}\, (\boldsymbol{\alpha}-\boldsymbol{\beta})\right] \tag{2.36}$$

with $\boldsymbol{\alpha} = (\alpha_1, \alpha_1^*, \ldots, \alpha_n, \alpha_n^*)^{\mathsf{T}} \in \mathbb{C}^{2n}$, and

$$\boldsymbol{\beta} = \mathbb{U}\,\mathbf{x} \quad \text{and} \quad \widetilde{\boldsymbol{\sigma}} = \mathbb{U}\,\boldsymbol{\sigma}\,\mathbb{U}^\dagger \tag{2.37}$$

where $\mathbb{U} = \oplus_{k=1}^n \mathbb{U}_1$ and

$$\mathbb{U}_1 = \frac{1}{2\sigma_0}\begin{pmatrix} 1 & i \\ 1 & -i \end{pmatrix}. \tag{2.38}$$

Thereafter, we introduce the matrices

$$\boldsymbol{\sigma}_Q = \widetilde{\boldsymbol{\sigma}} + \mathbb{1}_{2n}/2 \tag{2.39a}$$

$$\boldsymbol{A} = \boldsymbol{X}(\mathbb{1}_{2n} - \boldsymbol{\sigma}_Q^{-1}) \tag{2.39b}$$

$$\boldsymbol{\gamma}^{\mathsf{T}} = \boldsymbol{\beta}^\dagger \boldsymbol{\sigma}_Q^{-1} \tag{2.39c}$$

where $\mathbb{1}_{2n}$ is the $2n \times 2n$ identity matrix and $\boldsymbol{X} = \oplus_{s=1}^n \boldsymbol{\sigma}_x$, $\boldsymbol{\sigma}_x$ being the Pauli x-matrix. Then, the matrix element in the Fock basis $\rho_{\boldsymbol{mk}} = \langle \boldsymbol{m}|\rho|\boldsymbol{k}\rangle$, $|\boldsymbol{k}\rangle = |k_1\, k_2\, \ldots k_n\rangle$ and $|\boldsymbol{m}\rangle = |m_1\, m_2\, \ldots m_n\rangle$, reads:

$$\rho_{\boldsymbol{mk}} = T_{\boldsymbol{mk}} \prod_{s=1}^n \left(\frac{\partial}{\partial \alpha_s}\right)^{k_s} \left(\frac{\partial}{\partial \alpha_s^*}\right)^{m_s} \exp\left(\frac{1}{2}\boldsymbol{\alpha}^{\mathsf{T}}\boldsymbol{A}\boldsymbol{\alpha} + \boldsymbol{\gamma}^{\mathsf{T}}\boldsymbol{\alpha}\right)\Big|_{\boldsymbol{\alpha}=0} \tag{2.40}$$

where

$$T_{\boldsymbol{mk}} = \frac{1}{\sqrt{\det(\boldsymbol{\sigma}_Q)\prod_{s=1}^n k_s! m_s!}} \exp\left(-\frac{1}{2}\boldsymbol{\beta}^\dagger \boldsymbol{\sigma}_Q^{-1}\boldsymbol{\beta}\right). \tag{2.41}$$

We now list some fundamental properties of Gaussian states that will be helpful throughout the thesis:

- *Tensor products of Gaussian states are Gaussian.* That is, given two Gaussian states $\rho_A(B)$ with FM $\mathbf{R}_{A(B)}$ and CM $\boldsymbol{\sigma}_{A(B)}$, respectively, the bipartite state $\rho = \rho_A \otimes \rho_B$ is Gaussian with FM $\mathbf{R} = \mathbf{R}_A \oplus \mathbf{R}_B$ and CM $\boldsymbol{\sigma} = \boldsymbol{\sigma}_A \oplus \boldsymbol{\sigma}_B$.

- *The partial trace of a Gaussian state is Gaussian.* We consider a generic bipartite Gaussian state ρ_{AB}, with FM and CM:

$$\mathbf{R} = \begin{pmatrix} \mathbf{R}_A \\ \mathbf{R}_B \end{pmatrix}, \qquad \boldsymbol{\sigma} = \begin{pmatrix} \boldsymbol{\sigma}_A & \boldsymbol{\sigma}_{AB} \\ \boldsymbol{\sigma}_{AB} & \boldsymbol{\sigma}_B \end{pmatrix}. \tag{2.42}$$

  Then, $\rho_{A(B)} = \mathrm{Tr}_{B(A)}[\rho_{AB}]$ is still Gaussian with FM $\mathbf{R}_{A(B)}$ and covariance $\boldsymbol{\sigma}_{A(B)}$, that is the sub-blocks associated with subsystem $A(B)$ in $\mathbf{R}$ and $\boldsymbol{\sigma}$.

- *The purity and the von Neumann entropy of a Gaussian state only depend on its CM.* The purity of a Gaussian state $\rho_{\rm G}$, with CM $\boldsymbol{\sigma}$, is retrieved as:

$$\mu[\rho_{\rm G}] = {\rm Tr}[\rho_{\rm G}^2] = \frac{(\sigma_0^2)^n}{\sqrt{\det(\boldsymbol{\sigma})}}\,, \tag{2.43}$$

whereas its von Neumann entropy $S[\rho_{\rm G}] = -\,{\rm Tr}[\rho_{\rm G}\log_2\rho_{\rm G}]$ reads:

$$S\left[\rho_{\rm G}\right] = \sum_{j=1}^{n} h\left(\frac{{\rm d}_j/\sigma_0^2 - 1}{2}\right)\,, \tag{2.44}$$

where $h(x) = (x+1)\log_2(x+1) - x\log_2 x$, and $\{{\rm d}_j\}_j$ are the n symplectic eigenvalues of $\boldsymbol{\sigma}$, i.e. the positive eigenvalues of the $2n\times 2n$ matrix $i\Omega^{(n)}\boldsymbol{\sigma}$ [31, 33]. Closed expressions for the symplectic eigenvalues are available for systems of $n = 1, 2$ modes. In particular, for $n = 1$, we have ${\rm d}_1 = \sqrt{\det(\boldsymbol{\sigma})}$, whereas for $n = 2$ we express the CM in block form as in Eq. (2.42) and obtain:

$${\rm d}_{1(2)} = \sqrt{\frac{\Delta \pm \sqrt{\Delta^2 - 4I_4}}{2}}\,, \tag{2.45}$$

with $I_{1(2)} = \det(\boldsymbol{\sigma}_{A(B)})$, $I_3 = \det(\boldsymbol{\sigma}_{AB})$, $I_4 = \det(\boldsymbol{\sigma})$ and $\Delta = I_1 + I_2 + 2I_3$.

We now present some common examples of Gaussian states. Moreover, for single-mode states it is also possible to provide a graphical phase space representation, depicted in Fig. 2.2.1, obtained as the contour plot of the Wigner function $W(q,p)$ at the height of variances.

First of all, the vacuum $|0\rangle$ is a Gaussian state with $\mathbf{R} = \mathbf{0}$ and $\boldsymbol{\sigma} = \sigma_0^2\mathbb{1}_2$, being represented in the phase space as a circle with radius σ_0 centered in the origin, see Fig. 2.2.1(a). Also coherent states $|\alpha\rangle = D(\alpha)|0\rangle$ are Gaussian, with $\mathbf{R} = 2\sigma_0(\mathrm{Re}\,\alpha, \mathrm{Im}\,\alpha)$ and $\boldsymbol{\sigma} = \sigma_0^2\mathbb{1}_2$; thus the displacement operator acts as a translation in the phase space, see Fig. 2.2.1(b). Thermal states are Gaussian, with null FM and $\boldsymbol{\sigma} = \sigma_0^2(1+2\bar{n})$, see Fig. 2.2.1(c), being, therefore, represented as a circle with a bigger radius than the vacuum. Finally, the single-mode squeezed state is Gaussian, with null FM and CM

$$\boldsymbol{\sigma} = \sigma_0^2\begin{pmatrix} e^{2r} & 0 \\ 0 & e^{-2r}\end{pmatrix}\,, \tag{2.46}$$

where we assume $r \geq 0$: that is, the squeezing operator acts as a dilatation of the q-axis and a compression of the p axis, deforming the vacuum circle into an ellipse of bigger semi-axis equals to $e^r\sigma_0$ and smaller semi-axis $e^{-r}\sigma_0$, see Fig. 2.2.1(d). In the more general case $r = |r|e^{i\psi}$, the ellipse is rotated by an angle $\psi/2$. We also note that, starting from these basic examples, it is possible to reconstruct all single-mode Gaussian state. In fact, by the former definition of Gaussian states of Eq. 2.35, it follows that a generic single mode Gaussian state can always be written as a displaced squeezed thermal state $\rho_{\rm G} = D(\alpha)S(r)\nu^{\rm th}(\bar{n})S^\dagger(r)D^\dagger(\alpha)$, for some parameters $\alpha, r\in\mathbb{C}$ and $\bar{n}\geq 0$.

Finally, within the class two-mode states, the typical example of Gaussian state is the TMSV, having null FM and CM:

$$\boldsymbol{\sigma} = \sigma_0^2\begin{pmatrix} V\,\mathbb{1}_2 & Z\,\boldsymbol{\sigma}_z \\ Z\,\boldsymbol{\sigma}_z & V\,\mathbb{1}_2\end{pmatrix}\,, \tag{2.47}$$

where $V = \cosh(2r) = (1+\lambda^2)/(1-\lambda^2)$ is the so-called quadrature variance, $Z = \sinh(2r) = \sqrt{V^2-1}$ is the correlation term, and $\boldsymbol{\sigma}_z$ is the Pauli z-matrix.

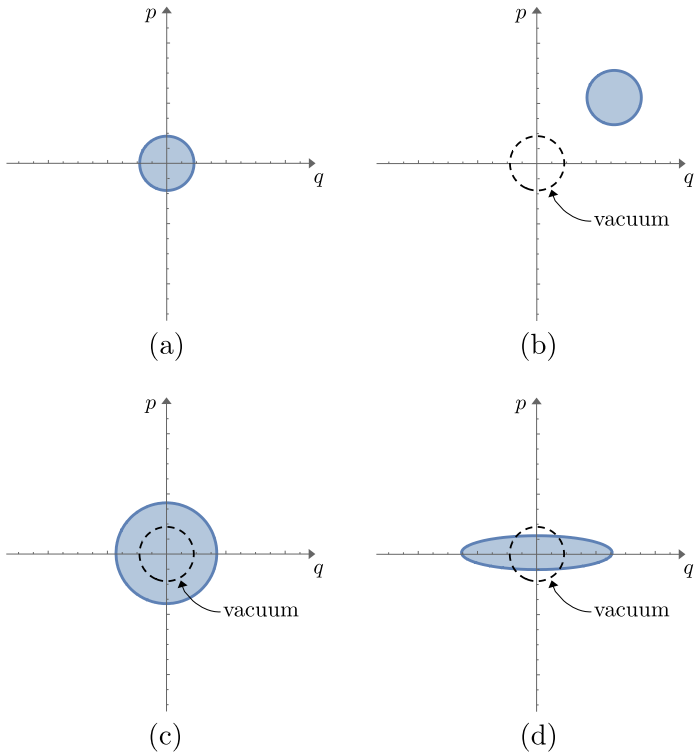


Figure 2.2.1: Phase space representation of Gaussian states: the vacuum $|0\rangle$ (a), a coherent state $|\alpha\rangle$ (b), $\alpha \in \mathbb{C}$, a thermal state $\nu^{\mathrm{th}}(\bar{n})$ (c), and a single-mode squeezed vacuum state $|r\rangle$, $r > 0$ (d).

2.3 Quantum evolution of optical states

The dynamics of a quantum optical system follows the prescriptions outlined in the previous Chapter. That is, in the presence of a closed system, we have a unitary dynamics governed by a self-adjoint Hamiltonian operator $\hat{H}$ through the Schrödinger evolution $d\rho/dt = -i[\hat{H}, \rho]$, where we adopted the natural units, $\hbar = 1$. Otherwise, open quantum dynamics are modeled by a suitable quantum master equation for the density operator ρ, obtained from a Hamiltonian dynamics over a larger system, that includes an environment, being, ultimately, traced out [26, 31]. Under proper dynamical assumptions, we retrieve a time-local master equation in the Lindblad form:

$$\frac{d\rho}{dt} = \gamma \sum_j \mathcal{L}[A_j]\,\rho\,, \tag{2.48}$$

where γ is a decoherence rate and $\mathcal{L}[A]\rho = A\rho A^\dagger - \{A^\dagger A, \rho\}/2$, $\mathcal{L}[A]$ being the so-called Lindblad superoperator [26].

In the following, we mainly focus on the special case of Gaussian dynamics, in which situation the theoretical description is rather simplified.

2.3.1 Gaussian dynamics

The class of Gaussian dynamics refers to evolutions of quantum states that preserve Gaussianity, namely mapping Gaussian states into Gaussian states. This corresponds either to unitary evolutions of closed systems associated with linear or bilinear Hamiltonian operators, or suitable master equations modeling quadratic interaction of an open system with a Gaussian environment [31, 33]. Since Gaussian states are completely characterized by first and second moments, we wonder to describe the dynamics in the phase space by introducing suitable transformation laws for the FM and the CM. In more detail, if $\rho_{\rm in(out)}$ is the initial (evolved) state, with FM $\mathbf{R}_{\rm in(out)}$ and CM $\boldsymbol{\sigma}_{\rm in(out)}$, the task is to determine transformation rules mapping $\mathbf{R}_{\rm in} \to \mathbf{R}_{\rm out}$ and $\boldsymbol{\sigma}_{\rm in} \to \boldsymbol{\sigma}_{\rm out}$. We consider both unitary and CP evolutions.

In the case of closed systems, a Gaussian evolution is a unitary evolution generated by linear or quadratic Hamiltonian $\hat{H}$. If $\hat{H}$ is linear, $\hat{H} = \mathbf{a}^{\mathsf{T}}\hat{\mathbf{r}}$, then the modes evolution reads [31, 33]:

$$\hat{\mathbf{r}}_{\rm out} = \hat{\mathbf{r}}_{\rm in} + \mathbf{d}\,, \tag{2.49}$$

with $\mathbf{d} = \Omega^{(n)}\mathbf{a}\,t$, t being the duration of the time evolution. That is, the unitary operator $\hat{U} = \exp(-i\hat{H}t)$ takes the form of a displacement operator, and, accordingly:

$$\mathbf{R}_{\rm out} = \mathbf{R}_{\rm in} + \mathbf{d} \qquad \text{and} \qquad \boldsymbol{\sigma}_{\rm out} = \boldsymbol{\sigma}_{\rm in}\,. \tag{2.50}$$

Othwerwise, if the Hamiltonian $\hat{H}$ is quadratic, namely in the form $\hat{H} = \hat{\mathbf{r}}^{\mathsf{T}}\,\mathbb{H}\,\hat{\mathbf{r}}/2$, then:

$$\hat{\mathbf{r}}_{\rm out} = e^{i\hat{H}t}\,\hat{\mathbf{r}}_{\rm in}\,e^{-i\hat{H}t} = S\,\hat{\mathbf{r}}_{\rm in}\,, \tag{2.51}$$

where $S = \exp[\Omega^{(n)}\mathbb{H}\,t]$ is a $2n \times 2n$ symplectic matrix, satisfying the fundamental property [31, 33]:

$$S\,\Omega^{(n)}\,S^{\mathsf{T}} = \Omega^{(n)}\,. \tag{2.52}$$

Then, the output first and second moments read:

$$\mathbf{R}_{\rm out} = S\,\mathbf{R}_{\rm in} \qquad \text{and} \qquad \boldsymbol{\sigma}_{\rm out} = S\,\boldsymbol{\sigma}_{\rm in}\,S^{\mathsf{T}}\,, \tag{2.53}$$

and the unitary evolution associated with $\hat{H}$ corresponds to a symplectic evolution of FM and CM under matrix S.

Finally, we present some examples of symplectic matrices associated with commonly encountered transformations.

- *Phase shift.* A phase shift is a single mode evolution associated with the unitary operator $U_\theta = \exp[-i\theta a^\dagger a]$. Its associated symplectic matrix is a rotation matrix of angle θ:

$$S = \begin{pmatrix} \cos\theta & \sin\theta \\ -\sin\theta & \cos\theta \end{pmatrix}. \tag{2.54}$$

- *Single-mode squeezing.* As introduced before, the single-mode squeezing evolution corresponds to the operator $S(r) = \exp[r(a^{\dagger 2} - a^2)/2]$. If $r > 0$, the associated symplectic matrix is:

$$S = \begin{pmatrix} e^r & 0 \\ 0 & e^{-r} \end{pmatrix}. \tag{2.55}$$

- *Beam splitter.* The beam splitter acts as a two-mode mixing evolution, mapping two input modes a and b, into two output ports, associated with modes c and d. It corresponds to the unitary operator $U_{\rm BS} = \exp[\theta\,(a^\dagger b - a b^\dagger)]$, such that $\cos^2\theta = T \leq 1$ is the beam splitter trasmissivity. The symplectic matrix is the 4×4 matrix:

$$S = \begin{pmatrix} \sqrt{T}\,\mathbb{1}_2 & \sqrt{1-T}\,\mathbb{1}_2 \\ -\sqrt{1-T}\,\mathbb{1}_2 & \sqrt{T}\,\mathbb{1}_2 \end{pmatrix}. \tag{2.56}$$

  Accordingly, the input-output relations read:

$$c = U_{\rm BS}^\dagger\, a\, U_{\rm BS} = \sqrt{T}\,a + \sqrt{1-T}\,b\,, \tag{2.57a}$$

$$d = U_{\rm BS}^\dagger\, b\, U_{\rm BS} = \sqrt{T}\,b - \sqrt{1-T}\,a\,. \tag{2.57b}$$

- *Two-mode squeezing.* The two-mode squeezing operator $S_2(r) = \exp[r(a^\dagger b^\dagger - ab)]$ generates a Gaussian dynamics associated with the 4×4 symplectic matrix:

$$S = \begin{pmatrix} \cosh(r)\,\mathbb{1}_2 & \sinh(r)\,\boldsymbol{\sigma}_z \\ \sinh(r)\,\boldsymbol{\sigma}_z & \cosh(r)\,\mathbb{1}_2 \end{pmatrix}, \tag{2.58}$$

  where we assumed $r \geq 0$. The input-output relations are the following:

$$c = S_2(r)^\dagger\, a\, S_2(r) = \cosh(r)\,a + \sinh(r)\,b^\dagger\,, \tag{2.59a}$$

$$d = S_2(r)^\dagger\, b\, S_2(r) = \cosh(r)\,b + \sinh(r)\,a^\dagger\,. \tag{2.59b}$$

In the opposite scenario of an open system, the Gaussian evolution of quantum states is provided by a suitable CP map, describing quadratic interaction with an environment prepared in a Gaussian state, and thereafter being traced out. Accordingly, following Kraus theorem, any open Gaussian dynamics can be retrieved as a symplectic joint evolution of system and environment. In more detail, if $\hat{\mathbf{r}}_{\rm in}$ and $\hat{\mathbf{r}}_{\rm in}^{(E)}$ are the input quadrature operator vectors of system and environment, respectively, and the environment is prepared in a Gaussian state with null FM and CM $\boldsymbol{\sigma}_{\rm in}^{(E)}$, there exists a symplectic matrix S, in the form:

$$S = \begin{pmatrix} X & B \\ C & D \end{pmatrix} , \tag{2.60}$$

such that

$$\begin{pmatrix} \hat{\mathbf{r}}_{\rm out} \\ \hat{\mathbf{r}}_{\rm out}^{(E)} \end{pmatrix} = S \begin{pmatrix} \hat{\mathbf{r}}_{\rm in} \\ \hat{\mathbf{r}}_{\rm in}^{(E)} \end{pmatrix} . \tag{2.61}$$

In turn, the input output relation for the system becomes:

$$\hat{\mathbf{r}}_{\rm out} = X\,\hat{\mathbf{r}}_{\rm in} + B\,\hat{\mathbf{r}}_{\rm in}^{(E)} , \tag{2.62}$$

and we obtain the FM and CM transformation rule as:

$$\mathbf{R}_{\rm out} = X\mathbf{R}_{\rm in} \qquad \text{and} \qquad \boldsymbol{\sigma}_{\rm out} = X\boldsymbol{\sigma}_{\rm in}X^{\mathsf{T}} + Y , \tag{2.63}$$

with $Y = B\,\boldsymbol{\sigma}_{\rm in}^{(E)}\,B^{\mathsf{T}}$.

In summary, a Gaussian CP map is defined by two $2n \times 2n$ matrices X and Y such that:

i) $\mathbf{R}_{\rm out} = X\mathbf{R}_{\rm in}$,

ii) $\boldsymbol{\sigma}_{\rm out} = X\boldsymbol{\sigma}_{\rm in}X^{\mathsf{T}} + Y$,

iii) $Y + i\sigma_0^2\Omega^{(n)} \geq i\sigma_0^2 X\Omega^{(n)}X^{\mathsf{T}}$,

where condition iii) guarantees that the additive noise matrix Ypreserves Heisenberg's uncertainty relations for the output state. In the particular case of X being a symplectic matrix and $Y = 0$, we regain the usual unitary evolution.

A paradigmatic example of a Gaussian CP map is the *thermal-loss channel*, corresponding to the loss master equation in the presence of a thermal bath:

$$\frac{d\rho}{dt} = \gamma(\bar{n}+1)\,\mathcal{L}[a]\,\rho + \gamma\bar{n}\,\mathcal{L}[a^\dagger]\,\rho , \tag{2.64}$$

wehre γ is the system-bath coupling rate and $\bar{n}$ is the mean number of photons of the bath. The resulting dynamics is equivalent to a Gaussian CP map associated with the matrices [31]:

$$X = \sqrt{T}\,\mathbb{1}_2 \quad \text{and} \quad Y = (1-T)(1+2\bar{n})\mathbb{1}_2 , \tag{2.65}$$

$\mathbb{1}_2$ being the 2×2 identity matrix, in which $T = \exp(-\gamma t) \leq 1$ is the channel transmissivity.

2.4 Quantum measurements of optical states

In this section, we conclude the presentation of the fundamental aspects of quantum optics by discussing the main examples of quantum measurements, i.e. POVMs, that can be implemented. First of all, we provide characterization of Gaussian measurements, such that, if performed on a Gaussian state, yield a Gaussian probability distribution and a Gaussian conditional state, and, subsequently, we present some relevant non-Gaussian schemes, based on photo-detection.

2.4.1 Gaussian measurements

Formally, with the term Gaussian measurement, we refer to a continuous-valued POVM $\{\Pi_{\mathbf{r}_\mathrm{m}}\}$, $\mathbf{r}_\mathrm{m} \in \mathbb{R}^{2n}$, whose elements $\Pi_{\mathbf{r}_\mathrm{m}}$ are associated with a Gaussian Wigner function:

$$W[\Pi_{\mathbf{r}_\mathrm{m}}](\mathbf{r}) = \frac{1}{(4\pi\sigma_0^2)^n} \frac{1}{(2\pi)^n \sqrt{\det(\boldsymbol{\sigma}_\mathrm{m})}} \exp\left[-\frac{1}{2}(\mathbf{r}-\mathbf{r}_\mathrm{m})^\intercal \boldsymbol{\sigma}_\mathrm{m}{}^{-1} (\mathbf{r}-\mathbf{r}_\mathrm{m})\right], \tag{2.66}$$

where $\mathbf{r}_\mathrm{m}$ is the outcome of the measurement and $\boldsymbol{\sigma}_\mathrm{m}$ is the so-called "covariance matrix of the measurement", being characteristic of the particular measurement performed. We also note that, unlike quantum states, the function $W[\Pi_{\mathbf{r}_\mathrm{m}}](\mathbf{r})$ is not normalized, as the POVM elements constitute a resolution of the identity, $\int d\mathbf{r}_\mathrm{m} \Pi_{\mathbf{r}_\mathrm{m}} = \hat{\mathbb{1}}$. In fact:

$$\begin{aligned} &\int_{\mathbb{R}^{2n}} d\mathbf{r}_\mathrm{m}\, W[\Pi_{\mathbf{r}_\mathrm{m}}](\mathbf{r}) = W\left[\int_{\mathbb{R}^{2n}} d\mathbf{r}_\mathrm{m} \Pi_{\mathbf{r}_\mathrm{m}}\right](\mathbf{r}) \\ &= W[\hat{\mathbb{1}}](\mathbf{r}) = \frac{1}{(4\pi\sigma_0^2)^n}, \end{aligned} \tag{2.67}$$

where we exploited the linearity of Wigner functions. Then, by applying the trace rule (2.26), when a Gaussian measurement is performed on a Gaussian state ρ_G with FM $\mathbf{R}$ and CM $\boldsymbol{\sigma}$, the probability of retrieving outcome $\mathbf{r}_\mathrm{m}$ reads:

$$p(\mathbf{r}_\mathrm{m}) = \mathrm{Tr}[\rho_\mathrm{G}\, \Pi_{\mathbf{r}_\mathrm{m}}] = (4\pi\sigma_0^2)^n \int_{\mathbb{R}^{2n}} d\mathbf{r}\, W[\rho_\mathrm{G}](\mathbf{r}) W[\Pi_{\mathbf{r}_\mathrm{m}}](\mathbf{r}) \tag{2.68}$$

$$= \frac{1}{(2\pi)^n \sqrt{\det(\boldsymbol{\sigma}+\boldsymbol{\sigma}_\mathrm{m})}} \times \exp\left[-\frac{1}{2}(\mathbf{r}_\mathrm{m}-\mathbf{R})^\intercal (\boldsymbol{\sigma}+\boldsymbol{\sigma}_\mathrm{m})^{-1} (\mathbf{r}_\mathrm{m}-\mathbf{R})\right]. \tag{2.69}$$

That is, the outcomes of the Gaussian measurement are Gaussian distributed, with average value $\mathbf{R}$ and covariance $\boldsymbol{\sigma}+\boldsymbol{\sigma}_\mathrm{m}$.

Finally, we also discuss the case of conditional measurements, that will be often encountered throughout the thesis. We consider a bipartite system AB, where subsystems A and B are composed of n_A an n_B modes, respectively. In the vector notation we have $\mathbf{a} = (\mathbf{a}_A, \mathbf{a}_B)$. We consider a bipartite quantum state ρ_{AB} with characteristic functions $\chi_{AB}(\boldsymbol{\alpha}) = \chi_{AB}(\boldsymbol{\alpha}_A, \boldsymbol{\alpha}_B)$. We now perform a quantum measurement on subsystem B, described my means of the positive-operator-valued measurement (POVM) $\{\Pi_{\mathbf{r}_\mathrm{m}}\}_{\mathbf{r}_\mathrm{m}}$, whose elements are associated with the characteristic function $\chi_{\mathbf{r}_\mathrm{m}}(\boldsymbol{\alpha}_B)$. By applying

the trace rule, the conditional state on A reads:

$$\begin{aligned}\rho_{A|\mathbf{r}_\mathrm{m}} &= \frac{1}{p(\mathbf{r}_\mathrm{m})}\,\mathrm{Tr}_B\left[\rho_{AB}\big(\mathbb{1}_A\otimes\Pi_{\mathbf{r}_\mathrm{m}}\big)\right]\\ &= \frac{1}{p(\mathbf{r}_\mathrm{m})}\int\frac{d^2\boldsymbol{\alpha}_A}{\pi^{n_A}}\,\chi_{A|\mathbf{r}_\mathrm{m}}(\boldsymbol{\alpha}_A)\,D_{\mathbf{a}_A}(\boldsymbol{\alpha}_A)^\dagger\,,\end{aligned}\tag{2.70}$$

where:

$$\chi_{A|\mathbf{r}_\mathrm{m}}(\boldsymbol{\alpha}_A)=\int\frac{d^2\boldsymbol{\alpha}_B}{\pi^{n_B}}\,\chi_{AB}(\boldsymbol{\alpha}_A,\boldsymbol{\alpha}_B)\,\chi_{\mathbf{r}_\mathrm{m}}(-\boldsymbol{\alpha}_B)\,,\tag{2.71}$$

and $p(\mathbf{r}_\mathrm{m})$ is the detection probability:

$$\begin{aligned}p(\mathbf{r}_\mathrm{m}) &= \mathrm{Tr}_{AB}\left[\rho_{AB}\big(\mathbb{1}_A\otimes\Pi_{\mathbf{r}_\mathrm{m}}\big)\right]\\ &= \mathrm{Tr}_A\left[\int\frac{d^2\boldsymbol{\alpha}_A}{\pi^{n_A}}\,\chi_{A|\mathbf{r}_\mathrm{m}}(\boldsymbol{\alpha}_A)\,D_{\mathbf{a}_A}\right]=\chi_{A|\mathbf{r}_\mathrm{m}}(\mathbf{0})\,.\end{aligned}\tag{2.72}$$

An interesting result is obtained for Gaussian states and Gaussian measurements. We now assume ρ_{AB} to be a Gaussian state with FM $\mathbf{R}=(\mathbf{R}_A,\mathbf{R}_B)$ and CM (written in block form)

$$\boldsymbol{\sigma}=\begin{pmatrix}\boldsymbol{\sigma}_A & \boldsymbol{\sigma}_Z\\ \boldsymbol{\sigma}_Z^\mathsf{T} & \boldsymbol{\sigma}_B\end{pmatrix}.\tag{2.73}$$

Moreover, we consider a Gaussian POVM $\{\Pi_{\mathbf{r}_\mathrm{m}}\}_{\mathbf{r}_\mathrm{m}}$, with CM $\boldsymbol{\sigma}_\mathrm{m}$. Then, the conditional state $\rho_{A|\mathbf{r}_\mathrm{m}}$ is still a Gaussian state with CM $\boldsymbol{\sigma}_{A|\mathbf{r}_\mathrm{m}}$ and FM $\mathbf{R}_{A|\mathbf{r}_\mathrm{m}}$ given by [31, 33, 34]:

$$\boldsymbol{\sigma}_{A|\mathbf{r}_\mathrm{m}}=\boldsymbol{\sigma}_A-\boldsymbol{\sigma}_Z(\boldsymbol{\sigma}_B+\boldsymbol{\sigma}_\mathrm{m})^{-1}\boldsymbol{\sigma}_Z^\mathsf{T}\,,\tag{2.74}$$

and

$$\mathbf{R}_{A|\mathbf{r}_\mathrm{m}}=\mathbf{R}_A+\boldsymbol{\sigma}_Z(\boldsymbol{\sigma}_B+\boldsymbol{\sigma}_\mathrm{m})^{-1}(\mathbf{r}_\mathrm{m}-\mathbf{R}_B)\,,\tag{2.75}$$

respectively.

2.4.1.1 Homodyne and double-homodyne detection

Typical examples of Gaussian measurements are the so-called *coherent detection schemes*, corresponding to homodyne and double-homodyne measurements. The name "coherent" arises from the fact that, in experimental implementations, a strong local oscillator is let impinge with the incoming optical signal, which implies the two fields to be perfectly phase-matched in both the spatial and temporal domain.

To begin with, we introduce the *homodyne measurement*. With this term, we refer to measurement of one of the field quadratures:

$$x_\phi=\cos\phi\,q+\sin\phi\,p=\sigma_0\left(ae^{-i\phi}+a^\dagger e^{i\phi}\right)\,,\tag{2.76}$$

$0\le\phi<\pi$. In turn, homodyne detection is described as a conventional projective measurement over the eigenstates of x_ϕ, namely $\Pi_{x_\phi}=|x_\phi\rangle\langle x_\phi|$, and the probability of obtaining outcome x from state ρ reads $P(x)=\langle x_\phi|\rho|x_\phi\rangle$.

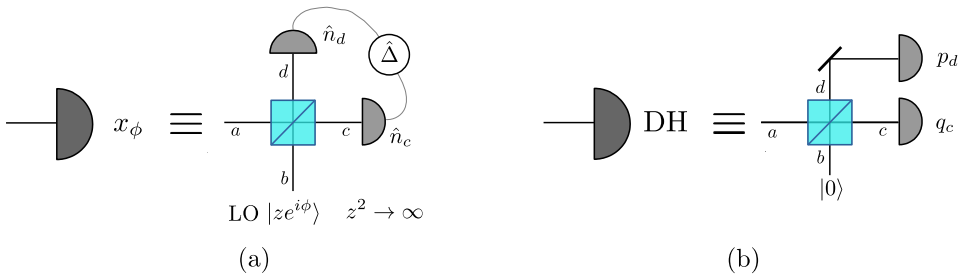


Figure 2.4.1: (a) Setup of homodyne detection of quadrature $x_\phi = \cos\phi\, q + \sin\phi\, p$. The signal interferes with a high-intensity LO $|ze^{i\phi}\rangle$ at a balanced beam splitter, with $z^2 \to \infty$; thereafter, photon-number detection is performed on both branches and the difference photocurrent $\hat{\Delta}$ is considered. (b) Setup of double homodyne (DH) detection. The incoming signal is divided into two parts at a balanced beam splitter, on which joint homodyne measurement of both quadratures q_c and p_d is performed.

Remarkably, homodyne is a Gaussian measurement, associated with the CM:

$$\boldsymbol{\sigma}_{\rm m} = \sigma_0^2 \lim_{z\to 0} \left\{ \mathcal{R}_\phi \begin{pmatrix} z & 0 \\ 0 & \frac{1}{z} \end{pmatrix} \mathcal{R}_\phi^{\mathsf{T}} \right\} , \tag{2.77}$$

where $\mathcal{R}_\phi$ is a rotation matrix of angle ϕ:

$$\mathcal{R}_\phi = \begin{pmatrix} \cos\phi & \sin\phi \\ -\sin\phi & \cos\phi \end{pmatrix} . \tag{2.78}$$

The practical implementation is achieved by the scheme reported in Fig. 2.4.1(a). At first, the incoming signal is mixed at a balanced beam splitter, with transmissivity $T = 1/2$, with a local oscillator (LO) excited in the coherent state $|ze^{i\phi}\rangle$, $z > 0$; thereafter photon-number detection is performed on both the output beams [38]. At the quantum limit, we describe the input optical modes associated with signal and LO by two bosonic operator a and b, respectively, while performing photon-number detection on the output modes c and d corresponds to measure the two Hermitian operators $\hat{n}_c = c^\dagger c$ and $\hat{n}_d = d^\dagger d$. Ultimately, we evaluate the difference photocurrent $\hat{\Delta} = \hat{n}_c - \hat{n}_d$. In the Heisenberg picture, namely by applying the modes transformations at a balanced beam splitter $a \to c = (a+b)/\sqrt{2}$ and $b \to d = (b-a)/\sqrt{2}$, we have [39]:

$$\hat{\Delta} = ab^\dagger + a^\dagger b\,. \tag{2.79}$$

Therefore, considering the state $|ze^{i\phi}\rangle$ of the LO as fixed, we have:

$$\langle ze^{i\phi}|\hat{\Delta}|ze^{i\phi}\rangle = \frac{z}{\sigma_0}\left(ae^{-i\phi} + a^\dagger e^{i\phi}\right) = \frac{z}{\sigma_0}\, x_\phi\,. \tag{2.80}$$

In turn, measuring the rescaled photocurrent $\hat{\Delta}/(z\sigma_0)$ may provide an indirect measurement of the quadratures of the input field. If we compute, however, the expectation value of $\hat{\Delta}^n$ we have:

$$\frac{\langle ze^{i\phi}|\hat{\Delta}^n|ze^{i\phi}\rangle}{(z/\sigma_0)^n} = x_\phi^n + \gamma_\phi^{(n)}(a, a^\dagger; z)\,, \tag{2.81}$$

where $\gamma_\phi^{(n)}(a,a^\dagger;z)$ is a function of both the field operators a and $a^\dagger$ and the LO intensity, to be explicitly calculated; for instance, $\gamma_\phi^{(1)}(a,a^\dagger;z)=0$, $\gamma_\phi^{(2)}(a,a^\dagger;z)=a^\dagger a/(z/\sigma_0)^2$, $\gamma_\phi^{(3)}(a,a^\dagger;z)=(3a^\dagger x_\phi\, a+x_\phi)/(z/\sigma_0)^2$ and

$$\gamma_\phi^{(4)}(a,a^\dagger)=\frac{3(a^\dagger)^2a^2+a^\dagger a}{(z/\sigma_0)^4}+\frac{6a^\dagger x_\phi^2\, a+4(x_\phi^2-1)+1}{(z/\sigma_0)^2}\,. \tag{2.82}$$

Therefore, it is clear that the actual measurement of the quadrature is achieved only in the limit $z^2\to\infty$ in which the measurement of the moments $(\hat{\Delta}/z)^n$ corresponds to measure x_ϕ^n [40]. Moreover, in practical realizations, in the presence of high LO, photon-number measurement is implemented by p-i-n photodiodes, namely photodetectors generating macroscopic photocurrents proportional to the intensity of the incoming light.

The homodyne measurement allows us to retrieve information on a single field quadrature, raising the question to design a scheme for the joint detection of the two canonical quadratures q and p. This task is not straightforward, as $[q,p]=2i\sigma_0^2$, therefore q and p cannot be jointly measured with maximum precision, according to Heisenberg's uncertainty principle. However, this kind of measurement can be realized in terms of a POVM, referred to as *double-homodyne* (DH) measurement.

Formally, DH detection is described as a 1-rank (non-orthogonal) projection on coherent states, with associated POVM:

$$\Pi_{q,p}=\frac{|\zeta_{q,p}\rangle\langle\zeta_{q,p}|}{2\pi\sigma_0^2}\,, \tag{2.83}$$

where $|\zeta_{q,p}\rangle$ is a coherent state with amplitude $\zeta_{q,p}=(q+ip)/2\sigma_0$, such that $\int dqdp\,\Pi_{q,p}=\hat{\mathbb{1}}$. The corresponding probability distribution is $P(q,p)=\langle\zeta_{q,p}|\rho|\zeta_{q,p}\rangle/2\pi\sigma_0^2=Q(q,p)$, that is the Husimi Q-function; whilst the CM of the measurement is $\boldsymbol{\sigma}_{\rm m}=\sigma_0^2\mathbb{1}_2$. In turn, measurement of both quadratures introduces a ineludible excess noise, equal to the shot noise variance, that makes the quadrature variances larger than the usual homodyne detection.

The practical implementation of this scheme is reported in Fig. 2.4.1(b). Now we split the incoming signal in two parts thanks to a balanced beam splitter, in whose second port we have the vacuum state $|0\rangle$. Then, we implement joint homodyne detection of quadrature $q_c=(q_a+q_b)/\sqrt{2}$ (corresponding to $\phi=0$) and $p_d=(p_b-p_a)/\sqrt{2}$ ($\phi=\pi/2$) on the transmitted and reflected branch c and d, respectively.

2.4.2 Some relevant examples of non-Gaussian measurements

Beyond the Gaussian realm, the paradigmatic example of a non-Gaussian measurement is provided by photo-detection, namely *photon-number measurement*, described as projection onto the Fock states, $\Pi_n=|n\rangle\langle n|$. Usually, photo-detection is also referred to as *incoherent detection* or *direct detection*, as it does not require the presence of auxiliary fields nor an interferometric scheme, as for homodyne detection. Nevertheless, from a practical point of view, resolving individual photons is a highly nontrivial task. In fact, all the existing photo-detectors actually implement a destructive measurement based on the photoelectric effect, and indirectly probe the particle-like properties of radiation by measuring the electron flow, i.e. the current, generated inside the detector by the absorption of photons. In light of this, some examples of commonly employed photo-detectors are the following:

- *p-i-n photodiodes*, namely proportional detectors that generate a macroscopic current proportional to the incoming number of photons. They provide an efficient solution for detection of semi-classical fields, e.g. homodyne detection, whilst not being able to resolve photons;

- *on-off detectors*, that is click-no click detectors that can only resolve the vacuum state, distinguishing the absence or presence of photons. Accordingly, they are described by the binary POVM $\{\Pi_{\rm off}, \Pi_{\rm on}\}$, with $\Pi_{\rm off} = |0\rangle\langle 0|$ and $\Pi_{\rm on} = \hat{\mathbb{1}} - \Pi_{\rm off}$;

- *photon-number resolving (PNR) detectors*, capable of resolving the lowest Fock states $n = 0, 1, \ldots, M$ up to a maximum number $M < \infty$.

Within these classes, PNR detectors provide the more advanced solution from the technological point of view, and its functioning will be discussed in detail in the following.

2.4.2.1 Photon-number resolving detection

As mentioned above, PNR detectors are able to resolve any number of photons n up to a maximum number $M < \infty$, hence referred to as the photon number resolution; to highlight this features, throughout this thesis we will refer to them as PNR(M) detectors. For instance, PNR(3) refers to a detector that has only four possible outcomes $n \in \{0, 1, 2, \geq 3\}$, where "$\geq 3$" means 3 or more photons. Clearly, PNR(1) detectors correspond to on-off detectors, whereas ideal photo-detection requires PNR(M) with $M = \infty$ [16]. Accordingly, we describe PNR(M) detection by a finite-valued POVM with $M + 1$ possible outcomes, $\{\Pi_0, \Pi_1, \ldots, \Pi_M\}$, with:

$$\Pi_n = \begin{cases} |n\rangle\langle n| & \text{if } n = 0, \ldots, M-1\,, \\ \hat{\mathbb{1}} - \displaystyle\sum_{j=0}^{M-1} |j\rangle\langle j| & \text{if } n = M. \end{cases} \tag{2.84}$$

As a consequence, if we are performing PNR(M) measurement on a generic coherent state $|\alpha\rangle$, $\alpha \in \mathbb{C}$, the probability of detecting the outcome $n = 0, \ldots, M$ reads:

$$p_n(N) = \langle\alpha|\Pi_n|\alpha\rangle = \begin{cases} e^{-N}\,\dfrac{N^n}{n!} & \text{if } n = 0, \ldots, M-1\,, \\ 1 - e^{-N} \displaystyle\sum_{j=0}^{M-1} \frac{N^j}{j!} & \text{if } n = M\,, \end{cases} \tag{2.85}$$

with a mean photon number $N = |\alpha|^2$, namely a truncated Poisson distribution.

Good candidates as PNR detectors are the hybrid photodetectors, which are endowed with partial photon-number resolution and a linear response up to 100 photons [41], though with a quantum efficiency of about 50% in the green spectral region. Very high quantum efficiencies are obtained with transition-edge sensors (TES), but their dynamic range falls to approximatively 10 photons [42, 43]. More recently, also Silicon photomultipliers (SiPMs) has been investigated as PNR detectors, since they are more compact and with higher dynamic range [44–46].

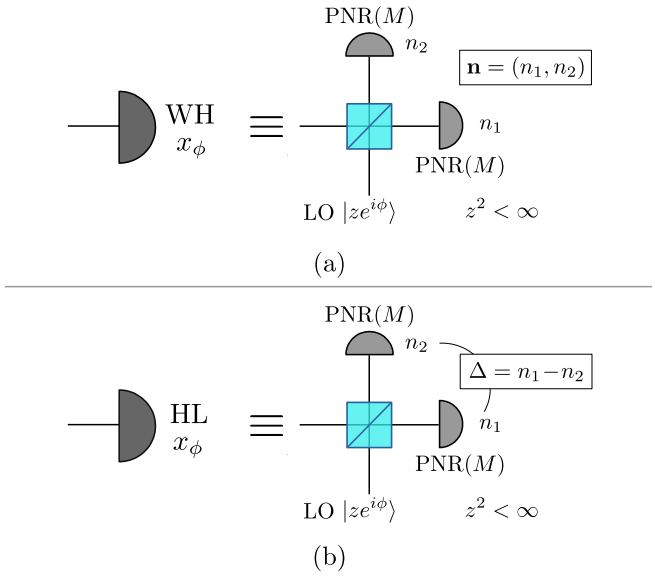


Figure 2.4.2: (a) Scheme of weak-field homodyne (WH) detection employing a low LO, $z^2 < \infty$, and PNR(M) detection. The outcome is a pair of integer values $\mathbf{n} = (n_1, n_2)$, $n_{1(2)} = 0, \dots, M$. (b) Homodyne-like (HL) detection, namely a WH scheme where we only consider the difference photocurrent $\Delta = -M, \dots, M$ at the output.

2.4.2.2 Weak-field homodyne detection

Given the previous considerations, an intriguing question arises: that is, to investigate the performance of the homodyne scheme, depicted in Fig. 2.4.1(a), beyond the high-LO limit, when $z^2 < \infty$, in which case the setup does not implement quadrature detection anymore.

We can identify two possible scenarios. The first one is referred to as weak-field homodyne (WH) detection, whose scheme is reported in Fig. 2.4.2(a): the conventional p-i-n photodiodes of the standard homodyne detection scheme are replaced by PNR(M) detectors [42, 47]. As a matter of fact, realistic PNR detectors have a finite resolution $M < \infty$, hence a low-intensity LO is required. The use of PNR detectors gives access to the two local photon-number statistics and allows jointly probing both the wake- and particle-like properties of the field. Accordingly, WH detection returns a pair of integer outcomes $\mathbf{n} = (n_1, n_2)$, $n_{1(2)} = 0, \dots, M$. Given an input coherent state $|\alpha\rangle$, $\alpha \in \mathbb{C}$, the resulting probability distribution reads:

$$P^{(\phi)}_{\mathbf{n}}(\alpha) = p_{n_1}\big(\mu_+(\alpha;\phi)\big) p_{n_2}\big(\mu_-(\alpha;\phi)\big)\,, \tag{2.86}$$

where

$$\mu_\pm(\alpha;\phi) = \frac{\left|\alpha \pm z e^{i\phi}\right|^2}{2}\,, \tag{2.87}$$

is the mean energy on the two output branches, respectively, and $p_n(\mu)$ is the PNR(M) distribution reported in Eq. (2.85).

In the second scenario we consider the WH scheme where we evaluate the difference Δ between the number of photons measured at output beams. Due to the clear analogy

with the standard homodyne detection, we refer to this configuration as homodyne-like (HL) detection, depicted in Fig. 2.4.2(b) [41, 44, 48]. The probability of obtaining the value $\Delta = n_1 - n_2$, with $-M \leq \Delta \leq M$, becomes:

$$\mathcal{S}_{\Delta}^{(\phi)}(\alpha) = \sum_{n_1,n_2=0}^{M} p_{n_1}\big(\mu_+(\alpha;\phi)\big) p_{n_2}\big(\mu_-(\alpha;\phi)\big)\, \delta_{n_1-n_2,\Delta}\,, \tag{2.88}$$

δ_{jk} being the Kronecker delta. In particular, when $M = \infty$, Δ represents the difference between two Poisson variables, thus Eq. (2.88) approaches a Skellam distribution [16].

CHAPTER 3

Fundamentals of quantum communication systems

In this last Chapter of Part I, we discuss the fundamental aspects of quantum communication systems, whose general goal is to transmit information between a sender and a receiver located at a certain distance. Given this scenario, different protocols can be designed, according to both the type of information to be shared, either classical information (e.g. a classical message) or quantum information (i.e. a quantum state), and the receiver's task. In particular, in the rest of the thesis we will deal with two different classes of protocols involving transmission of classical information carried by quantum states over a quantum channel, that is quantum state discrimination and continuous variable quantum key distribution. Instead, in this Chapter we maintain a general approach, and provide a general description, being valid for all the subsequent case studies.

The Chapter is organized as follows. At first, in Sec. 3.1, we present a general scheme of a telecommunication system, discussing the role and the composition of the sender and receiver stations. Then, we focus on two relevant aspects. In Sec. 3.2, we discuss in detail the methods adopted for encoding of classical information onto optical signals, both at the classical and quantum limit. Thereafter, in Sec. 3.3, we briefly review the basics of information theory, firstly developed by Shannon [49], that provide the theoretical description for all the considered protocols.

3.1 A general scheme of telecommunication systems

Generally speaking, any communication system, operating both at the classical and the quantum limit, involves two distant parties, the sender (also referred to as transmitter or modulator) and the receiver (or demodulator), usually renamed as Alice and Bob, respectively.

Alice handles a classical source that emits a message to be reliably transmitted to Bob via a communication channel. In more detail, the message m is a sequence of classical symbols $m = (x_1, \dots, x_n)$, for some $n \geq 1$, where the $\{x_j\}$ are outcomes of a random variable X, whose values x are drawn from a given alphabet $\mathcal{A}$ and distributed according to the probability $\{p(x)\}$. In classical information theory, the amount of information contained in each of these sequences is established by the first Shannon coding theorem, being equal to the minimum number of binary digits (bits) needed to determine its binary representation [15, 49]. In the aymptotic limit $n \gg 1$, this quantity is approximately equal to $nH(X)$, where

$$H(X) = \mathsf{H}[p(x)] \equiv -\sum_{x \in \mathcal{A}} p(x) \log_2 p(x) \tag{3.1}$$

is the Shannon entropy of the probability distribution $\{p(x)\}$. To convey this information to Bob, Alice encodes the message into optical signals, e.g. laser pulses, being injected into a communication channel, being, in general, noisy. In turn, at the channel end Bob receives a corrupted pulse, from which he extracts an approximate replica of the original message, $m' = (y_1, \dots, y_n)$. Practically, the optical transmitter is composed of three subsequent elements: the optical source, generating a carrier optical field, the modulator, that modifies the shape of the carrier field according to the encoded information (by typically varying its amplitude or phase), and a coupling device adapting the beam to the optical transmission medium, e.g. optical fibers, free space, water, ... Similarly, the receiver is composed of the cascade of a coupling device and a detector; therefore it ultimately implements a measurement of the received pulse, whose outcome provides a classical random variable Y correlated to X.

In general, the receiver may be designed to accomplish different objectives, that, accordingly, identify different kinds of communication protocols. Some common examples are the following:

i) *quantum state discrimination*, whose task is to distinguish between a set of possible symbols with the minimum decision error probability;

ii) *optical communication*, in which the goal is to reliably transmit classical information over the channel at the maximum rate;

iii) *quantum key distribution*, where the two parties aim at sharing a common random secure key, even if the channel is attacked by a third malicious party, the eavesdropper.

In this thesis, we will widely discuss cases i) and iii), that will be addressed in Parts II and III, respectively. On the contrary, here we maintain a general approach and present some basic features of both optical signaling and information theory that will be helpful throughout the rest of the work.

3.2 Encoding of optical signals

As previously mentioned, information is usually transmitted by electromagnetic waves that propagate throughout the physical channel. The sender encodes the input symbols into linearly polarized optical signals, e.g. laser pulses, located in temporal slots of duration $T = B^{-1}$, where B is the so-called *slot rate*, or *symbol period*, characterizing the width of the spectrum in the frequency domain [38, 50, 51]. Given that a laser source produces a narrowband radiation field, each single pulse is described by a quasi-monochromatic wavepacket:

$$\psi(t) = u(t)e^{-i\omega_0 t}\,, \tag{3.2}$$

where ω_0 is the carrier angular frequency, such that $2\pi B \ll \omega_0$, and $u(t)$ is the complex envelope of the waveform. The commonly adopted choices for $u(t)$ are twofold. The first one is to employ square waves, equal to:

$$u(t) = \begin{cases} u_0 & \text{for } 0 < t < T\,, \\ 0 & \text{elsewhere}\,, \end{cases} \tag{3.3}$$

for some complex constant $u_0 = |u_0|e^{i\phi_0} \in \mathbb{C}$. This choice will provide our benchmark scenario throughout the whole thesis. The latter is to use sinc waves, $u(t) =$

$u_0 \sin(\pi B t)/(\pi B t)$, overlapping in the temporal domain, in which case the slot rate B coincides with the signal bandwidth in the Fourier space [38, 50, 51].

From a classical viewpoint, the electric field associated with the wavepacket $\psi(t)$ is obtained as:

$$E(t) = \mathscr{E}_0 \left[u(t) e^{-i\omega_0 t} + u^*(t) e^{i\omega_0 t} \right], \tag{3.4}$$

$\mathscr{E}_0 = \sqrt{\hbar\omega_0/(2\epsilon A_{\text{eff}})}$ being the corresponding electric field per single photon, where $\hbar$, ϵ and A_{eff} are Planck's reduced constant, the electric permittivity of the propagation medium and the effective area of the transverse signal spatial mode, respectively [32]. Unlike the previous Chapter, for a clearer understanding here we choose not to adopt natural units, to emphasize the role of Planck's constant. In turn, the average optical power is obtained as:

$$P = \frac{1}{T} \int_0^T dt \int_{A_{\text{eff}}} d^2\mathbf{r} \left(\frac{1}{2} \epsilon \left| E(t) \right|^2 \right) = B\hbar\omega_0 \int_0^T dt \left| u(t) \right|^2, \tag{3.5}$$

that reduces to $P = B\hbar\omega_0 |u_0|^2$ in the presence of square waves.

On the contrary, at the quantum limit, each wavepacket is described by (possibly mixed) a quantum state ρ with mean energy, i.e. mean number of photons, equal to $\bar{n} = P/(B\hbar\omega_0)$; such that the previously introduced time integral of the complex envelope, $\int_0^T dt |u(t)|^2$, corresponds to the mean pulse energy. In particular, laser pulses (with stable phase) are well described by coherent states $\rho = |\alpha\rangle\langle\alpha|$, with $|\alpha\rangle = e^{-|\alpha|^2/2} \sum_n \alpha^n/\sqrt{n!} |n\rangle$, $\alpha \in \mathbb{C}$ and $|n\rangle$ being the n-photon state, containing $\bar{n} = |\alpha|^2$ mean photons [38]. In particular, for square-wave encoding we have $\bar{n} = \int_0^T dt |u(t)|^2 = |u_0|^2 T \equiv |\alpha|^2$, establishing the connection between the wavepacket and the coherent state amplitudes, respectively.

3.3 Elements of information theory

We now present the basic features of information theory, providing the framework to describe communication protocols operated in both the classical and quantum regimes.

In an optical communication protocol between a sender (Alice) and a receiver (Bob), the complex amplitude u_0 for a wavepacket $\psi(t) = u(t) e^{-i\omega_0 t}$ located in a given slot is randomly selected according to the outcome x of an input random variable X, associated with probability $p_A(x)$. Thereafter, Alice injects the signal into the noisy channel, corrupting the encoded symbol, and, after propagation, Bob, performs a suitable measurement, retrieving an outcome y, associated to a random variable Y [15, 38, 51, 52].

In a classical description in the absence of memory effects, the channel is characterized by a conditional probability distribution $p_{B|A}(y|x)$, such that the overall probability distribution of Y reads $p_B(y) = \sum_x p_A(x) p_{B|A}(y|x)$ [53]. As established by the second Shannon coding theorem, the amount of information about X extractable from Y is equal to the mutual information:

$$I(X;Y) = H(Y) - H(Y|X), \tag{3.6}$$

where $H(Y) = \mathsf{H}[p_B(y)]$ and $H(Y|X) = \sum_x p_A(x) \, \mathsf{H}[p_{B|A}(y|x)]$ are the average and conditional Shannon entropies, respectively [15, 38, 51]. Mutual information optimized over all possible input distributions yields the channel capacity:

$$C = \max_{p_A(x)} I(X;Y), \tag{3.7}$$

expressed in bits per time slot, i.e. per channel use, and representing the maximum amount of information extractable from the correlated variables X and Y. Accordingly, the maximum attainable transmission rate R, expressed in bits per unit time, is given by $\mathsf{R} = BC$ [38].

However, in many different conditions, e.g. high-loss transmission or long-distance communications, the probed signals are so attenuated that the granulosity of electromagnetic radiation emerges, thus a quantum description in terms of photons is required. In a quantum picture, Alice encodes symbols x onto quantum states of radiation ρ_x, the quantum channel is modeled as a quantum CP map $\mathcal{E}$, while Bob's detection is described by a POVM $\{\Pi_y\}_y$, $\Pi_y \geq 0$ and $\sum_y \Pi_y = \mathbb{1}$. In turn, the conditional distribution follows from the Born rule, $p_{B|A}(y|x) = \mathrm{Tr}[\mathcal{E}(\rho_x)\Pi_y]$ [23]. Within this framework, for each combined choice of both the carrier quantum states and the POVM at Bob's side we define a different classical channel, mapping the input variable X into its counterpart Y. Therefore, the classically-evaluated capacity C determines the maximum achievable information rate from given input ensemble $\{\rho_x\}_x$ and POVM $\{\Pi_y\}_y$.

Given this scenario, we may proceed beyond classical limits, and determine the ultimate channel capacity by optimization over all quantum measurements and state ensembles, thus obtaining the maximum information rate compatible with quantum mechanics laws. To this aim, we first resort to the Holevo theorem, establishing an upper bound to the mutual information of a channel whose symbols are encoded onto quantum states [54]. That is, for any choice of state ensemble and quantum measurement, associated with random variables X and Y, we have:

$$I(X;Y) \leq \chi(A;B)\,, \tag{3.8}$$

where $\chi(A;B)$ is the Holevo information between Alice and Bob:

$$\chi(A;B) = \mathsf{S}\left[\mathcal{E}\left(\sum_x p_A(x)\rho_x\right)\right] - \sum_x p_A(x)\mathsf{S}[\mathcal{E}(\rho_x)]\,, \tag{3.9}$$

$\mathsf{S}[\rho] = -\,\mathrm{Tr}[\rho \log_2 \rho]$ being the von Neumann entropy of state ρ [15]. We note that $\chi(A;B)$ has the same formal structure of the mutual information, being the difference between the von Neumann entropy of the average output quantum state after propagation and the average von Neumann entropy of individual output states. Importantly, it only depends on the input state ensemble $\{\rho_x\}$ and modulation $\{p_A(x)\}$ and not on the employed quantum measurement. Moreover, the coding theorem established by Holevo [11, 55] and by Schumacher–Westmoreland [56] proves that the bound (3.8) is saturable by a particular POVM, being, in general, a collective measurement. Accordingly, the ultimate transmission rate is provided by the so-called Holevo capacity, or classical capacity, equal to [55, 57]:

$$C_{\mathrm{H}} = \max_{\{\rho_x, p_A(x)\}} \chi(A;B)\,, \tag{3.10}$$

that can be regarded as the analog of the previously introduced second Shannon coding theorem.

As a final remark, we note that our analysis was focused on the transmission of classical messages, achieved by the so-called "classical–quantum" channels. Actually, this only provides the simplest scenario, operating single-letter encoding, such that a message $m = (x_1 \ldots, x_n)$ is encoded onto a factorized quantum state $\rho_{x_1} \otimes \ldots \otimes \rho_{x_n}$. Further improvements can be obtained by letting the sender use as input any (possibly entangled) quantum state, or by introducing cooperation between the input and output of the

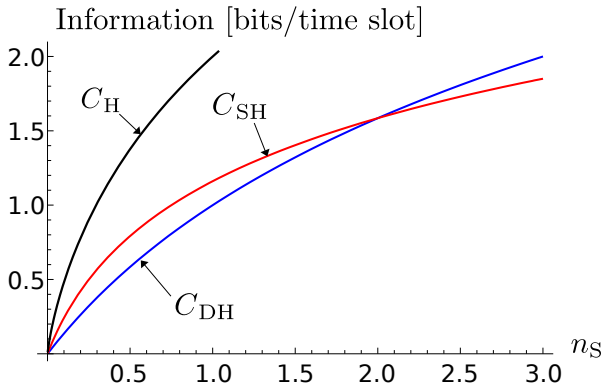


Figure 3.3.1: Plot of the Shannon capacities $C_{\rm r}$, ${\rm r} = {\rm SH}, {\rm DH}$, in Eq. (3.13), and the Gordon-Holevo capacity $C_{\rm H}$ in (3.15) as a function of the mean received energy $n_{\rm S}$ for zero excess noise photons $n_{\rm N} = 0$.

quantum channel, leading to the concept of "quantum channel capacity", as opposed to the classical channel capacity in Eq. (3.10) [15].

3.3.1 The capacity of the thermal-loss channel

As a milestone example, we now apply the previous analysis to assess the capacity of the thermal-loss channel, modeling transmission inside optical fibers in the presence of additive Gaussian excess noise, thus being also known with the term additive-white-Gaussian noise (AWGN) channel [38, 58, 59]. The channel is characterized by a transmissivity $T \leq 1$, quantifying signal attenuation, and a mean number of excess noise photons $n_{\rm N}$ added to the signal mode in each time slot. In particular, if Alice performs modulation of coherent states with average input energy $\bar{n}$, after transmission Bob probes a rescaled displaced-thermal state ensemble, with mean received energy

$$n_{\rm S} = T\bar{n}\,, \tag{3.11}$$

and thermal variance on both quadratures equal to $1+2n_{\rm N}$, expressed in shot-noise units (SNU).

Within a classical description of the channel, the maximum information rate follows from the the Shannon-Hartley theorem [49], and obtained via coherent-state encoding and measurement of either one or both canonical field quadratures q and p, that is by single- (SH) or double-homodyne (DH) detection, respectively [38, 39]. The corresponding Shannon channel capacity is reached with Gaussian modulation of the coherent state amplitude $\alpha = x_A + iy_A$. For the homodyne case, we set $y_A \equiv 0$ and the uni-variate modulation $p_A(x_A) = \mathcal{N}_{\sigma^2}(x_A)$, where

$$\mathcal{N}_{\sigma^2}(x) = \frac{\exp\left[-x^2/(2\sigma^2)\right]}{\sqrt{2\pi\sigma^2}}\,, \tag{3.12}$$

whereas in the presence of DH detection we adopt a bi-variate modulation, namely $p_A(x_A, y_A) = \mathcal{N}_{\sigma^2}(x_A)\mathcal{N}_{\sigma^2}(y_A)$. In turn, the average quantum state at Bob's side contains $n_{\rm S} = \sigma^2$ and $n_{\rm S} = 2\sigma^2$ mean photons, respectively. Then, the Shannon capacities

read:

$$C_{\mathrm{SH}} = \frac{1}{2}\log_2\left(1+\frac{4n_{\mathrm{S}}}{1+2n_{\mathrm{N}}}\right), \tag{3.13a}$$

$$C_{\mathrm{DH}} = \log_2\left(1+\frac{n_{\mathrm{S}}}{1+n_{\mathrm{N}}}\right), \tag{3.13b}$$

and are reported in Fig. 3.3.1 as functions of the mean received signal energy for zero excess noise photons. When $n_{\mathrm{N}} = 0$, we have $C_{\mathrm{SH}} \geq C_{\mathrm{DH}}$ for $n_{\mathrm{S}} \leq 2$, whereas for higher energy the DH capacity becomes larger than the single quadrature one. In fact, the joint measurement of both the non-commuting q and p operators, corresponding to the DH detection, introduces an ineludible excess noise equal to the shot-noise vacuum fluctuations, thus reducing the available signal-to-noise ratio (SNR) [38]. In turn, there is a tradeoff between this reduced SNR and the increase of accessible information due to the bi-variate signal modulation, such that if the signal energy is sufficiently low SH detection becomes preferable. Instead, in the opposite limit of large excess noise, $n_{\mathrm{N}} \gg 1$, we have:

$$C_{\mathrm{SH}} \approx \frac{1}{2}\log_2\left(1+2\frac{n_{\mathrm{S}}}{n_{\mathrm{N}}}\right) < \log_2\left(1+\frac{n_{\mathrm{S}}}{n_{\mathrm{N}}}\right) \approx C_{\mathrm{DH}}\,, \tag{3.14}$$

and for all SNR values DH detection is the preferable choice.

However, the Shannon capacity limit is obtained from two underlying assumptions, namely the adoption of coherent states as information carrier at the input and quadrature detection at the output. When both these limits are relaxed, we obtain the ultimate capacity of the channel, optimized over all measurement and quantum states, corresponding to the Gordon-Holevo capacity:

$$C_{\mathrm{H}} = g(n_{\mathrm{S}}+n_{\mathrm{N}}) - g(n_{\mathrm{N}})\,, \tag{3.15}$$

where $g(x) = (x+1)\log_2(x+1) - x\log_2 x$, see Fig. 3.3.1. In particular, for pure-loss transmission, $n_{\mathrm{N}} = 0$, we have $C_{\mathrm{H}} = g(n_{\mathrm{S}})$ and, in the high-energy regime $n_{\mathrm{S}} \gg 1$:

$$C_{\mathrm{H}} = g(n_{\mathrm{S}}) = \log_2(1+n_{\mathrm{S}}) + \log_2 e - \frac{\log_2 e}{2n_{\mathrm{S}}} + O(n_{\mathrm{S}}^{-2})\,. \tag{3.16}$$

The first term coincides with the Shannon DH capacity, therefore for high signal energy the Holevo capacity introduces a constant information enhancement equal to 1 nat $= \log_2 e \approx 1.44$ bits. On the contrary, when $n_{\mathrm{N}} \gg 1$, we have:

$$\begin{aligned} C_{\mathrm{H}} &= g(n_{\mathrm{S}}+n_{\mathrm{N}}) - g(n_{\mathrm{N}}) \\ &= C_{\mathrm{DH}} + \left(\frac{1}{n_{\mathrm{N}}} - \frac{1}{n_{\mathrm{S}}+n_{\mathrm{N}}}\right)\log_2 e + O(n_{\mathrm{N}}^{-2})\,, \end{aligned} \tag{3.17}$$

and DH detection re-approaches C_{H}.

Remarkably, we note that also the Gordon-Holevo capacity is reached by Gaussian modulation of coherent states, as for the Shannon case. However, the optimal POVM achieving (3.15) is a collective measurement, operating simultaneously on multiple time slots, whose associated detection scheme is still unknown [15, 38, 51]. Thus, the interest has been directed to either design simple collective measurements approximating the Holevo capacity in particular energy regimes [60, 61], or to find feasible suboptimal individual measurement performed on single time slots, e.g. photon-number measurement [52, 62–66].

Part II

Quantum state discrimination theory

CHAPTER 4

Introduction to quantum decision theory

The problem of performing discrimination of quantum states in efficient way is ubiquitous in quantum information, being at the basis of many communication and computing protocols, e.g. quantum key distribution and probabilistic computing algorithms. Furthermore, it also plays a crucial role in hypothesis testing scenarios, such as gravitational waves detection [67]. In fact, in all quantum information schemes, information carriers are provided by quantum states of a physical system. In turn, when the set of all possible output states is known, one has to infer which particular state was exploited in order to read out the encoded information. However, this task can be easily accomplished only with a family of mutually orthogonal states, whereas, in the presence of non-orthogonal states, quantum mechanics laws forbid exact discrimination. As a consequence, any discrimination strategy is associated with a decision error probability, and the optimum receiver is the one achieving the minimum error probability compatible with the quantum mechanical limits. Moreover, one can adopt different discrimination strategies according to the specific context under investigation, e.g. quantum quantum decision theory, unambiguous discrimination, and maximum confidence strategies [67].

Historically, the problem of quantum state discrimination has been firstly raised in the 1970's by the seminal works of Helstrom [9] and Holevo [15]. Following the subsequent developments of quantum information theory, there has been a revived interest in the 1990's, when Bennett et al. recognized that non-orthogonal states could be also used for quantum key distribution [68]. In parallel, the topic has been also investigated in the context of telecommunication engineering, whose technological progresses led to the experimental demonstration of non-negligible noise of quantum origin in long-distance and deep-space communications, that ultimately introduce a bit error rate on the information read out at the receiver [51].

In this Chapter, we provide the general framework of the theory, and then focus on the relevant scenario of binary quantum decision theory. In particular, we address discrimination of coherent states and present the most relevant examples of feasible quantum receivers, analyzing their performance also in the presence of realistic defects, e.g. non-unit quantum efficiency, dark counts, visibility reduction and phase diffusion noise. The structure of the Chapter is the following. In Sec. 4.1 we schematize the general features of quantum state discrimination, whereas Sec. 4.2 focuses itself on quantum decision theory, with particular reference to the binary case. Thereafter, in Sec. 4.3 we address binary discrimination of coherent states, and consider binary phase-shift keying modulation, in which information is encoded on the phase of a coherent signal with fixed mean energy. Furthermore, we present the benchmark examples of quantum receivers achieving a genuine quantum advantage over conventional schemes based on quadrature detection, namely the Kennedy, Dolinar, displacement feed-forward (DFFRE) and Sasaki-Hirota receivers. Then, in Sec. 4.4, we propose two new hybrid schemes, the

hybrid near-optimum (HYNORE) and the hybrid feed-forward (HFFRE) receivers, and obtain a further reduction of the error probability with respect to displacement-photon counting methods. Finally, in Sec.s 4.5 and 4.6, we analyze the performance of the proposed receivers in the presence of detection imperfections and phase noise, respectively.

4.1 Quantum state discrimination: the general framework

Generally speaking, the problem of quantum state discrimination is formulated as follows [51, 67, 69–74]. We have a physical system that can be prepared in $M \geq 2$ non-orthogonal quantum states $\{\rho_k\}_k$, $k = 0, \ldots, M-1$. The set of the possible states is typically referred to with the term *constellation*. A quantum source randomly generates one of the M states, preparing ρ_k with a priori probability $0 \leq q_k \leq 1$, $\sum_k q_k = 1$. The task is to implement a receiver to infer which was the prepared state. That is, we look for a POVM $\{\Pi_x\}_x$, $x \in \mathcal{X}$, $\Pi_x \geq 0$, and $\sum_x \Pi_x = \hat{\mathbb{1}}$, $\hat{\mathbb{1}}$ being the identity operator over the whole Hilbert space, associated with a decision rule, such that if the outcome x falls into a certain confidence region Δ_j, we infer the state generated by the source to be ρ_j.

The problem has no trivial solution, as perfect discrimination of non-orthogonal quantum states is not allowed by quantum mechanics laws. To better understand this point, we consider a paradigmatic example. We address binary discrimination of pure states, when the source emits either state $|\gamma_0\rangle$ or $|\gamma_1\rangle$, with $\langle\gamma_0|\gamma_1\rangle = X \neq 0$. In this case, we should design a binary receiver, associated with a POVM $\{\Pi_0, \Pi_1\}$, $\Pi_0 + \Pi_1 = \hat{\mathbb{1}}$. If the receiver were able to perform perfect discrimination, outcome "0" could not be retrieved from state "1" and vice versa, thus we would have:

$$\Pi_0|\gamma_1\rangle = 0 \quad \text{and} \quad \Pi_1|\gamma_0\rangle = 0\,. \tag{4.1}$$

However, this would also imply that:

$$0 = \langle\gamma_0|\Pi_0|\gamma_1\rangle + \langle\gamma_0|\Pi_1|\gamma_1\rangle = \langle\gamma_0|\left(\Pi_0 + \Pi_1\right)|\gamma_1\rangle = \langle\gamma_0|\gamma_1\rangle = X\,, \tag{4.2}$$

leading to contradiction. The former argument can be straightforwardly extended to statistical mixtures $\rho_k = \sum_s \lambda_s^{(k)} |\gamma_s^{(k)}\rangle\langle\gamma_s^{(k)}|$, $k = 0, 1$, with $\sum_s \lambda_s^{(k)} = 1$. In this case, the orthogonality condition becomes $\mathcal{S}_1 \perp \mathcal{S}_2$, $\mathcal{S}_k$ being the linear subspace spanned by states $\{|\gamma_s^{(k)}\rangle\}_s$, providing the support of operator ρ_k [67]. As a consequence, in the presence of non-orthogonal quantum states it is not possible to determine with certainty which state was prepared. This is one of the fundamental result in quantum theory, being in strict connection with the no-cloning theorem, according to which no physical operation can produce an identical copy of a given unknown quantum state [75–77].

In turn, when the outcome x is obtained from the measurement $\{\Pi_x\}_x$, the receiver can take the decision j even if the state $k \neq j$ was probed, resulting in a decision error. Thus, the paradigm of perfect discrimination should be abandoned and different strategies may be adopted, according to the specific context under investigation. Generally speaking, in literature there exists three main scenarios:

- *quantum decision theory*: it represents a conclusive discrimination strategy, being the first scenario historically addressed by Helstrom and Holevo [9, 15]. In this case, a final decision is always performed, even in the possible presence of decision errors. To have conclusive results only, each measurement outcome must be associated with one and only one of the constellation states, resulting in a finite-valued POVM, with exactly M elements. Then, the receiver is designed to minimize the overall decision error probability.

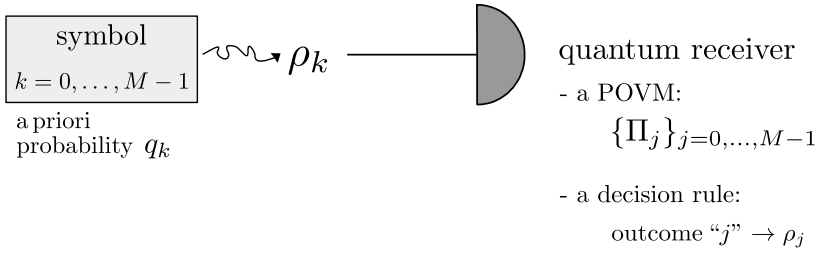


Figure 4.2.1: Schematic description of a quantum decision problem. A source encodes a classical symbol $k = 0, \ldots, M-1$, generated with a priori probability $q_k \leq 1$, onto non-orthogonal quantum states ρ_k. The task is to design a quantum receiver, namely a POVM $\{\Pi_j\}_j$, $j = 0, \ldots, M-1$, associated with a decision rule, that minimizes the decision error probability.

- *unambiguous discrimination strategy*: guaranteeing error-free discrimination, at the cost of introducing inconclusive measurement outcomes. That is, the receiver is described by a POVM with more than M elements: if we obtain an outcome associated with one of the constellation states, we perform a decision with certainty; otherwise, if an inconclusive outcome is retrieved, no decision is performed. In turn, the goal becomes to minimize the probability of obtaining inconclusive outcomes. The strategy was first introduced in [78] and then solved for binary pure-state discrimination in [79, 80].
- *maximum confidence strategy*: this provides an intermediate solution between the two former strategies, introduced in [81]. The receiver is optimized to maximize the confidence, namely the a posteriori probability $P(\rho_j|j)$ of inferring state ρ_j when outcome j is retrieved.

In the following, we only deal with the first scenario, being of particular relevance in the field of quantum communications.

4.2 Quantum decision theory

The paradigm of quantum decision theory can be easily embedded in the quantum communications scheme introduced in Chapter 3, where a sender and a receiver share classical information in the following way, schematized in Fig. 4.2.1. The sender encodes a classical symbol $k = 0, \ldots, M-1$ onto one of the M constellation states $\{\rho_k\}$ and, thereafter, sends them to the receiver who implements a quantum receiver to "decode" the value of the sent symbol. Following the previous considerations, the quantum receiver is described by a M valued POVM $\{\Pi_j\}$, $j = 0, \ldots, M-1$, $\Pi_j \geq 0$, $\sum_j \Pi_j = \hat{\mathbb{1}}$, such that obtaining outcome j infers symbol j. However, due to the non-orthogonality of the constellation states, any receiver is associated with an error probability, equal to:

$$P_{\text{err}} = 1 - \mathcal{P}_c \,, \tag{4.3}$$

where

$$\mathcal{P}_c = \sum_{k=0}^{M-1} q_k \, p(k|k) = \sum_{k=0}^{M-1} q_k \, \text{Tr}[\rho_k \Pi_k] \tag{4.4}$$

is the (overall) correct decision probability, $p(j|k) = \mathrm{Tr}[\rho_k \Pi_j]$ being the probability of performing decision j, when symbol k was sent. In turn, the goal is to find the *optimum* receiver, reaching the minimum error probability, or, equivalently, the maximum correct decision probability, compatible with quantum mechanics laws [9, 15, 51, 67].

In general, minimizing Eq. (4.3) over all possible POVMs represents a functional optimization problem, being non-easy to handle. The problem is rather simplified for the binary discrimination case, whereas treating M-ary state discrimination, with $M > 2$, requires the employment of advanced tools from linear algebra. For these reasons, in the following we will only focus on the binary case, completely characterized the mid-1970s by Helstrom's theory, where the minimum error probability gets analytical expression [9]. On the contrary, we leave the discussion of discrimination of multiple states for the next Chapter.

4.2.1 Quantum discrimination in the binary case

In the binary discrimination scenario, the receiver has to distinguish between two states ρ_0 and ρ_1, associated with a priori probabilities q_0 and q_1, respectively. Thus, it is described by a binary POVM $\{\Pi_0, \Pi_1\}$, where $\Pi_1 = \hat{\mathbb{1}} - \Pi_0$. This allows to re-express the error probability (4.3) as:

$$\begin{aligned} P_{\mathrm{err}} &= q_0 p(1|0) + q_1 p(0|1) \\ &= q_0 \,\mathrm{Tr}[\rho_0 \Pi_1] + q_1 \,\mathrm{Tr}[\rho_1 \Pi_0] \\ &= q_0 \,\mathrm{Tr}\left[\rho_0 \left(\hat{\mathbb{1}} - \Pi_0\right)\right] + q_1 \,\mathrm{Tr}[\rho_1 \Pi_0] \\ &= q_0 + \mathrm{Tr}[\Lambda \Pi_0] = q_1 - \mathrm{Tr}[\Lambda \Pi_1]\,, \end{aligned} \tag{4.5}$$

where we introduced the Hermitian operator:

$$\Lambda = q_1 \rho_1 - q_0 \rho_0\,. \tag{4.6}$$

Furthermore, we consider the spectral decomposition Λ, namely:

$$\Lambda = \sum_{\lambda \geq 0} \lambda \,|\lambda\rangle\langle\lambda| + \sum_{\lambda < 0} \lambda \,|\lambda\rangle\langle\lambda|\,, \tag{4.7}$$

where $|\lambda\rangle$ is the eigenstate associated with eigenvalue $\lambda \in \mathbb{R}$, and the contributions of the eigenspaces associated with positive and negative eigenvalues have been separated [9, 51, 67]. Given Eq. (4.5), minimizing P_{err} is equivalent to find a POVM satisfying the following conditions:

$$\min_{\Pi_0} \Big\{ \mathrm{Tr}[\Lambda \Pi_0] \Big\} \quad \text{and} \quad \max_{\Pi_1} \Big\{ \mathrm{Tr}[\Lambda \Pi_1] \Big\}\,. \tag{4.8}$$

Thanks to (4.7), we straightforwardly obtain the optimum POVM as:

$$\Pi_0^{(\mathrm{opt})} = \sum_{\lambda < 0} |\lambda\rangle\langle\lambda| \quad \text{and} \quad \Pi_1^{(\mathrm{opt})} = \sum_{\lambda \geq 0} |\lambda\rangle\langle\lambda|\,, \tag{4.9}$$

coinciding wit projection over the positive and negative parts of Λ, respectively. An intriguing particular case emerges when negative eigenvalues do not exist, as noted by Hunter [82]. In this case, we would have $\Pi_0^{(\mathrm{opt})} = 0$ and $\Pi_1^{(\mathrm{opt})} = \hat{\mathbb{1}}$, and the minimum

error probability is achieved by always inferring state "1", without performing any measurement. Analogous considerations hold in the opposite case, namely in the absence of positive eigenvalues.

The corresponding minimum error probability associated with the optimum POVM, referred to as the *Helstrom bound*, reads:

$$\begin{aligned} P_{\rm Hel} &= \frac{1}{2}\Big\{q_0 + {\rm Tr}[\Lambda\Pi_0] + q_1 - {\rm Tr}[\Lambda\Pi_1]\Big\} \\ &= \frac{1}{2}\Big\{1 + {\rm Tr}[\Lambda(\Pi_0 - \Pi_1)]\Big\} \\ &= \frac{1}{2}\left(1 + \sum_{\lambda<0}\lambda - \sum_{\lambda\geq 0}\lambda\right) = \frac{1}{2}\left(1 - \sum_{\lambda}|\lambda|\right) \\ &= \frac{1}{2}\left[1 - {\rm Tr}\left(|\Lambda|\right)\right] , \end{aligned} \tag{4.10}$$

where $|\Lambda| = (\Lambda^\dagger\Lambda)^{1/2}$. We also note that ${\rm Tr}(|\Lambda|) = \|\Lambda\|_1$, $\|\cdot\|_1$ being the 1-norm, thus $P_{\rm Hel} = (1 - \|q_1\rho_1 - q_0\rho_0\|_1)/2$, corresponding to the trace distance bewteen the weighted operators $q_1\rho_1$ and $q_0\rho_0$ [9, 51, 67].

The former expression further simplifies for pure-state discrimination of states $|\gamma_k\rangle$, $k = 0, 1$, with $X = \langle\gamma_0|\gamma_1\rangle \neq 0$. In this case, the eigenvalues of operator $\Lambda = q_1|\gamma_1\rangle\langle\gamma_1| - q_0|\gamma_0\rangle\langle\gamma_0|$ are equal to $\lambda_\pm = (q_1 - q_0 \pm \sqrt{1 - 4q_0q_1|X|^2})/2$, and the corresponding Helstrom bound becomes:

$$P_{\rm Hel} = \frac{1}{2}\left[1 - \sqrt{1 - 4q_0q_1|\langle\gamma_0|\gamma_1\rangle|^2}\right] . \tag{4.11}$$

The optimum projectors become $\Pi_0^{\rm (opt)} = |\lambda_-\rangle\langle\lambda_-|$ and $\Pi_1^{\rm (opt)} = |\lambda_+\rangle\langle\lambda_+|$, where:

$$|\lambda_-\rangle = \frac{1}{\mathcal{N}_-}\left(|\gamma_0\rangle + \frac{q_0X^*}{q_1 - \lambda_-}|\gamma_1\rangle\right) \quad \text{and} \quad |\lambda_+\rangle = \frac{1}{\mathcal{N}_+}\left(|\gamma_1\rangle + \frac{q_1X}{q_0 + \lambda_+}|\gamma_0\rangle\right) , \tag{4.12}$$

$\mathcal{N}_\pm$ being the normalization constant. That is, the optimum receiver is realized by a 1-rank projective measurement over a suitable linear combination of the encoded states [9, 51, 67].

4.3 Binary discrimination of coherent states

We now apply the tools of quantum decision theory, developed in the previous section, to the quantum communications systems presented in Chapter 3, where information is encoded onto coherent states, describing the radiation emitted by stable laser sources. That is, in each time slot, the sender encodes a binary symbol $k = 0, 1$ onto the coherent pulse $|\alpha_k\rangle$, generated with equal a priori probabilities $q_k = 1/2$. Thereafter, pulses are sent to the receiver though a channel, assumed here to be noiseless. Ultimately, we implement a quantum receiver, namely a binary POVM $\{\Pi_0, \Pi_1\}$, with $\Pi_1 = \mathbb{1} - \Pi_0$, to infer the transmitted symbol, associated with a nonzero error probability. In the presence of binary modulation, the encoding stage may be deployed according to two typical strategies [51]:

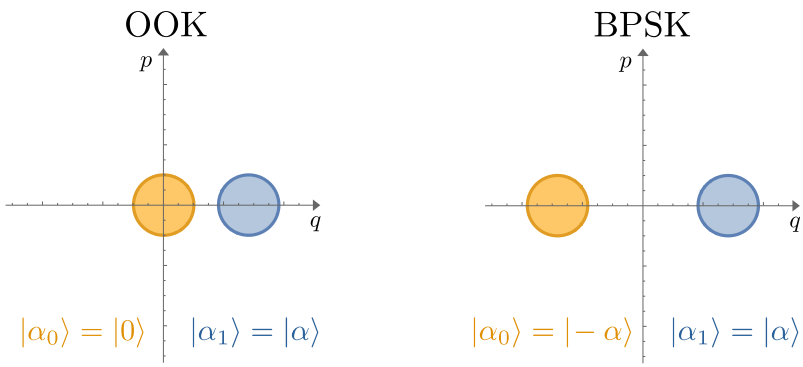


Figure 4.3.1: Phase space representation of the OOK (left) and BPSK (right) encodings. In the former case, information is encoded on the absence or presence of a given field with amplitude $\alpha > 0$, i.e. $|\alpha_0\rangle = |0\rangle$ and $|\alpha_1\rangle = |\alpha\rangle$, whilst in the latter scenario symbols are encoded on the field phase, $|\alpha_0\rangle = |-\alpha\rangle$ and $|\alpha_1\rangle = |\alpha\rangle$. We note that the overlap $|\langle\alpha_0|\alpha_1\rangle|^2$ is lower for BPSK modulation, leading to a lower value of the Helstrom bound.

- *on-off keying* (OOK): it represents the simplest scheme, in which symbol "0" is encoded onto the vacuum state $|\alpha_0\rangle = |0\rangle$, while symbol "1" corresponds to a coherent state with given amplitude $\alpha > 0$, i.e. $|\alpha_1\rangle = |\alpha\rangle$. Practically, this scheme is realized by either amplitude modulating a laser source at fixed frequency or, more simply, by switching on and off the laser itself according to the symbol to be transmitted;

- *binary phase-shift keying* (BPSK): now, a coherent state of mean energy α^2, $\alpha > 0$, is generated in all time slots, and information is encoded in the field phase, namely:

$$|\alpha_k\rangle = |e^{i(k+1)\pi}\alpha\rangle\,, \qquad k = 0, 1\,, \tag{4.13}$$

  such that $|\alpha_0\rangle = |-\alpha\rangle$ and $|\alpha_1\rangle = |\alpha\rangle$. That is, the two states has the same energy but are phase-shifted by π. This kind of encoding is practically implemented by phase modulation of an input laser beam.

The two modulation formats are schematized in Fig. 4.3.1. In the following, we will draw our attention on the sole BPSK case, since, as we can see, the overlap between the two encoded pulses is lower for the BPSK case than the OOK, leading to a lower value of the Helstrom bound, see Eq. (4.11). In fact, we have $|\langle 0|\alpha\rangle|^2 = \exp(-\alpha^2)$ for OOK and $|\langle -\alpha|\alpha\rangle|^2 = \exp(-4\alpha^2)$ for BPSK. However, from a more practical point of view, the preference for one format over the other is not only limited to theoretical reasons, but is also due to practical characteristics, concerning the technologies of the adopted equipment, the accuracy in the phase stabilization of the encoded signals, the achievable symbol repetition rates and so on [51].

In the presence of BPSK, thanks to Eq. (4.11), the minimum error probability, i.e. the Helstrom bound, becomes:

$$P_{\text{Hel}} = \frac{1}{2}\left[1 - \sqrt{1 - e^{-4\alpha^2}}\right]. \tag{4.14}$$

The optimal measurement strategy achieving such a minimum is the *"cat state" measurement*, defined by the two-valued POVM $\{\Pi_0, \mathbb{1} - \Pi_0\}$, $\Pi_0 = |\psi_{\text{cat}}\rangle\langle\psi_{\text{cat}}|$, where

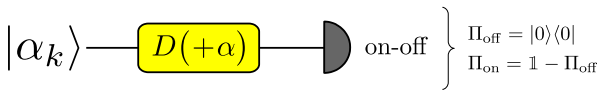


Figure 4.3.2: Setup of the Kennedy receiver. The incoming signal $|\alpha_k\rangle$, $k = 0, 1$, undergoes a displacement operation $D(\alpha)$ followed by on-off detection. The final decision is performed according to the rule: "off" $\rightarrow$ "0" and "on" $\rightarrow$ "1".

$|\psi_{\rm cat}\rangle = c_0(\alpha)|\alpha_0\rangle + c_1(\alpha)|\alpha_1\rangle$ is an optimized "cat state" [9]. However, a concrete realization of such a POVM is not an easy task.

On the contrary, the conventional binary receivers adopted in optical communication systems are based on homodyne detection, being sensitive to the field phase. The homodyne receiver works as follows. We perform measurement of the quadrature q and infer symbol "0" when the outcome $x \geq 0$ is retrieved, and symbol "1" when a negative value $x < 0$ is obtained. We remind that the homodyne distribution of states $|\alpha_k\rangle$ is equal to:

$$p_{\rm HD}(x|k) = \frac{\exp\left[-(x - 2\alpha_k)^2/2\right]}{\sqrt{2\pi}}\,, \tag{4.15}$$

expressed in shot-noise units, being limited by shot-noise due to vacuum fluctuations. In turn, there is a nonzero probability of retrieving outcomes $x \geq 0$ when state $|\alpha_0\rangle$ was sent, and vice versa. Accordingly, the error probability for the homodyne receiver reads

$$\begin{aligned} P_{\rm SQL} &= \frac{1}{2}\left[\int_0^\infty dx\, p_{\rm HD}(x|0) + \int_{-\infty}^0 dx\, p_{\rm HD}(x|1)\right] \\ &= \frac{1 - {\rm erf}\left(\sqrt{2}\alpha\right)}{2}\,, \end{aligned} \tag{4.16}$$

referred to as the *standard quantum limit* (SQL), or shot-noise limit. The SQL represent the best error probability achievable by semi-classical means in ideal conditions, being suboptimal with respect to the Helstrom bound, as $P_{\rm SQL} > P_{\rm Hel}$. Given this scenario, the task of quantum state discrimination theory is to design a feasible receiver outperforming the SQL and being as close as possible to the Helstrom bound. Several proposals of feasible optimum or near-optimum receivers have been advanced in literature, based on either single-shot discrimination or feedback-based strategies. In the following, we present the main ones, employing displacement operations and photon counting.

4.3.1 The Kennedy receiver

The first quantum receiver beating the SQL has been proposed in 1973 by Kennedy [83], whose scheme is reported in Fig. 4.3.2.

In the *Kennedy receiver*, or displacement receiver, the incoming signal $|\alpha_k\rangle$ undergoes the displacement operation [39] $D(\alpha)$, followed by on-off detection. As discussed in Sec. 2.3, the displacement may be implemented practically by letting the signals interfere with a suitable intense local oscillator at a beam splitter with large transmissivity [84]. We note that $D(\alpha)$ performs a nulling operation, leading to the mapping:

$$|-\alpha\rangle \rightarrow |0\rangle \quad \text{and} \quad |\alpha\rangle \rightarrow |2\alpha\rangle\,. \tag{4.17}$$

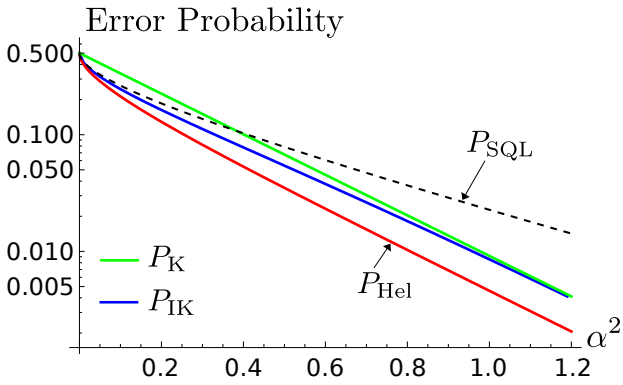


Figure 4.3.3: Log plot of the error probabilities of the standard and improved Kennedy receivers $P_{\rm K}$ and $P_{\rm IK}$, respectively, as a function of the signal energy α^2. $P_{\rm SQL}$ and $P_{\rm Hel}$ refer to the SQL (4.16) and the Helstrom bound (4.14), respectively.

This is the so-called "nulling" displacement, since one of the two signals is displaced into the vacuum state. Therefore, BPSK is turned into OOK and on-off detection provides the optimal measurement choice, with the following decision rule: "off" $\rightarrow$ "0" and "on" $\rightarrow$ "1". Thus, an error occurs when an "off" result is retrieved from state $|\alpha_1\rangle$, leading to the error probability

$$P_{\rm K} = q_1\, p(\text{off}|1) = \frac{1}{2}\big|\langle 0|2\alpha\rangle\big|^2 = \frac{e^{-4\alpha^2}}{2}\,, \tag{4.18}$$

depicted in Fig. 4.3.3 as a function of the signal energy and compared to both the SQL and the Helstrom limit. As we can see, in the high-energy limit $\alpha^2 \gg 1$ the Kennedy receiver is near-optimum, namely proportional to the Helstrom bound, as $P_{\rm K} \approx 2P_{\rm Hel}$. In fact:

$$P_{\rm Hel} = \frac{1}{2}\left[1-\sqrt{1-e^{-4\alpha^2}}\right] \approx \frac{1}{2}\left[1-\left(1-\frac{e^{-4\alpha^2}}{2}\right)\right] = \frac{P_{\rm K}}{2}\,, \tag{4.19}$$

where we used the Taylor expansion $\sqrt{1-x} = 1-x/2+O(x^2)$. Futhermore, the receiver also beats the SQL for $\alpha^2 > \alpha_{\rm K}^2$, with $\alpha_{\rm K}^2 \approx 0.38$ [16, 83].

The feasibility of the Kennedy setup has been demonstrated experimentally in [85–88]. The main drawback towards a practical implementation is represented by the local oscillator laser required to realize the displacement $D(\alpha)$, which need to be finely tuned in both frequency and phase with respect to the incoming signal. To overcome this problem, to date, many practical realizations employ a single laser source from which both the signal and the local oscillator are generated. This laser emits a high-intensity coherent state, being then splitted at a beam splitter with small transmissivity, such that the transmitted (weak) pulse is sent to the phase modulator, becoming the encoded state, while the reflected (strong) pulse plays the role of the local oscillator.

An improved version of the Kennedy receiver has been obtained by Takeoka and Sasaki by optimizing the displacement amplitude [89]. In their *improved Kennedy* (IK) receiver, the "nulling" displacement $D(\alpha)$ is replaced with a generic $D(\beta)$, $\beta > 0$, whose value is optimized to minimize the overall error probability. In turn, the encoded states

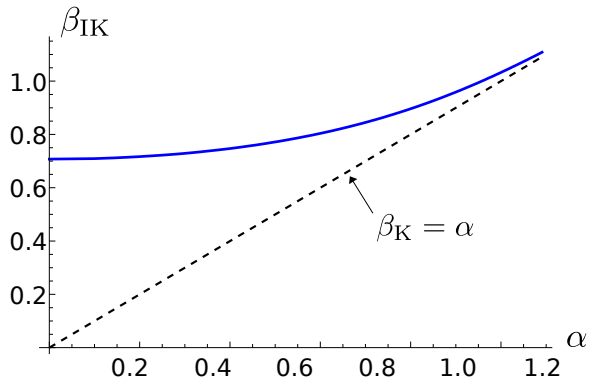


Figure 4.3.4: Optimized displacement $\beta_{\rm IK}$ of the IK receiver as a function of the coherent amplitude α of the incoming signal. The dashed line $\beta_{\rm K} = \alpha$ represents the (fixed) displacement amplitude of the standard Kennedy receiver.

are mapped into:

$$|-\alpha\rangle \rightarrow |\beta-\alpha\rangle \quad \text{and} \quad |\alpha\rangle \rightarrow |\beta+\alpha\rangle\,. \tag{4.20}$$

The final decision still follows from the outcomes of on-off detection but, differently from the standard Kennedy receiver, now, an error occurs either when a "off" result is retrieved from state $|\alpha_1\rangle$ or when a "on" is obtained from $|\alpha_0\rangle$. The resulting error probability reads:

$$P_{\rm IK} = \max_{\beta>0} P_{\rm IK}(\beta)\,, \tag{4.21}$$

where

$$P_{\rm IK}(\beta) = q_1\, p(\text{off}|1) + q_0\, p(\text{on}|0) = \frac{1}{2}\left[e^{-(\beta+\alpha)^2} + 1 - e^{-(\beta-\alpha)^2}\right]. \tag{4.22}$$

By nulling the derivative of $P_{\rm IK}(\beta)$ with respect to β, i.e. $dP_{\rm IK}(\beta)/d\beta = 0$, we find that the optimal displacement amplitude $\beta_{\rm IK}$ shall satisfy the following transcendental equation:

$$\frac{\beta_{\rm IK}-\alpha}{\beta_{\rm IK}+\alpha} = e^{-4\alpha\beta_{\rm IK}}\,, \tag{4.23}$$

to be solved numerically. The solution of Eq. (4.23) is plotted in Fig. 4.3.4 as a function of the coherent amplitude α of the encoded signal, together with $\beta_{\rm K} = \alpha$, being the displacement amplitude of the standard Kennedy receiver. As we see, the optimized displacement amplitude $\beta_{\rm IK}$ is always larger than α, but in the high-energy limit the two lines approach each other, thus making the IK receiver coincide with the Kennedy. In turn, as showed in Fig. 4.3.3, the IK receiver outperforms the Kennedy in the low-energy regime, whereas in the limit $\alpha^2 \gg 1$, $P_{\rm IK} \approx P_{\rm K}$ and the improvement due to the displacement optimization becomes negiglibile. Remarkably, the enhancement for small energies allows to beat the SQL for all $\alpha^2 > 0$.

Finally, it is worth to mention a further variation of the original Kennedy scheme, the so-called *displacement-photon-number-resolving receiver* (DPNR), originally introduced

in [90–93]. It consists of the same setup depicted in Fig. 4.3.2, where the on-off detector is replaced by a photon-number resolving (PNR) detector with finite resolution M, see Sec. 2.4.2.1. The final decision rule is then suitably adjusted to either include a given inconclusive-result probability [90, 91] or account for detection imperfections and noise [92, 93].

4.3.2 The Dolinar receiver

The Kennedy receiver presented above represents the typical benchmark for all sub shot-noise-limited quantum receivers, due to both its theoretical simplicity and its practical feasibility with the technologies commonly adopted in optical communications, based on linear optics and on-off detection. As a consequence, its scheme has provided a building block to construct more sophisticated receivers with better performances.

A paradigmatic example is represented by the *Dolinar receiver* [94]. By suitably generalizing the Kennedy scheme, in 1973 Dolinar proposed a feedback receiver employing conditional displacements and continuous-time photodetection, proving it to be optimum for all input energies.

The basic principle of the Dolinar receiver is to implement a real-time adjustment of the displacement operation of the Kennedy setup in both amplitude and phase, according to the obtained outcome of the photon counter, via closed-loop feedback control performed during the time processing of the encoded signal [51, 94, 95]. Thus, to compute the error probability we should resort to the temporal description presented in Sec. 3.2. The encoded pulse $|\alpha_k\rangle$, $k = 0, 1$, corresponds to a wavepacket $\psi_k(t)$ located in a time slot of duration T, equal to [51, 95]:

$$\psi_k(t) = e^{i\pi(k+1)}\psi\, e^{-i\omega t}\,, \qquad 0 < t \leq T\,, \tag{4.24}$$

ω being the carrier signal frequency and $\psi > 0$, with mean photon number

$$\bar{n}_k = \int_0^T |\psi_k(t)|^2 dt = \psi^2 T \equiv \alpha^2\,. \tag{4.25}$$

The overlap betweent the pulses is then retrieved as $|\langle\alpha_0|\alpha_1\rangle|^2 = \exp[-\int_0^T dt S(t)]$, where

$$S(t) = |\psi_0(t) - \psi_1(t)|^2 = 4\psi^2 \tag{4.26}$$

is the photon counting rate for a plane wave of complex envelope $\psi_0(t) - \psi_1(t)$ [94]. In turn, we have $|\langle\alpha_0|\alpha_1\rangle|^2 = \exp(-4\psi^2 T) = \exp(-4\alpha^2)$, as expected. The transition from the coherent pulse representation to the continuous-time picture is obtained as follows. We perform a coarse graining in time and divide the time slot into many temporal bins of duration $\delta t \ll T$. Thanks to the properties of coherent states, each time bin still contains a coherent state but with smaller amplitude, such that the reduced pulse in the time bin comprised between t and $t + \delta t$ is equal to $|\tilde{\alpha}_k(t)\rangle = |\alpha_k\sqrt{\delta t/T}\rangle$. Accordingly, for $t' \in (t, t + \delta t]$, the field value is equal to $\psi_k(t') \approx \psi_k(t)$, with mean energy $\psi^2\delta t$.

Given this scenario, the Dolinar receiver operates as depicted in Fig. 4.3.5. The setup consists of a photon counter performing on-off detection connected to a switch s, in which the field $\psi_k(t)$ in each time bin $(t, t + \delta t]$, corresponding to the reduced pulse $|\tilde{\alpha}_k(t)\rangle$, is sequentially injected [17, 95]. The switch switches back and forth between two positions, called $s = 0$ and $s = 1$, with each click of the detector, applying alternatively two different time-varying displacement operations

$$D\left(u_0(t)\right) \quad \text{if} \quad s(t) = 0\,, \tag{4.27}$$

$$D\left(u_1(t)\right) \quad \text{if} \quad s(t) = 1\,, \tag{4.28}$$

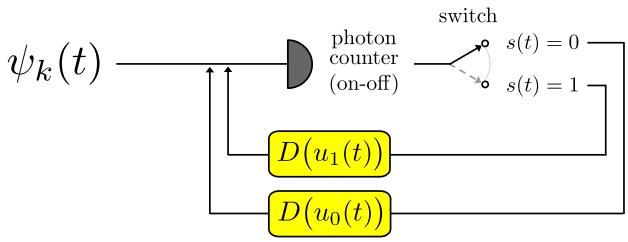


Figure 4.3.5: Setup of the Dolinar receiver. The field $\psi_k(t)$ in each time bin $(t, t+\delta t]$, associated with the reduced pulse $|\tilde{\alpha}_k(t)\rangle$, $k = 0, 1$, undergoes a displacement operation $D(u_0(t))$ or $D(u_1(t))$ determined by the position of a switch $s(t)$, changing at every count of the photodetector. After time T, when all time bins are processed, the value $s(T)$ gives the final decision.

such that $D\left(u_j(t)\right)\psi_k(t) = \psi_k(t) + u_j(t)$, $j, k = 0, 1$. In the above expression $s(t)$ refers to the position of the switch at time $t \leq T$. The initial position of the switch is set to $s(0) = 0$, meaning that the signal in the first time bin is displaced by $D(u_0(0))$. After the first photodetection, if the detector clicks the position of the switch is changed to $s(\delta t) = 1$ and the second copy will be displaced by $D(u_1(\delta t))$. Otherwise, we keep still $s(\delta t) = 0$ and the second copy will be displaced by $D(u_0(\delta t))$. The feedback loop continues according to this basic rule: at every click of the detector the switch changes its position. When all the time bins are processed, the final decision is obtained by reading the position of the switch, according to:

$$s(T) = 0 \quad \rightarrow \quad \text{infer state } |\alpha_0\rangle\,, \tag{4.29}$$

$$s(T) = 1 \quad \rightarrow \quad \text{infer state } |\alpha_1\rangle\,. \tag{4.30}$$

Now, the mathematical problem is to choose the functions $u_0(t)$ and $u_1(t)$ that maximize the correct detection probability at the end of the process, namely:

$$\mathcal{P}_{\rm Dol}(T) = q_0 P_{00}(T) + q_1 P_{11}(T)\,, \tag{4.31}$$

where $P_{kl}(t)$ is the probability of inferring state "l" at time $t \leq T$ if signal "k" is sent, $k, l = 0, 1$ [17, 95]. Actually, in his original proposal Dolinar inferred the optimal solution to the present problem and then verified its optimality afterwards [94]. On the contrary, here we follow an equivalent approach leading to the same solution adopted in [95]. Furthermore, we restrict to the case of symmetric solutions, i.e. $u_0(t) = -u_1(t) = u(t)$.

At first we assume that state $|\alpha_0\rangle = |-\alpha\rangle$ is sent. Then, $s(t)$ can be interpreted as a telegraph stochastic process [96], being alternately driven, in each time bin $(t, t+\delta t]$, by a inhomogeneous Poisson process with rates

$$\lambda_+(t) = |\psi_0(t) + u(t)|^2 \qquad \text{and} \qquad \lambda_-(t) = |\psi_0(t) - u(t)|^2\,. \tag{4.32}$$

At time $t + \delta t$ a correct decision is performed in two cases: firstly if $s(t) = 0$ and the detector detector does not click; secondly if $s(t) = 1$ and the photodetector clicks. Moreover, since $\delta t \ll T$, we may safely assume that the detector effectively measures no more than one photon, thus the probability of obtaining a non-click result in the former case reads $p(\text{off}|0) \approx 1 - \lambda_+(t)\delta t$, while the probability of a click in the latter scenario is equal to $p(\text{on}|0) \approx \lambda_-(t)\delta t$ [51]. Accordingly we have:

$$P_{00}(t+\delta t) = P_{00}(t)\big[1 - \lambda_+(t)\delta t\big] + \big[1 - P_{00}(t)\big]\lambda_-(t)\delta t\,, \tag{4.33}$$

leading to the following differential equation in the limit $\delta t \to 0$:

$$\frac{dP_{00}(t)}{dt} = \lambda_-(t) - \big[\lambda_+(t) + \lambda_-(t)\big] P_{00}(t)\,, \tag{4.34}$$

to be solved with the initial condition

$$P_{00}(0) = 1\,, \tag{4.35}$$

as the switch is initialized in position "0". In a similar way, we prove that $P_{11}(t)$ satisfies the same equation with initial condition $P_{11}(0) = 0$, thus we conclude that also $\mathcal{P}_{\rm Dol}(t)$ is a solution of Eq. (4.34) with $\mathcal{P}_{\rm Dol}(0) = 1/2$.

To solve it, we make the *ansatz* that, at any time $t \leq T$ there exists some value of the displacement amplitude $u(t)$ such that the provisional correct decision probability is exactly equal to the Helstrom bound relative to binary pulses of duration t, namely

$$\mathcal{P}_{\rm Dol}(t) = \frac{1}{2}\left[1 + \sqrt{1 - e^{-4\psi^2 t}}\right] \equiv \frac{1 + R(t)}{2}\,. \tag{4.36}$$

Actually, this is not a very restrictive requirement, as it has been proved that, when multiple identical copies of the encoded quantum states are available, the Helstrom bound can be reached by performing local adaptive measurements on single copies, each one being optimized according to the results measurements on the previous copies [95, 97, 98]. Moreover, if the number of these copies is sufficiently large, the encoded pulse is a sequence of weak coherent states and the optimum measurements are well approximated by suitable displacements and photon counting, retrieving the scenario of the Dolinar setup under investigation [95].

Given this considerations, we plug Eq. (4.36) into (4.34) and obtain:

$$\begin{aligned}\psi^2 e^{-2i\omega t}\,\frac{1 - R^2(t)}{R(t)} = \psi^2 e^{-2i\omega t} + u^2(t) + 2\psi e^{-i\omega t}\,u(t) \\ - \big[\psi^2 e^{-2i\omega t} + u^2(t)\big]\big[1 + R(t)\big]\,,\end{aligned} \tag{4.37}$$

which is solved by [99]

$$u_{\rm Dol}(t) = \frac{\psi\, e^{-i\omega t}}{R(t)} = \frac{\psi\, e^{-i\omega t}}{\sqrt{1 - e^{-4\psi^2 t}}}\,. \tag{4.38}$$

As a consequence, by implementing the time-varying displacement in the setup of Fig. 4.3.5 with the choice $u_0(t) = u_{\rm Dol}(t)$ and $u_1(t) = -u_{\rm Dol}(t)$, at time T we perform BPSK discrimination with the minimum error probability

$$P_{\rm Dol} = 1 - \mathcal{P}_{\rm Dol}(T) = \frac{1}{2}\left[1 + \sqrt{1 - e^{-4\alpha^2}}\right]\,, \tag{4.39}$$

proving the Dolinar receiver to be optimum. We also underline that the optimality of the Dolinar setup is guaranteed regardless the particular shape of the wavepacket $\psi_k(t)$, only provided that the corresponding optical field is described as a coherent state. In the presence of arbitary wavepackets, the optimal displacement amplitude derived by Dolinar with condition $u_0(t) = -u_1(t) = u(t)$, becomes $u_{\rm Dol}(t) = \psi_0(t)/R(t)$ [94].

However, even though theoretically optimum, the Dolinar scheme requires a nontrivial experimental implementation, for a twofold reason. On the one hand, to effectively process the signal in time as a sequence of shorter pulses of duration $\delta t \ll T$, the

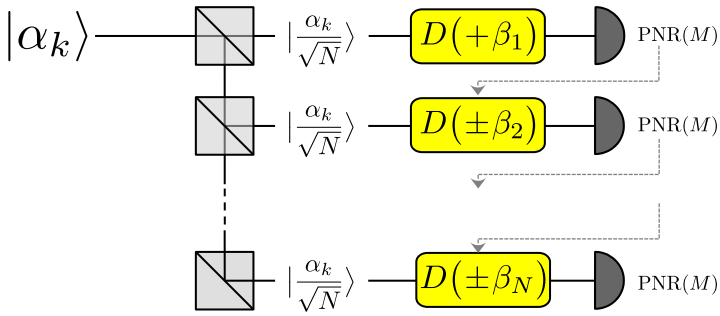


Figure 4.3.6: Scheme of the displacement feed-forward receiver (DFFRE) proposed in [101]. The incoming signal $|\alpha_k\rangle$, $k = 0, 1$, is split into N copies and undergoes a sequence of conditional displacements followed by photon counting. The first copy undergoes a positive displacement, whereas the sign of the subsequent displacements is decided via Bayesian inference.

bandwidth of both the detector and electronic components must be much larger than the symbol repetition rate. Moreover, the feedback circuit needs precise control of an optical-electrical loop to achieve fast response times, to avoid delays in the local oscillator adjustment. On the other hand, continuous measurements and feedback control require detectors with high performances, i.e. high quantum efficiency, low dark count rate, high visibility and short dead time. In fact, the presence of realistic inefficiencies induces unwanted decision errors during the signal processing, which accumulate in time and affect the feedback loop, degrading the quantum advantage of the receiver and overall resulting in a bad performance.

Due to all the previous drawbacks, it is not surprising that the first attempt to implement the Dolinar receiver dates back to 2006 by Lau *et al.* [85], 33 years after Dolinar's paper. The authors realized both a Dolinar and a Kennedy receiver, but the obtained performance was unsatisfactory, as the measured Dolinar error probability was even larger than the Kennedy. The biggest limitation that did not allow to prove the Dolinar optimality was the limited visibility of the amplitude modulator, which was approximately $\approx 98\%$ at the employed bandwidth, while the proper regime should have been $\approx 99.9\%$. Only a year later, in 2007 Cook *et al.* obtained a satisfactory practical implementation of the Dolinar receiver, close to the Helstrom bound in the low energy regime [100].

For all these reasons, the interest has been directed to feed-forward receivers, where the signal is split into a finite number of copies, to obtain a tradeoff between minimum-error discrimination and robustness in practical contexts, as discussed in the following.

4.3.3 The displacement feed-forward receiver

Following the previous philosophy, in 2016 Sych and Leuchs proposed a new receiver, the *displacement feed-forward receiver* (DFFRE), combining both the simplicity of the Kennedy scheme and the optimality of the Dolinar one [101]. The key idea is to split the encoded state $|\alpha_k\rangle$, $k = 0, 1$, into a finite number of copies N rather than a large number of time bins. Thereafter the displacement-photon counting scheme employed in the improved Kennedy receiver [89] is implemented on each copy, optimizing the displacement amplitude via feed-forward Bayesian inference. The initial splitting of the signal may be implemented either by time-multiplexing [102, 103] or by spatial separation into differ-

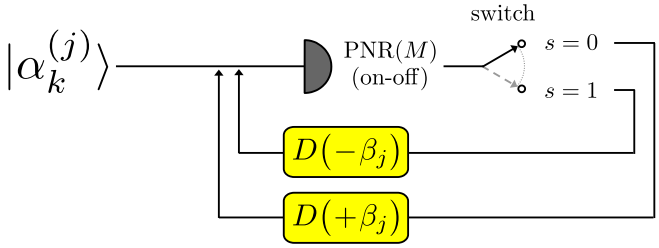


Figure 4.3.7: Equivalent scheme of the DFFRE. Each copy $|\alpha_k^{(j)}\rangle$ undergoes a displacement operation whose sign is determined by the position of a switch s.

ent modes thanks to an array of splitters, providing in both cases a feasible solution overcoming the fast measurements requirement of the Dolinar proposal.

The scheme of the DFFRE is depicted in Fig. 4.3.6. As discussed, the input state $|\alpha_k\rangle$ is split into N rescaled copies, that is

$$|\alpha_k\rangle \to \bigotimes_{j=1}^{N} |\alpha_k^{(j)}\rangle\,, \tag{4.40}$$

where $|\alpha_k^{(j)}\rangle = |\alpha_k/\sqrt{N}\rangle$. Then, each copy undergoes an optimized conditional displacement followed by PNR(M) detection. We start by displacing the first copy $|\alpha_k^{(1)}\rangle$ by $D(\beta_1)$, with amplitude $\beta_1 > 0$ maximizing the correct decision probability, thereafter we perform PNR(M) detection on the output signal $|\alpha_k/\sqrt{N} + \beta_1\rangle$. According to the maximum a posteriori probability (MAP) criterion based on Bayesian inference, the PNR(M) measurement outcome n is used to choose the sign of the optimized conditional displacement to be performed on the second copy. In other words, we infer the state "0" or "1" associated with the maximum a posteriori probability given the outcome n [16, 92, 101]. If "0" is inferred we displace the second copy $|\alpha_k^{(2)}\rangle$ by $D(\beta_2)$, otherwise we apply $D(-\beta_2)$, where $\beta_2 > 0$ is chosen to maximize the correct decision probability, too. Then, we perform again photodetection and repeat the process until the N-th copy.

With ideal detectors, the previous criterion is equivalent to performing on-off detection on each displaced copy. The j-th copy, $j = 1, \ldots, N$, undergoes the displacement operation $D(\sigma_j\beta_j)$, where $\beta_j > 0$ is the optimized amplitude and $\sigma_j = \pm 1$ is the sign of the displacement. The first displacement has a fixed sign, namely, $\sigma_1 = +1$. The other values of σ_j are assigned according to the following decision rule: if we get outcome "off" from the $(j-1)$-th measurement we set $\sigma_j = \sigma_{j-1}$, otherwise if a "on" is retrieved we switch $\sigma_j = -\sigma_{j-1}$. Ultimately, the outcome obtained from the last copy determines the final decision. Therefore, the outcome "off" infers state $|-\sigma_N\alpha\rangle$, outcome "on" infers state $|\sigma_N\alpha\rangle$, σ_N being the sign of the last displacement.

Therefore, the DFFRE mimics the functioning of the Dolinar receiver, albeit with a discrete number of modes, being then equivalent to scheme reported in Fig. 4.3.7. As in Sec. 4.3.2, we have a PNR(M) detector performing on-off detection connected to a switch s, switching at every click between $s = 0$ and $s = 1$, but, now, we process only N copies $|\alpha_k^{(j)}\rangle$, $j = 1, \ldots, N$ [17]. According to the position of the switch $s^{(j)}$ after the j-th copy

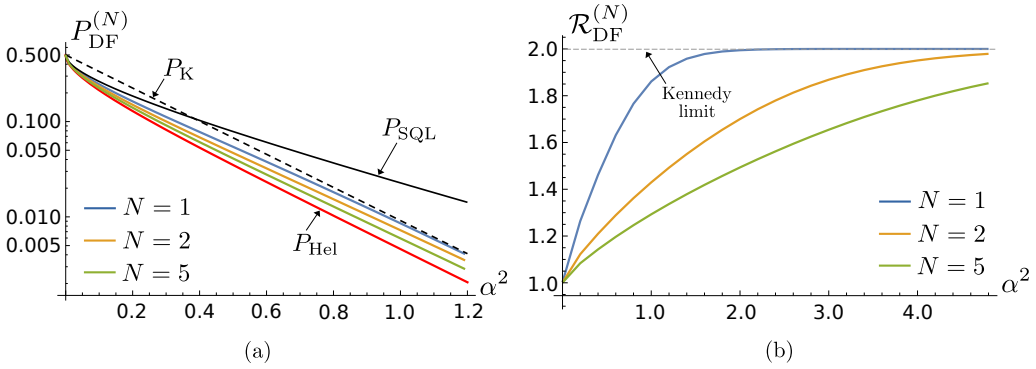


Figure 4.3.8: (a) Log plot of $P_{\rm DF}^{(N)}$ as a function of the signal energy α^2 for different number of copies N. $P_{\rm SQL}$, $P_{\rm Hel}$ and $P_{\rm K}$ refer to the SQL (4.16), the Helstrom bound (4.14), and the Kennedy error probability (4.18), respectively. (b) Plot of $\mathcal{R}_{\rm DF}^{(N)}$ as a function of α^2 for different N. For $\alpha^2 \gg 1$ all ratios approach the Kennedy limit.

is processed, we apply one of the two displacement operations:

$$D(+\beta_j) \quad \text{if} \quad s^{(j)} = 0\,, \tag{4.41}$$

$$D(-\beta_j) \quad \text{if} \quad s^{(j)} = 1\,, \tag{4.42}$$

where the value β_j is optimized to maximize the correct decision probability in each step [17]. If the initial position of the switch is set to $s^{(0)} = 0$, by retracing the passages in Sec. 4.3.2, we obtain the correct decision probability after j steps, namely $\mathcal{P}_{\rm DF}^{(j)} = q_0 P_{00}^{(j)} + q_1 P_{11}^{(j)}$, as:

$$\mathcal{P}_{\rm DF}^{(j)} = \max_{\beta_j} \left\{ \mathcal{P}_{\rm DF}^{(j-1)}\, q_{\rm off}\left(\lambda_-^{(j)}(\alpha)\right) + \left[1 - \mathcal{P}_{\rm DF}^{(j-1)}\right] q_{\rm on}\left(\lambda_+^{(j)}(\alpha)\right) \right\}, \tag{4.43}$$

to be solved with the initial condition $\mathcal{P}_{\rm DF}^{(0)} = 1/2$, where

$$q_{\rm off}(x) = e^{-x} \quad \text{and} \quad q_{\rm on}(x) = 1 - e^{-x}\,, \tag{4.44}$$

are the probabilities of "off" and "on" results, respectively, and

$$\lambda_\pm^{(j)}(\alpha) = \left| \beta_j \pm \frac{\alpha}{\sqrt{N}} \right|^2, \tag{4.45}$$

is the mean photon number of the resulting displaced copies. Ultimately, we retrieve the discrimination error probability of the DFFRE after N copies as:

$$P_{\rm DF}^{(N)} = 1 - \mathcal{P}_{\rm DF}^{(N)}\,. \tag{4.46}$$

Plots of $P_{\rm DF}^{(N)}$ are depicted in Fig. 4.3.8(a) as a function of the input energy α^2 and different values of N. The receivers is near-optimum and beat the SQL for all energies. For $N = 1$ the DFFRE coincides with the improved Kennedy receiver [89], and by increasing

N the error probability is further reduced for $\alpha^2 \ll 1$, coming closer to the Helstrom bound (4.14), as emerges by computing the ratio

$$\mathcal{R}_{\rm DF}^{(N)} = \frac{P_{\rm DF}^{(N)}}{P_{\rm Hel}}\,, \tag{4.47}$$

plotted in Fig. 4.3.8(b). In the regime $\alpha^2 \ll 1$, the larger the number of copies, the smaller the ratio $\mathcal{R}_{\rm DF}^{(N)}$, whereas in the asymptotic limit $\alpha^2 \gg 1$ the DFFRE approaches the Kennedy receiver for any N.

4.3.4 The Sasaki-Hirota receiver

To conclude, we present a further proposal of optimum receiver, suggested by Sasaki and Hirota in 1996 [104], who proved that it is possible to reach the Helstrom bound by recasting the problem into the two-dimensional subspace spanned by the encoded states.

At first, we perform the "nulling" displacement $D(\alpha)$ to he encoded signals $|\alpha_k\rangle$, $k = 0, 1$, as in the Kennedy scheme, shifting the discrimination problem to states $|0\rangle$ and $|2\alpha\rangle$. Now, we consider the following orthonormal basis of the subspace $\mathcal{S}$ spanned by $|0\rangle$ and $|2\alpha\rangle$:

$$|\eta_0\rangle = |0\rangle \quad \text{and} \quad |\eta_1\rangle = \frac{1}{\sqrt{1-X^2}}\big(|2\alpha\rangle - X\,|0\rangle\big)\,, \tag{4.48}$$

where $X = \langle 0|2\alpha\rangle$, and construct the unitary operator

$$U(\theta) = \cos\theta\,\Big(|\eta_0\rangle\langle\eta_0| + |\eta_1\rangle\langle\eta_1|\Big) + \sin\theta\,\Big(|\eta_0\rangle\langle\eta_1| - |\eta_1\rangle\langle\eta_0|\Big)\,, \tag{4.49}$$

depending on a free parameter θ. In the *Sasaki-Hirota receiver* the operator $U(\theta)$ is applied to the displaced signals $|0\rangle$ and $|2\alpha\rangle$, followed by a projective measurement onto the basis (4.48), namely:

$$\Pi_0 = |\eta_0\rangle\langle\eta_0| \quad \text{and} \quad \Pi_1 = |\eta_1\rangle\langle\eta_1|\,. \tag{4.50}$$

By numerical optimization of θ, the authors showed that the present scheme reaches the Helstrom bound [51, 104].

We note that, since $\langle 0|\eta_1\rangle = 0$, the projective measurement (4.50) may be safely replaced by on-off detection, making it feasible in realistic conditions. On the contrary, the unitary $U(\theta)$ is a non-Gaussian operation, whose realization would require highly nonlinear optical elements, thus making this kind of receiver not realizable with the usual practical linear optics components.

4.4 Hybrid receivers

As discussed in the previous section, most sub shot-noise-limited receivers are constructed via the displacement-photon counting technique, probing the particle-like behaviour of the encoded quantum field. On the contrary, the SQL is achieved by homodyne detection, which gives information on the field phase, thus probing the wave-like properties of radiation. Therefore, a natural question arises, that is whether or not it is

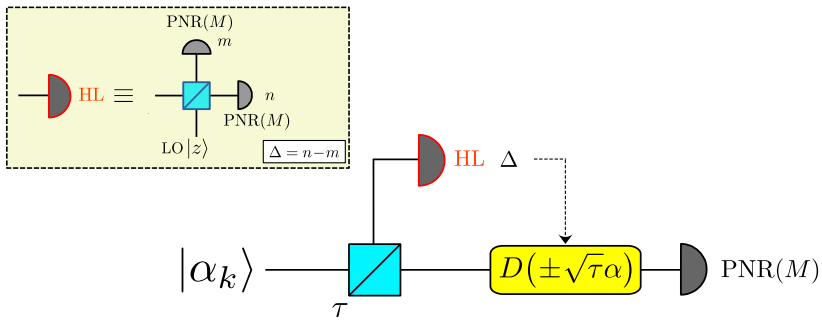


Figure 4.4.1: Scheme of the HYNORE. The incoming signal is split at a beam splitter with transmissivity τ, thereafter HL detection is implemented on the reflected branch. The outcome $\Delta = n - m$ is exploited to decide the displacement operation implemented on the transmitted signal. (Inset) Setup of the weak-field homodyne, or homodyne-like, detection. The signal is mixed at a balanced beam splitter with a low-intensity local oscillator (LO), and PNR(M) detection is performed on the output modes.

possible to design hybrid receivers employing both of the field properties to obtain a better performance in terms of error probability.

To this aim, in this section we firstly propose an innovative receiver: the *hybrid near-optimum receiver* (HYNORE), a single-shot receiver based on the combination of the homodyne-like detection presented in Sec. 2.4.2.2 and the displacement-photon counting scheme of the Kennedy setup [16]. Later on, we extend this approach to multi-copy receivers and construct the *hybrid feed-forward receiver* (HFFRE), by embedding homodyne-like detection into the DFFRE scheme [17]. In both our proposals, we adopt homodyne-like detection (employing PNR detectors) instead of the traditional homodyne scheme (implemented by p-i-n photodiodes). The motivation behind this choice is merely practical. In fact, from an experimental point of view, a hybrid scheme involving both homodyne detection and displacement-photon counting would require to employ different types of detectors for the two components of the setup: two proportional photodiodes producing macroscopic photocurrents to implement the standard homodyne measurement, and a PNR detector for the displacement receiver. Moreover, in the context of quantum discrimination, pulsed homodyne detection would be preferable for an experimental realization at telecom wavelength, due to the reduced response time of the measurement [105–107]. On the contrary, employing homodyne-like and low-intensity local oscillator provides a more fascinating solution since the resulting receiver is obtained with the use of sole PNR detectors.

In the following, we present in detail both the HYNORE and the HFFRE, comparing it to the Kennedy receiver and the DFFRE, respectively. The results obtained in both this section and the following ones are all original.

4.4.1 The hybrid near-optimum receiver

The scheme of the HYNORE is depicted in Fig. 4.4.1. The idea is to exploit a displacement-PNR(M) (DPNR) setup where the nulling displacement is not assigned a priori, but is conditioned on the outcome of a homodyne-like (HL) detection performed on a fraction of the input signal. More in detail, we split the input coherent state $|\alpha_k\rangle$, $k = 0, 1$, at a beam splitter of variable transmissivity τ (this can be obtained, for instance, considering

the polarization of the input states and by using a polarizing beam splitter), such that:

$$|\alpha_k\rangle \to |\alpha_k^{(r)}\rangle \otimes |\alpha_k^{(t)}\rangle = |-\sqrt{1-\tau}\alpha_k\rangle \otimes |\sqrt{\tau}\alpha_k\rangle\,. \tag{4.51}$$

Then, we perform HL detection on the reflected branch $|\alpha_k^{(r)}\rangle$ and, thereafter, apply a feed-forward nulling displacement operation on the transmitted part of the signal $|\alpha_k^{(t)}\rangle$ conditioned on the difference photocurrent $\Delta = n-m$ retrieved from the homodyne-like measurement:

$$\Delta \geq 0 \to \text{apply } D\left(\sqrt{\tau}\alpha\right)\,, \tag{4.52a}$$
$$\Delta < 0 \to \text{apply } D\left(-\sqrt{\tau}\alpha\right)\,, \tag{4.52b}$$

Finally, on the resulting displaced state we perform a PNR(M) measurement in terms of on-off detection: the photon number resolution of the detector will turn out to be useful in the presence of detection imperfections, as we will see in the following. The intuitive motivation behind the feed-forward rule of Eqs. (4.52) is the following. If we suppose that $|\alpha_0\rangle$ was sent, from the definition of the beam splitter operation of Eq. (4.51) it is more likely to obtain $\Delta > 0$. As a consequence, we decide to perform a positive displacement sending the transmitted signal into the vacuum such that the PNR(M) detector does not click and we refer to this event as "off". Of course there is still a non-zero probability to get $\Delta < 0$, and in that case we decide to apply a negative displacement such that the on-off detector is more likely count some photon. This event is called "on". Finally, for the case $\Delta = 0$, the displacement amplitude is chosen to be positive simply by convention. Analogous considerations may be obtained by considering state $|\alpha_1\rangle$. Given this scenario, the *decision rule* at the end of the final measurement is chosen according to Table 4.4.1.

outcomes		decision
$\Delta \geq 0$	off	"0"
$\Delta < 0$	on	"0"
$\Delta < 0$	off	"1"
$\Delta \geq 0$	on	"1"

Table 4.4.1: Decision strategy for the HYNORE in Fig. 4.4.1.

Since:

$$p(\Delta \geq 0; \text{on}|0) = p(\Delta < 0; \text{off}|1) = 0\,, \tag{4.53}$$

the error probability for the HYNORE reads:

$$\begin{aligned} P_{\text{HY}}(\tau, z) &= \frac{1}{2}\left[\, p(\Delta < 0; \text{off}|0) + p(\Delta \geq 0; \text{off}|1)\right] \\ &= \frac{1}{2}\left[\sum_{\Delta=-M}^{-1} \mathcal{S}_\Delta\big(\alpha_0^{(r)}\big)e^{-4\tau\alpha^2} + \sum_{\Delta=0}^{M} \mathcal{S}_\Delta\big(\alpha_1^{(r)}\big)e^{-4\tau\alpha^2}\right] \\ &= \frac{e^{-4\tau\alpha^2}}{2}\left[\sum_{\Delta=-M}^{-1} \mathcal{S}_\Delta(\sqrt{1-\tau}\alpha) + \sum_{\Delta=0}^{M} \mathcal{S}_\Delta(-\sqrt{1-\tau}\alpha)\right]\,, \end{aligned} \tag{4.54}$$

depending on the transmissivity τ, ruling the splitting of the incoming state, and the amplitude of the local oscillator (LO) $|z\rangle$, $z \geq 0$, of HL detection. We recall that the HL probability distribution reads:

$$\mathcal{S}_{\Delta}(\alpha_k^{(r)}) = \sum_{n,m=0}^{M} p_n\big(\mu_+(\alpha_k^{(r)})\big)\, p_m\big(\mu_-(\alpha_k^{(r)})\big)\, \delta_{(n-m),\Delta} \tag{4.55}$$

where $\delta_{k,j}$ is the Kronecker delta, M is the photon-number resolution,

$$\mu_{\pm}(\alpha_k^{(r)}) = \frac{|\alpha_k^{(r)} \pm z|^2}{2}\,, \tag{4.56}$$

is the mean energy on the two output branches, respectively, and

$$p_n(\mu) = \begin{cases} e^{-\mu}\,\dfrac{\mu^n}{n!} & \text{if } n < M\,, \\ 1 - e^{-\mu}\displaystyle\sum_{j=0}^{M-1}\frac{\mu^j}{j!} & \text{if } n = M\,. \end{cases} \tag{4.57}$$

For completeness, we note that performing standard homodyne detection instead of homodyne-like, the error probability of the previous equation becomes

$$P_{\rm HY}^{(\rm HD)}(\tau) = \frac{e^{-4\tau\alpha^2}}{2}\,\left\{1 - \mathrm{erf}\left[\sqrt{2(1-\tau)}\alpha\right]\right\}\,. \tag{4.58}$$

We also note that if $\tau = 0$ we have the homodyne receiver, whereas if $\tau = 1$ we retrieve the Kennedy one. This can be understood since when $\tau = 1$ the information coming from the homodyne receiver is inconclusive, as it measures the vacuum leading to a positive or negative outcome with 50% of probability. Therefore, known the outcome sign, we can apply the same inference strategy as in the Kennedy receiver.

Given this outline, in the following we compute the error probability of the HYNORE by considering two alternative scenarios involving either ideal photodetectors, namely PNR(M) detectors with $M = \infty$, or realistic PNR detectors with finite resolution M.

4.4.1.1 HYNORE with ideal photodetectors

At first, let us consider PNR(∞) detectors, and a LO $|z\rangle$ with fixed intensity z^2. In this case, the HL probability distribution (4.55) approaches a Skellam distribution, as discussed in Sec. 2.4.2.2. Under these conditions, we retrieve the HYNORE error probability by optimizing Eq. (4.54) with respect to τ, i.e. finding the transmissivity $\tau_{\rm opt}^{(\rm id)}$, that in general is a function of α^2, minimizing the value of $P_{\rm HY}(\tau, z)$ for every α^2. Consequently, we obtain the optimized error probability of our receiver as

$$P_{\rm HY}^{(\rm id)} = \min_{\tau} P_{\rm HY}(\tau, z) \qquad \text{for PNR}(\infty)\text{ detection}\,, \tag{4.59}$$

depicted in Fig. 4.4.4(a). As we see, the HYNORE proves to be near-optimum, outperforming the Kennedy receiver for all α^2.

To better enlighten this advantage, it is also relevant to introduce the ratio with the standard Kennedy receiver (4.18),

$$R_{h/K}^{(\rm id)} = \frac{P_{\rm HY}^{(\rm id)}}{P_K}\,. \tag{4.60}$$

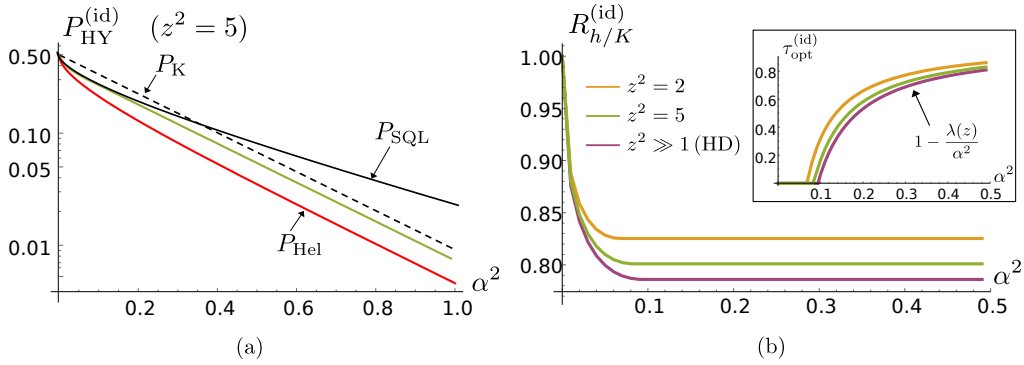


Figure 4.4.2: (a) Log plot of $P_{\rm HY}^{(\rm id)}$ as a function of α^2 for LO intensity $z^2=5$ compared to the Kennedy receiver (4.18), the SQL (4.16) and the Helstrom bound (4.14). (b) Plot of the ratio $R_{h/K}^{(\rm id)}$ as a function of α^2 for several values of the LO intensity z^2. In the inset, plot of the optimized transmissivity $\tau_{\rm opt}^{(\rm id)}$ as a function of α^2. For $\alpha^2 > N_{\rm th}(z)$ we have $\tau_{\rm opt}^{(\rm id)} = 1-\lambda(z)/\alpha^2$. In both the pictures we consider PNR(∞) detectors.

Plots of $R_{h/K}^{(\rm id)}$ and $\tau_{\rm opt}^{(\rm id)}$ (in the inset) are displayed in Fig. 4.4.4(b) for different LO intensity z^2. It emerges that $\tau_{\rm opt}^{(\rm id)}=0$ up to a threshold energy $N_{\rm th}(z)$ which depends on the LO amplitude z, while for $\alpha^2 > N_{\rm th}(z)$ it is an increasing function of the energy and reaches asymptotically 1. Note that in the limit $\tau \to 1$ some information about the signal reaches the homodyne receiver and we still have an improvement of the performance.

If $\alpha^2 \leq N_{\rm th}(z)$ the optimized strategy is realized with the sole homodyne-like setup, whereas for larger energies the more efficient scheme is obtained by the appropriate interplay between the homodyne-like and the DPNR parts of our receiver. The choice of the optimal τ makes the receiver near-optimum with a ratio $R_{h/K}^{(\rm id)}$ saturating to the value $R_{\infty}^{(\rm id)} < 1$ for every value of the LO intensity z^2.

As we noticed, if we increase the value of z^2, the performance of the homodyne-like detection approaches the standard homodyne one and the HYNORE performs better and better. In fact, the variance of the homodyne-like quadrature probability distribution decreases as the local oscillator energy becomes quite larger with respect to the input signal one [39]. In this case, the ratio in Eq. (4.60) reads

$$R_{h/K}^{(\rm HD)} = \frac{P_{\rm HY}^{(\rm HD)}}{P_K} = \frac{e^{4(1-\tau)\alpha^2}}{2}\left\{1-{\rm erf}\left[\sqrt{2(1-\tau)}\alpha\right]\right\}. \tag{4.61}$$

The saturation of $R_{h/K}^{(\rm id)}$ for large α^2 suggests the following ansatz on the expression of the optimized $\tau_{\rm opt}^{(\rm id)}$, namely:

$$\tau_{\rm opt}^{(\rm id)} = 1-\frac{\lambda(z)}{\alpha^2} \quad \text{for} \quad \alpha^2 > N_{\rm th}(z)\,, \tag{4.62}$$

where $\lambda(z) \in \mathbb{R}_+$ and depends on the LO amplitude z. As an example, for the homodyne limit $z^2 \to \infty$, by computing the derivative of Eq. (4.61) with respect to τ and inserting the expression in Eq. (4.62) we get the following relation that must be satisfied by $\lambda \equiv$

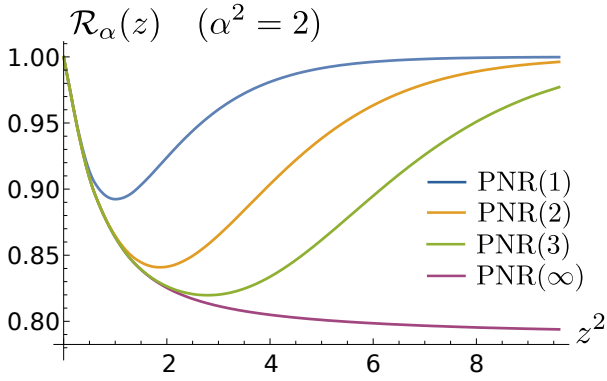


Figure 4.4.3: Plot of $\mathcal{R}_\alpha(z)$ as a function of the LO intensity z^2 for different resolution M and fixed signal energy $\alpha^2 = 2$. For $M < \infty$, $\mathcal{R}(z)$ exhibits a minimum at a finite LO intensity.

$\lambda(z = \infty)$:

$$\sqrt{\frac{2}{\pi\lambda}} - 4e^{2\lambda}\left[1 - \mathrm{erf}\left(\sqrt{2\lambda}\right)\right] = 0\,, \tag{4.63}$$

that leads to the numerical solution $\lambda \approx 0.094$. Then, the threshold $N_{\rm th}^{(\rm HD)} \equiv N_{\rm th}(z = \infty)$ can obtained by setting $\tau_{\rm opt}^{(\rm id)} = 0$, bringing to $N_{\rm th}^{(\rm HD)} = \lambda$ and the saturation ratio reads:

$$R_\infty^{(\rm HD)} = e^{4\lambda}\left[1 - \mathrm{erf}\left(\sqrt{2\lambda}\right)\right] \approx 0.786\,. \tag{4.64}$$

An identical analysis can be performed for the homodyne-like case, where we may expect $\lambda(z) < \lambda$.

4.4.1.2 HYNORE with finite photon-number resolution

We now consider the more realistic case of PNR(M) detectors having a finite photon number resolution M, being only able to resolve any number of photons n up to M. Clearly, PNR(1) is a on-off photodetector. In the absence of detection imperfections, the presence of a reduced resolution affects the sole homodyne-like setup, reducing the inferable information on the field phase, since the displacement-photon counting scheme performed on the transmitted branch is associated with on-off decision strategy regardless the value of M.

Differently from the ideal case, when $M < \infty$ the error probability (4.54) is not a monotonous function of the LO intensity. This emerges by computing the following z-dependent ratio, for fixed input signal energy and varying LO:

$$\mathcal{R}_\alpha(z) = \frac{\min_\tau P_{\rm HY}(\tau, z)}{P_{\rm K}}\,, \tag{4.65}$$

depicted in Fig. 4.4.3 for different values of M. As discussed above, in the ideal case, i.e. $M = \infty$, Eq. (4.65) descreases monotonically with z^2, proving the homodyne limit to be the best working regime. On the contrary, for $M < \infty$, $\mathcal{R}_\alpha(z)$ exhibits a minimum at a finite LO intensity. Indeed, if only few photons can be resolved, increasing the LO is useless since much of its energy could not be detected.

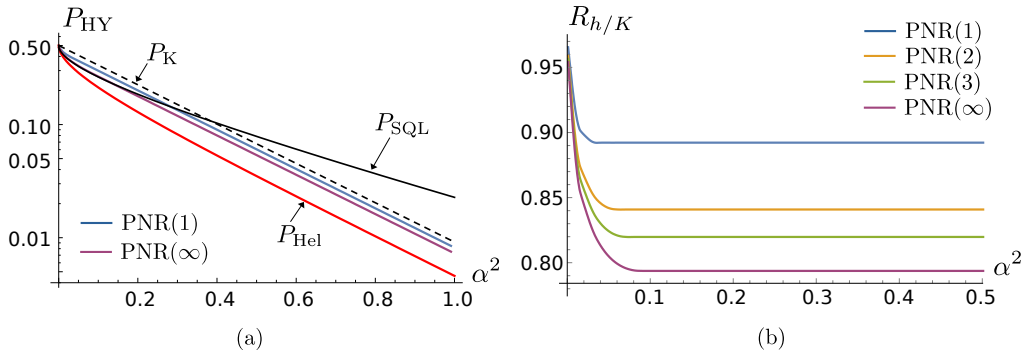


Figure 4.4.4: (a) Log plot of $P_{\rm HY}$ as a function of α^2 for different resolution M compared to the Kennedy receiver (4.18), the SQL (4.16) and the Helstrom bound (4.14). (b) Plot of the ratio $R_{h/K}$ as a function of α^2 for different M. The case $M = \infty$ refers to the homodyne limit (4.58) optimized over transmissivity.

In turn, to establish the performance of the HYNORE, we are entitled to optimize Eq. (4.54) over both τ and z, leading to the optimized error probability

$$P_{\rm HY} = \min_{\tau,z} P_{\rm HY}(\tau, z) \qquad \text{for PNR}(M) \text{ detection}\,, \tag{4.66}$$

together with the ratio

$$R_{h/K} = \frac{P_{\rm HY}}{P_K}\,, \tag{4.67}$$

where, for the sake of simplicity, the dependence on the resolution M has not been explicitly reported. Plots of $P_{\rm HY}$ and $R_{h/K}$ are depicted in Fig. 4.4.6(a) and (b), respectively, in which the case $M = \infty$ refers to the homodyne limit (4.58) optimized over transmissivity. As we can see, the effect of the finite resolution is to decrease the saturation ratio R_∞, which in any case is still less than 1, maintaining the advantages of HYNORE with respect to the Kennedy. We also note that employing high resolution detectors is not strictly required to obtain a performance close to the ideal case. Furthermore, the optimized transmissivity $\tau_{\rm opt}$ shows analogous behavior to the one depicted in the inset of Fig. 4.4.4(b), namely $\tau_{\rm opt} = 1 - \lambda(M)/\alpha^2$, $\lambda(M)$ being a increasing function of the PNR resolution M such that $\lambda(M) < \lambda \approx 0.094$. In contrast, the optimized LO intensity is of the order of the resolution for all input energies; in fact we have $z^2_{\rm opt} \lesssim M$.

4.4.2 The hybrid feed-forward receiver

As discussed above, employing a hybrid receiver like the HYNORE turns out to be beneficial for quantum discrimination, obtaining a better performance than the Kennedy receiver thanks to the splitting of the incoming signal into two beams, followed by a suitable adaptive operation. Given this consideration, a natural extension emerges. That is, the homodyne-like setup may be suitably embedded into the multi-copy approach described in Sec. 4.3.3 to construct a new kind of receiver, referred to as the *hybrid feed-forward receiver* (HFFRE) [17]. In more detail, the HFFRE is obtained by suitably merging the setups of both the HYNORE and the DFFRE, resulting in the scheme depicted in Fig. 4.4.5.

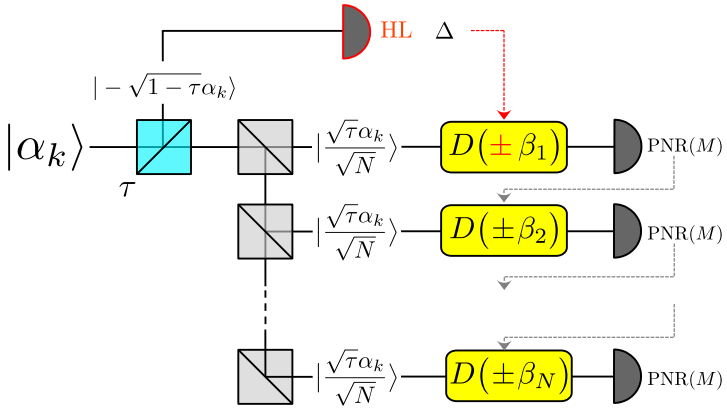


Figure 4.4.5: Scheme of the HFFRE. We split the incoming signal $|\alpha_k\rangle$, $k = 0, 1$, at a beam splitter of variable transmissivity τ. We perform HL detection on the reflected branch, whereas we implement the displacement feed-forward setup on the transmitted one. We exploit the HL outcome to decide the sign of the displacement operation on the first copy of the transmitted signal.

The insight is to exploit a HL measurement to guide the choice of the first displacement operation sign in the DFFRE. As for the HYNORE, we divide the incoming signal $|\alpha_k\rangle$, $k = 0, 1$, at a beam splitter with variable transmissivity τ, see Eq. (4.51). The reflected signal $|\alpha_k^{(r)}\rangle$ undergoes HL detection with difference photocurrent outcome Δ. Then, we split the transmitted state $|\alpha_k^{(t)}\rangle$ into N copies, $|\alpha_k^{(t)}/\sqrt{N}\rangle$, and implement the same procedure described in Sec. 4.3.3. The only difference with respect to the displacement feed-forward receiver lies in the displacement operation performed on the first copy. Indeed, the difference photocurrent Δ provides us with a priori information exploitable to decide the sign of the first optimized displacement operation, according to the HYNORE adaptive rule, namely:

$$\begin{cases} \Delta \geq 0 & \rightarrow \quad \text{apply } D(\beta_1) \\ \Delta < 0 & \rightarrow \quad \text{apply } D(-\beta_1)\,, \end{cases} \tag{4.68}$$

$\beta_1 > 0$. Displacements on the other copies are still conditioned on the outcomes of the $(j-1)$-th PNR(M) measurement.

Thus, the probability of performing a correct decision $\mathcal{P}_{\rm HF}^{(j)}(\tau, z)$ after j steps gets the same form of Eq. (4.43):

$$\mathcal{P}_{\rm HF}^{(j)}(\tau, z) = \max_{\beta_j} \Big\{ \mathcal{P}_{\rm HF}^{(j-1)}(\tau, z) q_{\rm off}\Big(\lambda_-^{(j)}(\sqrt{\tau}\alpha)\Big) + \Big[1 - \mathcal{P}_{\rm HF}^{(j-1)}(\tau, z)\Big] q_{\rm on}\Big(\lambda_+^{(j)}(\sqrt{\tau}\alpha)\Big) \Big\}\,, \tag{4.69}$$

with the rates $\lambda_\pm^{(j)}$ in Eq. (4.45), albeit to be solved with a different initial condition, that is:

$$\mathcal{P}_{\rm HF}^{(0)}(\tau, z) = \frac{1}{2}\left[\sum_{\Delta=-M}^{-1} \mathcal{S}_\Delta\Big(\alpha_1^{(r)}\Big) + \sum_{\Delta=0}^{M} \mathcal{S}_\Delta\Big(\alpha_0^{(r)}\Big)\right],$$

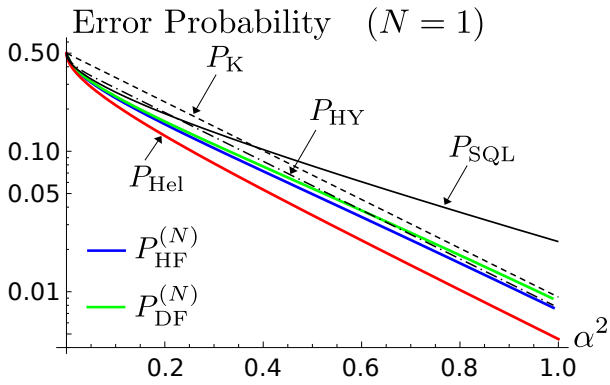


Figure 4.4.6: Log plot of $P_{\rm HF}^{(N)}$ and $P_{\rm DF}^{(N)}$ as a function of the signal energy α^2 for $N = 1$. The PNR resolution is $M = 2$. $P_{\rm SQL}$, $P_{\rm Hel}$, $P_{\rm K}$ and $P_{\rm HY}$ refer to the SQL (4.16), the Helstrom bound (4.14), and the error probabilities of the Kennedy receiver (4.18) and the HYNORE (4.66), respectively.

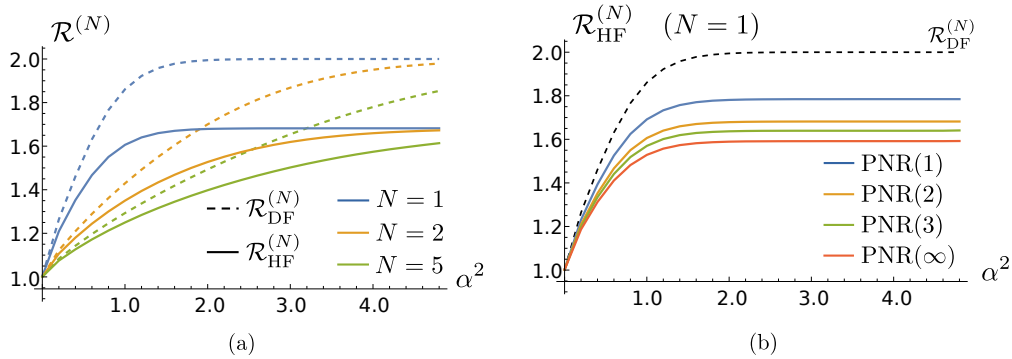


Figure 4.4.7: (a) Plot of $\mathcal{R}_{\rm p}^{(N)}$, $\rm p = DF, HF$, as a function of α^2 for different number of copies N. The PNR resolution is $M = 2$. (b) Plot of $\mathcal{R}_{\rm HF}^{(N)}$ as a function of α^2 for $N = 1$ and different PNR resolutions M. The dashed line corresponds to $\mathcal{R}_{\rm DF}^{(N)}$ for $N = 1$.

corresponding to the probability of correct decision after the HL measurement. Clearly, if $\tau = 1$ we retrieve the results of the DFFRE.

As both τ and z are free parameters, after N copies the error probability reads

$$P_{\rm HF}^{(N)} = 1 - \max_{\tau,z} \mathcal{P}_{\rm HF}^{(N)}(\tau, z)\,, \tag{4.70}$$

depicted in Fig. 4.4.6 as a function of the input energy α^2 and compared to the DFFRE error probability $P_{\rm DF}^{(N)}$ in Eq. (4.46). The HFFRE outperforms the DFFRE, $P_{\rm HF}^{(N)} \leq P_{\rm DF}^{(N)}$. Both the receivers are near-optimum and beat the SQL for all energies, but we observe different asymptotic scalings. Indeed, for $\alpha^2 \gg 1$, the DFFRE approaches the Kennedy receiver, $P_{\rm DF}^{(N)} \approx P_{\rm K}$, whereas the HFFRE reaches the HYNORE, $P_{\rm HF}^{(N)} \approx P_{\rm HY}$, with the $P_{\rm HY}$ in Eq. (4.66). As a consequence, exploiting information on both the phase and the photon statistics of the field proves to be a powerful tool to reduce the error probability.

Furthermore, by increasing the number of copies N the performance of both the feed-forward receivers improves for $\alpha^2 \ll 1$, coming closer to the Helstrom bound (4.14), as

emerges by computing the ratio

$$\mathcal{R}_{\rm p}^{(N)} = \frac{P_{\rm p}^{(N)}}{P_{\rm Hel}}\,, \quad ({\rm p} = {\rm DF}, {\rm HF})\,, \tag{4.71}$$

plotted in Fig. 4.4.7(a).

In the regime $\alpha^2 \ll 1$, the larger the number of copies, the smaller the ratio $\mathcal{R}_{\rm p}^{(N)}$, whereas in the asymptotic limit $\alpha^2 \gg 1$ the displacement and hybrid receiver converge to Kennedy and HYNORE, respectively, regardless the value of N. Moreover, the ratio for the hybrid receiver $\mathcal{R}_{\rm HF}^{(N)}$ may be further reduced by increasing the PNR resolution M, as shown in Fig. 4.4.7(b). In particular, the asymptotic ratio is reduced for greater values of M and reaches its minimum value for PNR(∞) detectors, i.e. ideal photodetectors, in which case the HL distribution in Eq. (4.55) becomes a Skellam distribution.

4.5 Quantum receivers in the presence of detection imperfections

So far, we described the structure of quantum receivers by considering an ideal scenario involving perfect detection schemes and excluding imperfections within each element of the setups. In these conditions, we proved the hybrid receivers, namely the HYNORE and HFFRE, to outperform the receivers based on displacement strategies, i.e. the Kennedy receiver and the DFFRE, respectively. Now, we may wonder whether or not the obtained enhancement in the error probability could be effectively realized in practical experiments. This raises the problem of the robustness of the proposed receivers in the presence of realistic conditions, e.g. limited quantum detection efficiency, dark counts and visibility reduction in the adopted displacement operations.

As one may expect, in a realistic scenario neither the hybrid nor the displacement receiver remain near-optimum, therefore they are not able to approach the Helstrom bound (4.14) anymore. Accordingly, a new goal emerges, that is to show whether or not these receivers are still able to beat the SQL (4.16) even in the presence of practical imperfections. Indeed, in this case we would get a robust quantum advantage with respect to the best receiver achievable with semi-classical means.

In the following, we compare the performance of the proposed hybrid receivers with respect to their corresponding displacement-photon counting schemes in the presence of the typical imperfections occurring in PNR detection [16, 17]. In particular, we consider a non-unit quantum efficiency $\eta \leq 1$ of the PNR(M) detectors, as well as the presence of dark counts. Moreover, since the displacement operation is realized into practice by letting the signal interfere with a suitable LO at a beam splitter [84], we also address the effects of non-unit visibility $\xi \leq 1$.

4.5.1 HYNORE vs displacement receiver

At first, we start by addressing the robustness of single-copy receivers, namely the HYNORE and the displacement receiver. For a better clarity, we discuss separately the impact on the receiver performance of three experimental defects above presented, namely quantum efficiency, dark counts and reduced visibility.

4.5.1.1 Reduced quantum efficiency

Concerning the inefficient photodetection, the introduction of a quantum efficiency η has the effect of re-scaling all the coherent amplitudes of the measured pulses by a factor $\sqrt{\eta}$, since it corresponds to a photon loss.

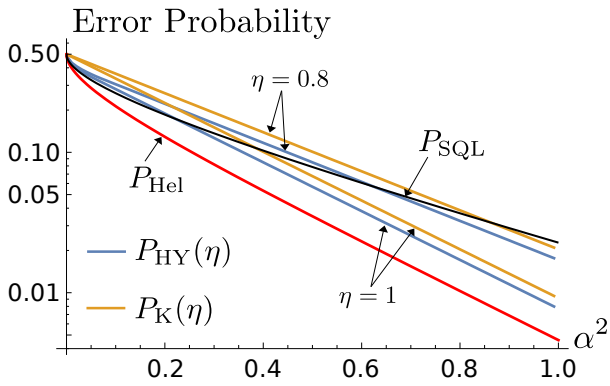


Figure 4.5.1: Log plot of $P_{\rm HY}(\eta)$ and $P_{\rm K}(\eta)$ as a function of the signal energy α^2 for different quantum efficiency η. The PNR resolution is $M = 2$. $P_{\rm SQL}$ and $P_{\rm Hel}$ refer to the SQL (4.16) and the Helstrom bound (4.14), respectively.

Thus, for the Kennedy receiver employing inefficient on-off detection, the error probability is changed into:

$$P_{\rm K}(\eta) = \frac{e^{-4\eta\alpha^2}}{2} \,. \tag{4.72}$$

Instead, in the HYNORE, the efficiency affects both the HL and the PNR(M) measurement schemes. For the HL detection the rates in Eq. (4.56) are changed into $\mu_\pm \to \eta\mu_\pm$, obtaining:

$$\mathcal{S}_\Delta(\eta;\alpha_k^{(r)}) = \sum_{n,m=0}^{M} p_n\big(\eta\,\mu_+(\alpha_k^{(r)})\big)\, p_m\big(\eta\,\mu_-(\alpha_k^{(r)})\big)\, \delta_{(n-m),\Delta} \,. \tag{4.73}$$

On the other hand, an inefficient on-off detection by the PNR implies the substitution $\exp(-4\tau\alpha^2) \to \exp(-4\eta\tau\alpha^2)$. By performing these substitutions into Eq. (4.54) we get the corresponding error probability:

$$P_{\rm HY}(\eta) = \min_{\tau,z} P_{\rm HY}(\tau, z; \eta) \,, \tag{4.74}$$

with

$$P_{\rm HY}(\tau, z; \eta) = \frac{e^{-4\eta\tau\alpha^2}}{2} \left[\sum_{\Delta=-M}^{-1} \mathcal{S}_\Delta(\eta;\alpha_0^{(r)}) + \sum_{\Delta=0}^{M} \mathcal{S}_\Delta(\eta;\alpha_1^{(r)}) \right] . \tag{4.75}$$

The error probabilities $P_{\rm K}(\eta)$ and $P_{\rm HY}(\eta)$ are depicted in Fig. 4.5.1 for PNR(2) receivers. The behavior is analogous for all resolution M. As expected, the performance of both detector is degraded for lower quantum efficiency, but, interestingly, for a given value of η, exploiting the HYNORE is always preferable than the Kennedy, as $P_{\rm HY}(\eta) \leq P_{\rm K}(\eta)$. In particular, the relative ratio

$$R_{h/K}(\eta) = \frac{P_{\rm HY}(\eta)}{P_{\rm K}(\eta)} \,, \tag{4.76}$$

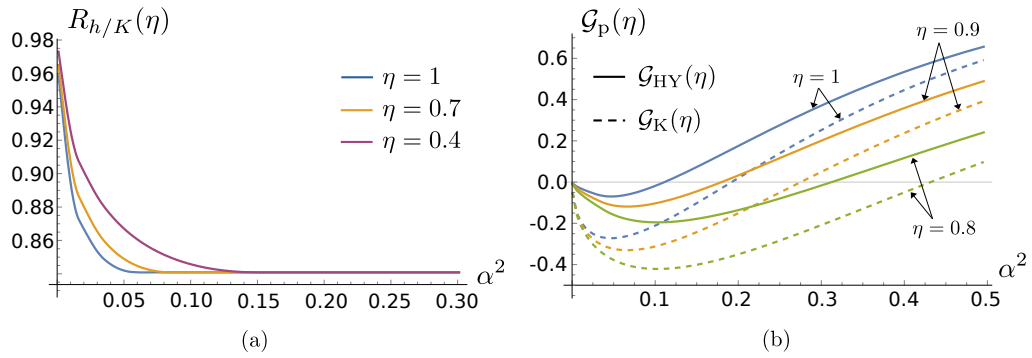


Figure 4.5.2: (a) Plot of the ratio $R_{h/K}(\eta)$ as a function of α^2 for different η. (b) Plot of the gain $\mathcal{G}_{\rm p}(\eta)$, ${\rm p} = {\rm K}, {\rm HY}$, as a function of α^2 for different η. The PNR resolution is $M = 2$.

reported in Fig. 4.5.2(a), saturates to the same R_∞ obtained for $\eta = 1$, regardless the value of quantum efficiency. Furthermore, in the high-energy regime, both receivers beat the SQL (4.16). To better highlight this feature, we consider the gain

$$\mathcal{G}_{\rm p}(\eta) = 1 - \frac{P_{\rm p}(\eta)}{P_{\rm SQL}}\,, \quad {\rm p} = {\rm K}, {\rm HY}\,, \tag{4.77}$$

plotted in Fig. 4.5.2(b). Accordingly, the SQL is outpermed when $\mathcal{G}_{\rm p}(\eta) > 0$. We observe that there exists a threshold energy $\alpha^2_{\rm p}(\eta)$ after which the discussed receivers beat the SQL, that is $\mathcal{G}_{\rm p}(\eta) > 0$ for $\alpha^2 > \alpha^2_{\rm p}(\eta)$, and we have $\alpha^2_{\rm HY}(\eta) \leq \alpha^2_{\rm K}(\eta)$. By reducing the quantum efficiency η, the gain and the threshold energy decrease and increase, respectively.

4.5.1.2 Dark counts

Dark counts are random clicks of the PNR due to environmental noise and so not directly correlated to the properties of the coherent measured pulse. They can be described in terms of Poisson counting [108], occurring at rate ν which in many realistic conditions takes values $\nu \lesssim 10^{-3}$ [109–113]. Generally speaking, the outcome n of an ideal PNR measurement on a generic coherent state $|\zeta\rangle$ in the presence of dark counts turns out to be the sum of two Poisson variables and, therefore, still follows a Poisson distribution with rate equal to $|\zeta|^2 + \nu$ [1]. In turn, in the presence of a PNR(M) we have a probability $p_n(\mu)$ as in Eq. (4.57) but with rate $\mu = |\zeta|^2 + \nu$.

The presence of dark counts has a significant effect on the performances of quantum receivers. In particular, it becomes detrimental for the Kennedy receiver, as the receiver registers environmental clicks uncorrelated to the probed signal, inducing unwanted decision errors and undermining the "nulling" displacement technique. In fact, in such a situation the on-off detector may click even if the vacuum is measured.

Displacement-PNR receiver. As anticipated in Sec. 4.3.1, to counteract this effect, DiMario and Becerra proposed the displacement-PNR (DPNR) receiver, namely a Kennedy

[1] The sum of two Poisson independent random variables is still a Poisson random variable. If $x \sim \mathbb{P}(\mu)$ and $y \sim \mathbb{P}(\lambda)$ are two Poisson independent random variables with rates μ and λ respectively, the probability that $x + y$ gets the value k reads $p(x + y = k) = \sum_{l=0}^{k} p(x = l)p(y = k - l) = e^{-\mu-\lambda} \sum_{l=0}^{k} \mu^l \lambda^{k-l}/(l!(k-l)!) = e^{-\mu-\lambda}(\mu + \lambda)^k/k! \sim \mathbb{P}(\mu + \lambda)$.

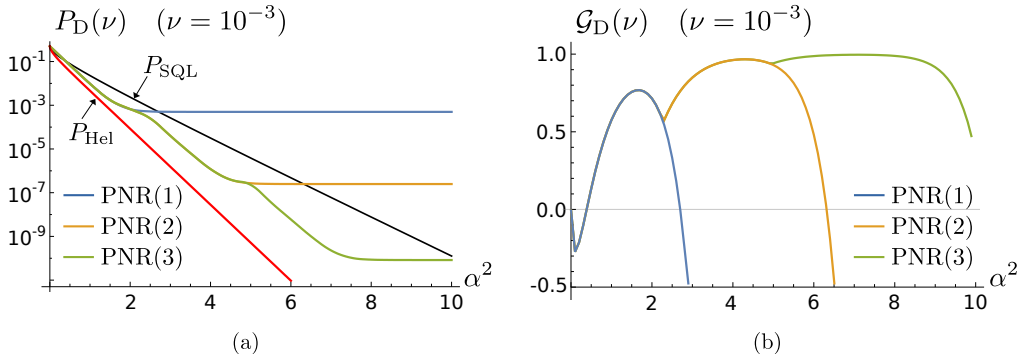


Figure 4.5.3: (a) Log plot of $P_{\rm D}(\nu)$ as a function of the signal energy α^2 for different resolution M. $P_{\rm SQL}$ and $P_{\rm Hel}$ refer to the SQL (4.16) and the Helstrom bound (4.14), respectively. (b) Plot of the gain $\mathcal{G}_{\rm D}(\nu)$ as a function of α^2 for different M. In both the pictures, the dark count rate is set to $\nu = 10^{-3}$.

setup employing PNR(M) detectors instead of on-off, and exploit the photon number resolution to choose the decision rule for discrimination in a more accurate way [92, 93]. In fact, in place of the usual on-off strategy, in the presence of dark counts the decision rule should be changed according to the *maximum a posteriori probability criterion* (MAP), discussed in App. A.1. If $|\alpha_0\rangle$ is sent the probability of detecting n photons is $p_n(\nu)$, whereas if $|\alpha_1\rangle$ is sent the probability is $p_n(4\alpha^2+\nu)$. The error probability for the DPNR receiver is then obtained as:

$$P_{\rm D}(\nu) = 1 - \frac{1}{2}\sum_{n=0}^{M} \max\left[p_n(\nu),\, p_n(4\alpha^2+\nu)\right]. \tag{4.78}$$

The procedure of maximizing the a posteriori probability is equivalent to defining a threshold count $n_{\rm th}(\nu) \leq M$ such that all measurement outcomes $n \geq n_{\rm th}(\nu)$ are assigned to state "1" and all $n < n_{\rm th}(\nu)$ are assigned to state "0". The threshold number is obtained by equating the photon number distributions of the two displaced states, namely $p_{\bar{n}}(\nu) = p_{\bar{n}}(4\alpha^2+\nu)$, $\bar{n} \in \mathbb{R}$, and considering the lowest integer greater than the obtained root $\bar{n}$, namely $n_{\rm th}(\nu) = \lceil \bar{n} \rceil$, where $\lceil \cdot \rceil$ is the ceiling function. Ultimately, we have:

$$n_{\rm th}(\nu) = \min\left[\left\lceil \frac{4\alpha^2}{\ln\left(1+4\alpha^2/\nu\right)} \right\rceil, M\right], \tag{4.79}$$

We note that the threshold is a function of α^2, namely $n_{\rm th}(\nu) = n_{\rm th}(\nu;\alpha^2)$. For the case of PNR(1) we have $n_{\rm th}(\nu) = 1$, retrieving the on-off discrimination of the standard Kennedy receiver. Furthermore, in the limit $\nu \to 0$, $n_{\rm th}(\nu)$ approaches 1, retrieving the usual Kennedy configuration.

Plots of the error probabilities for different PNR(M) detectors are depicted in Fig. 4.5.3(a), where it emerges that dark counts have a drastic effect for large energies, making the error probability saturating. The step-like behaviour of the curves follows from the adopted discrimination strategy: for $\alpha^2 \ll 1$, according to (4.79), the optimized discrimination threshold is equal to $n_{\rm th}(\nu) = 1$, equivalent to on-off detection, whereas, for increasing α^2, $n_{\rm th}(\nu)$ jumps to higher integer values up to $n_{\rm th} = M$ in the regime $\alpha^2 \gg 1$.

In turn, at every change in the threshold, the corresponding error probability exhibit a cusp. Moreover, when $n_{\rm th}(\nu) = M$, the sole outcome M will infer state "1" and all other outcomes smaller than M will infer state "0". In such a situation the receiver makes the wrong decision only if a M outcome were actually induced by the state $|\alpha_0\rangle$. Then, the error probability for large α^2 should be:

$$P_{\rm D}(\nu) \approx \frac{p_M(\nu)}{2} = \frac{1}{2}\left[1 - e^{-\nu}\sum_{j=0}^{M-1}\frac{\nu^j}{j!}\right] , \tag{4.80}$$

being independent of the pulse energy α^2 and making $P_{\rm D}(\nu)$ saturate.

Finally, we note that, in the presence of dark counts, neither the DPNR is near optimum, since it outperforms the SQL only for particular values of the signal energy. To highlight this, we consider the gain

$$\mathcal{G}_{\rm D}(\nu) = 1 - \frac{P_{\rm D}(\nu)}{P_{\rm SQL}} , \tag{4.81}$$

plotted in Fig. 4.5.3(b). As expected, the gain is not monotonic with α^2, but it exhibits M jumps before decreasing monotonously. As we can see, the DPNR receiver outperforms the SQL in the low-energy limit and only in particular intervals of α^2.

HYNORE. On the contrary, when considering the HYNORE setup, the presence of dark counts afflicts both PNR(M) detection on the transmitted branch and HL detection on the reflected one. Indeed, the probability of obtaining the photocurrent difference $\Delta = -M, \ldots, M$ now becomes:

$$\mathcal{S}_\Delta(\nu;\alpha_k^{(r)}) = \sum_{n,m=0}^{M} p_n\big(\mu_+(\alpha_k^{(r)}) + \nu\big)\, p_m\big(\mu_-(\alpha_k^{(r)}) + \nu\big)\, \delta_{(n-m),\Delta} . \tag{4.82}$$

Given all the previous considerations, the decision rule for the HYNORE in presence of dark counts should be modified into that of Table 4.5.1, provided that the threshold count $n_{\rm th}$ in Eq. (4.79) is now computed by considering only the transmitted fraction of the energy $\tau\alpha^2$, namely $n_{\rm th}(\nu) = n_{\rm th}(\nu;\tau\alpha^2)$.

Ultimately, the error probability reads:

$$P_{\rm HY}(\nu) = \min_{\tau,z} P_{\rm HY}(\tau, z;\nu) , \tag{4.83}$$

outcomes		decision
$\Delta \geq 0$	$n < n_{\rm th}(\nu)$	"0"
$\Delta < 0$	$n \geq n_{\rm th}(\nu)$	"0"
$\Delta < 0$	$n < n_{\rm th}(\nu)$	"1"
$\Delta \geq 0$	$n \geq n_{\rm th}(\nu)$	"1"

Table 4.5.1: Decision strategy for the HYNORE in the presence of a nonzero dark count rate ν.

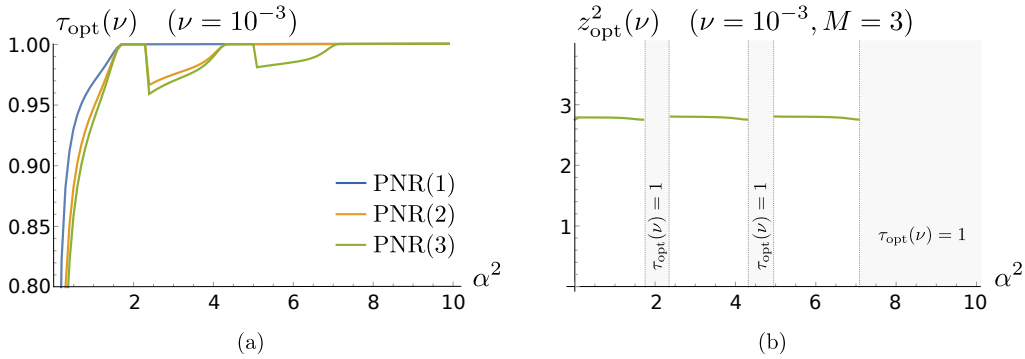


Figure 4.5.4: (a) Plot of the optimized transmissivity $\tau_{\rm opt}(\nu)$ as a function of α^2 for different PNR resolution M. (b) Plot of the optimized LO intensity $z^2_{\rm opt}(\nu)$ as a function of α^2 for $M = 3$. In the shaded regions we have $\tau_{\rm opt}(\nu) = 1$ and the HYNORE performs as a DPNR receiver.

with

$$
\begin{aligned}
P_{\rm HY}(\tau, z; \nu) &= \frac{1}{2}\left[p(\Delta < 0; n < n_{\rm th}(\nu)|0) + p(\Delta \geq 0; n \geq n_{\rm th}(\nu)|0)\right] \\
&\quad + \frac{1}{2}\left[p(\Delta < 0, n \geq n_{\rm th}(\nu)|1) + p(\Delta \geq 0, n < n_{\rm th}(\nu)|1)\right] \\
&= \frac{1}{2}\sum_{n=0}^{n_{\rm th}(\nu)-1} p_n(4\tau\alpha^2 + \nu)\left[\sum_{\Delta=-M}^{-1} \mathcal{S}_\Delta(\nu; \alpha_0^{(r)}) + \sum_{\Delta=0}^{M} \mathcal{S}_\Delta(\nu; \alpha_1^{(r)})\right] \\
&\quad + \frac{1}{2}\sum_{n=n_{\rm th}(\nu)}^{M} p_n(\nu)\left[\sum_{\Delta=-M}^{-1} \mathcal{S}_\Delta(\nu; \alpha_1^{(r)}) + \sum_{\Delta=0}^{M} \mathcal{S}_\Delta(\nu; \alpha_0^{(r)})\right].
\end{aligned} \tag{4.84}
$$

Plots of the optimized transmissivity $\tau_{\rm opt}(\nu)$ and LO intensity $z^2_{\rm opt}(\nu)$ are reported in Fig. 4.5.4(a) and (b), respectively. We see that, differently from the ideal scenario described in Sec. 4.4.1, the optimized transmissivity $\tau_{\rm opt}(\nu)$ is not anymore a monotonous function of α^2 asymptotically reaching 1. On the contrary, for nonzero dark count rate, at first the value of $\tau_{\rm opt}(\nu)$ increases with α^2 until to reach exactly the value 1, i.e. performing as a DPNR receiver. For larger energies, according to the resolution M, there appears $M - 1$ "sawteeth", that is other $M - 1$ regions in which $\tau_{\rm opt}(\nu)$ decreases to a value smaller than 1 and increases further to reach again 1. Finally, in the high-energy limit $\alpha^2 \gg 1$, we have $\tau_{\rm opt}(\nu) \equiv 1$ and the HYNORE leads to the same performance of the DPNR, namely saturation to the value (4.80). Accordingly, when $\tau_{\rm opt}(\nu) < 1$, the optimized LO is $z^2_{\rm opt}(\nu) \lesssim M$.

In turn, the HYNORE outperforms the DPNR receiver only in some energy regimes. For a better visualization of the advantages brought by the hybrid receiver, we consider the relative ratio

$$
R_{h/D}(\nu) = \frac{P_{\rm HY}(\nu)}{P_{\rm D}(\nu)}, \tag{4.85}
$$

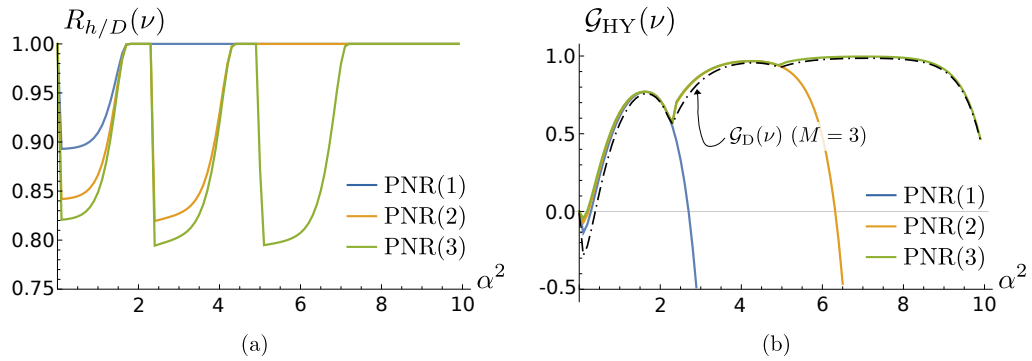


Figure 4.5.5: (a) Plot of the ratio $R_{h/D}(\nu)$ as a function of α^2 for different M. (b) Plot of the gain $\mathcal{G}_{\rm HY}(\nu)$ as a function of α^2 for different M. The dot-dashed line refers to the DPNR gain $\mathcal{G}_{\rm D}(\nu)$ for PNR(3) detection.

and the gain

$$\mathcal{G}_{\rm HY}(\nu) = 1 - \frac{P_{\rm HY}(\nu)}{P_{\rm SQL}}\,, \tag{4.86}$$

depicted in Fig. 4.5.5(a) and (b), respectively. Consistently with the previous discussion, $R_{h/D}(\nu)$ is not a monotonous function of α^2 and exhibits M sawteeth when $\tau_{\rm opt}(\nu) < 1$, in which case the corresponding gain is $\mathcal{G}_{\rm HY}(\nu) > \mathcal{G}_{\rm D}(\nu)$. In particular, the advantage over the DPNR is increased for larger PNR resolution M. This happens because of the HL part of the setup, retrieving more information on the reflected pulse when increasing M. Instead, when $\tau_{\rm opt}(\nu) = 1$ the HYNORE performs as a DPNR and $\mathcal{G}_{\rm HY}(\nu) = \mathcal{G}_{\rm D}(\nu)$. Furthermore, the saturation of the error probabilities forbids to beat the SQL in the high-energy regime. Indeed, both the gains $\mathcal{G}_{\rm p}(\nu)$, $\rm p = D, HY$, are positive up to a maximum energy $\alpha^2_{\rm p}(\nu)$, coinciding for both DPNR and HYNORE.

4.5.1.3 Visibility reduction

Finally, we address the effects of the interference visibility of the displacement operations employed in the realization of the receivers. This effect is consequence of the mode mismatch at the beam splitter which implements practically a displacement. We introduce the value $\xi \leq 1$ to quantify the overlap between the spatial areas of the signal and the auxiliary field mixed at the beam splitter. As a consequence, interference is only achieved between the field fractions being effectively superimposed, while the remaining parts do not interact with each other, resulting in an imperfect realization of mode-mixing operations [114]. A detailed model of the visibility reduction process is derived in App. A.2. In realistic conditions, the values of ξ ranges from 0.90 to 0.999, according to the accuracy of the experimental setup [85, 92, 93, 114]. As discussed in [92, 93], a reduction of the visibility affects crucially the performances of quantum receivers.

Generally speaking, we consider a coherent state $|\zeta\rangle$ which we want to displace by a quantity β into the state $|\zeta+\beta\rangle$. For the sake of simplicity, we assume $\zeta, \beta \in \mathbb{R}$. Then we can describe the effect induced by imperfect mode matching by stating that the outcome n of the subsequent PNR measurement follows a Poisson distribution with rate

$$\mu = \zeta^2 + \beta^2 + 2\xi\zeta\beta \neq (\zeta+\beta)^2\,. \tag{4.87}$$

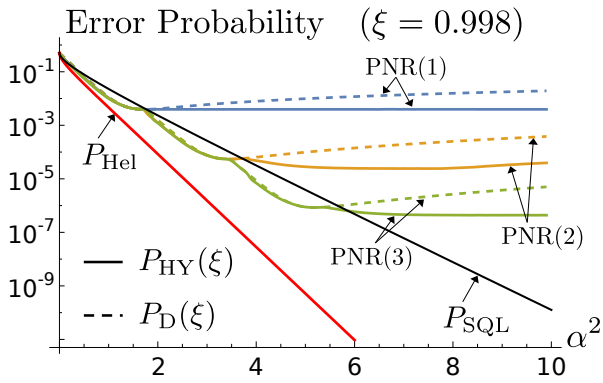


Figure 4.5.6: Log plot of $P_{\rm HY}(\xi)$ and $P_{\rm K}(\xi)$ as a function of the signal energy α^2 for different PNR resolution M and $\xi = 0.998$. $P_{\rm SQL}$ and $P_{\rm Hel}$ refer to the SQL (4.16) and the Helstrom bound (4.14), respectively.

As for the case of dark counts, non-unit visibility is detrimental for the Kennnedy receiver, making the DPNR as the more adequate solution to implement a displacement receiver. As in the previous subsection, in the following we first analyze the case of DPNR receiver and then address the HYNORE.

D-PNRM receiver. In the presence of a visibility reduction the approach is quite similar to the dark count case. Given Eq. (4.87), if $|\alpha_0\rangle$ is sent the probability of detecting outcome n is $p_n(2\alpha^2(1-\xi))$, whereas for $|\alpha_1\rangle$ the probability becomes $p_n(2\alpha^2(1+\xi))$. By following the MAP criterion, the error probability then reads

$$P_{\rm D}(\xi) = 1 - \frac{1}{2}\sum_{n=0}^{M} \max\left[p_n(g_-),\, p_n(g_+)\right] , \tag{4.88}$$

where

$$g_\pm = 2\alpha^2(1 \pm \xi) , \tag{4.89}$$

associated to the threshold outcome $n_{\rm th}(\xi) = n_{\rm th}(\xi;\alpha^2)$:

$$n_{\rm th}(\xi) = \min\left[\left\lceil \frac{4\xi\alpha^2}{\ln(1+\xi) - \ln(1-\xi)} \right\rceil , M\right] . \tag{4.90}$$

We recall that the case of PNR(1) is equivalent to the on-off Kennedy receiver. The consequences of a non-unit visibility on the error probability is shown in Fig. 4.5.6. As for dark counts, the visibility reduction makes the error probability non monotonic, and in particular increasing for large α^2. As before, this is a consequence of the finite resolution M. In the regime of large α^2 the threshold outcome becomes $n_{\rm th}(\xi) = M$, thus the error probability is due to outcomes M induced by the state $|\alpha_0\rangle$ which is not perfectly "nulled" due to the imperfect displacement operation. Therefore we have:

$$P_{\rm D}(\xi) \approx \frac{p_M(g_-)}{2} = \frac{1}{2}\left[1 - e^{-2\alpha^2(1-\xi)} \sum_{j=0}^{M-1} \frac{\left(2\alpha^2(1-\xi)\right)^j}{j!}\right] , \tag{4.91}$$

which is an increasing function of α^2.

outcomes		decision
$\Delta \geq 0$	$n < n_{\rm th}(\xi)$	"0"
$\Delta < 0$	$n \geq n_{\rm th}(\xi)$	"0"
$\Delta < 0$	$n < n_{\rm th}(\xi)$	"1"
$\Delta \geq 0$	$n \geq n_{\rm th}(\xi)$	"1"

Table 4.5.2: Decision strategy for the HYNORE in the presence of visibility reduction $\xi \leq 1$.

HYNORE. In the HYNORE, we should also include the effect of visibility reduction in the balanced beam splitter inside the HL detector. As a consequence, the probability of measuring the photocurrent $\Delta = -M, \ldots, M$ is changed into:

$$\mathcal{S}_\Delta(\xi;\alpha_k^{(r)}) = \sum_{n,m=0}^{M} p_n\big(\mu_+(\alpha_k^{(r)};\xi)\big)\, p_m\big(\mu_-(\alpha_k^{(r)};\xi)\big)\, \delta_{(n-m),\Delta}\,, \tag{4.92}$$

where

$$\mu_\pm(\alpha_k^{(r)};\xi) = \frac{\big(\alpha_k^{(r)}\big)^2 + z^2 \pm 2\xi\, z\, \alpha_k^{(r)}}{2}\,. \tag{4.93}$$

The decision rule for the HYNORE, displayed in Table 4.5.2, is identical to the case of dark counts, with the threshold $n_{\rm th}(\xi) = n_{\rm th}(\xi;\tau\alpha^2)$. The error probability then reads:

$$P_{\rm HY}(\xi) = \min_{\tau,z} P_{\rm HY}(\tau,z;\xi)\,, \tag{4.94}$$

where

$$\begin{aligned} P_{\rm HY}(\tau,z;\xi) &= \frac{1}{2}\left[p(\Delta<0; n<n_{\rm th}(\xi)|0) + p(\Delta\geq 0; n\geq n_{\rm th}(\xi)|0)\right] \\ &\quad + \frac{1}{2}\left[p(\Delta<0, n\geq n_{\rm th}(\xi)|1) + p(\Delta\geq 0, n<n_{\rm th}(\xi)|1)\right] \\ &= \frac{1}{2}\sum_{n=0}^{n_{\rm th}(\xi)-1} p_n(\tau g_+)\left[\sum_{\Delta=-M}^{-1}\mathcal{S}_\Delta(\xi;\alpha_0^{(r)}) + \sum_{\Delta=0}^{M}\mathcal{S}_\Delta(\xi;\alpha_1^{(r)})\right] \\ &\quad + \frac{1}{2}\sum_{n=n_{\rm th}(\xi)}^{M} p_n(\tau g_-)\left[\sum_{\Delta=-M}^{-1}\mathcal{S}_\Delta(\xi;\alpha_1^{(r)}) + \sum_{\Delta=0}^{M}\mathcal{S}_\Delta(\xi;\alpha_0^{(r)})\right], \end{aligned} \tag{4.95}$$

with the $g_\pm$ in Eq. (4.89).

Plots of $P_{\rm HY}(\xi)$ are reported in Fig. 4.5.6. If α^2 is small we observe the same step-like behaviour of the dark count case, and the HYNORE beats the DPNR only for particular values of the signal energy. On the contrary, for large α^2 the HYNORE significantly outperforms the DPNR, as $P_{\rm HY}(\xi) < P_{\rm D}(\xi)$. The difference between the two regimes becomes clearer by looking at the optimized transmissivity $\tau_{\rm opt}(\xi)$ and LO $z^2_{\rm opt}(\xi)$, depicted in Fig. 4.5.7(a) and (b), respectively. In the low-energy regime, similarly to Fig. 4.5.4, $\tau_{\rm opt}(\xi)$ is a non-monotonous function of α^2, exhibiting $M-1$ sawteeth, whilst the optimized LO is $z^2_{\rm opt}(\xi) \lesssim M$. On the other hand, for large α^2 the transmissivity changes discontinuously, and becomes a decreasing function of α^2, saturating for $\alpha^2 \gg 1$ to an asymptotic value $\tau_\infty \neq 0$. Remarkably, $\tau_\infty < 1$, thus by appropriately choosing the

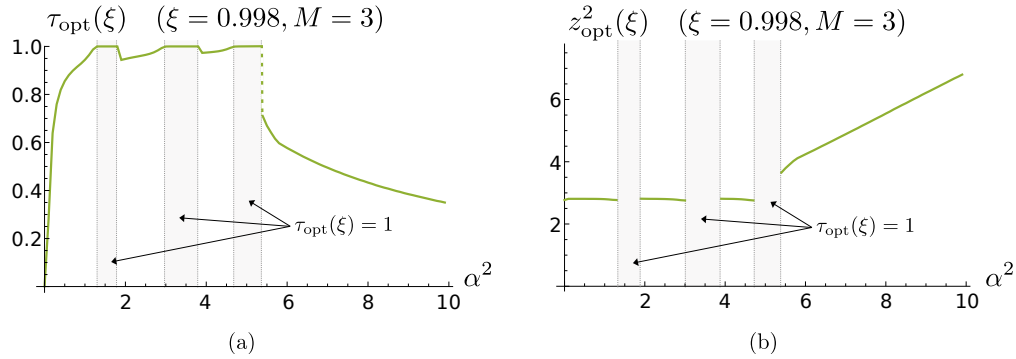


Figure 4.5.7: Plot of the optimized transmissivity $\tau_{\rm opt}(\xi)$ (a) and LO intensity $z^2_{\rm opt}(\xi)$ (b) as a function of α^2 for $\xi = 0.998$. The PNR resolution is $M = 3$. In the shaded regions we have $\tau_{\rm opt}(\xi) = 1$ and the HYNORE performs as a DPNR receiver.

energy of the signals undergoing the HL and the DPNR measurements it is possible to regain part of the information lost by to the finite resolution of the detectors. As a result, the interplay between the two schemes allows to mitigate the negative effects introduced by the visibility reduction. In these conditions, $z^2_{\rm opt}(\xi)$ is not constant anymore, and increases with α^2, being a linear function for α^2.

The existence of two different energy regimes affects also the relative ratio

$$R_{h/D}(\xi) = \frac{P_{\rm HY}(\xi)}{P_{\rm D}(\xi)}\,, \tag{4.96}$$

shown in Fig. 4.5.8(a). In fact, in the low-energy regime, $R_{h/D}(\xi)$ exhibits M sawteeth, whilst, after the jump in the transmissivity $\tau_{\rm opt}(\xi)$, becomes a decreasing function of α^2. Finally, to quantify the quantum advantage over the SQL, we consider the gain

$$\mathcal{G}_{\rm p}(\xi) = 1 - \frac{P_{\rm p}(\xi)}{P_{\rm SQL}}\,, \quad {\rm p} = {\rm D}, {\rm HY}\,, \tag{4.97}$$

plotted in Fig. 4.5.8(b) for different PNR resolution. As for dark counts, both DPNR and HYNORE beat the SQL only in particular energy regimes. Even in this case, the gains are positive up to a maximum energy $\alpha^2_{\rm p}(\xi)$, which, now, is different between the two receivers, as $\alpha^2_{\rm HY}(\xi) \geq \alpha^2_{\rm D}(\xi)$.

4.5.2 HFFRE vs DFFRE

After widely discussing the robustness of single-copy receivers, we now extend the comparison to multi-copy receivers, namely DFFRE and HFFRE. In both cases, splitting the encoded signal into many rescaled copies makes the decision errors induced by practical imperfections accumulate during the feed-forward loop, leading to a non-trivial behaviour. For the sake of simplicity, in the following we will perform the analysis by considering the sole HFFRE. In fact, as discussed in Sec. 4.4.2, the error probability associated with the DFFRE may be retrieved in an analogous way from the DFFRE scheme in Fig. 4.4.5 by setting $\tau = 1$.

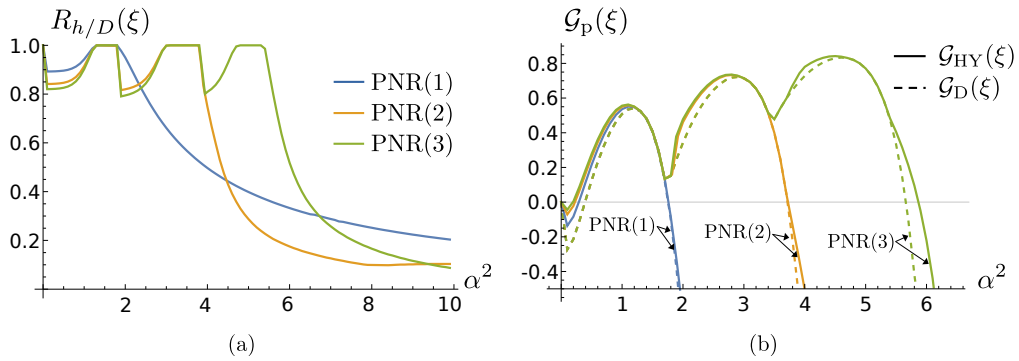


Figure 4.5.8: (a) Plot of the ratio $R_{h/D}(\xi)$ as a function of α^2 for different M. (b) Plot of the gain $\mathcal{G}_{\rm p}(\xi)$, p $=$ D, HY, as a function of α^2 for different M. We set the value $\xi = 0.998$.

4.5.2.1 Reduced quantum efficiency

The presence of a quantum efficiency $\eta \leq 1$ requires only to rescale the coherent amplitudes of all the measured pulses by a factor $\sqrt{\eta}$, as no mixedness is introduced at the detectors. Thereafter, in the HFFRE scheme of Fig. 4.4.5 the HL probability distribution of the reflected signal $|\alpha_k^{(r)}\rangle$ becomes $\mathcal{S}_\Delta(\eta\alpha_k^{(r)})$ with the $\mu_\pm$ in Eq. (4.56). The effect is the same on the transmitted branch, where the average photon numbers of the displaced copies $\lambda_\pm$, see Eq. (4.45), are replaced by $\eta\lambda_\pm$. In turn, the correct decision probability $\mathcal{P}_{\rm HF}^{(j)}(\eta;\tau,z)$ becomes

$$\begin{aligned}\mathcal{P}_{\rm HF}^{(j)}(\eta;\tau,z) = \\ \max_{\beta_j}\Big\{&\mathcal{P}_{\rm HF}^{(j-1)}(\eta;\tau,z)\, q_{\rm off}\Big(\eta\lambda_-^{(j)}(\sqrt{\tau}\alpha)\Big) \\ &+\Big[1-\mathcal{P}_{\rm HF}^{(j-1)}(\eta;\tau,z)\Big] q_{\rm on}\big(\eta\lambda_+^{(j)}(\sqrt{\tau}\alpha)\big)\Big\}\,,\end{aligned} \tag{4.98}$$

with the quantities introduced in (4.44), to be solved with the initial condition

$$\mathcal{P}_{\rm HF}^{(0)}(\eta;\tau,z) = \frac{1}{2}\left[\sum_{\Delta=-M}^{-1}\mathcal{S}_\Delta\Big(\eta\alpha_1^{(r)}\Big) + \sum_{\Delta=0}^{M}\mathcal{S}_\Delta\Big(\eta\alpha_0^{(r)}\Big)\right],$$

and the associated error probability reads

$$P_{\rm HF}^{(N)}(\eta) = 1 - \max_{\tau,z}\mathcal{P}_{\rm HF}^{(N)}(\eta;\tau,z)\,. \tag{4.99}$$

The error probability for the DFFRE $P_{\rm DF}^{(N)}(\eta)$ may be derived from the previous equations by fixing $\tau = 1$. Plots of $P_{\rm HF}^{(N)}(\eta)$ and $P_{\rm DF}^{(N)}(\eta)$ are depicted in Fig. 4.5.9, showing that the presence of a non-unit quantum efficiency increases the error probability, preventing the receivers to approach the Helstrom bound. Nevertheless, we still have

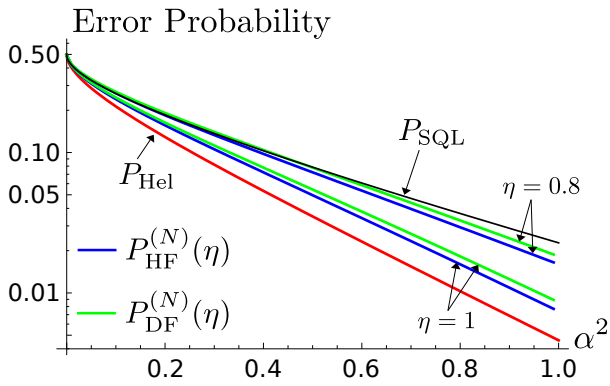


Figure 4.5.9: Log plot of $P^{(N)}_{\rm HF}(\eta)$ and $P^{(N)}_{\rm DF}(\eta)$ as a function of the signal energy α^2 for $N = 1$ and different values of η. The PNR resolution is $M = 2$.

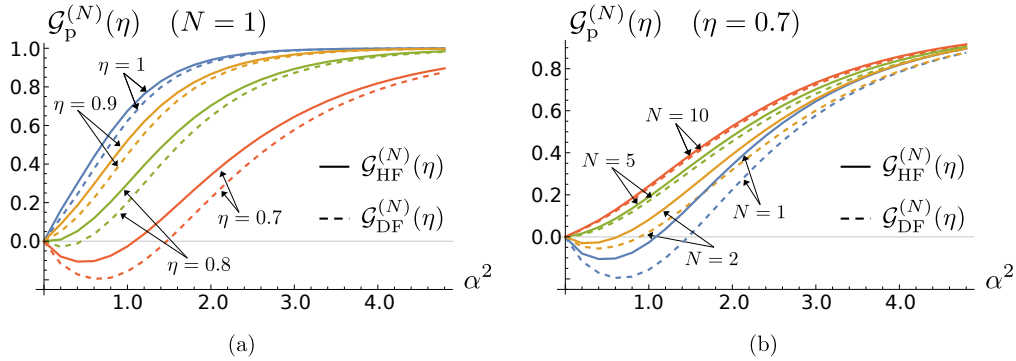


Figure 4.5.10: (a) Plot of the gain $\mathcal{G}^{(N)}_{\rm p}(\eta)$, p $=$ DF, HF, as a function of the signal energy α^2 for $N = 1$ and different quantum efficiency η. (Bottom) Plot of the gain $\mathcal{G}^{(N)}_{\rm p}(\eta)$, p $=$ DF, HF, as a function of α^2 for $\eta = 0.7$ and different number of copies N. In both the pictures, the PNR resolution is $M = 2$.

$P^{(N)}_{\rm HF}(\eta) \leq P^{(N)}_{\rm DF}(\eta)$ and, remarkably, in the high-energy regime both the discussed receivers beat the SQL (4.16). To better highlight this feature, we consider the gain

$$\mathcal{G}^{(N)}_{\rm p}(\eta) = 1 - \frac{P^{(N)}_{\rm p}(\eta)}{P_{\rm SQL}}\,, \quad (p = {\rm DF}, {\rm HF}\,, \tag{4.100}$$

plotted in Fig.s 4.5.10(a) and (b). Accordingly, the SQL is outperformed when $\mathcal{G}^{(N)}_{\rm p}(\eta) \geq 0$.

If we consider a fixed number of copies N, see Fig. 4.5.10(a), there exists a threshold energy $\alpha^2_{\rm p}(N,\eta)$ after which the discussed receivers beat the SQL, that is $\mathcal{G}^{(N)}_{\rm p}(\eta) \geq 0$ for $\alpha^2 \geq \alpha^2_{\rm p}(N,\eta)$. By reducing the quantum efficiency η, the gain and the threshold energy decrease and increase, respectively. More interestingly, in the opposite scenario where we fix η and let N vary, as in Fig. 4.5.10(b), we see that increasing the number of copies mitigates the detriments of the quantum efficiency, and makes the gain increase. In particular, for a sufficiently large N, $\alpha^2_{\rm p}(N,\eta)$ may be made arbitrarily small, main-

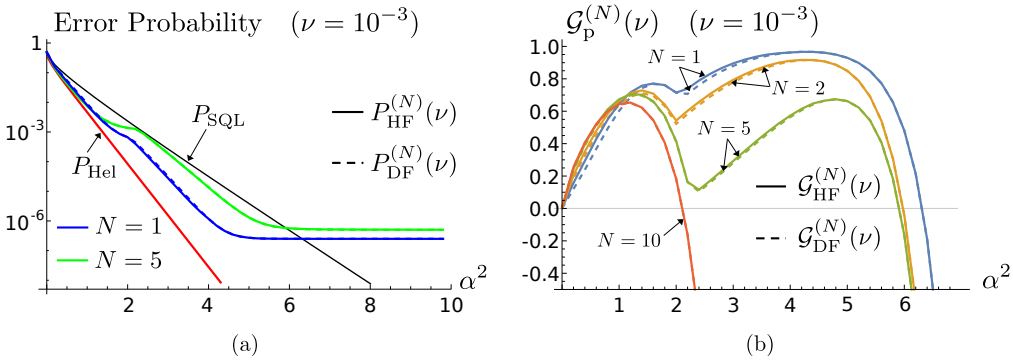


Figure 4.5.11: (a) Log plot of $P^{(N)}_{\rm HF}(\nu)$ and $P^{(N)}_{\rm DF}(\nu)$ as a function of the signal energy α^2 for different values of N. (b) Plot of the gain $\mathcal{G}^{(N)}_{\rm p}(\nu)$, p = DF, HF, as a function of α^2 for different N. In both the pictures, the PNR resolution is $M = 2$ and the dark count rate is $\nu = 10^{-3}$.

taining $\mathcal{G}^{(N)}_{\rm p}(\eta) \geq 1$ for all energies. In all cases, the HFFRE outperforms the DFFRE, as $\mathcal{G}^{(N)}_{\rm HF}(\eta) \geq \mathcal{G}^{(N)}_{\rm DF}(\eta)$ and $\alpha^2_{\rm HF}(N,\eta) \leq \alpha^2_{\rm DF}(N,\eta)$.

4.5.2.2 Dark counts

More drastic effects appear in the presence of dark counts. The HL probability distribution of the reflected signal $|\alpha^{(r)}_k\rangle$ is equal to (4.82), as discussed in the former section. A more detrimental effect is observed in the displacement-photon counting scheme performed on the transmitted signal. Indeed, in the presence of dark counts the MAP criterion does not coincide anymore with on-off discrimination and, in principle, one should perform a different Bayesian inference process after each detection stage. However, for the sake simplicity here we adopt a simpler decision rule. We introduce a fixed threshold outcome $1 \leq n_{\rm th} \leq M$ such that if we get outcome $n < n_{\rm th}$ from the $(j-1)$-th PNR(M) measurement we set $\sigma_j = \sigma_{j-1}$ and, then, displace the j-th copy by $D(\sigma_j\beta_j)$; otherwise if $n \geq n_{\rm th}$ we choose $\sigma_j = -\sigma_{j-1}$. In the ideal scenario with zero dark count rate we have $n_{\rm th} = 1$. The final decision rule becomes: $n < n_{\rm th} \to |-\sigma_N\alpha\rangle$ and $n \geq n_{\rm th} \to |\sigma_N\alpha\rangle$.

As a consequence, the correct decision probability $\mathcal{P}^{(j)}_{\rm HF}(\nu;\tau,z)$ satisfies:

$$\mathcal{P}^{(j)}_{\rm HF}(\nu;\tau,z) = \max_{\beta_j}\left\{\mathcal{P}^{(j-1)}_{\rm HF}(\nu;\tau,z)\,\widetilde{q}_0\big(\lambda^{(j)}_-(\sqrt{\tau}\alpha;\nu);n_{\rm th}\big) + \Big[1-\mathcal{P}^{(j-1)}_{\rm HF}(\nu;\tau,z)\Big]\widetilde{q}_1\big(\lambda^{(j)}_+(\sqrt{\tau}\alpha;\nu);n_{\rm th}\big)\right\}, \tag{4.101}$$

where

$$\widetilde{q}_0(x;n_{\rm th}) = \sum_{s=0}^{n_{\rm th}-1} e^{-x}\frac{x^s}{s!}\,, \tag{4.102}$$

$$\widetilde{q}_1(x;n_{\rm th}) = 1-\widetilde{q}_0(x;n_{\rm th})\,, \tag{4.103}$$

and

$$\lambda_{\pm}^{(j)}(\alpha;\nu) = \lambda_{\pm}^{(j)}(\alpha) + \nu\,. \tag{4.104}$$

The initial condition of Eq. (4.101) reads

$$\mathcal{P}_{\rm HF}^{(0)}(\nu;\tau,z) = \frac{1}{2}\left[\sum_{\Delta=-M}^{-1}\mathcal{S}_{\Delta}\left(\nu;\alpha_1^{(r)}\right) + \sum_{\Delta=0}^{M}\mathcal{S}_{\Delta}\left(\nu;\alpha_0^{(r)}\right)\right],$$

and the associated error probability is obtained as

$$P_{\rm HF}^{(N)}(\nu) = 1 - \max_{\tau,z,n_{\rm th}}\mathcal{P}_{\rm HF}^{(N)}(\nu;\tau,z)\,, \tag{4.105}$$

where, differently from the other cases, we perform optimization also over the threshold discrimination outcome $n_{\rm th}$. As before, with the choice $\tau = 1$ we retrieve the probability $P_{\rm DF}^{(N)}(\nu)$ associated with the displacement receiver.

The plots of $P_{\rm HF}^{(N)}(\nu)$ and $P_{\rm DF}^{(N)}(\nu)$ are reported in Fig. 4.5.11(a) for different number of copies N and $M = 2$. As discussed in Sec. 4.5.1, the step-like behaviour of the curves follows from the adopted discrimination strategy: for $\alpha^2 \ll 1$ the optimized discrimination threshold is equal to $n_{\rm th} = 1$, equivalent to on-off detection, whereas, for increasing α^2, $n_{\rm th}$ jumps to higher integer values up to $n_{\rm th} = M$ in the regime $\alpha^2 \gg 1$. In turn, at every change in the threshold, the corresponding error probabilities exhibit a cusp.

Remarkably, in the presence of dark counts the performance of the receivers is not improving anymore with larger number of copies. In fact, increasing N induces a reduction of the error probability only for $\alpha^2 \ll 1$. On the contrary, for large energies employing many copies becomes detrimental. Indeed, it has been shown in the previous section that dark counts induce decision errors, letting the error probability saturate for $\alpha^2 \gg 1$. Accordingly, when we split the signal into N copies, the decision errors induced by dark counts accumulate, letting the error probability reach higher saturating values.

To quantify the present effect, some analytical results may be retrieved in the limit $\alpha^2 \gg 1$. For the DFFRE, numerical results show that, in the regime $\alpha^2 \gg 1$, the optimized displacement amplitudes are $\beta_j \approx \alpha/\sqrt{N}$ and $n_{\rm th} = M$. Thus, we have $\lambda_{-}^{(j)}(\alpha;\nu) = \nu$ and $\lambda_{+}^{(j)}(\alpha;\nu) = \nu + 4\alpha^2/N \gg 1$. This implies that an error occurs only when the outcome M is obtained from the input $|\alpha_0\rangle$, in turn the correct decision probability at the j-th step reads:

$$\mathcal{P}_{\rm DF}^{(j)}(\nu) \approx \mathcal{P}_{\rm DF}^{(j-1)}(\nu)\,\widetilde{q}_0(\nu) + \left[1 - \mathcal{P}_{\rm DF}^{(j-1)}(\nu)\right], \tag{4.106}$$

with $\widetilde{q}_0(\nu) = \widetilde{q}_0(\nu;M)$. By iteration, we get:

$$P_{\rm DF}^{(N)}(\nu) \approx 1 - \left\{\frac{[\widetilde{q}_0(\nu)-1]^N}{2} + \frac{1-[\widetilde{q}_0(\nu)-1]^N}{1-[\widetilde{q}_0(\nu)-1]}\right\}, \tag{4.107}$$

being independent of the energy α^2 and, therefore, letting the error probability saturate. The same result also holds for the HFFRE, since the optimized transmissivity $\tau_{\rm opt}$ in the high-energy regime is equal to $\tau_{\rm opt} = 1$.

Finally, we note that the benefits of the hybrid scheme are more relevant for $N \lesssim 5$. For larger number of copies the improvement becomes negligible: as we can see, for

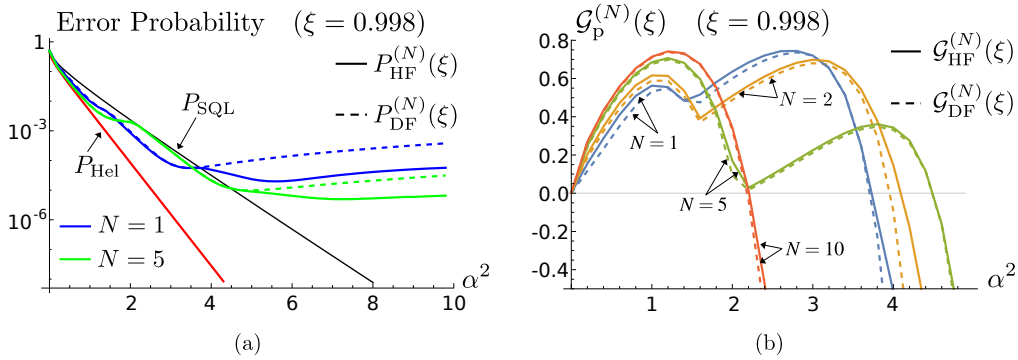


Figure 4.5.12: (a) Log plot of $P^{(N)}_{\rm HF}(\xi)$ and $P^{(N)}_{\rm DF}(\xi)$ as a function of the signal energy α^2 for different values of N. (b) Plot of the gain $\mathcal{G}^{(N)}_{\rm p}(\xi)$, p $=$ DF, HF, as a function of α^2 for different N. In both the pictures, the PNR resolution is $M = 2$ and the visibility is $\xi = 0.998$.

instance, in Fig. 4.5.11(a), the curves associated with the HFFRE and DFREE lines for $N = 10$ are superimposed and fully indistinguishable.

The saturation of the error probability forbids to beat the SQL in the large energy regime. Indeed, the gain

$$\mathcal{G}^{(N)}_{\rm p}(\nu) = 1 - \frac{P^{(N)}_{\rm p}(\nu)}{P_{\rm SQL}}\,, \quad {\rm p} = {\rm DF}, {\rm HF}\,, \tag{4.108}$$

plotted in Fig. 4.5.11(b), is positive up to a maximum energy $\alpha^2_{\rm p}(N,\nu)$. Here the tradeoff between the number of copies and the error probability is clearer: for larger values of N we increase $\mathcal{G}^{(N)}_{\rm p}(\nu)$ in the low-energy regime $\alpha^2 \ll 1$, at the expense of reducing also $\alpha^2_{\rm p}(N,\nu)$. If on the one hand we reduce the error probability for low energies, on the other one we inevitably reduce the range in which the receivers exhibit a quantum advantage.

4.5.2.3 Visibility reduction

Finally, we address the impact of reduced visibility $\xi \leq 1$. In the HFFRE we observe a visibility reduction both in the HL setup, where the signal is mixed with the LO $|z\rangle$, and in the conditional displacement operations governed by the feed-forward rule. The HL probability distribution of the reflected signal $|\alpha^{(r)}_k\rangle$ is reported in Eq. (4.92), whereas for the feed-forward rule on the transmitted signal, we proceed as for the case of dark counts and introduce the threshold outcome $1 \leq n_{\rm th} \leq M$.

Accordingly, the correct decision probability $\mathcal{P}^{(j)}_{\rm HF}(\xi;\tau,z)$ satisfies:

$$\begin{aligned}\mathcal{P}^{(j)}_{\rm HF}(\xi;\tau,z) = \max_{\beta_j}\Big\{&\mathcal{P}^{(j-1)}_{\rm HF}(\xi;\tau,z)\,\widetilde{q}_0\Big(\lambda^{(j)}_-(\sqrt{\tau}\alpha;\xi);n_{\rm th}\Big)\\ &+\Big[1-\mathcal{P}^{(j-1)}_{\rm HF}(\xi;\tau,z)\Big]\widetilde{q}_1\Big(\lambda^{(j)}_+(\sqrt{\tau}\alpha;\xi);n_{\rm th}\Big)\Big\}\,,\end{aligned} \tag{4.109}$$

with the same $\widetilde{q}_k(x;n_{\rm th})$, $k=0,1$, introduced in Eq. (4.102), the rates

$$\lambda_{\pm}^{(j)}(\alpha;\xi)=\frac{\alpha^2}{N}+\beta_j^2\pm\frac{2\xi\beta_j\alpha}{\sqrt{N}}\,, \tag{4.110}$$

and the initial condition

$$\mathcal{P}_{\rm HF}^{(0)}(\xi;\tau,z)=\frac{1}{2}\left[\sum_{\Delta=-M}^{-1}\mathcal{S}_{\Delta}\left(\xi;\alpha_1^{(r)}\right)+\sum_{\Delta=0}^{M}\mathcal{S}_{\Delta}\left(\xi;\alpha_0^{(r)}\right)\right].$$

Finally, the error probability writes:

$$P_{\rm HF}^{(N)}(\xi)=1-\max_{\tau,z,n_{\rm th}}\mathcal{P}_{\rm hyb}^{(N)}(\xi;\tau,z)\,, \tag{4.111}$$

whereas for $\tau=1$ we obtain the corresponding $P_{\rm DF}^{(N)}(\xi)$.

As depicted in Fig. 4.5.12(a), the behaviour of $P_{\rm HF}^{(N)}(\xi)$ and $P_{\rm DF}^{(N)}(\xi)$ is similar to the case of dark counts, with a step-like behaviour induced by the jump in the threshold $n_{\rm th}$. Even in this case, increasing the number of copies N reduces the error probability for low energies, $\alpha^2\ll 1$, but, differently from the dark counts case, this reduction holds also in the high-energy regime $\alpha^2\gg 1$. In fact, the detriments of the visibility reduction are more relevant for strong signals and, in turn, the error probability for $\alpha^2\gg 1$ becomes an increasing function of the energy [16]. As a consequence, splitting the incoming signal into a larger number of copies N reduces the energy of each displaced copy, thus partially mitigating the effects of the imperfect displacements.

With a similar argument to the one adopted for dark counts, we can obtain the analytic expression for the error probability in the high-energy regime. For the DFFRE, we have:

$$P_{\rm DF}^{(N)}(\xi)\approx 1-\left\{\frac{[\widetilde{q}_0(g)-1]^N}{2}+\frac{1-[\widetilde{q}_0(g)-1]^N}{1-[\widetilde{q}_0(g)-1]}\right\}, \tag{4.112}$$

with $\widetilde{q}_0(g)=\widetilde{q}_0(g;M)$ and $g=2\alpha^2(1-\xi)/N$, being an increasing function of α^2. On the contrary, the HFFRE beats the DFFRE since the optimized transmissivity τopt for the HFFRE is <1, and combining HL and displacement results in a lower error probability.

Anyway, there still exist an intermediate region, comprised between the regimes $\alpha^2\ll 1$ and $\alpha^2\gg 1$, where increasing N is not beneficial anymore. Moreover, we note in the high-energy regime the HFFRE outperforms significantly the DFFRE, because of the higher degree of robustness of HL with respect to visibility reduction [16].

The existence of three different energy regimes affects also the gain with respect to the SQL,

$$\mathcal{G}_{\rm p}^{(N)}(\xi)=1-\frac{P_{\rm p}^{(N)}(\xi)}{P_{\rm SQL}}\,,\quad {\rm p}={\rm DF},{\rm HF}\,, \tag{4.113}$$

plotted in Fig. 4.5.12(b). As for the case of dark counts, we have $\mathcal{G}_{\rm p}^{(N)}(\xi)\geq 0$ up to a maximum energy $\alpha_{\rm p}^2(N,\xi)$, but the behaviour of $\alpha_{\rm p}^2(N,\xi)$ is not monotonic with the number of copies N. For $N\lesssim 5$, splitting the signal into more copies improves the robustness of the quantum advantage, letting $\alpha_{\rm p}^2(N,\xi)$ increase. On the contrary, for larger N the error probabilities surpass the SQL already in the intermediate energy regime and, in turn, $\alpha_{\rm p}^2(N,\xi)$ decreases.

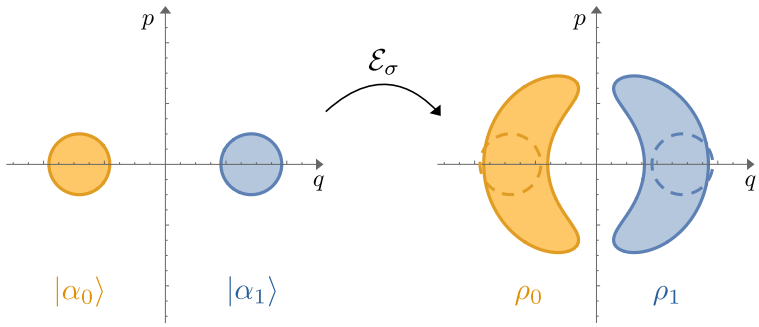


Figure 4.6.1: Phase space representation of the BPSK encoding before (left) and after (right) the application of phase diffusion. The phase diffusion CP map $\mathcal{E}_\sigma$ transforms the initial coherent signals into a Gaussian mixture of phase-shifted coherent states, reducing both purity and coherence.

4.6 Quantum receivers in the presence of phase noise

Throughout this Chapter, we performed a detailed analysis of binary quantum decision theory in the presence of coherent-state encoding, namely BPSK. Within this framework, the goal is to perform discrimination between two symbols $k = 0, 1$, encoded into two π phase-shifted (pure) coherent states. As discussed, the Dolinar receiver provides the optimum POVM, even though its practical implementation remains a challenging task, whereas both displacement receivers, e.g. Kenendy and DFFRE, and hybrid receivers, namely HYNORE and HFFRE, provide feasible near-optimum schemes, beating the SQL and enhancing information transfer over attenuating (Gaussian) channels [19]. Furthermore, they are robust against the typical practical inefficiencies and preserve the quantum advantage over the SQL in several regimes.

Beside this, the performance of quantum receivers in the presence of noisy non-Gaussian channels is another fundamental task towards the realistic implementation of quantum optical communications. A paradigmatic example is provided by phase noise [115–118], which represents the most detrimental source of noise for phase-shift encoding, destroying the coherence and the purity of the employed coherent pulses [119, 120].

In the presence of a phase diffusion channel, the problem of BPSK discrimination is remarkably different with respect to the scenario discussed in the previous sections. In fact, the encoded coherent states evolve according to a suitable master equation [119], being equivalent to the completely positive (CP) map $\mathcal{E}_\sigma$, such that:

$$|\alpha_k\rangle \xrightarrow{\mathcal{E}_\sigma} \rho_k = \int_{\mathbb{R}} d\phi \, g_\sigma(\phi) \, |\alpha_k e^{-i\phi}\rangle\langle\alpha_k e^{-i\phi}| \, , \qquad k = 0, 1 \, , \tag{4.114}$$

where $g_\sigma(\phi) = \exp[-\phi^2/(2\sigma^2)]/\sqrt{2\pi\sigma^2}$ is a Gaussian distribution whose standard deviation $\sigma > 0$ quantifies the amount of noise. That is, the overall effect of phase diffusion is the application of a Gaussian-distributed random phase shift to the incoming signal, resulting in a overall non-Gaussian CP map.

Given the previous considerations, in the presence of BPSK the effect of phase diffusion is detrimental: it reduces both the coherence and the purity of the encoded coherent states as emerges from Fig. 4.6.1, reporting the phase space representation of the quantum states before and after the noisy channel. In turn, the quantum receiver has

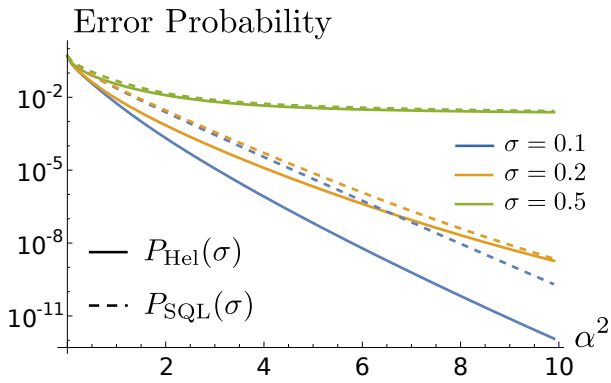


Figure 4.6.2: Log plot of the Helstrom bound $P_{\rm Hel}(\sigma)$ and the SQL $P_{\rm SQL}(\sigma)$ as a function of the signal energy α^2 for different values of phase noise σ. In the limit of large noise, the homodyne receiver becomes near optimum and $P_{\rm SQL}(\sigma) \approx P_{\rm Hel}(\sigma)$.

to discriminate between the two mixed phase-diffused states ρ_0 and ρ_1. The Helstrom bound becomes [9, 18, 51, 67, 121]:

$$P_{\rm Hel}(\sigma) = \frac{1}{2}\left[1 - {\rm Tr}\left(|\Lambda|\right)\right] , \tag{4.115}$$

with

$$\begin{aligned}\Lambda &= \frac{1}{2}(\rho_0 - \rho_1) \\ &= \frac{e^{-\alpha^2}}{2} \sum_{n,m=0}^{\infty} \frac{e^{-(n-m)^2\sigma^2/2}}{\sqrt{n!m!}} \alpha^{n+m} \left[(-1)^{n-m} - 1\right] |n\rangle\langle m| ,\end{aligned} \tag{4.116}$$

expanded in the Fock basis $\{|n\rangle\}_n$. Plots of $P_{\rm Hel}(\sigma)$ are reported in Fig. 4.6.2 as a function of the mean signal energy α^2 for different values of noise. As expected, the presence of the noise makes the error probability increase. In particular, for small α we may truncate Λ at low dimension, achieving the analytic expression

$$P_{\rm Hel}(\sigma) \approx \frac{1}{2}\left[1 - \alpha\, e^{-\sigma^2/2}\right] , \qquad \text{for } \alpha \ll 1 , \tag{4.117}$$

whereas in the limit of large noise, i.e. $\sigma \gg 1$, we have:

$$P_{\rm Hel}(\sigma) \approx \frac{1}{2}\left[1 - f_{\rm Hel}(\alpha) e^{-\sigma^2/2}\right] , \qquad \text{for } \sigma \gg 1 , \tag{4.118}$$

$f_{\rm Hel}(\alpha)$ being a decreasing function of α [121].

On the contary, the SQL, obtained with homodyne detection, reads [18, 121]:

$$P_{\rm SQL}(\sigma) = \frac{1}{2}\left[\int_0^{\infty} dx\, p_{\rm HD}^{(\sigma)}(x|0) + \int_{-\infty}^{0} dx\, p_{\rm HD}^{(\sigma)}(x|1)\right] , \tag{4.119}$$

depicted in Fig. 4.6.2, where

$$p_{\rm HD}^{(\sigma)}(x|k) = \int_{\mathbb{R}} d\phi\, g_\sigma(\phi)\, \frac{\exp\left[-(x - 2\alpha_k \cos\phi)^2/2\right]}{\sqrt{2\pi}} \tag{4.120}$$

is the homodyne probability of obtaining outcome x given the state $|\alpha_k\rangle$, expressed in shot-noise units. For small values of the coherent amplitude we get the analytic expression

$$P_{\rm SQL}(\sigma) \approx \frac{1}{2}\left[1-\alpha\sqrt{\frac{2}{\pi}}e^{-\sigma^2/2}\right], \qquad \text{for } \alpha \ll 1\,, \tag{4.121}$$

whereas in the limit of large noise, i.e. $\sigma \gg 1$, we have:

$$P_{\rm SQL}(\sigma) \approx \frac{1}{2}\left[1-f_{\rm SQL}(\alpha)e^{-\sigma^2/2}\right], \qquad \text{for } \sigma \gg 1\,, \tag{4.122}$$

where $f_{\rm SQL}(\alpha)$ is a decreasing function of α such that $f_{\rm SQL}(\alpha) < f_{\rm Hel}(\alpha)$ which approaches $f_{\rm Hel}(\alpha)$ for increasing coherent amplitude α [121].

As we can see from the plot, the homodyne receiver is quite robust with respect to the noise, as, for $\sigma \lesssim 0.2$ and low energy α^2, the value of $P_{\rm SQL}$ is almost constant. In contrast, when $\sigma > 0$, in the high-energy limit $\alpha^2 \gg 1$ we have $P_{\rm SQL} \approx P_{\rm Hel}$ and homodyne detection becomes near-optimum, as emerges from the asymptotic expansions (4.118) and (4.122). Furthermore, as σ increases, the gap between $P_{\rm SQL}$ and $P_{\rm Hel}$ is closed and, for $\sigma \gtrsim 0.5$, the two quantities almost coincide.

Given this scenario, a natural question arises, that is to quantify the performance of other quantum receivers, such as displacement and hybrid receivers, in the presence of phase diffusion, and assess whether or not their quantum advantage over the SQL is maintained [18]. For the sake of simplicity, in the following we investigate only single-copy receivers, namely the displacement receiver and the HYNORE, leaving the analysis of multi-copy schemes as an open problem for future developments. Moreover, we note that the presence of phase noise is detrimental for the Kennedy receiver [121]. Indeed, the Kennedy receiver is no longer near-optimum and its performance is severely degraded for $\sigma > 0$, since the displacement does not implement anymore a "nulling" operation, as in the presence of dark counts and visibility reduction [121]. Following the same philosophy adopted in the former section, we take the DPNR receiver as a benchmark, whose performance is discussed in the following [92, 93].

4.6.1 DPNR receiver in the presence of phase diffusion

In the presence of phase noise, the displacement operation $D(\alpha)$ of the DPNR scheme maps states ρ_k into $\Phi_k = D(\alpha)\rho_k D(\alpha)^\dagger$, equal to:

$$\Phi_k = \int_{\mathbb{R}} d\phi\, g_\sigma(\phi)\, \left|\sqrt{\mu_k(\alpha^2,\phi)}\, e^{-i\phi/2}\right\rangle \left\langle \sqrt{\mu_k(\alpha^2,\phi)}\, e^{-i\phi/2}\right|, \tag{4.123}$$

where

$$\mu_0(\alpha^2,\phi) = 4\alpha^2\sin^2(\phi/2) \quad \text{and} \quad \mu_1(\alpha^2,\phi) = 4\alpha^2\cos^2(\phi/2)\,. \tag{4.124}$$

Differently from the noiseless case, the nulling operation implemented by $D(\alpha)$ is not perfect and the output state Φ_0 still contains some photons. Thereby, on-off detection is not the most appropriate strategy anymore and the DPNR setup is expected to outperform the Kennedy.

The PNR(M) probability distribution of the displaced states Φ_k reads:

$$\mathsf{P}_\sigma(n|k) = \int_{\mathbb{R}} d\phi\, g_\sigma(\phi)\, p_n\left(\mu_k(\alpha^2,\phi)\right), \quad (n=0,\dots,M)\,, \tag{4.125}$$

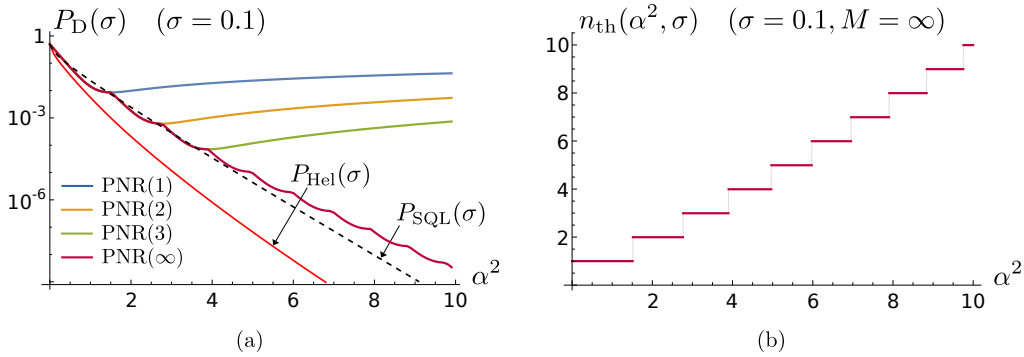


Figure 4.6.3: (a) Error probability $P_{\rm D}(\sigma)$ of the DPNR receiver as a function of the signal energy α^2 for different photon number resolution M. The PNR(1) case corresponds to the Kennedy receiver. (b) Threshold count $n_{\rm th}$ as a function of the signal energy α^2 for PNR(∞) detectors. In both the pictures we fix the noise value to $\sigma = 0.1$.

with the probability $p_n(\mu)$ and the count rates $\mu_k(\alpha^2, \phi)$ defined in Eq.s (4.57) and (4.124), respectively. The final decision is performed according to the maximum a posteriori probability (MAP) criterion: given the outcome $n = 0, \ldots, M$, we infer the state "0" or "1" associated with the maximum a posteriori probability [92, 93]. Again, this is equivalent to introducing a threshold $n_{\rm th} = n_{\rm th}(\alpha^2, \sigma) \leq M$ such that all outcomes $n < n_{\rm th}$ correspond to decision "0", while outcomes $n \geq n_{\rm th}$ infer state "1" [16]. The threshold is obtained numerically by equating the photon number distributions of the two displaced phase-diffused states, namely $\mathsf{P}_\sigma(\bar{n}|0) = \mathsf{P}_\sigma(\bar{n}|1)$, $\bar{n} \in \mathbb{R}$, and considering the lowest integer greater than the obtained root $\bar{n}$, namely $n_{\rm th}(\alpha^2, \sigma) = \lceil \bar{n} \rceil$. In turn, the error probability of the DPNR receiver reads:

$$P_{\rm D}(\sigma) = \frac{1}{2}\left[\sum_{n=0}^{n_{\rm th}-1} \mathsf{P}_\sigma(n|1) + \sum_{n=n_{\rm th}}^{M} \mathsf{P}_\sigma(n|0)\right], \tag{4.126}$$

and with PNR(1) detection we retrieve the Kennedy receiver.

Plots of $P_{\rm D}(\sigma)$ as a function of the signal energy α^2 are reported in Fig. 4.6.3(a) for the realistic noise value $\sigma = 0.1$ [122]. The error probability is not a monotonic function of α^2 and, as demonstrated in [121], the Kennedy receiver is not near-optimum anymore in the presence of noise. The Kennedy is beaten by DPNR receivers with higher resolution M, whose corresponding error probabilities exhibit a step-like behaviour. This follows from the application of MAP criterion: as displayed in Fig. 4.6.3(b), for $\alpha^2 \ll 1$ the threshold decision count is equal to $n_{\rm th} = 1$, equivalent to on-off detection, whilst for larger α^2 it jumps to higher integer values, until reaching $n_{\rm th} = M$ in the high-energy limit $\alpha^2 \gg 1$. Accordingly, the error probability has a cusp at every change in the value of $n_{\rm th}$ and, once $n_{\rm th} = M$, it becomes an increasing function of the energy. In fact, in the high-energy limit a decision error occurs only when outcome $n = M$ is retrieved from state ρ_0, therefore the error probability is equal to [16, 17]:

$$P_{\rm D}(\sigma) \approx \frac{\mathsf{P}_\sigma(M|0)}{2} = \frac{1}{2}\left[1 - \sum_{j=0}^{M-1} \int_{\mathbb{R}} d\phi\, g_\sigma(\phi)\, e^{-\mu_0(\phi)} \frac{\mu_0(\phi)^j}{j!}\right], \tag{4.127}$$

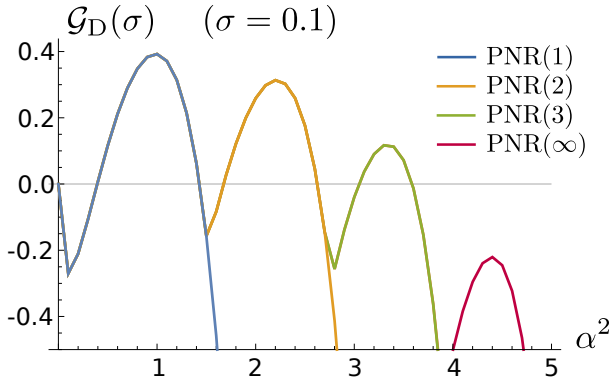


Figure 4.6.4: Gain $\mathcal{G}_{\rm D}(\sigma)$ of the DPNR receiver with respect to the SQL as a function of the signal energy α^2 for different photon number resolution M, when $\mathcal{G}_{\rm D}(\sigma) > 0$ we beat the SQL. The PNR(1) case corresponds to the Kennedy receiver. We fix the noise value to $\sigma = 0.1$.

being an increasing function of α^2. On the contrary, PNR(∞) detectors do not have a finite resolution, therefore $n_{\rm th}(\sigma)$ can get arbitrary large values and the step-like behaviour is observed in every energy regime, as shown in Fig. 4.6.3(a).

Differently from the noiseless case, the SQL is beaten by DPNR receivers only in particular energy regimes. To highlight this, we consider the gain

$$\mathcal{G}_{\rm D}(\sigma) = 1 - \frac{P_{\rm D}(\sigma)}{P_{\rm SQL}(\sigma)}\,, \tag{4.128}$$

plotted in Fig. 4.6.4. In turn, we have a genuine quantum advantage over the SQL when $\mathcal{G}_{\rm D}(\sigma) > 0$. As expected, the gain $\mathcal{G}_{\rm D}(\sigma)$ is not monotonic with α^2, but it exhibits M jumps before decreasing monotonously. The DPNR receiver outperforms the SQL in the low-energy limit and only in particular intervals of α^2. Remarkably, for a given noise σ we obtain the maximal region of positive gain with PNR(M) detectors having sufficiently small M, whereas increasing the resolution further is not necessary to enhance the violation of the SQL.

In Fig. 4.6.5(a) and (b) we report the error probability $P_{\rm D}(\sigma)$ as a function of the noise σ for low and high energy values $\alpha^2 = 1$ and $\alpha^2 = 4$, respectively. In both the cases DPNR receivers beat the SQL only for small noise, whilst in the large-noise limit the SQL becomes near optimum [121]. We also note that for $\alpha^2 = 1$ the performance of PNR(M) detectors with $M \geq 2$ is the same, since in this case the threshold count is equal to $n_{\rm th} = 2$. On the contrary, for $\alpha^2 = 4$ increasing the PNR resolution is beneficial to reduce the error probability.

Given the previous considerations, we introduce as a figure of merit the maximum tolerable phase noise $\sigma^{(\rm D)}_{\rm max}$, namely the maximum level of noise for which $\mathcal{G}_{\rm D}(\sigma) \geq 0$ for a given signal energy α^2, depicted in Fig. 4.6.6. Thus, the DPNR receiver outperforms the SQL if $\sigma < \sigma^{(\rm D)}_{\rm max}$, corresponding to the undergraph region of $\sigma^{(\rm D)}_{\rm max}$. We have $\sigma^{(\rm D)}_{\rm max} = 0$ for $\alpha^2 < \alpha^2_{\rm K} \approx 0.38$, since in that regime the DPNR does not beat the SQL neither in the noiseless case (in which it performs as a Kennedy); then the plot exhibits M peaks and, thereafter, it decreases towards 0.

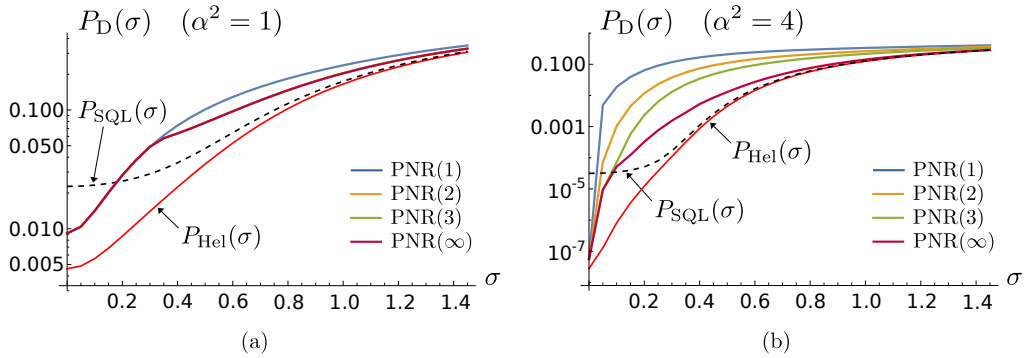


Figure 4.6.5: Error probability $P_{\rm D}(\sigma)$ of the DPNR receiver as a function of the noise σ for $\alpha^2=1$ (a) and $\alpha^2=4$ (b). For $\alpha^2=1$, the curves of PNR(M) detection with $M\geq 2$ are superimposed and, thus, indistinguishable. Given the energy α^2, the DPNR receiver outperforms the SQL in the small-noise regime, whereas for large noise the SQL becomes near-optimum.

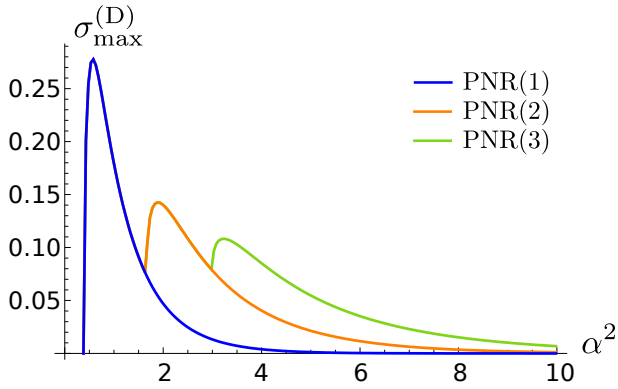


Figure 4.6.6: Maximum tolerable phase noise $\sigma_{\rm max}^{\rm (D)}$ as a function of the signal energy α^2 for different photon number resolution M. The DPNR receiver beats the SQL in the undergraph region, namely $\sigma<\sigma_{\rm max}^{\rm (D)}$.

4.6.2 HYNORE in the presence of phase diffusion

Now, we address the role of the HYNORE for BPSK discrimination of phase-diffused coherent states. As discussed above, quantum receivers based on either quadrature measurements or displacement and photon counting show different degrees of robustness against phase noise, therefore a hybrid scheme like the HYNORE, based on the combination of both of them, provides a good candidate to better mitigate the impact of the noise.

To evaluate the performance of the HYNORE we proceed as follows. After the beam splitter with transmissivity τ, the dephased signal ρ_k is split into the separable bipartite state

$$\Xi_k = \int_{\mathbb{R}} d\phi\, g_\sigma(\phi) \left|\alpha_k^{(r)} e^{-i\phi}\right\rangle \left\langle \alpha_k^{(r)} e^{-i\phi}\right| \otimes \left|\alpha_k^{(t)} e^{-i\phi}\right\rangle \left\langle \alpha_k^{(t)} e^{-i\phi}\right| , \tag{4.129}$$

with $\alpha_k^{(r)}$ and $\alpha_k^{(t)}$ introduced in Eq. (4.51). Then, we perform HL detection on the first branch obtaining outcome Δ and displace the conditional state on the second branch accordingly, obtaining the (not normalized) state $\Phi_k(\Delta) = \mathrm{Tr}_r[U\,\Xi_k\,U^\dagger]$, where the reflected beam has been traced out, and

$$U = \mathbb{P}_\Delta \otimes D\big\{\Theta(\Delta)\sqrt{\tau}\alpha + [1-\Theta(\Delta)](-\sqrt{\tau}\alpha)\big\} , \tag{4.130}$$

$\mathbb{P}_\Delta$ being the projection operator over the eigenspace associated with the outcome Δ and $\Theta(\Delta)$ is the Heaviside Theta function, returning 1 for $\Delta \geq 0$ and 0 elsewhere. In turn, we have:

$$\Phi_k(\Delta) = \int_{\mathbb{R}} d\phi\, g_\sigma(\phi)\, \mathcal{S}(\Delta|\alpha_k^{(r)} e^{-i\phi}) \left|\alpha_k(\tau,\phi)\, e^{-i\phi/2}\right\rangle \left\langle \alpha_k(\tau,\phi)\, e^{-i\phi/2}\right| , \tag{4.131}$$

with:

$$\alpha_k(\tau,\phi) = \Theta(\Delta)\sqrt{\mu_k(\tau\alpha^2,\phi)} + [1-\Theta(\Delta)]\sqrt{\mu_{k\oplus 1}(\tau\alpha^2,\phi)} , \tag{4.132}$$

$\mathcal{S}(\Delta|\alpha_k^{(r)} e^{-i\phi})$ being the HL probability of Eq. (4.55) and "$\oplus$" denoting the mod 2 sum. Finally, we implement PNR(M) detection on states $\Phi_k(\Delta)$. The resulting joint probability of outcomes $-M \leq \Delta \leq M$ and $n = 0, \ldots, M$ reads:

$$\begin{aligned} \mathsf{P}_\sigma(\Delta, n|k) = \int_{\mathbb{R}} & d\phi\, g_\sigma(\phi)\, \mathcal{S}(\Delta|\alpha_k^{(r)} e^{-i\phi}) \\ & \times p_n\Big\{\Theta(\Delta)\,\mu_k(\tau\alpha^2,\phi) + [1-\Theta(\Delta)]\,\mu_{k\oplus 1}(\tau\alpha^2,\phi)\Big\} . \end{aligned} \tag{4.133}$$

We perform discrimination according to the MAP criterion, i.e. by considering the threshold count depicted in Fig. 4.6.3(b), with the remark that the energy value to be considered is now the transmitted fraction $\tau\alpha^2$, namely $n_{\mathrm{th}} = n_{\mathrm{th}}(\tau\alpha^2, \sigma)$. Accordingly, the decision rule is modified as in Table 4.6.1.

The error probability is obtained as

$$P_{\mathrm{HY}}(\sigma) = \min_{\tau,z} P_{\mathrm{HY}}(\tau, z; \sigma) , \tag{4.134}$$

outcomes		decision
$\Delta \geq 0$	$n < n_{\rm th}$	"0"
$\Delta < 0$	$n \geq n_{\rm th}$	"0"
$\Delta < 0$	$n < n_{\rm th}$	"1"
$\Delta \geq 0$	$n \geq n_{\rm th}$	"1"

Table 4.6.1: Decision strategy for the HYNORE in the presence of phase diffusion.

where

$$
\begin{aligned}
P_{\rm HY}(\tau,z;\sigma) &= \frac{1}{2}\big[\mathsf{P}_\sigma(\Delta<0,n<n_{\rm th}|0)+\mathsf{P}_\sigma(\Delta\geq 0,n\geq n_{\rm th}|0)\\
&\quad+\mathsf{P}_\sigma(\Delta<0,n\geq n_{\rm th}|1)+\mathsf{P}_\sigma(\Delta\geq 0,n<n_{\rm th}|1)\big]\\
&= \frac{1}{2}\int_{\mathbb{R}} d\phi\, g_\sigma(\phi)\left\{\sum_{n=0}^{n_{\rm th}-1} p_n\left(\mu_1(\tau\alpha^2,\phi)\right)\right.\\
&\quad\times\left[\sum_{\Delta=-M}^{-1}\mathcal{S}(\Delta|\alpha_0^{(r)}e^{-i\phi})+\sum_{\Delta=0}^{M}\mathcal{S}(\Delta|\alpha_1^{(r)}e^{-i\phi})\right]\\
&\quad+\sum_{n=n_{\rm th}}^{M} p_n\left(\mu_0(\tau\alpha^2,\phi)\right)\\
&\quad\left.\times\left[\sum_{\Delta=-M}^{-1}\mathcal{S}(\Delta|\alpha_1^{(r)}e^{-i\phi})+\sum_{\Delta=0}^{M}\mathcal{S}(\Delta|\alpha_0^{(r)}e^{-i\phi})\right]\right\}. \qquad (4.135)
\end{aligned}
$$

Plots of $P_{\rm HY}(\sigma)$ are reported in Fig. 4.6.7(a). Like the DPNR receiver, the error probability $P_{\rm HY}(\sigma)$ exhibits a step-like behaviour induced by the change in the threshold $n_{\rm th}$. The HYNORE outperforms the DPNR, $P_{\rm HY}(\sigma)\leq P_{\rm D}(\sigma)$, especially in the high-energy limit $\alpha^2\gg 1$, where the error probability is reduced of a factor $\approx 5,15,20$ for $M=1,2,3$, respectively, showing higher robustness in mitigating the phase noise. Moreover, we observe a quantum advantage also in the low-energy regime, as emerges by computing the gain

$$
\mathcal{G}_{\rm HY}(\sigma)=1-\frac{P_{\rm HY}(\sigma)}{P_{\rm SQL}(\sigma)}, \qquad (4.136)
$$

depicted in Fig. 4.6.7(b). We have $\mathcal{G}_{\rm HY}(\sigma)\geq\mathcal{G}_{\rm D}(\sigma)$ and, differently from the DPNR case, improving the resolution M makes the gain increase, since the HL scheme performs better and better, coming closer to the homodyne limit. As one may expect, the best performance is obtained with PNR(∞) detectors, where the HL performs as standard homodyne detection and $\mathcal{G}_{\rm HY}(\sigma)\geq 0$ for all energies.

The physical meaning of the present results is clearer when considering the optimized transmissivity $\tau_{\rm opt}(\sigma)$ and LO amplitude $z^2_{\rm opt}(\sigma)$ obtained after the minimization in Eq. (4.134), reported in Fig. 4.6.8(a) and (b), respectively, for the case of PNR(3) detectors. Analogous results can be retrieved for other values of the resolution M. The results are similar those obtained in Sec. 4.5.1 in the presence of reduced visibility $\xi\leq 1$. In fact, in the low-energy limit, the transmissivity $\tau_{\rm opt}(\sigma)$ increases with α^2 up to reach 1 (corresponding to DPNR). Thereafter, we observe $M-1$ "sawteeth", namely regions where

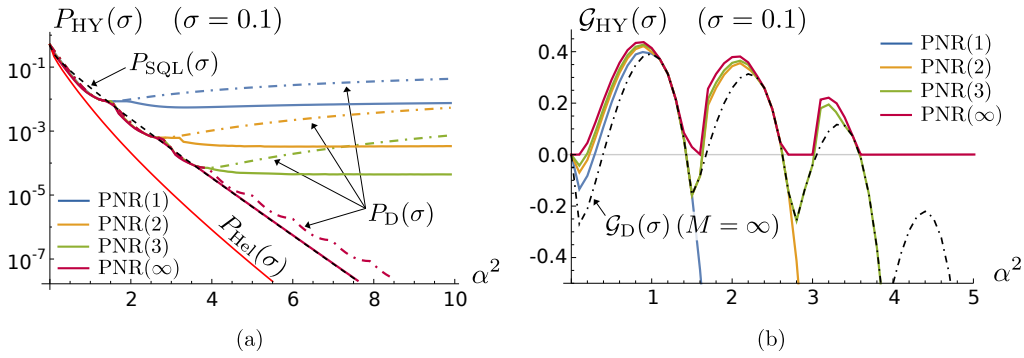


Figure 4.6.7: (a) Error probability $P_{\rm HY}(\sigma)$ of the HYNORE as a function of the signal energy α^2 for different photon number resolution M. The dot-dashed lines are the error probabilities of the DPNR receiver. (b) Gain $\mathcal{G}$HY(σ) of the HYNORE with respect to the SQL as a function of the signal energy α^2. In both the pictures we fix the noise value to $\sigma = 0.1$.

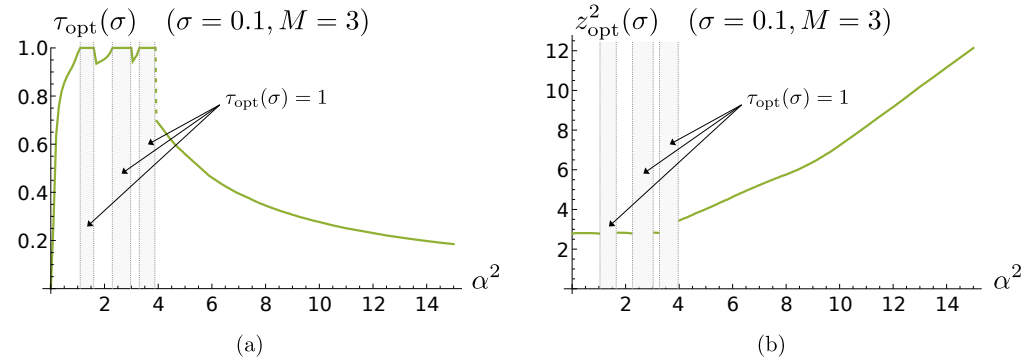


Figure 4.6.8: Optimized transmissivity $\tau_{\rm opt}(\sigma)$ (a) and LO $z^2_{\rm opt}(\sigma)$ (b) as a function of the signal energy α^2 for PNR(3) detectors. Both the quantities have been obtained by numerical optimization. In the shaded regions we have $\tau_{\rm opt}(\sigma) = 1$ and the HYNORE performs as a DPNR receiver. We fix the noise value to $\sigma = 0.1$.

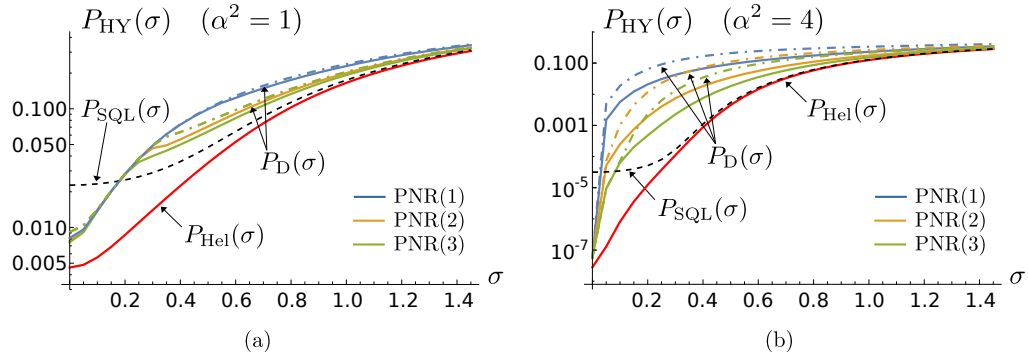


Figure 4.6.9: Error probability $P_{\rm HY}(\sigma)$ of the DPNR receiver as a function of the noise σ for $\alpha^2=1$ (a) and $\alpha^2=4$ (b), compared to the DPNR receiver.

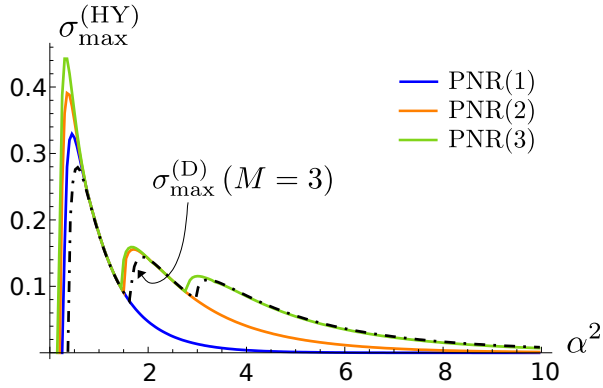


Figure 4.6.10: Maximum tolerable phase noise $\sigma_{\rm max}^{\rm (HY)}$ as a function of the signal energy α^2 for different photon number resolution M. The HYNORE receiver beats the SQL in the undergraph region, namely $\sigma<\sigma_{\rm max}^{\rm (HY)}$. The dot-dashed line refers to $\sigma_{\rm max}^{\rm (D)}$ for $M=3$.

$\tau_{\rm opt}(\sigma)<1$ before increasing to again reach 1. Accordingly, when $\tau_{\rm opt}(\sigma)<1$ the LO is $z_{\rm opt}^2(\sigma)\approx M$ and the HYNORE outperforms the DPNR, whilst when $\tau_{\rm opt}(\sigma)=1$ all signal is sent to the transmitted DPNR setup. On the contrary, in the high-energy limit the transmissivity jumps discontinuously and becomes a decreasing function of α^2, saturating for $\alpha^2\gg 1$ to an asymptotic value $\tau_\infty\neq 0$. Remarkably, $\tau_\infty<1$, therefore the optimal strategy is obtained with a proper combination of both the HL and the DPNR schemes. In this regime, $z_{\rm opt}^2(\sigma)$ increases with α^2, being a linear function for $\alpha^2\gg 1$.

Finally, in Fig. 4.6.9 we plot $P_{\rm HY}(\sigma)$ (solid lines) as a function of the noise σ for $\alpha^2=1$ (left panel) and $\alpha^2=4$ (right panel), respectively, comparing it to the DPNR (dot-dashed lines). We see that $P_{\rm HY}(\sigma)\leq P_{\rm D}(\sigma)$ in both the small- and large-noise limits and the enhancement is more relevant for large α^2, consistently with the previous analysis. As a consequence, the HYNORE increases the maximum tolerable phase noise $\sigma_{\rm max}^{\rm (HY)}$, as depicted in Fig. 4.6.10. In fact, we have $\sigma_{\rm max}^{\rm (HY)}\geq\sigma_{\rm max}^{\rm (D)}$ for all energies, and $\sigma_{\rm max}^{\rm (HY)}=0$ for $\alpha^2<\alpha_{\rm HY}^2(M)$, enlarging the region of quantum advantage with respect to the DPNR. Moreover, increasing the resolution M lets the height of the peaks increase, improving further the robustness of the receiver.

CHAPTER 5

Discrimination in multilevel quantum communications systems

In this Chapter, we proceed beyond binary decision theory and tackle the problem of discrimination of a constellation of $M \geq 2$ non-orthogonal quantum states. This represents a relevant issue in digital communication systems operated at the quantum limit, that leads to the appearance of a nonzero bit error rate due to decision errors induced by the nonzero overlap between the encoded states. In particular, the decision problem can be recast into a convex optimization problem, and, thanks to advanced tools of linear algebra, there are well established necessary and sufficient conditions to be fulfilled by the optimum receiver. To date, unlike the binary case, the general expression of the optimum POVM is not known, and the optimum receiver is explicitly constructed only in the presence of pure states with geometrically uniform symmetry (GUS) [51, 54, 83, 123–125]. To overcome these limitations, suboptimal methods have been established, e.g. the pretty good measurement (PGM) method, yielding the optimal decision under certain conditions [126–134].

The Chapter is organized as follows. In Sec. 5.1, we present a comprehensive review of the results of M-ary quantum decision theory, together with the characterization of the optimum receiver guaranteed by Yuen's theorem. On the other hand, Sec. 5.2 focuses in detail on pure-state discrimination, providing a further characterization of quantum receivers. Thereafter, in Sec. 5.3 we introduce the concept of GUS and perform explicit construction of the optimum POVM achieving the minimum decision error probability. Instead, in Sec. 5.4, we analyze the PGM method, that, in general, determines a suboptimal receiver (not achieving minimum error probability), whilst becoming optimal in the presence of pure-state discrimination and GUS. Finally, as a paradigmatic case study, in Sec. 5.5 we apply the obtained results to quadrature phase-shift keying (QPSK) discrimination of coherent states, presenting some relevant examples of quantum receivers, namely the Bondurant, quaternary displacement (QDRE) and quaternary displacement feed-forward (QDFFRE) receivers.

5.1 Discrimination of M-ary constellations

In the previous chapter we widely investigated the problem of binary discrimination, firstly developed by Helstrom's theory, and, thereafter, we considered a relevant application for quantum communications, namely coherent state discrimination, providing a few examples of feasible quantum receivers. Now, we proceed beyond the binary case and present the general theory for M-ary state discrimination, mainly developed by Yuen, Holevo and Kennedy [51, 54, 83, 123–125]. Differently from Helstrom's theory, in this case the solution to the decision problem, that is the optimum POVM achieving

minimum error probability, is highly nontrivial and requires advanced tools from linear algebra.

To begin with, we start by reviewing the scenario under investigation. We have a source that encodes a set of classical symbols $k = 0, \dots, M-1$, onto a *constellation* of non-orthogonal quantum states $\mathcal{C} = \{\rho_k\}_k$, ρ_k being a positive semidefinite operator acting on a Hilbert space $\mathcal{H}$, with $\mathrm{Tr}[\rho_k] = 1$, and generated with a priori probability $0 \leq q_k \leq 1$, $\sum_k q_k = 1$. The number M of the constellation states is typically referred to as *modulation order*. The task is to implement a quantum receiver to infer which was the state emitted by the source. The receiver is described by a M-valued POVM $\mathbf{\Pi} = \{\Pi_j\}_j$, $j = 0, \dots, M-1$, with $\Pi_j \geq 0$ and $\sum_j \Pi_j = \hat{\mathbb{1}}$, associated with a decision rule, such that, when outcome j is retrieved, we infer the probed state to be ρ_j. Due the non orthogonality of the constellation states, any receiver is associated with an error probability $P_{\mathrm{err}} = 1 - \mathcal{P}_c$, $\mathcal{P}_c$ being the correct decision probability, equal to:

$$\mathcal{P}_c = \sum_{k=0}^{M-1} q_k \, p(k|k) \,, \tag{5.1}$$

where $p(j|k) = \mathrm{Tr}[\rho_k \Pi_j]$ is the probability of inferring symbol j when state ρ_k was sent. Therefore, the goal is to identify the optimum receiver, achieving the minimum error probability $P_{\mathrm{err}}^{(\mathrm{min})}$ or, equivalently, the maximum correct decision probability $\mathcal{P}_c^{(\mathrm{max})}$ compatible with quantum mechanics laws [51].

The decision problem presented above can be recast into the framework of convex *semidefinite programming* (SDP), namely optimization of a linear cost function with (linear) constraints over the closed convex cone of positive semidefinite operators [51, 135, 136]. In fact, for a given constellation, we should determine the POVM that maximizes the functional:

$$\mathcal{J}(\mathbf{\Pi}) = \sum_{j=0}^{M-1} \mathrm{Tr}[\widetilde{\rho}_j \Pi_j] \,, \quad \Pi_j \in \mathcal{B} \,, \tag{5.2}$$

where $\widetilde{\rho}_j = q_j \rho_j$ are the weighted density operators and $\mathcal{B}$ is the set of Hermitian operators on $\mathcal{H}$. That is, we should solve the following SDP problem:

$$\begin{aligned} &\max_{\Pi_j \in \mathcal{B}} \mathcal{J}(\mathbf{\Pi}) \,, \\ &\text{subject to:} \\ &\Pi_j \geq 0 \,, \quad j = 0, \dots, M-1 \,, \quad \text{and} \quad \sum_j \Pi_j = \hat{\mathbb{1}} \,. \end{aligned} \tag{5.3}$$

The first constraint in (5.3) defines the cone set of Hermitian positive semidefinite operators, being the proper domain of functional $\mathcal{J}$, while the second one provides a linear constraint on the variables Π_j.

Within this framework, a first characterization of the optimum POVM has been carried out independently in the early 1970s by both Yuen [123, 124] and Holevo [54]. In particular, in 1970 Yuen determined a class of necessary and sufficient conditions to be satisfied in the presence of equiprobable symbols, even though his proof contained redundant constraints and did not hold anymore in the presence of infinite dimensional Hilbert spaces. On the contrary, in 1972, Holevo derived the sufficient condition for optimality with different approach, but he did not establish that it was also necessary.

Instead, he found a necessary condition, different than the sufficient one, being valid for any functional of the POVM $\mathbf{\Pi}$, even non-linear. A unified description was finally achieved by Yuen *et al.* in 1975 [125], after private communications with Holevo. This ultimate proof removes the redundancies of the previous version and properly extends its validity to non-uniform a priori probability and infinite dimensional spaces.

Yuen's proof exploits the Lagrange duality theorem in convex programming. The principle behind it is to transform constrained maximization into a dual minimization problem, where the constraints are included as Lagrange multipliers [135–137]. The construction of the dual problem requires technical concepts and properties from topology theory, therefore we decided not to report it here, as it goes beyond the purpose of this dissertation. Its derivation is explicitly reported in [125] for both finite and infinite dimensional Hilbert spaces. Ultimately, Yuen *et al.* derived the following equivalence:

$$\max_{\substack{\Pi_j\in\mathcal{B}\\ \Pi_j\geq 0\\ \sum_j \Pi_j=\hat{\mathbb{1}}}} \sum_j \mathrm{Tr}[\widetilde{\rho}_j\Pi_j] = \min_{\substack{\Lambda\in\mathcal{T}\\ \Lambda-\widetilde{\rho}_j\geq 0}} \mathrm{Tr}[\Lambda]\,, \tag{5.4}$$

where $\Lambda \in \mathcal{T}$, $\mathcal{T} \subset \mathcal{B}$ being the subset of the trace-class Hermitian operators on $\mathcal{H}$, namely $\mathcal{T} = \{T \in \mathcal{B} : \mathrm{Tr}[T] < \infty\}$. The right-hand side problem,

$$\min_{\Lambda\in\mathcal{T}} \mathrm{Tr}[\Lambda]\,,$$

subject to:

$$\Lambda - \widetilde{\rho}_j \geq 0\,, \quad j = 0, \ldots, M-1\,, \tag{5.5}$$

is the dual problem of (5.3). Thanks to topological arguments, they established the existence of a solution to problems (5.3)-(5.5), therefore there exists a POVM $\mathbf{\Pi}_{\mathrm{opt}}$ and a corresponding trace-class operator Λ_{opt} such that:

$$\mathcal{J}(\mathbf{\Pi}_{\mathrm{opt}}) = \mathrm{Tr}[\Lambda_{\mathrm{opt}}] = \mathcal{P}_c^{(\max)}\,, \tag{5.6}$$

retrieving the maximum correct decision probability.

Furthermore, they formulated the theorem, from now on referred to as "Yuen's theorem", providing a complete characterization of the optimum POVM, determining necessary and sufficient conditions to be fulfilled by $\mathbf{\Pi}_{\mathrm{opt}}$. To prove it, we need the following lemma.

Lemma 5.1. *Let X and Y be two positive semidefinite operators of an arbitrary Hilbert space. Then*

$$\mathrm{Tr}[XY] \geq 0\,, \tag{5.7}$$

and $\mathrm{Tr}[XY] = 0$ if and only if $XY = YX = 0$.

Proof. Since both X and Y are positive, they admit a unique positive semidefinite square root $X^{1/2}$ and $Y^{1/2}$ such that $X = \left(X^{1/2}\right)^2$ and $Y = \left(Y^{1/2}\right)^2$, respectively. Then:

$$\begin{aligned}\mathrm{Tr}[XY] &= \mathrm{Tr}\left[\left(X^{1/2}\right)^2\left(Y^{1/2}\right)^2\right]\\ &= \mathrm{Tr}\left[\left(X^{1/2}Y^{1/2}\right)^\dagger\left(X^{1/2}Y^{1/2}\right)\right] \geq 0\,.\end{aligned} \tag{5.8}$$

From (5.8) and the ciclicity of the trace, it follows that $\mathrm{Tr}[XY] = 0$ if and only if $X^{1/2}Y^{1/2} = Y^{1/2}X^{1/2} = 0$. Then, if $X^{1/2}Y^{1/2} = 0$, we have $XY = 0$. On the other hand, $XY = 0$ also implies that $(XY)^\dagger = YX = 0$, thus X and Y commute, i.e. $[X, Y] = 0$. In turn, all their powers commute with one another and, in particular, $[X^{1/2}, Y] = [X^{1/2}, Y^{1/2}] = 0$. Therefore, $XY = (X^{1/2}Y^{1/2})^\dagger (X^{1/2}Y^{1/2}) = 0$, implying $X^{1/2}Y^{1/2} = 0$. □

We are now ready to enunciate Yuen's theorem.

Theorem 5.1. (Yuen *et al.*, 1975) *In a M-ary system characterized by the weighted density operators $\widetilde{\rho}_j = q_j \rho_j$, $j = 0, \dots, M-1$, the POVM $\mathbf{\Pi} = \{\Pi_j\}_j$ is optimal if and only if the following two conditions hold:*

$$\sum_j \widetilde{\rho}_j \Pi_j = \sum_j \Pi_j \widetilde{\rho}_j \,, \tag{5.9a}$$

$$\sum_s \widetilde{\rho}_s \Pi_s - \widetilde{\rho}_j \geq 0 \,, \quad j = 0, \dots, M-1 \,. \tag{5.9b}$$

Proof. " $\Rightarrow$ ": we start by proving the necessity of conditions (5.9). Let $\mathbf{\Pi}^{(0)} = \{\Pi_j^{(0)}\}_j$ and $\Lambda^{(0)}$ solve the SDP problems (5.3) and (5.5), respectively. Then, thanks to (5.4), we have:

$$\sum_j \mathrm{Tr}\left[\Pi_j^{(0)} \left(\Lambda^{(0)} - \widetilde{\rho}_j\right)\right] = 0 \,. \tag{5.10}$$

Lemma 5.1 then yields:

$$\Pi_j^{(0)} \left(\Lambda^{(0)} - \widetilde{\rho}_j\right) = \left(\Lambda^{(0)} - \widetilde{\rho}_j\right) \Pi_j^{(0)} = 0 \,, \quad j = 0, \dots, M-1 \,. \tag{5.11}$$

We perform summation over index j and obtain:

$$\Lambda^{(0)} = \sum_j \widetilde{\rho}_j \Pi_j^{(0)} = \sum_j \Pi_j^{(0)} \widetilde{\rho}_j \,, \tag{5.12}$$

thus proving (5.9a). Moreover, Eq. (5.12), together with the dual problem constraint $\Lambda_{\mathrm{opt}} \geq \rho_j$ for all j, leads to (5.9b).

" $\Leftarrow$ ": to show sufficiency we first derive a general property. Let $\mathbf{\Pi} = \{\Pi_j\}_j$ and Λ be arbitrary operators that only satisfy the constraints of the SDP problem. In particular, we have $\Lambda - \widetilde{\rho}_s \geq 0$ for all $s = 0, \dots, M-1$. Then, by Lemma 5.1, we have $\mathrm{Tr}[\Pi_s(\Lambda - \widetilde{\rho}_s)] \geq 0$, therefore:

$$\mathrm{Tr}\left[\sum_s \widetilde{\rho}_s \Pi_s\right] \leq \mathrm{Tr}[\Lambda] \,. \tag{5.13}$$

Now, let $\mathbf{\Pi}^{(0)} = \{\Pi_j^{(0)}\}_j$ be a POVM that also satisfies (5.9). We claim that $\mathbf{\Pi}^{(0)}$ is optimal. In fact, we define the operator $\Lambda^{(0)} = \sum_s \widetilde{\rho}_s \Pi_s^{(0)}$, which satisfies $\Lambda^{(0)} - \widetilde{\rho}_j \geq 0$ thanks to (5.9b) and saturates the equality in Eq. (5.13), thus maximizing $\mathrm{Tr}\left[\sum_s \widetilde{\rho}_s \Pi_s\right]$. □

Yuen's theorem is a cornerstone result of quantum decision theory, even though it does not provide a method to construct the optimal measurement. Moreover, we

note that the optimum POVM $\mathbf{\Pi}_{\rm opt}$ is not unique in general. As an example, we consider the case where the constellation states $\{\rho_k\}_k$ commute with one another, namely $[\rho_k, \rho_j] = 0$ [138, 139]. In this case, there exists a common set of eigenstates $\{|\mu_{l_j}\rangle\}_j$, $l_j \in \{0, \ldots, M-1\}$ for all j, that diagonalizes all states. The optimum POVM $\{\Pi_j\}_j$ is constructed from the projectors $\mathbb{P}_{l_j} = |\mu_{l_j}\rangle\langle\mu_{l_j}|$, according to the maximum a posteriori probability (MAP) criterion: given projector $\mathbb{P}_{l_n}$, we infer the state ρ_n with the highest a posteriori probability $\mathrm{Tr}[\widetilde{\rho}_n \mathbb{P}_{l_n}] > \mathrm{Tr}[\widetilde{\rho}_k \mathbb{P}_{l_n}]$, for all $k \neq n$. In this case, we set $\Pi_n = \mathbb{P}_{l_n}$. On the contrary, if there exists l'_n such that, for some ρ_m and ρ_n, we have:

$$\mathrm{Tr}[\widetilde{\rho}_m \mathbb{P}_{l'_n}] = \mathrm{Tr}[\widetilde{\rho}_n \mathbb{P}_{l'_n}] > \mathrm{Tr}[\widetilde{\rho}_k \mathbb{P}_{l'_n}] \quad \forall k \neq m \neq n\,, \tag{5.14}$$

then we may choose either $\Pi_n = \mathbb{P}_{l'_n}$ or $\Pi_m = \mathbb{P}_{l'_n}$ with the same overall correct decision probability [138, 139].

Furthermore, from Yuen's theorem we derive the following result.

Corollary 5.1. *If the POVM $\mathbf{\Pi} = \{\Pi_j\}_j$ is optimum, then*

$$\Pi_j \left(\sum_s \widetilde{\rho}_s \Pi_s - \widetilde{\rho}_j \right) = \left(\sum_s \widetilde{\rho}_s \Pi_s - \widetilde{\rho}_j \right) \Pi_j = 0\,, \tag{5.15}$$

for all $j = 0, \ldots, M-1$.

Proof. The result follows directly from Eq.s (5.11) and (5.12). □

The corollary provides us with a recipe to construct the optimal measurement, according to the following outline:

- at first, we solve the dual problem (5.5), retrieving the optimum operator $\Lambda_{\rm opt}$ and the corresponding maximum correct decision probability $\mathcal{P}_c^{(\max)} = \mathrm{Tr}[\Lambda_{\rm opt}]$;
- then, from Theorem 5.1 we know that the optimum POVM $\mathbf{\Pi}_{\rm opt} = \{\Pi_j^{(\rm opt)}\}_j$ is related to $\Lambda_{\rm opt}$ via the equality $\Lambda_{\rm opt} = \sum_s \widetilde{\rho}_s \Pi_s^{(\rm opt)}$. Therefore, thanks to Corollary 5.1, we obtain the optimal measurement operators as solutions of the system of equations:

$$(\Lambda_{\rm opt} - \widetilde{\rho}_j)\Pi_j^{(\rm opt)} = 0\,, \tag{5.16}$$

for all $j = 0, \ldots, M-1$, with the further request $\sum_j \Pi_j^{(\rm opt)} = \hat{\mathbb{1}}$. In the matrix notation, we have:

$$\begin{pmatrix} \Lambda_{\rm opt} - \widetilde{\rho}_0 & 0 & \cdots & 0 \\ 0 & \Lambda_{\rm opt} - \widetilde{\rho}_1 & \cdots & 0 \\ & & \ddots & \\ 0 & 0 & \cdots & \Lambda_{\rm opt} - \widetilde{\rho}_{M-1} \\ \hat{\mathbb{1}} & \hat{\mathbb{1}} & \cdots & \hat{\mathbb{1}} \end{pmatrix} \begin{pmatrix} \Pi_0^{(\rm opt)} \\ \Pi_1^{(\rm opt)} \\ \vdots \\ \Pi_{M-1}^{(\rm opt)} \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \\ \vdots \\ 0 \\ \hat{\mathbb{1}} \end{pmatrix}\,, \tag{5.17}$$

where we deal with a rectangular $(M+1) \times M$ matrix to include the identity resolution constraint [140].

However, generally speaking, analytic solution to this problem cannot be reached. Nevertheless, the dual problem (5.5) can be numerically solved efficiently thanks to SDP algorithms, providing the maximum correct decision probability in several cases of practical interest [51, 135, 136].

Finally, to conclude the presentation of the general quantum decision theory, we report a further property satisfied by the optimum POVM, derived by Eldar *et al.* in 2003, that holds in the presence of finite-dimensional Hilbert spaces $\mathcal{H}$ [140].

Proposition 5.1. *In the presence of a finite dimensional Hilbert space $\mathcal{H}$, $\dim(\mathcal{H}) = d < \infty$, the optimal POVM elements Π_j have rank not higher than that of the associated constellation state, namely:*

$$\operatorname{rank}(\Pi_j) \leq \operatorname{rank}(\rho_j)\,, \quad j = 0, \ldots, M-1\,. \tag{5.18}$$

The proof of the proposition invokes the *rank-nullity theorem*, a result from linear algebra providing a relation between the rank and nullity of a linear operator A acting on a finite dimensional vector space V. The rank of A is equal to the dimension of its image, i.e. $\operatorname{rank}(A) = \dim(\operatorname{Im}(A))$, while the nullity is the dimension of its kernel, i.e. the null space $\ker(A) = \{v \in V : Av = 0\}$. The theorem states that $\operatorname{rank}(A) + \dim(\ker(A)) = \dim(V)$ [25].

Proof. We first note that it is not restrictive to assume that the constellation states span the whole Hilbert space $\mathcal{H}$. Otherwise, we can rephrase the problem on the subspace $\mathcal{S} \subset \mathcal{H}$ spanned by the eigenstates of $\{\rho_k\}_k$, having finite dimension too, as $\dim(\mathcal{S}) \leq \dim(\mathcal{H}) < \infty$. Now, let $\mathbf{\Pi} = \{\Pi_j\}_j$ be an optimum POVM, and $\Lambda = \sum_s \widetilde{\rho}_s \Pi_s$ its associated solution to the dual problem. Then, by Corollary 5.1, it follows that, for all j, the image of Π_j lies in the kernel of $\Lambda - \widetilde{\rho}_j$, as all vectors in the form $\Pi_j|h\rangle$, for some $|h\rangle \in \mathcal{H}$, satisfy $(\Lambda - \widetilde{\rho}_j)\Pi_j|h\rangle = 0$. In turn, $\operatorname{Im}(\Pi_j) \subset \ker(\Lambda - \widetilde{\rho}_j)$ and, consequently,

$$\operatorname{rank}(\Pi_j) \leq d - \operatorname{rank}(\Lambda - \widetilde{\rho}_j)\,. \tag{5.19}$$

We also note that Λ is a full-rank operator. In fact, we have $\Lambda - \widetilde{\rho}_j \geq 0$ for all j thanks to the constraints of the dual problem and, since and the eigenvectors of the constellation states span $\mathcal{H}$, for any $|h\rangle \in \mathcal{H}$, there exists an index k such that $\langle h|\rho_k|h\rangle > 0$. These two conditions imply $\langle h|\Lambda|h\rangle > 0$ for all $|h\rangle \in \mathcal{H}$, therefore the kernel of Λ only contains the null vector, $\ker(\Lambda) = \{0\}$. From the subadditivity of the rank, i.e. $\operatorname{rank}(A + B) \leq \operatorname{rank}(A) + \operatorname{rank}(B)$ for any two linear operators A and B [25], we have $d = \operatorname{rank}(\Lambda) \leq \operatorname{rank}(\Lambda - \widetilde{\rho}_j) + \operatorname{rank}(\widetilde{\rho}_j)$ which, together with Eq. (5.19), leads to:

$$\operatorname{rank}(\Pi_j) \leq \operatorname{rank}(\widetilde{\rho}_j) = \operatorname{rank}(\rho_j)\,, \tag{5.20}$$

proving the desired result. □

As a final remark, we stress that Proposition (5.1) is only valid if the dimension of the Hilbert space $\mathcal{H}$ is finite, or, at least, if the subspace spanned by the eigenstates of the constellation states is finite-dimensional. Otherwise, in the presence of infinite-dimensional vector spaces the rank-nullity theorem does not hold anymore, and the argument of the proof vanishes.

5.2 Pure-state discrimination

The problem of the optimal decision is considerably simplified if the constellation $\mathcal{C} = \{\rho_k\}_k$ is composed of linearly independent pure states, namely:

$$\rho_k = |\gamma_k\rangle\langle\gamma_k|\,, \qquad k = 0, \ldots, M-1\,. \tag{5.21}$$

To quantify the overlap between the encoded states, it is convenient to introduce the *Gram matrix* G, that is the $M \times M$ matrix of the inner products:

$$G = \big(\langle\gamma_l|\gamma_k\rangle\big)_{l,k}\,, \qquad l, k = 0, \ldots, M-1\,, \tag{5.22}$$

which is $G \neq \mathbb{1}_M$ for non-orthogonal states, $\mathbb{1}_M$ being the $M \times M$ identity matrix. It is not restrictive to reduce the problem to the M dimensional subspace spanned by the encoded states, $\mathcal{S} = \mathrm{span}\{|\gamma_k\rangle : k = 0, \ldots, M-1\}$ and to find a M-valued POVM $\mathbf{\Pi} = \{\Pi_j\}_j$, such that

$$\Pi_j \geq 0 \quad \text{and} \quad \sum_j \Pi_j = \mathbb{P}_{\mathcal{S}}\,, \tag{5.23}$$

$\mathbb{P}_{\mathcal{S}}$ being the projection operator onto subspace $\mathcal{S}$ [51, 141]. In fact, if we decompose each POVM element as $\Pi_j = \Pi'_j + \Pi''_j$, with Π'_j and Π''_j having support equal to $\mathcal{S}$ and $\mathcal{S}^{\perp}$, respectively, we would have $\Pi''_j|\gamma_k\rangle = 0$ for all k, thus the two POVM sets $\{\Pi_j\}_j$ and $\{\Pi'_j\}_j$ would be associated with the same correct decision probability. Moreover, due to the linearly independence of constellation states, subspace $\mathcal{S}$ has dimension equal to M, therefore Proposition 5.1 holds. In more detail, the following theorem, firstly proved by Kennedy in 1973, provides characterization of the optimum POVM [142].

Theorem 5.2. (Kennedy, 1973) *In a M-ary system specified by M pure states $\{|\gamma_k\rangle\}_k$, the optimum POVM $\mathbf{\Pi} = \{\Pi_j\}_j$ is a 1-rank projective measurement, namely:*

$$\Pi_j = |\mu_j\rangle\langle\mu_j|\,, \qquad j = 0, \ldots, M-1\,, \tag{5.24}$$

for some measurement vectors $\{|\mu_j\rangle\}_j$ satisfying $\langle\mu_j|\mu_k\rangle = \delta_{jk}$.

Proof. Thanks to Proposition 5.1, the optimal measurement is composed of 1-rank operators, hence Eq. (5.24) follows. It only remains to prove the orthonormality relation among the measurement vectors. Following the same arguments reported above, it is not restrictive to assume that $|\mu_j\rangle \in \mathcal{S}$ for all j. Then, the POVM elements resolve the identity over $\mathcal{S}$, $\sum_j |\mu_j\rangle\langle\mu_j| = \mathbb{P}_{\mathcal{S}}$, and

$$|\mu_k\rangle = \mathbb{P}_{\mathcal{S}}|\mu_k\rangle = \sum_j |\mu_j\rangle\langle\mu_j|\mu_k\rangle\,, \tag{5.25}$$

which yields $\langle\mu_j|\mu_k\rangle = \delta_{jk}$. □

In particular, the measurement vectors $\{|\mu_j\rangle\}_j$ provide an orthonormal basis of subspace $\mathcal{S}$.

5.2.1 Characterization of M-ary pure-state discrimination receivers

Given the Kennedy theorem, the decision problem in the presence of pure states may be recast into a geometric optimization task. Indeed, we introduce the state and measurement (row) matrices [19]:

$$\Gamma = \Big(|\gamma_0\rangle, \ldots, |\gamma_{M-1}\rangle \Big) \quad \text{and} \quad \mathbb{M} = \Big(|\mu_0\rangle, \ldots, |\mu_{M-1}\rangle \Big) , \tag{5.26}$$

respectively. With this notation, the Gram matrix (5.22) is retrieved as $G = \Gamma^\dagger \Gamma$, whereas, due to the orthonormality of the measurement vectors $\mathbb{M}^\dagger \mathbb{M} = \mathbb{1}_M$, $\mathbb{1}_M$ being the $M \times M$ identity matrix. Since $\{|\mu_j\rangle\}_j \subset \mathcal{S}$, the measurement vectors are expressible as a linear combination of the state vectors, $|\mu_j\rangle = \sum_k a_{kj} |\gamma_k\rangle$, $a_{kj} \in \mathbb{C}$, or equivalently,

$$\mathbb{M} = \Gamma \, A \, , \tag{5.27}$$

A being a $M \times M$ matrix with coefficients $(a_{kj})_{k,j}$.

In turn, we provide characterization of any quantum receiver by its corresponding matrix A, subject to the constraint:

$$A A^\dagger = G^{-1} \, , \tag{5.28}$$

guaranteeing the identity resolution of the resulting POVM [19].

Eq. (5.28) can be derived as follows. For all vectors $|\psi\rangle \in \mathcal{S}$, we have $\mathbb{P}_{\mathcal{S}} |\psi\rangle = |\psi\rangle$, where $|\psi\rangle = \sum_s b_s |\gamma_s\rangle$, $b_s \in \mathbb{C}$. Thanks to Eq.s (5.23) and (5.27), the following equations hold:

$$\left[\sum_j \Big(\sum_{k,l} a_{kj} a_{lj}^* |\gamma_k\rangle\langle\gamma_l| \Big) \right] \sum_s b_s |\gamma_s\rangle = \sum_t b_t |\gamma_t\rangle \, , \tag{5.29}$$

$$\sum_k \Big(\sum_{j,l,s} a_{kj} {a_{jl}}^\dagger G_{ls} b_s \Big) |\gamma_k\rangle = \sum_t b_t |\gamma_t\rangle \, , \tag{5.30}$$

where $G_{ls} = \langle \gamma_l | \gamma_s \rangle$. In the matrix notation we have $A A^\dagger G \, \mathbf{b} = \mathbf{b}$ to be satisfied for all $\mathbf{b} = (b_0, \ldots, b_{M-1})$. This implies:

$$A A^\dagger G = \mathbb{1}_M \, , \tag{5.31}$$

and, ultimately, $A A^\dagger = G^{-1}$.

5.2.2 Consequences of Yuen's theorem

A further characterization of the receiver, being somehow specular to (5.27), can be obtained by expanding the state vectors on the orthonormal basis composed of the measurement vectors, $|\gamma_k\rangle = \sum_j b_{jk} |\mu_j\rangle$ or, equivalently

$$\Gamma = \mathbb{M} \, B \, , \tag{5.32}$$

where:

$$B_{kj} = \langle \mu_j | \gamma_k \rangle \, , \qquad k, j = 0, \ldots, M-1 \, , \tag{5.33}$$

are the inner products between the elements of the two vector systems, describing the geometry between the state and measurement vectors. Since $\mathbb{M}^\dagger\,\mathbb{M} = \mathbb{1}_M$, the relation between matrices A and B is:

$$B = \mathbb{M}^\dagger\,\Gamma = A^\dagger\,G\,, \tag{5.34}$$

implying $B^\dagger\,B = \Gamma^\dagger\,\Gamma = G$.

If matrix A provides a characterization of the quantum receiver, as $\mathbb{M} = \Gamma\,A$, the properties of matrix B determine its optimality for the decision problem. In fact, the maximum correct decision probability can be re-expressed as a function of the sole matrix B, since the conditional probability of obtaining outcome j if the k-th state is probed is given by

$$p(j|k) = \mathrm{Tr}[\rho_k\,\Pi_j] = |\langle\mu_j|\gamma_k\rangle|^2 = |B_{kj}|^2\,. \tag{5.35}$$

In turn, we have:

$$\mathcal{P}_c = \sum_{k=0}^{M-1} q_k\,|B_{kk}|^2\,. \tag{5.36}$$

Yuen's theorem can be specified to the pure-state discrimination scenario, finding necessary and sufficient conditions that should be fulfilled by B. Accordingly, Theorem 5.1 leads to the following corollary [51].

Corollary 5.2. *In a M-ary system specified by M pure states $\Gamma = \{|\gamma_k\rangle\}_k$, generated with a priori probabilities $\{q_k\}_k$, the optimum measurement vectors $\mathbb{M} = \{|\mu_j\rangle\}_j$ must verify the following conditions:*

$$q_j B_{jj}^* B_{kj} - q_k B_{kk} B_{jk}^* = 0\,, \quad k,j = 0,\ldots,M-1\,, \tag{5.37a}$$

$$\left(\sum_{s=0}^{M-1} q_s B_{ss} |\mu_s\rangle\langle\gamma_s|\right) - q_j|\gamma_j\rangle\langle\gamma_j| \geq 0\,, \quad j = 0,\ldots,M-1\,. \tag{5.37b}$$

Proof. Eq. (5.37a) follows from condition (5.9a) of Yuen's theorem, namely $L = \sum_j q_j\rho_j\Pi_j = \sum_j q_j\Pi_j\rho_j = L^\dagger$. In the pure-state discrimination scenario, we have:

$$\begin{aligned} L &= \sum_j q_j\langle\gamma_j|\mu_j\rangle\,|\gamma_j\rangle\langle\mu_j| \\ &= \sum_j q_j B_{jj}^* \left(\sum_k B_{kj}|\mu_k\rangle\right)\langle\mu_j| \\ &= \sum_{jk} q_j B_{jj}^* B_{kj}|\mu_k\rangle\langle\mu_j|\,. \end{aligned} \tag{5.38}$$

Imposing $L = L^\dagger$ leads to:

$$\sum_{jk}\left(q_j B_{jj}^* B_{kj} - q_k B_{kk} B_{jk}^*\right)|\mu_k\rangle\langle\mu_j| = 0\,, \tag{5.39}$$

from which we obtain (5.37a). With analogous argument, we retrieve Eq. (5.37b) from condition (5.9b). □

In principle, one may claim to construct the optimal matrix B by solving the nonlinear system determined by Eq.s (5.37a) together with condition $B^\dagger B = G$, and, then, retrieve the maximum correct decision probability. In particular, the system is composed of $M(M+1)/2$ equations, and its physical solutions will be only those verifying (5.37b). However, it has been showed that this procedure is rather cumbersome, as the search of an exact solution is nontrivial [51]. On the contrary, numerical algorithms based on the SDP approach remain the preferable choice due to their computational efficiency, even in the presence of pure states.

5.3 The geometrically uniform symmetry

Generally speaking, the search for the optimum POVM, both in the presence of mixed- and pure-state discrimination, turns out to be simpler if the constellation $\mathcal{C} = \{\rho_k\}_k$ exhibits some degree of symmetry. In fact, the symmetries of the encoded states may be exploited to further characterize the optimal measurement, thus reducing the complexity of the SDP problem. In particular, the most relevant example is provided by the *geometrically uniform symmetry* (GUS), being also verified in several practical optical communications systems, e.g. phase-shift keying [51, 126, 132, 134, 143, 144].

We start by considering the most general scenario in which ρ_k are mixed states. The constellation $\mathcal{C} = \{\rho_k\}_k$, $k = 0, \dots, M-1$, satisfies the GUS if there exists a unitary *symmetry operator* S, with $S^\dagger S = \hat{\mathbb{1}}$, such that:

$$\rho_k = S^k \, \rho_0 \left(S^\dagger\right)^k \qquad \text{and} \qquad S^M = \hat{\mathbb{1}} \,, \tag{5.40}$$

$\hat{\mathbb{1}}$ being the identity operator over the Hilbert space $\mathcal{H}$. That is, in the presence of GUS, all states $\rho_k \in \mathcal{C}$ can be retrieved from a single "reference" state ρ_0 by sequential application of the symmetry operator S. From now on, for consistency with the symmetry of $\mathcal{C}$, we will assume *equal a priori probabilities*

$$q_k = \frac{1}{M} \,, \quad k = 0, \dots, M-1 \,, \tag{5.41}$$

such that also the weighted operators $\{\widetilde{\rho}_k\}_k$ have the GUS, i.e. $\widetilde{\rho}_k = S^k \, \widetilde{\rho}_0 (S^\dagger)^k$ [51, 126, 132, 134]. Even though this choice may appear more restrictive, it is still of great interest since uniform sampling represents the standard scenario occurring in practical quantum communications formats [19, 20, 51]. In this condition, the GUS can be also embedded into the optimal measurement, according to the following proposition [51, 144].

Proposition 5.2. *If the weighted constellation states $\{\widetilde{\rho}_k\}_k$ verify the GUS for some operator S, then it is not restrictive to assume that also the optimum POVM $\mathbf{\Pi} = \{\Pi_j\}_j$ verifies the GUS for the same symmetry operator, that is:*

$$\Pi_j = S^j \, \Pi_0 \left(S^\dagger\right)^j \,, \quad j = 0, \dots, M-1 \,. \tag{5.42}$$

Proof. Let $\mathbf{\Pi} = \{\Pi_j\}_j$ be an optimum POVM satisfying Theorem 5.1, and maximizing the functional $\mathcal{J}(\mathbf{\Pi})$ defined in (5.2). We note that, in general, this measurement does not satisfy the GUS. To prove the proposition, starting from $\mathbf{\Pi}$, we construct another POVM $\mathbf{\Upsilon} = \{\Upsilon_j\}_j$, that now satisfies the GUS for operator S, and prove it to be optimum too. To this aim, we set:

$$\Upsilon_0 = \frac{1}{M} \sum_{n=0}^{M-1} \left(S^\dagger\right)^n \Pi_n \, S^n \,, \tag{5.43a}$$

$$\Upsilon_j = S^j\,\Upsilon_0\,\left(S^\dagger\right)^j\ ,\ j=1,\ldots,M-1\,, \tag{5.43b}$$

where q_n is the a priori probabilities associated with state ρ_n. The collection $\boldsymbol{\Upsilon}$ is a POVM, as $\Upsilon_j \geq 0$ by construction and

$$\begin{aligned}\sum_j \Upsilon_j &= \frac{1}{M}\sum_{j,n} S^{j-n}\,\Pi_n\big(S^\dagger\big)^{j-n} = \frac{1}{M}\sum_{m,n} S^m\,\Pi_n\big(S^\dagger\big)^m \\ &= \frac{1}{M}\sum_m S^m\left(\sum_n \Pi_n\right)\left(S^\dagger\right)^m = \hat{\mathbb{1}}\,,\end{aligned} \tag{5.44}$$

where we performed the change of variables $m = j-n$ and exploit the periodicity of the symmetry operator S.

Now, we compute:

$$\begin{aligned}\mathcal{J}(\boldsymbol{\Upsilon}) &= \sum_j \mathrm{Tr}[\widetilde{\rho}_j\Upsilon_j] = \sum_j \mathrm{Tr}\left[S^j\widetilde{\rho}_0\Upsilon_0\big(S^\dagger\big)^j\right] \\ &= \sum_j \mathrm{Tr}[\widetilde{\rho}_0\Upsilon_0] = M\,\mathrm{Tr}[\widetilde{\rho}_0\Upsilon_0] \\ &= \sum_n \mathrm{Tr}\left[\widetilde{\rho}_0\left(S^\dagger\right)^n\Pi_n\,S^n\right] = \sum_n \mathrm{Tr}\left[S^n\widetilde{\rho}_0\left(S^\dagger\right)^n\Pi_n\right] = \mathcal{J}(\boldsymbol{\Pi})\,.\end{aligned} \tag{5.45}$$

Thus, the two POVMs $\boldsymbol{\Pi}$ and $\boldsymbol{\Upsilon}$ has the same correct decision probability. We conclude that $\boldsymbol{\Upsilon}$ is an optimum measurement that satisfies the GUS. □

From the previous proof, we note that, in the presence of a POVM $\boldsymbol{\Pi} = \{\Pi_j\}_j$ satisfying the GUS, the calculation of the correct decision probability reduces to:

$$\mathcal{P}_c = M\,\mathrm{Tr}[\widetilde{\rho}_0\Pi_0] = \mathrm{Tr}[\rho_0\Pi_0]\,. \tag{5.46}$$

Furthermore, the SDP problem (5.4) is also simplified as:

$$\max_{\Pi_0\geq 0}\mathrm{Tr}[\rho_0\Pi_0] = \min_{\substack{\Lambda-\widetilde{\rho}_0\geq 0\\ [\Lambda,S]=0}}\mathrm{Tr}[\Lambda]\,, \tag{5.47}$$

where the dual problem is now subject to the two constraints $\Lambda-\widetilde{\rho}_0\geq 0$ and $[\Lambda,S] = \Lambda S - S\Lambda = 0$ [51, 144]. Therefore, in the presence of GUS (and equiprobable symbols), the optimum POVM is completely specified by operators S, ρ_0 and Π_0, inducing a simplification in the numerical SDP algorithms providing solutions to the dual problem [51].

5.3.1 Pure-state discrimination

We now address the pure-state discrimination case, where the presence of GUS provides analytic solution to the decision problem, leading to exact expressions for both the maximum correct decision probability and the optimum POVM [19].

In the presence of a pure-state constellation, specified by the state matrix $\Gamma = \big(|\gamma_k\rangle\big)_k$, $k=0,\ldots,M-1$, and equiprobable symbols $q_k = 1/M$, the GUS is satisfied if there exists a unitary symmetry operator S, $S^\dagger S = \hat{\mathbb{1}}$, such that [19, 51, 126, 132, 134]

$$|\gamma_k\rangle = S^k\,|\gamma_0\rangle \qquad \text{and} \qquad S^M = \hat{\mathbb{1}}\,. \tag{5.48}$$

In this case, the Gram matrix $G = \Gamma^\dagger \Gamma$ is a circulant matrix, having the form [19, 51, 145]

$$G = \begin{pmatrix} G_{00} & G_{M-1\,0} & \dots & G_{10} \\ G_{10} & G_{00} & \dots & G_{20} \\ \vdots & \vdots & \ddots & \vdots \\ G_{M-1\,0} & G_{M-2\,0} & \dots & G_{00} \end{pmatrix} . \tag{5.49}$$

That is, its elements only depend on the difference modulo M between the indices, i.e. $G_{jk} = G_{(j-k) \bmod M,0}$: indeed, $G_{jk} = \langle \gamma_j | \gamma_k \rangle = \langle \gamma_0 | S^{k-j} | \gamma_0 \rangle = \langle \gamma_{(j-k) \bmod M} | \gamma_0 \rangle$.

Furthermore, the following property holds.

Proposition 5.3. *In the presence of GUS, the symmetry operator S commutes with the Gram operator*

$$T \equiv \Gamma \, \Gamma^\dagger = \sum_{k=0}^{M-1} |\gamma_k\rangle\langle\gamma_k| \, , \tag{5.50}$$

that is $[S, T] = ST - TS = 0$.

Proof. By the definition of the Gram operator and the unitarity of S, for which $S^\dagger = S^{-1}$, we have $T = \sum_k S^k |\gamma_0\rangle\langle\gamma_0| S^{-k}$, therefore:

$$\begin{aligned} TS &= \sum_k S^k |\gamma_0\rangle\langle\gamma_0| S^{-k+1} = S \sum_k S^{k-1} |\gamma_0\rangle\langle\gamma_0| S^{-(k-1)} \\ &= S \sum_j S^j |\gamma_0\rangle\langle\gamma_0| S^{-j} = ST \, . \end{aligned} \tag{5.51}$$

□

5.3.1.1 Properties of circulant matrices

As will become clearer, the circulant structure is a fundamental tool to construct the optimal solution to the decision problem. In particular, circulant matrices satisfy the following properties, that will be helpful throughout the text.

- Any circulant matrix $C = (C_{jk})_{jk}$, $j, k = 0, \dots, M-1$, $C_{jk} = C_{(j-k) \bmod M,0}$, is diagonalizable by the unitary matrix $\mathbb{U} = \mathbb{F}^{-1}$, $\mathbb{F} = (F_{jk})_{jk}$ being the discrete Fourier transform matrix, with: [145]

$$F_{jk} = \frac{e^{-i2\pi jk/M}}{\sqrt{M}} \, , \quad j, k = 0, \dots, M-1 \, . \tag{5.52}$$

- The spectral decomposition of C then reads:

$$C = \mathbb{U} \, \Lambda_C \, \mathbb{U}^\dagger \, , \tag{5.53}$$

  where $\Lambda_C = \mathrm{diag}(\lambda_0, \dots, \lambda_{M-1})$, is the diagonal matrix composed of the eigenvalues $\{\lambda_j\}_j$ of C, given by the discrete Fourier transform of the circulant vector $\mathbf{r} = (r_p)_p \equiv (C_{p \bmod M,0})_p$, $p = 0, \dots, M-1$, namely [51, 145]:

$$\lambda_p = \sum_{q=0}^{M-1} \mathbb{U}_{pq} r_q \, . \tag{5.54}$$

- Since all circulant matrices are diagonalized by the same unitary $\mathbb{U}$, we conclude that circulant matrices form a commutative algebra. That is, for any pair of circulant matrices C_1 and C_2, also C_1C_2 and C_2C_1 are circulant, and $[C_1, C_2] = 0$ [145]. In particular, if C is circulant, then $C^\dagger$ is also circulant and $[C, C^\dagger] = 0$.

5.3.1.2 Construction of the optimum POVM for pure-state constellations with GUS

Thanks to the circulant property, we are now able to provide an exact derivation of the optimum POVM in the presence of a pure-state constellation satisfying the GUS for operator S [19]. To our knowledge, this method is original and, remarkably, it provides a simpler strategy to retrieve the optimum receiver than the traditional derivation, based on the symmetry of suboptimal receivers, that will be described in Sec. 5.4.1.

By invoking Proposition 5.2, we assume that also the optimal measurement vectors $\mathbb{M} = \left(|\mu_j\rangle\right)_j$, $j = 0, \ldots, M-1$, exhibit the GUS for the same operator S, thus the optimum POVM $\{\Pi_j\}_j$ is identified by a single "reference" measurement vector:

$$|\mu_0\rangle = \sum_{k=0}^{M-1} a_{k0} \, |\gamma_k\rangle \, , \tag{5.55}$$

$a_{k0} \in \mathbb{C}$, while all the others will be retrieved as $|\mu_j\rangle = S^j|\mu_0\rangle$, $j = 0, \ldots, M-1$. Consequently, the matrix A in (5.27) is a circulant matrix, as $a_{kj} = a_{(k-j) \bmod M, 0}$. Its eigendecomposition is given by

$$A = \mathbb{U} \, \Lambda_A \, \mathbb{U}^\dagger \, , \tag{5.56}$$

where $\Lambda_A = \mathrm{diag}(\lambda_0, \ldots, \lambda_{M-1})$, is the diagonal matrix composed of the eigenvalues $\{\lambda_j\}_j$ of A. Furthermore, $A^\dagger$ is also circulant and commutes with A, thereby, $A^\dagger = \mathbb{U}\Lambda_A{}^\dagger\mathbb{U}^\dagger$ and Eq. (5.28) becomes:

$$\mathbb{U} \, |\Lambda_A|^2 \, \mathbb{U}^\dagger = G^{-1} \, , \tag{5.57}$$

where $|\Lambda_A|^2 = \mathrm{diag}(|\lambda_0|^2, \ldots, |\lambda_{M-1}|^2)$. We conclude that A and G^{-1} are simultaneously diagonalizable and $|\lambda_j|^2 = g_j^{-1}$, $\{g_j\}_j$ being the eigenvalues of the Gram matrix (5.22) listed in increasing order, that is, $g_0 \geq g_1 \geq \ldots \geq g_{M-1}$. In conclusion, the matrix A may be re-expressed in the following form:

$$A \equiv A_{\boldsymbol{\phi}} = \mathbb{U} \, \Lambda_A^{(\boldsymbol{\phi})} \, \mathbb{U}^\dagger \, , \tag{5.58}$$

where:

$$\Lambda_A^{(\boldsymbol{\phi})} = \mathrm{diag}\left(\left\{ \lambda_j^{(\boldsymbol{\phi})} \right\}_{j=0,\ldots,M-1} \right) , \tag{5.59}$$

and

$$\lambda_j^{(\boldsymbol{\phi})} = e^{i\phi_j} g_j^{-1/2} \, , \tag{5.60}$$

in which the relative phases $\boldsymbol{\phi} = (\phi_0, \ldots, \phi_{M-1})$ provide the only free parameters. Furthermore, the matrix $A_{\boldsymbol{\phi}}$ is defined up to an overall phase due to (5.27), therefore we may fix $\phi_0 = 0$, ending up with $M-1$ phases whose value can be arbitrarily chosen. We

conclude that, in the presence of GUS, every pure-state discrimination receiver is ultimately identified by the set of phases $\boldsymbol{\phi}$, which may be properly chosen to maximize the correct decision probability $\mathcal{P}_c$, thus transforming a convex functional optimization task into optimization of a real function with $M-1$ real variables [19].

Thanks to Eq. (5.46), the correct decision probability, when both the state and measurment vectors verify GUS and $q_k = 1/M$, reduces to:

$$\mathcal{P}_c = |\langle \mu_0 | \gamma_0 \rangle|^2 = |B_{00}|^2 \,, \tag{5.61}$$

with the matrix $B = A^\dagger G$ introduced in (5.32). Since both $A^\dagger$ and G are circulant, we conclude that also B is circulant, and equal to:

$$B \equiv B_{\boldsymbol{\phi}} = \mathbb{U}\, \Lambda_B^{(\boldsymbol{\phi})}\, \mathbb{U}^\dagger \,, \tag{5.62}$$

where:

$$\Lambda_B^{(\boldsymbol{\phi})} = \mathrm{diag}\left(\left\{ e^{-i\phi_j} g_j^{1/2} \right\}_{j=0,\ldots,M-1} \right), \tag{5.63}$$

with the quantities introduced in Eq. (5.58). In turn, for every tuple of relative phases $\boldsymbol{\phi} = (\phi_0, \ldots, \phi_{M-1})$, the corresponding correct decision probability becomes:

$$\mathcal{P}_c(\boldsymbol{\phi}) = \left| (B_{\boldsymbol{\phi}})_{00} \right|^2 = \left| \frac{1}{M} \sum_{j=0}^{M-1} \left(e^{-i\phi_j} g_j^{1/2} \right) \right|^2 . \tag{5.64}$$

That is, the correct decision probability is determined by the square modulus of the sum of the M complex numbers $e^{-i\phi_j} g_j^{1/2}$. From geometric considerations, we conclude that its maximum value is achieved when the relative phases ϕ_j are all equal with one another. In turn, the optimum receiver is defined by the choice:

$$\boldsymbol{\phi}_{\mathrm{opt}} = \mathbf{0} = (0, \ldots, 0) \,, \tag{5.65}$$

with the corresponding maximum correct decision probability:

$$\mathcal{P}_c^{(\max)} = \mathcal{P}_c(\boldsymbol{\phi}_{\mathrm{opt}}) = \left| \frac{1}{M} \sum_{j=0}^{M-1} g_j^{1/2} \right|^2 = \left| \left(G^{1/2} \right)_{00} \right|^2 , \tag{5.66}$$

where $G^{1/2}$ is the square root of the Gram matrix. Finally, the optimal matrix A becomes

$$A_{\mathrm{opt}} = G^{-1/2} \,, \tag{5.67}$$

that defines the optimal measurement vectors via $\mathbb{M}_{\mathrm{opt}} = \Gamma\, A_{\mathrm{opt}}$ [19].

In conclusion, the presence of GUS makes the problem of designing the optimum receiver for pure-state discrimination solvable. The optimum POVM, as well as the maximum correct decision probability, is completely characterized by the Gram matrix G, i.e. by the geometry of the constellation. However, from a wider viewpoint, we remark that Eq. (5.58) provides characterization of any M-valued projective measurement to be performed on a pure-state constellation, and its validity goes further beyond the framework of quantum discrimination. As a consequence, the phases $\boldsymbol{\phi}$ can be determined to optimize any desired figure of merit according to the context under investigation, not only the correct decision probability. As will be discussed in Sec. 9.2, this will be the starting point to address the role of the class of M-valued quantum receivers for continuous-variable quantum key distribution.

5.4 The pretty good measurement method

In the previous sections, we described the fundamental results of quantum decision theory, providing characterization of the optimum POVM for M-ary discrimination. The optimum receiver has to satisfy Yuen's theorem, see Theorem 5.1, which, however, does not yield a method to construct the associated POVM. In general, optimization can be carried out numerically by solving the dual problem (5.5), and a closed-form analytic expression for the optimum POVM is known only in few cases, e.g. binary discrimination or M-ary pure-state constellations with equiprobable symbols satisfying the GUS.

In turn, one may claim for simpler methods that, although being suboptimal, reduce the complexity of the problem. That is we look for a suboptimal POVM that does not achieve the maximum correct decision probability anymore, but, in turn, that can be constructed in a simpler way with respect to the optimum receiver satisfying Theorem 5.1. Within suboptimal methods, the most important is represented by the *pretty good measurement* (PGM) method, being also referred to as *square root measurement* (SRM) or *least square measurement* (LSM) method [126–134].

The method was firstly proposed in 1994 by Hausladen *et al.* [127, 128], who considered the problem of distinguishing between an arbitrary set of pure states which, in general, can be linearly dependent. The authors propose a quantum receiver composed of 1-rank operators that performs "pretty good" discrimination, even though not being, in general, optimum. Later on, this measurement has been also called SRM, since the pretty good measurement is obtained by computing the square root of the Gram operator [129–131]. Instead, the LSM method was subsequently developed by Eldar and Forney in 2001 [132, 133], with the goal of designing a 1-rank POVM, projecting on measurement vectors that minimize the sum of the squared norms of the differences between each corresponding state and measurement vector. In particular, Eldar and Forney investigated the connection between their method and the other types of measurements, proving the LSM technique to be equivalent to the SRM. Thereafter, the method has been extended to mixed state discrimination [134].

The PGM is a cornerstone example of suboptimal POVM. In fact, its construction is simple, as it is directly derived from the given collection of states, it is "pretty good" when the states to be distinguished are equiprobable and almost orthogonal, namely it is asymptotically optimal [127, 128, 146]. Remarkably, it becomes optimal in the presence of pure-state constellations satisfying the GUS. For these reasons, in more recent times, it has been systematically applied to the performance evaluation of typical quantum communications systems [147, 148], and also experimentally implemented in the framework of cavity quantum electrodynamics [129, 130].

In the following, we present the detailed derivation of the PGM following the approach of Eldar and Forney, which provides a simple geometric interpretation. We start by reviewing a fundamental theorem of linear algebra, namely the singular value decomposition (SVD) of a matrix [25, 51, 132], which is widely invoked in the construction of the measurement.

Theorem 5.3. [Singular value decomposition (SVD)] *Let Φ be an arbitrary $n \times m$ complex matrix of rank $r \leq \min\{n, m\}$. Then, there exist a unitary $n \times n$ matrix U, a diagonal $n \times m$ matrix Σ, and a unitary $m \times m$ matrix V such that:*

$$\Phi = U \, \Sigma \, V^{\dagger} = \sum_{i=0}^{r-1} \sigma_i \, |u_i\rangle\langle v_i| \, , \tag{5.68}$$

where:

i) Σ *is a diagonal* $n \times m$ *matrix whose first* r *diagonal elements are* $\sigma_i > 0$*, and whose remaining* $m - r$ *diagonal elements are* 0*. The numbers* σ_i*, referred to as the singular values of* Φ*, are equal to* $\sigma_i = \sqrt{\lambda_i}$*, where* $\{\lambda_i\}_j$*,* $i = 0, \ldots, r-1$*, are the eigenvalues of the* r*-rank positive semidefinite matrix* $S = \Phi^\dagger \Phi$*;*

ii) V *is a* $m \times m$ *unitary matrix whose first* r *columns are the orthonormal eigenvectors* $|v_i\rangle$*, spanning a subspace* $\mathcal{V} \subseteq \mathbb{C}^m$*, and whose remaining* $m - r$ *columns span the orthogonal complement* $\mathcal{V}^\perp \subseteq \mathbb{C}^m$*. In particular,* V *diagonalizes matrix* $S = \Phi^\dagger \Phi$*, as* $\Phi^\dagger \Phi = V(\Sigma^\dagger \Sigma)V^\dagger = \sum_{i=0}^{r-1} \sigma_i^2 \, |v_i\rangle\langle v_i| = \sum_{i=0}^{r-1} \lambda_i \, |v_i\rangle\langle v_i|$*;*

iii) U *is a* $n \times n$ *unitary matrix whose first* r *columns are the orthonormal eigenvectors* $|u_i\rangle$*, spanning a subspace* $\mathcal{U} \subseteq \mathbb{C}^n$*, and whose remaining* $n - r$ *columns span the orthogonal complement* $\mathcal{U}^\perp \subseteq \mathbb{C}^n$*. In particular,* U *diagonalizes matrix* $T = \Phi\Phi^\dagger$*, as* $\Phi\Phi^\dagger = U(\Sigma\Sigma^\dagger)U^\dagger = \sum_{i=0}^{r-1} \sigma_i^2 \, |u_i\rangle\langle u_i| = \sum_{i=0}^{r-1} \lambda_i \, |u_i\rangle\langle u_i|$*.*

In particular, we note that the eigenvectors of U and V provide a complete orthonormal system of $\mathbb{C}^n$ and $\mathbb{C}^m$, respectively, and further satisfy:

$$\sum_{i=0}^{r-1} |u_i\rangle\langle u_i| = \mathbb{P}_{\mathcal{U}} \qquad \text{and} \qquad \sum_{i=0}^{r-1} |v_i\rangle\langle v_i| = \mathbb{P}_{\mathcal{V}} \,, \tag{5.69}$$

$\mathbb{P}_{\mathcal{U}}$ and $\mathbb{P}_{\mathcal{V}}$ being the projectors onto subspaces $\mathcal{U}$ and $\mathcal{V}$, respectively.

However, in practical applications, computing the full SVD, including a full unitary decomposition of the null-space of Φ, is rather useless. Instead, if the matrix Φ has no full rank, i.e. $r < \min\{n, m\}$, it suffices to adopt the *reduced SVD*, namely:

$$\Phi = \sum_{i=0}^{r-1} \sigma_i \, |u_i\rangle\langle v_i| = U_r \, \Sigma_r \, V_r^\dagger \,, \tag{5.70}$$

where the matrices U_r and V_r only contain the first r eigenvectors of U and V, respectively, and Σ_r is a $r \times r$ diagonal matrix that only contains the nonzero singular values $\sigma_i > 0$. In turn, U_r and V_r become $n \times r$ and $r \times m$ matrices, respectively [25, 51].

Given these results, we are now ready to introduce the PGM method. Following Eldar and Forney's approach, we present the theory for pure-state discrimination and equiprobable symbols, as in the original proposal [132, 133]. The extension to mixed states will be briefly mentioned therafter.

5.4.1 Derivation of the pretty good measurement

To begin with, we consider the problem of M-ary pure state discrimination of the constellation $\mathcal{C} = \{|\gamma_k\rangle\langle\gamma_k|\}_k$, $k = 0, \ldots, M-1$, described by the state matrix:

$$\Gamma = \Big(|\gamma_0\rangle, \ldots, |\gamma_{M-1}\rangle \Big) \,, \tag{5.71}$$

see Sec. 5.2.1. Even though in practical scenarios the constellation states are linearly independent, here we assume the possible presence of linearly dependent vectors, and let Γ have rank $r \leq M$, such that the subspace $\mathcal{S} = \mathrm{span}\{|\gamma_k\rangle : k = 0, \ldots, M-1\}$ has dimension $r \leq M$. Furthermore, we assume equiprobable symbols, namely equal a priori probabilities:

$$q_k = \frac{1}{M} \,, \quad k = 0, \ldots, M-1 \,. \tag{5.72}$$

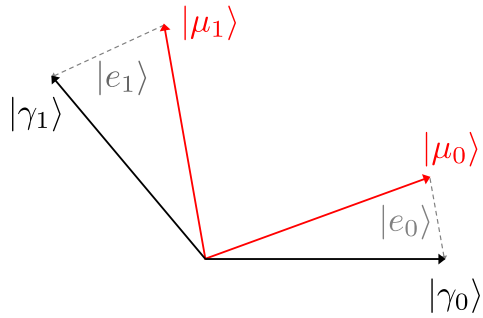


Figure 5.4.1: Two-dimensional example of the PGM method. Given the constellation states $\{|\gamma_k\rangle\}_k$, we seek for a 1-rank POVM $\{\Pi_j\}_j$, with $\Pi_j = |\mu_j\rangle\langle\mu_j|$, such that the error vectors $|e_j\rangle = |\gamma_j\rangle - |\mu_j\rangle$ minimize the squared error E in Eq. (5.75), subject to the normalization constraint $\sum_j |\mu_j\rangle\langle\mu_j| = \mathbb{P}_{\mathcal{S}}$.

The method can be extended to non-uniform generation by substituting the constellation states with the weighted states $\sqrt{q_k}|\gamma_k\rangle$ [132]. The goal of the PGM scheme is to define a suitable M-valued 1-rank POVM $\{\Pi_j\}_j$, $j = 0, \ldots, M-1$, with $\Pi_j = |\mu_j\rangle\langle\mu_j|$, associated with the measurement matrix:

$$\mathbb{M} = \Big(|\mu_0\rangle, \ldots, |\mu_{M-1}\rangle \Big) . \tag{5.73}$$

We may safely assume the measurement vectors to be $|\mu_j\rangle \in \mathcal{S}$, thus we have $\mathbb{M} = \Gamma\, A$ for some $M \times M$ matrix A, see Sec. 5.2.1, and:

$$\mathbb{M}\mathbb{M}^\dagger = \sum_j |\mu_j\rangle\langle\mu_j| = \mathbb{P}_{\mathcal{S}} . \tag{5.74}$$

Instead, in general, we do not require the vectors $\{|\mu_j\rangle\}_j$ to be orthogonal or normalized [19, 51, 132, 133].

To construct such a measurement, we seek for measurement vectors $\{|\mu_j\rangle\}_j$ "close" to the states $\{|\gamma_k\rangle\}_k$, i.e. making the difference vectors $|e_j\rangle = |\gamma_j\rangle - |\mu_j\rangle$ as "small" as possible, as schematized in Fig. 5.4.1. More precisely, we look for a measurement vector set $\{|\mu_j\rangle\}_j$ that minimize the squared error:

$$E = \sum_{j=1}^{M} \langle e_j | e_j \rangle = \sum_{j=1}^{M} \Big(\langle \gamma_j | - \langle \mu_j | \Big) \Big(|\gamma_j\rangle - |\mu_j\rangle \Big) , \tag{5.75}$$

subject to the normalization constraint (5.74) [51, 132, 133]. We note that, if the state vectors were orthonormal, the minimum of E, compatible with (5.74), would be trivially reached by the choice $|\mu_j\rangle = |\gamma_j\rangle$ for all j, with $E_{\min} = 0$. On the contrary, the problem is nontrivial in the presence of non-orthogonal states. To determine the solution, we first re-express Eq. (5.75) in terms of the state and measurement matrices as:

$$E = \mathrm{Tr}\Big[(\Gamma - \mathbb{M})^\dagger (\Gamma - \mathbb{M}) \Big] = \mathrm{Tr}\Big[(\Gamma - \mathbb{M}) (\Gamma - \mathbb{M})^\dagger \Big] . \tag{5.76}$$

We now employ the reduced SVD of the state matrix Γ, i.e. $\Gamma = U_r\,\Sigma_r\,V_r^\dagger$. Since the columns of Γ are composed by states $|\gamma_k\rangle \in \mathcal{S}$, we conclude that Γ is a square $M \times M$ matrix with rank $r \leq M$. In turn, U_r is a $M \times r$ unitary matrix that diagonalizes the Gram operator $T = \Gamma\,\Gamma^\dagger = \sum_k |\gamma_k\rangle\langle\gamma_k|$, whose eigenvectors provide a complete orthonormal system of the subspace $\mathcal{S}$, i.e. $\sum_{i=0}^{r-1} |u_i\rangle\langle u_i| = \mathbb{P}_{\mathcal{S}}$. Given this considerations, we perform the trace in (5.76) over the U_r-eigenbasis, obtaining:

$$E = \sum_{i=0}^{r-1} \langle u_i|\,(\Gamma - \mathbb{M})\,(\Gamma - \mathbb{M})^\dagger\,|u_i\rangle = \sum_{i=0}^{r-1} \langle d_i|d_i\rangle\,, \tag{5.77}$$

where

$$|d_i\rangle = (\Gamma - \mathbb{M})^\dagger\,|u_i\rangle = \Gamma^\dagger|u_i\rangle - |a_i\rangle\,, \quad i = 0, \ldots, r-1\,, \tag{5.78}$$

with $|a_i\rangle = \mathbb{M}^\dagger|u_i\rangle$. Thanks to the reduced SVD of $\Gamma^\dagger$, i.e. $\Gamma_r^\dagger = V_r\,\Sigma_r\,U_r^\dagger = \sum_{i=0}^{r-1} \sigma_i|v_i\rangle\langle u_i|$, we have $\Gamma^\dagger|u_i\rangle = \sigma_i|v_i\rangle$ for $i = 0 \ldots, r-1$. Moreover, vectors $\{|a_i\rangle\}_i$, $i = 0, \ldots, r-1$, provide an orthonormal set of $\mathcal{S}$. In fact, we have $\langle a_i|a_j\rangle = \langle u_i|\mathbb{M}\mathbb{M}^\dagger|u_j\rangle = \langle u_i|\mathbb{P}_{\mathcal{S}}|u_j\rangle = \delta_{ij}$.

Then, the problem of designing a POVM minimizing (5.75) reduces to finding a set of r orthonormal vectors $\{|a_i\rangle\}_i$ that minimizes

$$E = \sum_{i=0}^{r-1} \langle d_j|d_j\rangle = \sum_{i=0}^{r-1} \left[\left(1 + \sigma_i^2\right) - 2\sigma_i \mathrm{Re}\left(\langle a_i|v_i\rangle\right)\right]\,. \tag{5.79}$$

The minimum is achieved when $\mathrm{Re}(\langle a_i|v_i\rangle)$ gets its largest value for all $i = 0, \ldots, r-1$. Since also vectors $\{|v_i\rangle\}_i$ are orthonormal, we conclude that the minimizing vectors should be $|a_i\rangle = |v_i\rangle$, $i = 0, \ldots, r-1$ [51, 132, 134].

In turn, the PGM is defined by the relation $\mathbb{M}_{\mathrm{PGM}}|u_i\rangle = |v_i\rangle$ or, equivalently:

$$\mathbb{M}_{\mathrm{PGM}} = U_r V_r^\dagger = \sum_{i=0}^{r-1} |u_i\rangle\langle v_i|\,, \tag{5.80}$$

associated with the minimum square error $E_{\min} = \sum_{i=0}^{r-1}(1-\sigma_i)^2$. Thanks to the reduced SVD of Γ, Eq. (5.80) can be expressed in equivalent way as a function of both the Gram matrix $G = \Gamma^\dagger\,\Gamma$ and the Gram operator $T = \Gamma\,\Gamma^\dagger$ as:

$$\mathbb{M}_{\mathrm{PGM}} = U_r V_r^\dagger = T^{-1/2}\Gamma = \Gamma\,G^{-1/2}\,, \tag{5.81}$$

where $T^{-1/2}$ and $G^{-1/2}$ should be intended as square-root Moore-Penrose pseudo-inverses of T and G, respectively, when matrix Γ is not full-rank, i.e. $r < M$. In particular, from Eq. (5.81) we obtain the PGM measurement vectors as:

$$|\mu_j\rangle_{\mathrm{PGM}} = T^{-1/2}|\gamma_j\rangle\,, \quad j = 0, \ldots, M-1\,, \tag{5.82}$$

and $\Pi_j^{(\mathrm{PGM})} = T^{-1/2}|\gamma_j\rangle\langle\gamma_j|T^{-1/2}$. Equivalently, given the relation $\mathbb{M} = \Gamma\,A$ derived in Sec. 5.2.1, the coefficient matrix A for the PGM reads:

$$A_{\mathrm{PGM}} = G^{-1/2}\,. \tag{5.83}$$

We also note, that the PGM measurement vectors are orthogonal only in the presence of linearly independent constellation states, when matrix Γ has full rank $r = M$. Indeed, in that case we have

$$\mathbb{M}_{\mathrm{PGM}}^{\dagger}\,\mathbb{M}_{\mathrm{PGM}} = \Big({}_{\mathrm{PGM}}\langle\mu_j|\mu_k\rangle_{\mathrm{PGM}}\Big)_{jk} = G^{-1/2}\,G\,G^{-1/2} = \mathbb{1}_M\,. \tag{5.84}$$

On the contrary, if $r < M$, we should consider Moore-Pensore pseudo-inverses and the previous argument does not hold anymore. Then, the M measurement vectors cannot be mutually orthonormal since they span the r- dimensional subspace $\mathcal{S}$.

Finally, we now evaluate the correct decision probability associated with the PGM with the methods of Sec. 5.2.2. We obtain the matrix $B = \mathbb{M}^{\dagger}\,\Gamma = A^{\dagger}\,G$ as:

$$B_{\mathrm{PGM}} = G^{1/2}\,, \tag{5.85}$$

such that the probability of obtaining outcome j when state $|\gamma_k\rangle$ was sent reads $p_{\mathrm{PGM}}(j|k) = |{}_{\mathrm{PGM}}\langle\mu_j|\gamma_k\rangle|^2 = |B_{kj}|^2 = |(G^{1/2})_{kj}|^2$. The correct decision probability then becomes:

$$\mathcal{P}_c^{(\mathrm{PGM})} = \frac{1}{M}\sum_{k=0}^{M-1}\left|\left(G^{1/2}\right)_{kk}\right|^2\,, \tag{5.86}$$

where we recall that we considered equiprobable symbols.

5.4.1.1 On the optimality of the PGM

Generally speaking, the PGM provides a suboptimal POVM for the decision problem, leading to a lower bound of the maximum achievable correct decision probability. This raises the problem to understand how "close" it is with the respect to the optimum receiver. As a first fundamental result, the PGM is asymptotically optimal, namely it becomes optimal when the Gram matrix tends to the identity $G \to \mathbb{1}_M$. As firstly, proved by Holevo in 1979 with independent methods, the minimum error probability $P_{\min} = 1 - \mathcal{P}_c^{(\max)}$ is related to the PGM error probability $P_{\mathrm{PGM}} = 1 - \mathcal{P}_c^{(\mathrm{PGM})}$ by: [146]

$$P_{\min} \le P_{\mathrm{PGM}} \le \frac{2}{M}\,\mathrm{Tr}\left[\mathbb{1}_M - G^{1/2}\right]\,, \tag{5.87}$$

thus in the limit $G \to \mathbb{1}_M$ we have $P_{\mathrm{PGM}} \approx P_{\min}$.

More importantly, Eldar and Forney proved that the PGM becomes optimal when the constellation states satisfy the GUS with equiprobable symbols [51, 132]. Indeed, we note that the PGM matrix $A_{\mathrm{PGM}} = G^{-1/2}$ coincides with the optimum one derived in Sec. **??** for pure-state constellations with GUS. Equivalently, we prove that matrix $B_{\mathrm{PGM}} = G^{1/2}$ satisfies the necessary and sufficient conditions for optimality outlined in Corollary 5.2. That is, we have to prove that $B_{\mathrm{PGM}} = (B_{kj})_k j$ verifies:

$$B_{jj}^{*}B_{kj} - B_{kk}B_{jk}^{*} = 0\,, \quad k,j = 0,\ldots,M-1\,, \tag{5.88a}$$

$$\left(\sum_{s=0}^{M-1} B_{ss}|\mu_s\rangle_{\mathrm{PGM}}\langle\gamma_s|\right) - |\gamma_j\rangle\langle\gamma_j| \ge 0\,, \quad j = 0,\ldots,M-1\,, \tag{5.88b}$$

where we considered equiprobable symbols, i.e. $q_k = 1/M$. We remark that, in the presence of GUS, G is circulant, thus $B_{\mathrm{PGM}} = G^{1/2}$ is also circulant and its element only

depends on the difference between indices, i.e. $B_{jk} = \langle \mu_j | \gamma_k \rangle = w(k-j)$, where w is a complex-valued function satisfying $w^*(j) = w(-j)$. Then, we have:

$$B^*_{jj} B_{kj} - B_{kk} B^*_{jk} = w(0)^* w(j-k) - w(0) w(k-j)^* = 0\,, \tag{5.89}$$

and condition (5.89) is satisfied. To prove (5.88b), we consider the operator:

$$L = \sum_s B_{ss} |\mu_s\rangle_{\rm PGM} \langle \gamma_s| = w(0) \sum_s |\mu_s\rangle_{\rm PGM} \langle \gamma_s|\,. \tag{5.90}$$

We now construct the reduced SVD of Γ in the presence of GUS. First of all, we note that, in the presence of GUS, Γ is full-rank and the Gram matrix G is diagonalized by the unitary $\mathbb{F}^{-1}$, $\mathbb{F}$ being the discrete Fourier transform matrix, see Sec. 5.3.1.1. Therefore, the right unitary V_r in the SVD corresponds to $\mathbb{F}^{-1}$, its column vectors being equal to $|F_i\rangle = (e^{2\pi i j k} M/\sqrt{M})_j$, $i,j = 0,\ldots,M-1$. Furthermore, the matrix of the singular values $\Sigma = \mathrm{diag}(\{\sigma_j\}_j)$ has nonzero diagonal values, and rank equal to M. Then, it is easy to check that the choice $\mathbb{Y} = \Gamma(\mathbb{F}^{-1})\Sigma^{-1}$ yield the left unitary matrix U_r of the SVD. In turn, we have:

$$\Gamma = \mathbb{Y}\,\Sigma\,\left(\mathbb{F}^{-1}\right)^\dagger = \sum_{i=0}^{M-1} \sigma_i\, |u_i\rangle \langle F_i|\,, \tag{5.91}$$

where the eigenvectors of $\mathbb{Y}$ are equal to $|u_i\rangle = \Gamma\,|F_i\rangle/\sigma_i$, $i = 0,\ldots,M-1$. The PGM is obtained as:

$$\mathbb{M}_{\rm PGM} = \mathbb{Y}\,\left(\mathbb{F}^{-1}\right)^\dagger = \sum_{i=0}^{M-1} |u_i\rangle \langle F_i|\,. \tag{5.92}$$

As a consequence, the following relations hold: Then,

$$|\gamma_s\rangle = \mathbb{Y}\Sigma |F_s\rangle \quad \text{and} \quad |\mu_s\rangle_{\rm PGM} = \mathbb{Y}|F_s\rangle\,, \tag{5.93}$$

and Eq. (5.88b) reduces to:

$$\mathbb{Y}\Big(w(0)\Sigma - \Sigma|F_j\rangle\langle F_j|\Sigma\Big)\mathbb{Y}^\dagger \geq 0\,, \quad j = 0,\ldots,M-1\,. \tag{5.94}$$

It is, therefore, sufficient to show that operator $T_j = w(0)\Sigma - \Sigma|F_j\rangle\langle F_j|\Sigma$ is positive semidefinite for all j. To this aim, we recall that $w(0) = {}_{\rm PGM}\langle \mu_j | \gamma_j \rangle = \langle F_j|\Sigma|F_j\rangle$ and we invoke the Cauchy-Schwartz inequality [25]. Thereby, for any $|h\rangle \in \mathcal{S}$, we have:

$$\begin{aligned}
\langle h|T_j|h\rangle &= \langle F_j|\Sigma|F_j\rangle\langle h|\Sigma|h\rangle - |\langle h|\Sigma|F_j\rangle|^2 \\
&\geq \langle F_j|\Sigma|F_j\rangle\langle h|\Sigma|h\rangle - \langle h|\Sigma|h\rangle\langle F_j|\Sigma|F_j\rangle \\
&= 0\,.
\end{aligned} \tag{5.95}$$

Thus, also condition (5.88b) is verified, proving the PGM as the optimum receiver in the presence of GUS.

5.4.2 Extension to mixed states

The PGM has been originally formulated for pure-state discrimination, in which case the construction of the POVM follows the geometric intuition depicted in Fig. 5.4.1. However, in 2004 Eldar and Forney derived an extension of the method for mixed-state discrimination of constellations $\mathcal{C} = \{\rho_k\}_k$, $k = 0, \ldots, M-1$. [51, 134]. The principle behind the generalization is the so-called *factor decomposition* of the density operators ρ_k [51].

The factor decomposition of a general positive semidefinite matrix ρ is equal to:

$$\rho = \gamma\gamma^\dagger \,, \tag{5.96}$$

achieved for some matrix γ, which does not need to be diagonal. The existence of a factor follows from the positivity of ρ. In particular, given the spectral decomposition of ρ, i.e. $\rho = \sum_{j=0}^{r-1} \rho_j |\phi_j\rangle\langle\phi_j| = \Phi D \Phi^\dagger$, with $\rho_j \geq 0$, $r = \mathrm{rank}(\rho)$, $D = \mathrm{diag}(\{\rho_j\}_j)$ and $\Phi = (|\phi_0\rangle, \ldots, |\phi_{r-1}\rangle)$, we immediately derive $\gamma = \Phi\sqrt{D}$ as a factor of ρ [51].

Once obtained the factors γ_k for each state ρ_k, we define the state matrix Γ as:

$$\Gamma = \Big(\gamma_0, \ldots, \gamma_{M-1}\Big) \,, \tag{5.97}$$

where the number of columns is now equal to $H \geq M$, with the associated Gram matrix and operator:

$$G = \Gamma^\dagger\Gamma = \Big(\gamma_j^\dagger \gamma_k\Big)_{jk} \quad \text{and} \quad T = \Gamma\,\Gamma^\dagger = \sum_{j=0}^{M-1} \gamma_j \gamma_j^\dagger \,, \tag{5.98}$$

where $G_{jk} = \gamma_j^\dagger \gamma_k$ now is the (j,k)-block of matrix G, $j,k = 0, \ldots, M-1$.

We now look for a POVM $\{\Pi_j\}_j$ in the form $\Pi_j = \mu_j \mu_j^\dagger$, where now the $\{\mu_j\}_j$ represent the measurement factors. Then, the construction in Sec. 5.4.1 still holds and the PGM is defined, accordingly, by:

$$\mathbb{M}_{\mathrm{PGM}} = (\mu_0, \ldots, \mu_{M-1}) = T^{-1/2}\,\Gamma = G^{-1/2}\,\Gamma \,. \tag{5.99}$$

We have $B_{\mathrm{PGM}} = \mathbb{M}_{\mathrm{PGM}}^\dagger \Gamma = G^{1/2}$, with the corresponding correct decision probability:

$$\mathcal{P}_c^{(\mathrm{PGM})} = \frac{1}{M} \sum_{k=0}^{M-1} \mathrm{Tr}\left[\left(G_{kk}^{1/2}\right)^\dagger G_{kk}^{1/2}\right] \,, \tag{5.100}$$

$G_{kk}^{1/2}$ being the (k,k)-block of $G^{1/2}$.

As regards the optimality, we underline that, differently from the case of pure states, in the presence of mixed-state constellation with GUS, the PGM, in general, is not optimal anymore. To achieve optimality, a further condition is required, namely:

$$(B_{\mathrm{PGM}})_{00} = G_{00}^{1/2} = \alpha\, \mathbb{1}_H \,, \tag{5.101}$$

where α is an arbitrary proportionality constant and $\mathbb{1}_H$ is the $H \times H$ identity matrix [134]. Satisfying condition (5.101) is nontrivial. As an example, in the commonly exploited quantum communication systems, based on phase-shift keying and pulse-position modulation, Eq. (5.101) is not verified, thus the PGM is not optimum even in the presence of GUS [51].

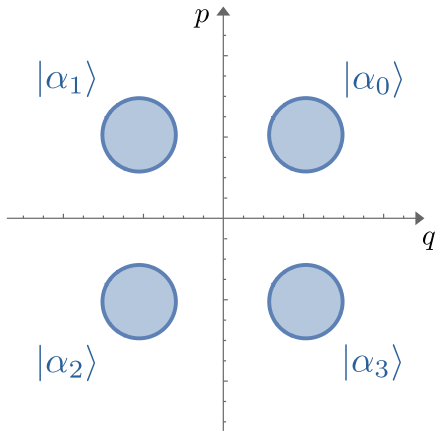


Figure 5.5.1: Phase space representation of the QPSK encoding, where information is encoded in the coherent states $|\alpha_k\rangle = |\alpha\, e^{\pi(2k+1)/M}\rangle$, $k = 0, \ldots, M-1$ and $M = 4$. The constellation satisfies the GUS for the symmetry operator $S_\theta = \exp(-i\theta a^\dagger a)$, $\theta = 2\pi/M$, namely the phase-shift operator.

5.5 Quantum receivers for quadrature phase-shift keying discrimination

As in the previous Chapter, we now consider the application of the quantum decision theory developed in the former section to a realistic quantum communication scenario, involving M-ary coherent state encoding, see Chapter 3. Differently from Sec. 4.3, in the presence of multilevel communication systems, there exist different formats for coherent state modulation, e.g. phase-shift keying, quadrature amplitude modulation, amplitude phase-shift keying, whose corresponding constellations exhibit different kinds of symmetry. Here, we focus our attention on a paradigmatic example, namely phase-shift keying (PSK), that provides the simplest scheme for practical implementation, as it only requires phase modulation of a carrier laser beam with given intensity [51]. In more detail, a PSK(M) constellation is composed of the M coherent states:

$$|\alpha_k\rangle = |\alpha\, e^{i\pi(2k+1)/M}\rangle\,, \qquad k = 0, \ldots, M-1\,, \tag{5.102}$$

where $\alpha \geq 0$, generated with equal a priori probabilities $q_k = 1/M$. That is, the constellation is composed of M coherent states with the same energy α^2 and phase-shifted by $\theta = 2\pi/M$; therefore, it satisfies the GUS for the phase-shift symmetry operator $S_\theta = \exp(-i\theta\hat{n})$, $\hat{n}$ being the photon-number quantum operator [19, 51]. In the following, we focus on the special case $M = 4$, reported in Fig. 5.5.1, also referred to as *quadrature phase-shift keying* (QPSK). The QPSK constellation is a cornerstone example in M-ary quantum communications, being investigated in several frameworks, ranging from quantum decision theory [51, 92, 109, 113, 149–155], information transmission over a quantum channel [156–161], and continuous variable quantum key distribution [19, 162–169].

The QPSK scheme satisfies the GUS, therefore the PGM provides the optimal solution to the decision problem. That is, the optimum receiver, leading to the maximum correct decision probability, is obtained by the 1-rank projective POVM $\{\Pi_j\}_j$, $\Pi_j = |\mu_j\rangle\langle\mu_j|$,

$j = 0, \ldots, M-1$, satisfying $\mathbb{M} = \Gamma\, A$ with the optimal coefficient matrix $A = G^{-1/2}$, see Sec. **??**, where the Gram matrix $G = (G_{jk})_{jk}$, $j, k = 0, \ldots, 3$, is defined as:

$$G_{jk} = \langle \alpha_j | \alpha_k \rangle = \exp\left\{-\alpha^2 \left[1 - \cos\left(\frac{\pi(k-j)}{2}\right)\right]\right\} \times \exp\left\{-i\,\alpha^2 \sin\left(\frac{\pi(k-j)}{2}\right)\right\}. \tag{5.103}$$

Thereafter, we obtain the minimum error probability allowed by quantum mechanics as:

$$P_{\min} = 1 - \left|\left(G^{1/2}\right)_{00}\right|^2 = 1 - \frac{1}{16}\left(\sum_{j=0}^{3} g_j^{1/2}\right)^2, \tag{5.104}$$

where $\{g_j\}_j$ are the eigenvalues of the Gram matrix. Since G is circulant, it is diagonalized by the inverse discrete Fourier transform matrix $\mathbb{F}^{-1}$ in Eq. 5.52, therefore $g_j = (\mathbb{F}\, G\, \mathbb{F}^{-1})_{jj}$. Straightforward calculation leads to:

$$\begin{aligned} g_0 &= 2e^{-\alpha^2}(\cosh\alpha^2 + \cos\alpha^2)\,, \\ g_1 &= 2e^{-\alpha^2}(\sinh\alpha^2 + \sin\alpha^2)\,, \\ g_2 &= 2e^{-\alpha^2}(\cosh\alpha^2 - \cos\alpha^2)\,, \\ g_3 &= 2e^{-\alpha^2}(\sinh\alpha^2 - \sin\alpha^2)\,. \end{aligned} \tag{5.105}$$

In literature, the error probability (5.104) is sometimes referred to as the *QPSK Helstrom bound* (with partial abuse of language), since derivation of the optimum QPSK receiver was also carried out by Helstrom in [9]. We also note that the optimum POVM, equal to the PGM, corresponds to projection over a suitable linear superpositions of the constellation states $\{|\alpha_k\rangle\}_k$, i.e. $|\mu_j\rangle = \sum_k (G^{-1/2})_{kj} |\alpha_k\rangle$, as for binary coherent state discrimination. However, differently from the binary case where the PGM is implemented via the Dolinar receiver [94, 95], in the presence of QSPK designing a feasible optimum receiver is an open problem, and, from a practical point of view, there is no clear idea on its experimental implementation [19].

On the other hand, the standard quantum limit (SQL), namely the error probability associated with conventional QPSK receivers, is achieved by double homodyne detection. That is, we perform joint measurement of quadratures q and p on the incoming signal, retrieving a pair of real outcomes $\mathbf{x} = (x, y) \in \mathbb{R}^2$, and adopt the following decision rule: if both $x, y \geq 0$ we infer state "0", if $x < 0$ and $y \geq 0$ we infer "1", if both $x, y < 0$ we infer "2" and, finally, if $x \geq 0$ and $y < 0$, we infer "3". The double homodyne probability distribution of state $|\alpha_k\rangle$ reads:

$$p_{\mathrm{DH}}(\mathbf{x}|k) = \frac{1}{4\pi} \exp\left\{-\frac{[x - 2\,\mathrm{Re}(\alpha_k)]^2 + [y - 2\,\mathrm{Im}(\alpha_k)]^2}{4}\right\}, \tag{5.106}$$

expressed in shot-noise units, such that the probability $p_{\mathrm{DH}}(j|k)$ of performing the decision j when state k is sent is equal to $p_{\mathrm{DH}}(j|k) = \int_{Q_j} d\mathbf{x}\, p_{\mathrm{DH}}(\mathbf{x}|k)$, where Q_j is the $(j+1)$-th quadrant of the (x, y) plane, corresponding to the confidence region derived

from the previous decision rule. In particular, for all $k = 0, \ldots, 3$, we have:

$$p_{\rm DH}(k|k) = p_{\rm DH}(0|0) = \int_0^\infty dx \int_0^\infty dy\, p_{\rm DH}(\mathbf{x}|k) = \left[\frac{1 + \mathrm{erf}\left(\alpha/\sqrt{2}\right)}{2}\right]^2 , \tag{5.107}$$

and, accordingly, we retrieve the SQL as:

$$P_{\rm SQL} = 1 - \frac{1}{4}\sum_{k=0}^{3} p_{\rm DH}(k|k) = 1 - \frac{1}{4}\left[1 + \mathrm{erf}\left(\frac{\alpha}{\sqrt{2}}\right)\right]^2 , \tag{5.108}$$

such that $P_{\rm SQL} > P_{\rm min}$. In particular, in the high-energy limit $\alpha^2 \gg 1$, we have $P_{\rm SQL} \approx \sqrt{2/(\pi\alpha^2)}e^{-\alpha^2/2}$ and $P_{\rm min} \approx e^{-2\alpha^2}/2$: thereby, the two error probabilities show different dependence on the input energy, and the ratio $P_{\rm SQL}/P_{\rm min} \to \infty$ when $\alpha^2 \to \infty$.

As a consequence, we claim to design quantum receivers that beat the SQL and provide a genuine quantum advantage, even though they are not able to reach the minimum error probability. Following the philosophy adopted for BPSK discrimination, the first idea in this direction is to provide suitable generalization of the Dolinar receiver, and investigate its optimality. This approach has been carried out by Bondurant in 1993, who designed a QPSK feedback receiver based on conditional nulling displacements [150]. Unfortunately, the Bondurant receiver is not optimum, and, to date, it is not known whether or not the PGM can be implemented by optical feedback and linear optics. Nevertheless, the Bondurant receiver outperforms the SQL in the high-energy limit, thus providing anyway a cornerstone example in the field of M-ary quantum communication systems. Its functioning is explained in detail here below.

5.5.1 The Bondurant receiver

Starting from the Dolinar receiver, that provides optimal binary discrimination by conditional time-dependent displacements and feedback control, see Sec. 4.3.2, it is possible to design feedback receivers for M-ary discrimination by suitable extension of the scheme in Fig. 4.3.5 [170]. The first attempt in this direction has been made in 1993 by Bondurant, who proposed a feedback receiver for QPSK discrimination [150]. In particular, he designed two kinds of receivers, referred to as *type I* and *type II Bondurant receiver*, respectively, and obtain a near-optimum performance, beating the SQL in the high-energy regime.

As in Sec. 4.3.2, since we deal with coherent states, the analysis can be conducted by considering the time-dependent wavepackets $\psi_k(t)$, associated with the encoded states $|\alpha_k\rangle$, $k = 0, \ldots, 3$, equal to:

$$\psi_k(t) = e^{i\pi(2k+1)/4}\,\psi\, e^{-i\omega t}\,, \qquad 0 < t \leq T\,, \tag{5.109}$$

with $\psi > 0$, and ω and T being the carrier signal frequency and the time slot duration, respectively. Accordingly, the mean energy of each pulse reads $\bar{n}_k = \psi^2 T = \alpha^2$.

Similarly to the Dolinar scheme, the Bondurant receiver implements a feedback loop, applying a time-dependent "nulling" displacement $D(-\psi_j(t))$ to the incoming signal $\psi_k(t)$, $j, k = 0, \ldots, 3$, where the nulled symbol j is decided according to the outcome of a photodetector, performing continuous-time measurement The receiver is realized by a photon counter performing on-off detection connected to a switch s, that, now, can assume the four positions, namely $s = 0, \ldots, 3$, as depicted in Fig. 5.5.2. The position $s(t)$ at time $t \leq T$ determines the amplitude of a nulling displacement operation $D(-\psi_j(t))$,

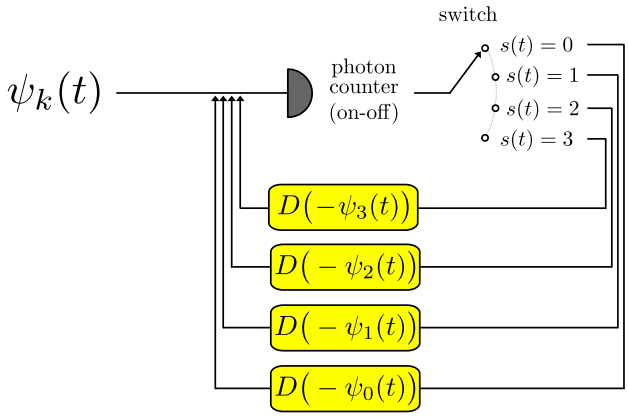


Figure 5.5.2: Setup of the Bondurant receiver. The field $\psi_k(t)$ undergoes a nulling displacement operation $D(-\psi_j(t))$, $j,k=0,\ldots,3$, the value of j being determined by the position of a switch $s(t)$, with initial condition is $s(0)=0$. In the type I receiver, $s(t)$ increases in sequential fashion at every count of the photodetector, whereas in the type II receiver $s(t)$ is suitably determined from the the time arrival distribution of the clicks. After time T, the value $s(T)$ gives the final decision.

with $j=s(t)$, to be performed on the field $\psi_k(t)$. To determine the value of $s(t)$ at each time, different switching rules are considered for the type I and type II scheme.

In particular, the type I Bondurant receiver tries to null out the incoming field *in sequential order*. The initial position of the switch is set to $s(0)=0$, and the signal at time $t=0$ is displaced by $D(-\psi_0(0))$. Then, at every click of the detector, the switch increases its position by 1, proceeding in sequential fashion, namely $0\to 1\to 2\to 3$. As an example, if the detector register clicks at times t_1, t_2 and t_3, the displacement is changed to $D(-\psi_1(t))$ for $t_1<t\leq t_2$, $D(-\psi_2(t))$ for $t_2<t\leq t_3$ and $D(-\psi_3(t))$ for $t_3<t\leq T$. After the whole signal is processed, the switch position $s(T)$ infers the probed state to be $|\alpha_{s(T)}\rangle$.

The calculation of the error probability follows from the properties of Poisson stochastic processes [96]. In particular, if state k is probed and symbol j is nulled, the displaced field $D(-\psi_j(t))\psi_k(t)=\psi_k(t)-\psi_j(t)$, is associated with Poisson photon counting statistics, and the outcome of the photon counter is described as a stationary Poisson stochastic process with rate:

$$\lambda_{jk}=|\psi_k(t)-\psi_j(t)|^2=2\psi^2\left\{1-\cos\left[\frac{\pi(j-k)}{2}\right]\right\}, \tag{5.110}$$

such that the probability of registering a click in a time bin of duration $\delta t\ll T$ is equal to $\lambda_{jk}\delta t$ [96]. In turn, the probability $\pi_{jk}^{(0)}(t_1,t_2)$ that the detector does not click in the time interval $(t_1,t_2]$ reads:

$$\pi_{jk}^{(0)}(t_1,t_2)=\lim_{\delta t\to 0}\left(1-\lambda_{jk}\delta t\right)^{\frac{t_2-t_1}{\delta t}}=e^{-\lambda_{jk}(t_2-t_1)}. \tag{5.111}$$

Given this results, the receiver performs a decision error when not enough photocounts are registered, i.e. when the detector at time T experiences $n_c<k$ clicks if state k is probed, with the consequence that the "nulling" displacement $D(-\psi_k(t))$ is not imple-

mented at all. Accordingly, the error probability $P_{\mathrm{Bon}}^{(\mathrm{I})}(k)$ given state k is equal to

$$P_{\mathrm{Bon}}^{(\mathrm{I})}(k) = \sum_{n_{\mathrm{c}}=0}^{k-1} p(n_{\mathrm{c}}|k)\,, \tag{5.112}$$

where $p(n_{\mathrm{c}}|k)$ is the probability of retrieving n_{c} clicks if state k was sent. If $k = 0$ no errors are made, since state "0" is always nulled thanks to the initial condition $s(0) = 0$. On the contrary, if $k = 1$ an error occurs if no clicks are registered over the whole interval $(0, T]$, as in this case the receiver always implements $D(-\psi_0(t))$ and, ultimately, performs the decision "0". The error probability $P_{\mathrm{Bon}}^{(\mathrm{I})}(1)$ reads:

$$P_{\mathrm{Bon}}^{(\mathrm{I})}(1) = p(n_{\mathrm{c}} = 0|1) = \pi_{01}^{(0)}(0, T) = e^{-2\psi^2 T} = e^{-2\alpha^2}\,. \tag{5.113}$$

If state $k = 2$ is sent, we have a decision error if either zero or one click is registered. The probability in the former case is equal to $p(n_{\mathrm{c}} = 0|2) = \pi_{02}^{(0)}(0, T) = \exp(-4\alpha^2)$, whereas in the latter one we have a single click at time $t_1 \leq T$, thus:

$$\begin{aligned} p(n_{\mathrm{c}} = 1|2) &= \int_0^T dt_1\, \pi_{02}^{(0)}(0, t_1)\, \lambda_{02}\, \pi_{12}^{(0)}(t_1, T) \\ &= \int_0^T dt_1\, e^{-4\psi^2 t_1} \left(4\psi^2\right) e^{-2\psi^2 (T - t_1)} \\ &= 2e^{-2\alpha^2} \left(1 - e^{-2\alpha^2}\right)\,. \end{aligned} \tag{5.114}$$

Summing up the two contributions, we get:

$$P_{\mathrm{Bon}}^{(\mathrm{I})}(2) = 2e^{-2\alpha^2} - e^{-4\alpha^2}\,. \tag{5.115}$$

Finally, in the case $k = 3$ errors are obtained if the photon counter clicks at most twice. We have:

$$p(n_{\mathrm{c}} = 0|3) = e^{-2\alpha^2}\,, \tag{5.116a}$$

$$p(n_{\mathrm{c}} = 1|3) = e^{-2\alpha^2} - e^{-4\alpha^2}\,, \tag{5.116b}$$

while the probability of getting two clicks at times $t_1 \leq T$ and $t_2 > t_1$ reads:

$$\begin{aligned} p(n_{\mathrm{c}} = 2|3) &= \int_0^T dt_1 \int_{t_1}^T dt_2\, \pi_{03}^{(0)}(0, t_1)\, \lambda_{03}\, \pi_{13}^{(0)}(t_1, t_2)\, \lambda_{13}\, \pi_{23}^{(0)}(t_2, T) \\ &= \int_0^T dt_1 \int_{t_1}^T dt_2\, e^{-2\psi^2 t_1} \left(2\psi^2\right) e^{-4\psi^2 (t_2 - t_1)} \left(4\psi^2\right) e^{-2\psi^2 (T - t_2)} \\ &= 4\alpha^2 e^{-2\alpha^2} - 2e^{-2\alpha^2} \left(1 - e^{-2\alpha^2}\right)\,. \end{aligned} \tag{5.117}$$

Ultimately, $P_{\mathrm{Bon}}^{(\mathrm{I})}(3)$ reads:

$$P_{\mathrm{Bon}}^{(\mathrm{I})}(3) = 4\alpha^2 e^{-2\alpha^2} + e^{-4\alpha^2}\,, \tag{5.118}$$

and the overall error probability of the type I Bondurant receiver is obtained as:

$$P_{\mathrm{Bon}}^{(\mathrm{I})} = \frac{1}{4} \sum_{k=0}^{3} P_{\mathrm{Bon}}^{(\mathrm{I})}(k) = e^{-2\alpha^2} \left(\alpha^2 + \frac{3}{4}\right)\,. \tag{5.119}$$

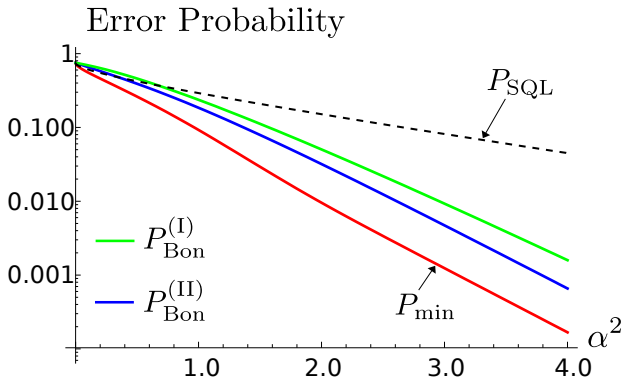


Figure 5.5.3: Log plot of $P^{(\rm p)}_{\rm Bon}$, p = I, II, as a function of the signal energy α^2. $P_{\rm SQL}$ and $P_{\rm min}$ refer to the SQL (5.108) and the minimum error probability (5.104) achieved by the PGM, respectively. Type I and type II receivers beat the SQL for $\alpha^2 \geq \alpha^2_{\rm p}$, p = I, II, whereas, in the limit $\alpha^2 \gg 1$, we have $P^{(\rm I)}_{\rm Bon} \approx \alpha^2 e^{-2\alpha^2}$ and $P^{(\rm II)}_{\rm Bon} \approx e^{-2\alpha^2}$, proving type II receiver to be near-optimum.

The plot of $P^{(\rm I)}_{\rm Bon}$ is reported in Fig. 5.5.3, together with the SQL (5.108) and the minimum error probability (5.104). As we can see, the receiver is not optimum, as in the high-energy limit $\alpha^2 \gg 1$ we have $P^{(\rm I)}_{\rm Bon} \approx \alpha^2 e^{-2\alpha^2}$, whilst $P_{\rm min} \approx e^{-2\alpha^2}$. Nevertheless, it still beats the SQL for $\alpha^2 \geq \alpha^2_{\rm I} \approx 0.68$, providing a quantum advantage for a wide range of signal energies.

The performance of the type I receiver can be enhanced by suitably improving the the ordering of the pulse nulling. In fact, we note that the most detrimental effect on $P^{(\rm I)}_{\rm Bon}$ is determined by the probability $p(n_{\rm c} = 2|3)$ in Eq. (5.117), containing the term proportional to $\alpha^2 e^{-2\alpha^2}$. This contribution can be significantly reduced by extracting some information on the signal from the time arrival distribution of the first two clicks. In fact, if state $k = 3$ is sent, the counting rate switches from $\lambda_{03} = 2\psi^2$ to $\lambda_{13} = 4\psi^2$ when the first click is registered, therefore we expect the second click to occur more quickly then the first one. That is, if the photon counter clicked at times t_1 and t_2, it would be more likely that $t_1 > (t_2 - t_1)$. On the contrary, we would have $t_1 \leq (t_2 - t_1)$ if state $k = 2$ were sent, as, now, the count rate would be reduced after the first click, since $\lambda_{02} = 4\psi^2$ and $\lambda_{12} = 2\psi^2$. Following this considerations, we construct the type II receiver from the same scheme in Fig. 5.5.2, albeit with the following improved switching rule:

- the switch is initialized in position 0, $s(0) = 0$. If no clicks are registered, i.e. $n_{\rm c} = 0$, at time T we infer state "0";
- if a click is registered at time $t_1 \leq T$, the switch moves to position $s(t) = 1$ for $t > t_1$. If no more clicks are registered, at time T we infer state "1";
- if a second click is obtained at $t_2 > t_1$, then:
  a) if $t_1 \leq (t_2 - t_1)$, i.e. $t_2 \geq 2t_1$, we set $s(t) = 2$ and perform the displacement $D(-\psi_2(t))$ for $t > t_2$. If no more counts are registered until time T, we infer state "2"; otherwise, if another count occurs, we infer state "3".
  b) if $t_1 > (t_2 - t_1)$, i.e. $t_2 < 2t_1$, we set $s(t) = 3$ and perform the displacement $D(-\psi_3(t))$ for $t > t_1$. If no more counts are registered until time T, we infer state "3"; otherwise, if another count occurs, we infer state "2".

In turn, the error probabilities for given input state $P^{(\mathrm{II})}_{\mathrm{Bon}}(k)$ only differ for $k = 2, 3$, while $P^{(\mathrm{II})}_{\mathrm{Bon}}(0) = P^{(\mathrm{I})}_{\mathrm{Bon}}(0) = 0$ and $P^{(\mathrm{II})}_{\mathrm{Bon}}(1) = P^{(\mathrm{I})}_{\mathrm{Bon}}(1) = \exp(-2\alpha^2)$. On the contrary, if state $k = 2$ was sent, errors occur when either the number of total clicks is $n_{\mathrm{c}} < 2$, see Eq. (5.121), or $n_{\mathrm{c}} = 2$ clicks are obtained at times t_1 and t_2, with $t_2 < \min\{2t_1, T\}$. In this latter case, we have:

$$\begin{aligned} &p(n_{\mathrm{c}} = 2, t_2 < \min\{2t_1, T\}|2) \\ &\quad = \int_0^T dt_1 \int_{t_1}^{\min\{2t_1,T\}} dt_2\, \pi^{(0)}_{02}(0, t_1)\, \lambda_{02}\, \pi^{(0)}_{12}(t_1, t_2)\, \lambda_{12}\, \pi^{(0)}_{32}(t_2, T) \\ &\quad = \int_0^T dt_1 \int_{t_1}^{\min\{2t_1,T\}} dt_2\, e^{-4\psi^2 t_1}\, \left(4\psi^2\right)\, e^{-2\psi^2(t_2-t_1)}\, \left(2\psi^2\right)\, e^{-2\psi^2(T-t_2)} \\ &\quad = 2e^{-4\alpha^2} \left(1 - e^{\alpha^2}\right)^2 , \end{aligned} \tag{5.120}$$

therefore:

$$P^{(\mathrm{II})}_{\mathrm{Bon}}(2) = e^{-4\alpha^2} \left(1 - 2e^{\alpha^2}\right)^2 . \tag{5.121}$$

Finally, if state $k = 3$ we have a decision error when either $n_{\mathrm{c}} < 2$, see Eq. (5.116), or when $n_{\mathrm{c}} = 2$ clicks are obtained at times t_1 and t_2, with $t_2 \geq \min\{2t_1, T\}$, with associated probability:

$$\begin{aligned} &p(n_{\mathrm{c}} = 2, t_2 \geq \min\{2t_1, T\}|3) \\ &\quad = \int_0^T dt_1 \int_{\min\{2t_1,T\}}^{T} dt_2\, \pi^{(0)}_{03}(0, t_1)\, \lambda_{03}\, \pi^{(0)}_{13}(t_1, t_2)\, \lambda_{13}\, \pi^{(0)}_{23}(t_2, T) \\ &\quad = \int_0^T dt_1 \int_{\min\{2t_1,T\}}^{T} dt_2\, e^{-2\psi^2 t_1}\, \left(2\psi^2\right)\, e^{-4\psi^2(t_2-t_1)}\, \left(4\psi^2\right)\, e^{-2\psi^2(T-t_2)} \\ &\quad = 2e^{-4\alpha^2} \left(1 - e^{\alpha^2}\right)^2 , \end{aligned} \tag{5.122}$$

such that

$$P^{(\mathrm{II})}_{\mathrm{Bon}}(3) = P^{(\mathrm{II})}_{\mathrm{Bon}}(2) = e^{-4\alpha^2} \left(1 - 2e^{\alpha^2}\right)^2 . \tag{5.123}$$

Ultimately, we retrieve the error probability of the type II Bondurant receiver as:

$$P^{(\mathrm{II})}_{\mathrm{Bon}} = \frac{1}{4} \sum_{k=0}^{3} P^{(\mathrm{II})}_{\mathrm{Bon}}(k) = \frac{3}{4} e^{-4\alpha^2} - 2e^{-3\alpha^2} + 2e^{-2\alpha^2} , \tag{5.124}$$

reported in Fig. 5.5.3. We have $P^{(\mathrm{II})}_{\mathrm{Bon}} \geq P^{(\mathrm{I})}_{\mathrm{Bon}}$ for all energies and beats the SQL for $\alpha^2 \geq \alpha^2_{\mathrm{II}} \approx 0.35 < \alpha^2_{\mathrm{I}}$. Remarkably, in the high-energy regime we have:

$$P^{(\mathrm{II})}_{\mathrm{Bon}} \approx 2e^{-2\alpha^2} = 4P_{\min} \qquad \text{for } \alpha^2 \gg 1 , \tag{5.125}$$

proving the type II receiver to be near-optimum.

The two Bondurant receivers represent a benchmark for all the QPSK receivers proposed thereafter. In particular, in 2015 Müller *et al.* designed an improved version by

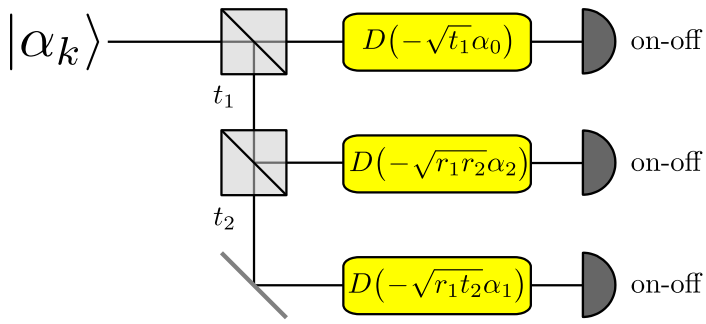


Figure 5.5.4: Scheme of the QDRE proposed in [109]. The incoming signal $|\alpha_k\rangle$ is split into 3 branches thanks to a pair of beam splitters with transmissivity $t_{1(2)}$ (and corresponding reflectivity $r_{1(2)} = 1 - t_{1(2)}$. On the 3 signals, we implement the "nullling" displacements $D(-\sqrt{t_1}\alpha_0)$, $D(-\sqrt{r_1 r_2}\alpha_2)$ and $D(-\sqrt{r_1 t_2}\alpha_1)$, respectively, followed by on-off detection. We perform the final decision according to the outcomes of the 3 detection schemes: if a "off" is obtained on the first branch, we infer state "0"; if "on" and "off" are retrieved from the first and second branch, respectively, we infer "2"; if two "on" and a "off" are registered on the first, second and third branch, respectively, we infer "1"; otherwise, we perform decision "3".

optimizing the displacement amplitude [155]. That is, they replaced the "nulling" displacements $D(-\psi_j(t))$ with optimized displacements $D(u_j(t))$, with

$$u_j(t) = e^{i\pi(2j+1)/4}\, u\, e^{-i\omega t}\,, \qquad j = 0, \ldots, 3\,, \tag{5.126}$$

where the wavepacket amplitude u is optimized to minimize the resulting error probability. Differently to exact-nulling schemes, now the total number of detection events is, in general, unbounded, as the clicks registered by the photon counter at time T may be $n_c > 3$. Therefore, the authors considered two different switching rules: either cyclic probing, where $s(t)$ is changed in cyclic order $0 \to 1 \to 2 \to 3 \to 0 \to \ldots$, or Bayesian probing, based on the maximum a posteriori probability (MAP) criterion. In both the cases, they obtain a quantum advantage for all input energy, beating the SQL for all $\alpha^2 > 0$ and outperforming also the type I Bondurant receiver [155].

However, despite its theoretical relevance, due to the technical difficulties in implementing the feedback loop, the first experimental realization of the Bondurant scheme has been obtained only in 2020 by Jabir *et al.* [170]. The authors implement Müller's improved scheme with the cyclic probing rule, where the real-time displacement adjustment is implemented by a field-programmable gate array (FPGA), stimulated by the electric pulses produced by the photon detector. The experimental data prove a quantum advantage over the SQL only in the low energy regime, due to the presence of a reduced visibility $\xi \approx 0.997$ that prevents an efficient decision strategy for large energies, making the error probability increase when $\alpha^2 \gg 1$.

5.5.2 The quaternary displacement receiver

As discussed above, the Bondurant receiver represents a challenging solution from a practical point of view, as its implementation requires continuous photo-detection and fast electrical feedback. As a consequence, simpler feasible receivers have been proposed thereafter, splitting the coherent signal into a finite number of copies, and employing

the displacement-photon counting technique. These receivers have been designed in different forms, either employing feed-forward strategies [92, 109, 151, 153–155] or not [109, 152, 153, 169].

In particular, displacement receivers without feed-forward can be constructed as a generalization of the Kennedy receiver, described in Sec. 4.3.1, where, now, the input signal should be divided in 3 copies, as at most 3 nulling displacements are necessary to perform a conclusive decision. The first proposal in this direction has been raised by Izumi *et al.* in 2012 [109], whose scheme is reported in Fig. 5.5.4. In the following, we will refer to this scheme as the *quaternary displacement receiver* (QDRE).

In the QDRE, the incoming signal $|\alpha_k\rangle$, $k = 0, \dots, 3$, is split in three branches thanks to a pair of beam splitters with transmissivity $t_{1(2)}$ (and corresponding reflectivity $r_{1(2)} = 1 - t_{1(2)}$). Following Kennedy's philosophy, the signal in the first branch, $|\sqrt{t_1}\alpha_k\rangle$, undergoes the displacement $D(-\sqrt{t_1}\alpha_0)$, nulling symbol "0", followed by on-off detection. If the measurement outcome is "off", we directly infer state $|\alpha_0\rangle$, and the corresponding probability $p(0|k)$ reads:

$$p(0|k) = e^{-t_1|\alpha_k-\alpha_0|^2} = e^{-2t_1\alpha^2[1-\cos(k\pi/2)]}. \tag{5.127}$$

Otherwise, if we obtain "on" from the first detection, we discard the hypothesis "0" and consider the subsequent branch. The signal $|\sqrt{r_1 r_2}\alpha_k\rangle$ on the second branch is then displaced by $D(-\sqrt{r_1 r_2}\alpha_2)$. We choose to null symbol "2" instead of "1" because $|\alpha_2 - \alpha_0|^2 \geq |\alpha_1 - \alpha_0|^2$, therefore, if a "on" is retrieved on the first branch, it would be more likely that state "2" was sent. As before, we perform again on-off detection: if the result is "off," then we infer state $|\alpha_2\rangle$, otherwise symbol "2" is discarded and a final decision between states "1" and "3" is performed according to the result on the third branch. The probability $p(2|k)$ of performing decision "2" when state k is sent is then equal to:

$$\begin{aligned} p(2|k) &= \left(1 - e^{-t_1|\alpha_k-\alpha_0|^2}\right) e^{-r_1 r_2|\alpha_k-\alpha_2|^2} \\ &= \left(1 - e^{-2t_1\alpha^2[1-\cos(k\pi/2)]}\right) e^{-2r_1 r_2\alpha^2[1-\cos((k-2)\pi/2)]}. \end{aligned} \tag{5.128}$$

Finally, if the result is "on" also on the second branch, we displace the signal on the third one $|\sqrt{r_1 t_2}\alpha_k\rangle$ by $D(-\sqrt{r_1 t_2}\alpha_1)$: if the result is "off," we infer state $|\alpha_1\rangle$, otherwise we infer state $|\alpha_3\rangle$. The corresponding probabilities then read:

$$\begin{aligned} p(1|k) &= \left(1 - e^{-t_1|\alpha_k-\alpha_0|^2}\right)\left(1 - e^{-r_1 r_2|\alpha_k-\alpha_2|^2}\right) e^{-r_1 t_2|\alpha_k-\alpha_1|^2} \\ &= \left(1 - e^{-2t_1\alpha^2[1-\cos(k\pi/2)]}\right)\left(1 - e^{-2r_1 r_2\alpha^2[1-\cos((k-2)\pi/2)]}\right) \times \\ &\qquad e^{-2r_1 t_2\alpha^2[1-\cos((k-1)\pi/2)]}, \end{aligned} \tag{5.129}$$

and

$$\begin{aligned} p(3|k) &= \left(1 - e^{-t_1|\alpha_k-\alpha_0|^2}\right)\left(1 - e^{-r_1 r_2|\alpha_k-\alpha_2|^2}\right)\left(1 - e^{-r_1 t_2|\alpha_k-\alpha_1|^2}\right) \\ &= \left(1 - e^{-2t_1\alpha^2[1-\cos(k\pi/2)]}\right)\left(1 - e^{-2r_1 r_2\alpha^2[1-\cos((k-2)\pi/2)]}\right) \times \\ &\qquad \left(1 - e^{-2r_1 t_2\alpha^2[1-\cos((k-1)\pi/2)]}\right). \end{aligned} \tag{5.130}$$

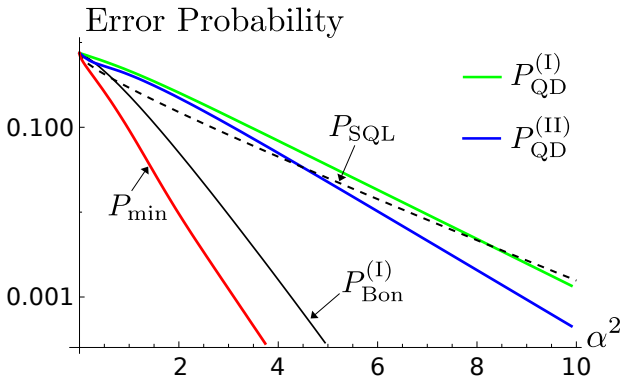


Figure 5.5.5: Log plot of $P_{\rm QD}^{(\rm p)}$, $\rm p = I, II$, as a function of the signal energy α^2. $P_{\rm SQL}$, $P_{\rm min}$, and $P_{\rm Bon}^{(\rm I)}$ refer to the SQL (5.108), the minimum error probability (5.104) achieved by the PGM, and the error probability of type I Bondurant receiver (5.121).

Summing up all the contributions, we obtain the error probability as:

$$P_{\rm QD}(t_1, t_2) = 1 - \frac{1}{4}\sum_{k=0}^{3} p(k|k)\,, \tag{5.131}$$

that depends on the values of the transmissivities $t_{1(2)}$.

We identify two scenarios. In the former, referred to as case I, we consider coherent-state splitting in equal copies, corresponding to $t_1 = 1/3$ and $t_2 = 1/2$; in the latter, called case II, we optimize the values $t_{1(2)}$ for each α^2 to minimize Eq. (5.131). That is,

$$\begin{aligned} P_{\rm QD}^{(\rm I)} &= P_{\rm QD}(t_1 = 1/3, t_2 = 1/2) \\ &= \frac{1}{4} e^{-8\alpha^2/3}\left(1 - e^{2\alpha^2/3} + 4e^{2\alpha^2}\right)\,, \end{aligned} \tag{5.132}$$

and

$$P_{\rm QD}^{(\rm II)} = \min_{t_1,t_2} P_{\rm QD}(t_1, t_2)\,. \tag{5.133}$$

Plots of $P_{\rm QD}^{(\rm p)}$, $\rm p = I, II$, are reported in Fig. 5.5.5 as a function of α^2. As we can see, in both the cases the QDRE beats the SQL for sufficiently high α^2, and $P_{\rm QD}^{(\rm II)} \leq P_{\rm QD}^{(\rm I)}$, proving optimization of the splitted signal fractions as crucial factor to maximize the receiver performance. In particular, the numerically optimized transmissivities in the limit $\alpha^2 \gg 1$ are $t_1 \approx 2/5$ and $t_2 \approx 1/3$, therefore:

$$P_{\rm QD}^{(\rm II)} \approx \frac{5}{4} e^{-4\alpha^2/5} \qquad \text{for } \alpha^2 \gg 1\,, \tag{5.134}$$

whereas $P_{\rm QD}^{(\rm I)} \approx \exp(-2\alpha^2/3) > P_{\rm QD}^{(\rm II)}$.

5.5.3 The quaternary displacement feed-forward receiver

The QDRE performance may be significantly improved by considering displacement feed-forward receivers. This class of receivers provide a particularly attractive solution,

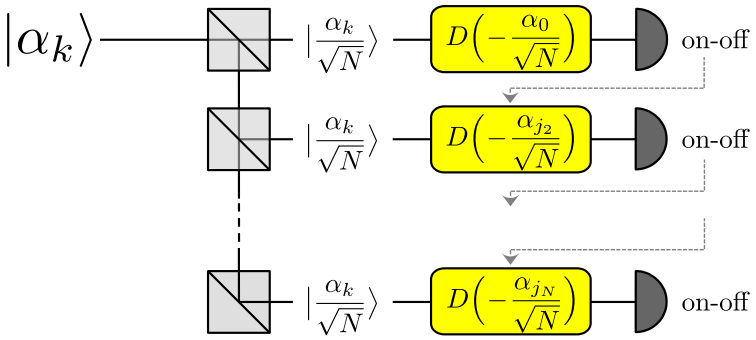


Figure 5.5.6: Scheme of the QDFFRE proposed in [109]. The incoming signal $|\alpha_k\rangle$ is split into N copies. Each copy $m = 1, \ldots, N$ undergoes a conditional displacement $D(-\alpha_{j_m}/\sqrt{N})$ followed by on-off detection. For the first copy we have $j_1 = 0$. For the others, the outcome of the $(m-1)$-th detection sets out the displacement amplitude j_m to be implemented on the following copy.

leading to error probabilities closer to the Bonduarant limit, albeit with few adaptive steps, simpler setup and less-demanding requirements in terms of detection efficiency, dark count rate and visibility reduction [19, 109]. As a paradigmatic example, here, we focus on the proposal of the *quaternary displacement feed-forward receiver* (QDFFRE) presented in [109] and depicted in Fig. 5.5.6.

The QDFFRE is based on the slicing property of coherent states: indeed, thanks to an array of splitters, the incoming signal $|\alpha_k\rangle$ is split into $N \geq 3$ identical copies with reduced amplitude $|\alpha_k/\sqrt{N}\rangle$. Then, each m-th copy, $m = 1, \ldots, N$, undergoes a conditional displacement operation followed by an on-off detection which returns a click-no click result. The first copy is displaced by $D(-\alpha_{j_1}/\sqrt{N})$, with $j_1 = 0$, being mapped into the coherent state $|(\alpha_k - \alpha_{j_1})/\sqrt{N}\rangle$. In turn, if $k = 0$ the incoming signal is displaced into the vacuum and the subsequent on-off detector will not click, whereas if $k \neq 0$ the detector is more likely to click with a probability $1 - p_k$, where

$$\begin{aligned} p_0 &= 1\,, \\ p_1 &= p_3 = e^{-2\alpha^2/N}\,, \\ p_2 &= e^{-4\alpha^2/N}\,. \end{aligned} \tag{5.135}$$

According to the result of the first detection, we decide what would be the value of the amplitude of the displacement $D(-\alpha_{j_2}/\sqrt{N})$ applied to the second copy: if an "off" result is registered, that is the detector does not click, we set $j_2 = j_1 = 0$; otherwise we discard hypothesis "$k = 0$", set $j_2 = j_1 + 1$ and probe the final hypothesis from the remaining set $k = 1, 2, 3$. We proceed iteratively in this way until the last copy is processed, following the feed-forward rule: if the $(m-1)$-th detection gives outcome "off" we displace the m-th copy by $D(-\alpha_{j_m}/\sqrt{N})$ with $j_m = j_{m-1}$, if an "on" is obtained we set $j_m = j_{m-1} + 1$, discard all states $j \leq j_{m-1}$ and restrict the decision to the states $j_m, \ldots, 3$. The outcome of the last detection determines the final decision. If an "off" is retrieved, we decide the state $j = j_m$ has been sent, otherwise we perform a random decision among the remaining states.

The conditional probabilities $p^{(N)}(j|k)$ of inferring the state $j = 0, \ldots, 3$ after N

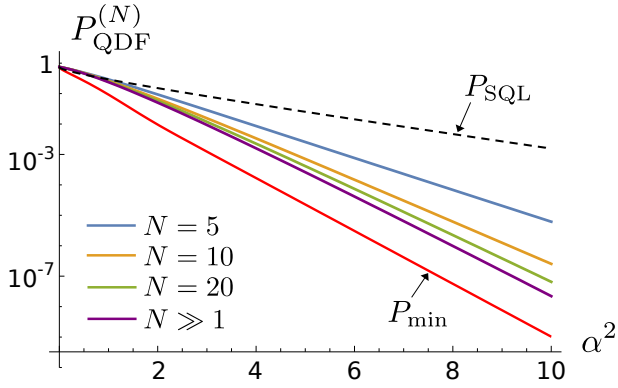


Figure 5.5.7: Log plot of the decision error probability $P_{\mathrm{QDF}}^{(N)}$ as a function of the signal energy α^2 for different N, compared to both the SQL (5.108) and the minimum error probability (5.104) achieved by the PGM. The QDFFRE beats the SQL only in the regime $\alpha^2 \gg 1$ and, for large N, scales as $P_{\mathrm{QDF}}^{(N)} \approx \alpha^2 e^{-2\alpha^2}$, approaching the type I Bondurant receiver, whilst the minimum error probability is $P_{\min} \approx e^{-2\alpha^2}$.

copies if state $k = 0, \ldots, 3$ was sent read:

$$p^{(N)}(0|k) = p_k^N \,, \tag{5.136a}$$

$$p^{(N)}(1|k) = \sum_{t=0}^{N-2} p_k^t \,(1-p_k)\, p_{(k-1) \bmod 4}^{N-1-t} + \frac{p_k^{N-1}(1-p_k)}{3} \,, \tag{5.136b}$$

$$\begin{aligned} p^{(N)}(2|k) = \sum_{t=0}^{N-3} \sum_{s=0}^{N-3-t} & p_k^t \,(1-p_k)\, p_{(k-1) \bmod 4}^s \,(1-p_{(k-1) \bmod 4}) \times \\ & p_{(k-2) \bmod 4}^{N-2-t-s} + \sum_{t=0}^{N-2} p_k^t \,(1-p_k)\, \frac{p_{(k-1) \bmod 4}^{N-2-t}(1-p_{(k-1) \bmod 4})}{2} \\ & + \frac{p_k^{N-1}(1-p_k)}{3} \,, \end{aligned} \tag{5.136c}$$

$$\begin{aligned} p^{(N)}(3|k) = \sum_{t=0}^{N-3} \sum_{s=0}^{N-3-t} \sum_{u=0}^{N-3-t-s} & p_k^t \,(1-p_k)\, p_{(k-1) \bmod 4}^s \times \\ & (1-p_{(k-1) \bmod 4})\, p_{(k-2) \bmod 4}^u \,(1-p_{(k-2) \bmod 4})\, p_{(k-3) \bmod 4}^{N-3-t-s-u} \\ & + \sum_{t=0}^{N-2} p_k^t \,(1-p_k)\, \frac{p_{(k-1) \bmod 4}^{N-2-t}(1-p_{(k-1) \bmod 4})}{2} \\ & + \frac{p_k^{N-1}(1-p_k)}{3} \,. \end{aligned} \tag{5.136d}$$

Then, the associated decision error probability reads:

$$P_{\mathrm{QDF}}^{(N)} = 1 - \frac{1}{4}\sum_{k=0}^{3} p^{(N)}(k|k)\,, \tag{5.137}$$

depicted in Fig. 5.5.7 as a function of α^2 for different N. As emerges from the plot, the present displacement receiver outperforms the SQL achieved with double homodyne detection only in the high-energy regime $\alpha^2 \gg 1$. We also note that, in the limit $N \gg 1$, we have $P_{\mathrm{QDF}}^{(N)} \approx e^{-2\alpha^2}(\alpha^2 + 3/4)$, and the QDFFRE approaches the type I Bondurant receiver [150].

The gap between $P_{\mathrm{QDF}}^{(N)}$ and P_{min} can be further reduced by optimizing the receiver setup in Fig. 5.5.6. In particular, Izumi *et al.* obtained a better performance in the low-energy regime by changing the order of the nulling displacements from the sequenatial fashion $0 \to 1 \to 2 \to 3$ to $0 \to 2 \to 1 \to 3$, following the scheme of the QDRE, such that, if the first "on" is retrieved from the $(m-1)$-th copy, we displace the m-th one by $D(-\alpha_2/\sqrt{N})$ instead of $D(-\alpha_1/\sqrt{N})$. This choice reduces the error probability for $\alpha^2 < 1$, but it worsen the receiver performance in the asymptotic limit $\alpha^2 \gg 1$ [109]. Further improvements in the low-energy regime may be obtained by replacing on-off detectors by photon-number resolving detectors to adopt the maximum a posteriori probability criterion [151, 153], and by optimizing the displacement amplitude, following Müller's approach [154, 155]. With these methods, we obtain an improved version of the QDFFRE, being able to beat the SQL for all energies and maximizing the performance of the displacement-photon counting setup.

Part III

Continuous variable quantum key distribution

CHAPTER 6

Quantum key distribution: the general framework

The third Part of the thesis is devoted to the field of quantum key distribution (QKD), that has received increasing attention in the latest years, as it guarantees unconditionally secure communication between two distant parties connected by an untrusted quantum channel. In fact, while the current cryptographic systems, e.g. public-key cryptography, only offer *conditional* security based on assumptions on the computational complexity of specific tasks, QKD makes sender and receiver share a random secure key with *unconditional* security, regardless the action of any third malicious party, e.g. an eavesdropper [171–174]. This powerful property directly follows from the quantum mechanics laws, that impose ineludible limits on any possible eavesdropping strategy, and, accordingly, lead to general security proofs only based on few basic assumption. Nevertheless, in practical conditions dealing with unconditional security may be excessive, as a realistic eavesdropper may encounter further limitations due to both the available state-of-art technologies and the particular composition of the adopted experimental setup, therefore, in time, different security layers have been established, according to the level of trust of the equipment, e.g. the trusted-device scenario and the wiretap channel assumption.

In this Chapter, we discuss the fundamental aspects of QKD, with particular attention to continuous variable QKD (CVQKD), in which the key is distilled after the exchange of coherent states of radiation. Then, we provide a detailed analysis of the unconditional security framework. At first, we present the GG02 protocol, providing the milestone CVQKD scheme proposed by Grosshans and Grangiér in 2002, employing Gaussian modulation of coherent states and Gaussian detection at the receiver [14, 175–177]. Then, we prove the "optimality of Gaussian attacks" theorem, independently established in 2006 by both Navascués *et al.* [178] and García-Patrón *et al.* [179, 180], that provides a sufficient condition to assess unconditional security of protocols employing non-Gaussian modulation and Gaussian detection, and study discrete modulation CVQKD with both the phase-shift keying (PSK) and quadrature amplitude modulation (QAM) formats.

The structure of the Chapter is the following. At first, in Sec. 6.1 we give a general overview on QKD, together with an historical outline, and highlight the fundamental features of all protocols, introducing the key generation rate (KGR) as the main figure of merit. Thereafter, in Sec. 6.2, we widely discuss CVQKD, and outline the different security frameworks to conduct the security analysis. Given these premises, Sec. 6.3 presents the GG02 protocol, for which the KGR can be exactly computed. Subsequently, in Sec. 6.4 we prove the "optimality of Gaussian attacks" theorem, and exploit it in Sec. 6.5 to address unconditional security of the PSK and QAM protocol, employing discrete modulation.

6.1 Basic notions on quantum key distribution

The cryptographic systems currently employed for secure communications are mostly based on public-key cryptography, which allows two distant parties to exchange confidential messages without pre-sharing a secret key. It provides a convenient solution for practical applications but, unfortunately, only offers conditional security, as it usually relies on some assumptions on both the computational resources of a possible eavesdropper and the complexity of an underlying mathematical problem, e.g. the difficulty of factoring large integers in the Rivest-Shamir-Adleman (RSA) algorithm [181]. On the other hand, the one-time pad [182], together with analogous cryptographic techniques, offer unconditional security (guaranteed by information theory), albeit with much less practical implementation, as they require the involved parties to share in advance a secret key with the same length as the confidential message, to keep it secret, and to use it only once [49]. In practice, the one-time pad technique shifts the security problem from the transmission of the confidential message to the distribution of a secure key. However, since distributing long keys is practically not convenient and may pose a significant security risk, public-key cryptography is more widely used than the one-time pad.

Nevertheless, the rapidly emerging progress in the field of quantum computation represents a potential threat for conventional classical cryptosystems. In fact, the quantum factoring algorithm developed by Shor allows to perform probabilistic factorization of non-trivial integers in bounded-error polynomial time [27, 183]. A further weakening for public-key protocols may also arise from future advances in number theory, where an efficient factorization algorithm for classical Turing machines may be developed [184]. In contrast, a possible solution to the problem of secure key distillation is offered by quantum key distribution (QKD), allowing to share a secret key through the exchange of quantum states [171–174]. The very laws of quantum mechanics, like the uncertainty principle, the no-cloning theorem, or the monogamy of entanglement, guarantee the unconditional security of QKD protocols, making the two communicating parties detect the intrusion of any malicious eavesdropper [75].

Historically, the first QKD protocols have been designed for discrete variable (DV) systems, i.e. qubits. Preliminary ideas in this direction dates back to the early 1970s, when Wiesner speculated about the design of bank notes robust to counterfeiting [185, 186], until 1984, when Bennett and Brassard introduced the first seminal DVQKD protocol, referred to as BB84 [13], which nowadays is the main one being commercially distributed. In time, several DVQKD schemes have been proposed, e.g. employing entangled photons [187], non-orthogonal quantum states [68] and decoy states [188–190]. However, from a practical point of view, the large-scale implementation of DV systems is highly nontrivial for a twofold reason. The main obstacle is represented by the generation of single photons, whose polarization provides the proper degree of freedom to encode the secure bits. Furthermore, the technology required by DVQKD is not compatible with the that of classical telecommunication systems, which, instead, are based on exchange of laser pulses and homodyne or double homodyne (DH) measurements of optical signals [38, 191–193].

For these reasons, from the late 1990s, proposals of QKD protocols on continuous variable (CV) platforms were developed [194–199]. Ultimately, in 2002 Grosshans and Grangier proposed the first genuine CVQKD protocol based on Gaussian modulation of coherent states and single quadrature detection at the receiver's side, referred to as GG02 [14, 175–177]. Later, a no-switching scheme where the single quadrature measurement is replaced by DH detection has also been proposed by Weedbrook *et al.* [200]. More recently, also squeezed-state protocols have been developed, obtaining further advantages

in the case of long-distance transmission [201–205].

6.1.1 The general structure of a QKD protocol

Regardless the particular platform employed to transmit quantum states between the two parties, either DV or CV, all QKD protocols share the same fundamental structure, being divided into two main parts, that is a quantum communication stage followed by classical post-processing [174].

The first one represents the quantum part of the protocol. Here, the sender, Alice, encodes the outcomes of a classical random variable α, generated with a priori probability $p_A(\alpha)$, onto an ensemble of quantum states, being not necessarily orthogonal with one another. These states are, then, sent to the receiver, Bob, throughout a quantum channel. More precisely, with the term "quantum channel" we refer to the physical support connecting Alice and Bob, in which the encoded signals propagate. In practical contexts, it describes different physical systems according to the adopted platform, e.g. optical fibers, free-space settings, fading channels or underwater communications [191, 206–208]. Beside, the channel is typically noisy, and introduces distortions of the input signals; therefore, it is considered as *untrusted*, assuming these distortions to be produced by a third malicious party, the eavesdropper (Eve), who is interested in extracting the secure key generated by Alice and Bob. After the channel, Bob probes his received signals by performing a measurement, described by a suitable POVM, retrieving a random outcomes β, associated with probability $p_B(\beta)$, being partially correlated to Alice's ones. In turn, after repeated iterations of the present scheme, Alice and Bob share a set of raw data described by the two correlated classical variables α and β.

For what concerns the post-processing part, we can divide it into three steps.

- *Channel evaluation*: Alice and Bob use part of their raw data to assess the characteristics of the channel, by performing estimation of the channel parameters, such as its transmissivity and added noise.

- *Reconciliation*: starting from the results of channel estimation, Alice and Bob partially share a subset of their data to perform error correction, which allows them to detect and eliminate errors induced by the signal transmission, and ultimately, agree on a common raw key. We note that, at this stage, this raw common bit string can be partially known by the eavesdropper which can intercept the flow of information.

- *Privacy amplification*: the raw key undergoes a stage of privacy amplification, implemented via numerical codes based on hash functions,e.g. low density parity check (LDPC) codes [209, 210], which allows the trusted parties to reduce the eavesdropped information to a negligible amount, at the cost of reducing the length of the common bit string. The result of this stage provides the secure key, which is typically much shorter than the raw one.

In some particular protocols, like BB84, a further step, called *sifting*, is introduced: in this case, the two parties perform classical communication to agree on a subset of their raw data, while discarding the rest, according to the measurement bases that they chose independently in each repetition of the protocol [171, 172, 174].

Remarkably, we underline that the reconciliation step requires a public exchange of information, performed on a classical authenticated channel. Therefore the secure key can be distilled only thanks to proper interplay between quantum and classical communication stages; whereas the sole quantum communication is insufficient to the task.

Moreover, reconciliation can be performed in two alternative ways, according to the party that publicly reveals part of his data. We have *direct reconciliation* (DR) if this party is Alice, and Bob post-processes its outcomes accordingly to infer Alice's encodings. This procedure is typically realized via forward classical communication Alice $\rightarrow$ Bob. In the opposite scenario, referred to as *reverse reconciliation* (RR), the situation is reversed; now, we have backward classical communication Bob $\rightarrow$ Alice, and Alice post-processes her data to infer Bob's variable [174].

6.1.2 Eavesdropping strategies

The figure of merit to assess the security of the protocol is the key generation rate (KGR), also referred to as secret key rate, expressed in bits per time slot, i.e. per channel use, and defined as the difference between the amount of information shared by Alice and Bob and the information lost throughout channel propagation, assumed to be intercepted by Eve. Given this premise, security can be investigated in two different conditions. The former, called *asymptotic security*, requires the two parties to perform $N \gg 1$ repetitions of the protocol, thus possessing an infinite dataset of variables (α, β). In particular, this implies that the channel parameters can be estimated with no uncertainty, according to the Cramér-Rao theorem [211]. Clearly, the asymptotic security provides a simpler, although less realistic, scenario. On the other hand, when the number of repetitions N is not large enough to reach the asymptotic regime, we deal with *finite size effects*, which introduce ineludible inefficiencies in all the post-processing stages, thus weakening security of the scheme.

Let us start with the asymptotic case. Now, the possible attacks that Eve may launch can be divided into three main class, namely individual, collective, and coherent, according to the amount of resources in her hands. In *individual attacks*, Eve performs an independent and identically distributed (i.i.d.) attack on each single intercepted signal. That is, at every repetition of the protocol, she prepares a fresh ancillary state which interacts with the transmitted signal and is individually measured thereafter. The individual measurements can be either performed on-the-fly or delayed at the end of the protocol, letting Eve optimize them according to the public information shared on the classical authenticated channel. Therefore, in this case the three parties, Alice, Bob and Eve, end up with three classical correlated random variables α, β and γ, respectively. The asymptotic KGR is then obtained as the difference between the mutual information shared by the various parties, namely:

$$K_{\text{ind}} = \beta I(A;B) - I(A;E) \qquad \text{for DR,} \tag{6.1a}$$

$$K_{\text{ind}} = \beta I(A;B) - I(B;E) \qquad \text{for RR,} \tag{6.1b}$$

where $\beta \leq 1$ is the reconciliation efficiency, quantifying the procedural errors of both error correction and privacy amplification, $I(A;B)$ is Alice and Bob's mutual information associated with the variables α and β, whilst $I(A;E)[I(B;E)]$ is the mutual information shared by Alice (Bob) and Eve, corresponding to the variables α (β) and γ. Clearly, the protocol is successful iff the KGR is larger than 0, meaning that the information shared between Alice and Eve is larger than that intercepted by Eve.

On the contrary, we have *collective attacks* when Eve still launches an i.i.d. attach using a fresh ancilla per channel use, but now, she stores all the interpreted states into a quantum memory, being collectively measured only at the end of the protocol. If so, we should assume Eve to achieve the maximum amount of information allowed by quantum mechanics laws, corresponding to the Holevo information (which, indeed, is

achieved by collective measurement). Thus, the KGR becomes:

$$K_{\text{coll}} = \beta I(A;B) - \chi(A;E) \qquad \text{for DR,} \tag{6.2a}$$

$$K_{\text{coll}} = \beta I(A;B) - \chi(B;E) \qquad \text{for RR,} \tag{6.2b}$$

where $\chi(A;E) = \mathsf{S}[\rho_E] - \int d\alpha\, p_A(\alpha)\mathsf{S}[\rho_{E|\alpha}]$ and $\chi(B;E) = \mathsf{S}[\rho_E] - \int d\beta\, p_B(\beta)\mathsf{S}[\rho_{E|\beta}]$ are the Holevo information between Alice and Eve, and Bob and Eve, respectively. In the former expression, ρ_E represents the average state in Eve's hands, $\rho_{E|\alpha(\beta)}$ is Eve's state conditioned to the outcome $\alpha(\beta)$, associated with probability $p_A(\alpha)[p_B(\beta)]$, and $\mathsf{S}[\varrho] = -\operatorname{Tr}[\varrho \log_2 \varrho]$ is the von Neumann entropy of state ϱ.

Finally, in the case of *coherent attacks*, the i.i.d. hypothesis is relaxed. That is, Eve prepares a global non-factorized ancillary state on a set of correlated modes, which jointly interacts with all the encoded signals via collective unitary operation. The output state is then stored in a quantum memory, and collectively measured at the end of the protocol. Coherent attacks provide the most powerful eavesdropping strategy; however, in the asymptotic scenario, Renner proved that they can be reported back to collective attacks thanks to quantum de Finetti reduction [212–214].

Beyond asymptotic security, finite-size effects arise in the presence of a finite number N of protocol repetitions. In this case, the KGR should be appropriately modified to take into account the inefficiencies introduced in each post-processing step, namely parameter estimation, error correction and privacy amplification. On the one hand, channel evaluation is not exact with a finite statistical sample, and the estimated parameters are associated with a confidence interval of finite width; on the other hand, error correction and privacy amplification are practically implemented by probabilistic routines, thus being associated with a nonzero failure probability that scales with the length of the processed dataset. In turn, in the finite-size setting perfect security cannot be achieved, but we are limited to ε-security: that is, we introduce a (possibly small) ε parameter, quantifying the error probability of each protocol step, meaning that the protocol is successful with probability $\geq 1 - \varepsilon$. The security proofs conducted in this framework falls under the *composable security* paradigm, currently established for many DV and CV schemes [167, 168, 206, 215–221].

6.2 Continuous variable QKD

In this thesis, we restrict ourselves to the analysis of CVQKD schemes, which can be divided into two main categories, according to the quantum states of radiation employed by Alice to encode her random variable, being either coherent or squeezed signal states [174, 222]. In more detail, we only consider protocols employing coherent-state modulation, focusing on asymptotic security under collective attacks. Instead, a detailed discussion on the fundamental issues of the finite-size setting is reported in [180, 206, 220]. Moreover, we focus on RR strategies, that provide a more powerful solution for long-distance communications, whilst DR is intrinsically bounded to a 3 dB-limit of channel losses, as more than 50% of the signal must arrive to the receiver in order to have the information shared between sender and receiver larger than the one shared between sender and eavesdropper [174, 222].

Here, we present the basic features of coherent-state protocols. First of all, we underline the security analysis can be carried out under two equivalent frameworks. The former, referred to as the *prepare and measure* (PM) protocol, represents the most intuitive and feasible scheme. Here, Alice samples a random variable drawn from a suitable probability distribution, either discrete or continuous, and encodes its value onto optical

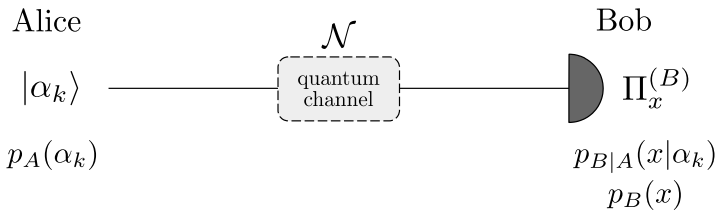


Figure 6.2.1: Scheme of the PM version of CVQKD. Alice randomly generates a coherent state $|\alpha_k\rangle$ with probability $p_A(\alpha_k)$ and sends it to Bob throughout an untrusted noisy quantum channel, described by the quantum CP map $\mathcal{N}$. Bob performs the POVM $\{\Pi_x^{(B)}\}_x$ on the received signals, obtaining a set of outcomes x correlated to Alice's ones.

signals. The signals are then sent to Bob, who implements a quantum measurement to infer the value of the encoded variable. The latter is the *entanglement-based* (EB) protocol, being a theoretical scheme, equivalent to the PM, in which Alice's preparation is modeled as a quantum measurement over one branch of a two-mode entangled state, that projects the remaining mode onto the signal state transmitted throughout the channel [174, 222]. Despite this more elaborated structure, the EB scheme turns out to provide a simpler theoretical analysis, as will become clearer in the following.

6.2.1 Prepare and measure protocol

The prepare and measure (PM) version of CVQKD, corresponding to the practical implementation scheme of the protocol, is depicted in Fig. 6.2.1. In the PM protocol, Alice prepares a coherent state drawn from a constellation $\{|\alpha_k\rangle\}_k$, $k \in \mathcal{K}$, sampling the k-th state with a priori probability $p_A(\alpha_k)$, such that $\sum_k p_A(\alpha_k) = 1$. Here, we adopt a general description, where the random variable of Alice's source may be either continuous or discrete [222, 223]. When the constellation contains an infinite number of states, the set $\mathcal{K}$ has infinite cardinality and we deal with *continuous modulation* [14, 175–177, 200], whereas in the presence of a finite number of the constellation states, $\mathcal{K}$ contains a finite number of elements $k = 0, \dots, M-1$, and we have *discrete modulation* [20, 162, 164, 165, 223–235]. The average state generated at Alice's side then reads:

$$\rho = \sum_{k \in \mathcal{K}} p_A(\alpha_k) |\alpha_k\rangle\langle\alpha_k| \,. \tag{6.3}$$

We note that ρ is a density operator acting on the subspace spanned by the constellation states, namely $\rho \in \mathcal{L}(\mathcal{S})$, $\mathcal{S} = \mathrm{span}\{|\alpha_k\rangle : k \in \mathcal{K}\}$, which in the presence of continuous modulation typically coincides with the whole Hilbert space. On the contrary, in discrete modulation schemes, ρ is a convex mixture of M linearly independent vectors, thus $\mathrm{rank}(\rho) = M$. In turn, the mean photon number employed at the modulation stage, referred to as the *modulation energy* reads:

$$\bar{n} = \sum_k p_A(\alpha_k) |\alpha_k|^2 \,. \tag{6.4}$$

After modulation, the encoded pulses are injected into the untrusted noisy channel, described by a quantum CP map $\mathcal{N}$ until to reach Bob, who performs a suitable quantum measurement on the received signals, described by the POVM $\{\Pi_x^{(B)}\}_x$, $\Pi_x^{(B)} \geq 0$,

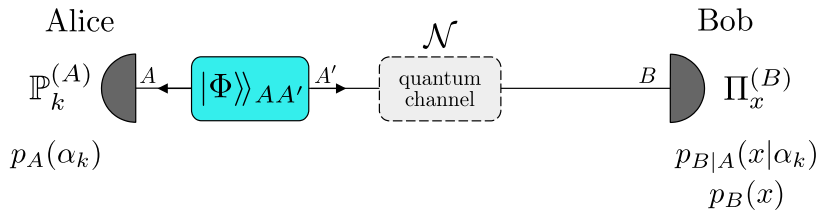


Figure 6.2.2: Scheme of the EB version of CVQKD. Now, Alice holds the two-mode entangled state $|\Phi\rangle\!\rangle_{AA'}$ on two modes A and A'; when she performs the projective measurement $\mathbb{P}_k^{(A)}$ on mode A, mode A' is projected into the coherent state $|\alpha_k\rangle_{A'}$ with probability $p_A(\alpha_k)$. The prepared state is then injected into the noisy untrusted channel, associated with the CP map $\mathcal{N} : A' \to B$, to Bob, who implements his POVM $\{\Pi_x^{(B)}\}_x$.

$\sum_x \Pi_x^{(B)} = \hat{\mathbb{1}}$, and retrieves the outcome $x \in \mathcal{X}$. Typically, one consider Gaussian measurements, either homodyne or DH. The outcomes x are distributed according to the conditional probability distribution $p_{B|A}(x|\alpha_k)$ when Alice sent the k-th state, from which we retrieve the overall probability distribution $p_B(x) = \sum_k p_A(\alpha_k) p_{B|A}(x|\alpha_k)$.

6.2.2 Entanglement based protocol

An equivalent version of the former PM protocol is the entanglement based (EB) scheme. While the PM protocol represents the actual practical implementation of CVQKD, the corresponding EB version provides a simpler theoretical analysis. In fact, the two schemes are indistinguishable from the perspective both of Bob and Eve, therefore they share the same security and are equivalent between each other [174, 222, 223].

The key idea to construct the EB scheme is to model Alice's state preparation as the result of a quantum measurement performed onto an ancillary physical system. As depicted in Fig. 6.2.2, in the EB protocol Alice holds a bipartite entangled state $|\Phi\rangle\!\rangle_{AA'}$ on two modes A and A', expressed in the form:

$$|\Phi\rangle\!\rangle_{AA'} = \sum_k \sqrt{p_A(\alpha_k)}\, |\psi_k\rangle_A\, |\alpha_k\rangle_{A'}\,, \tag{6.5}$$

where ${}_A\langle\psi_j|\psi_k\rangle_A = \delta_{jk}$, with $j, k \in \mathcal{K}$. Thereby, when Alice performs the projective measurement $\mathbb{P}_k^{(A)} = |\psi_k\rangle_A\langle\psi_k|$ on mode A, mode A' is projected into the coherent state $|\alpha_k\rangle_{A'}$ with probability $p_A(\alpha_k)$. The prepared signal on A' is then injected into the untrusted channel and probed by Bob, as in the PM protocol [222, 223]. Moreover, we note that the average state on mode A' being sent to Bob is equal to the state ρ reported in Eq. (6.3):

$$\mathrm{Tr}_A\left[|\Phi\rangle\!\rangle_{AA'}\langle\!\langle\Phi|\right] = \sum_k p_A(\alpha_k) |\alpha_k\rangle_{A'}\langle\alpha_k| = \rho_{A'}\,, \tag{6.6}$$

where the pedix A' underlines the optical mode on which the state is generated. This guarantees the equivalence of the EB protocol with the PM. However, we remind that the choice of the purification is highly not unique, therefore there exist infinitely many choices of both $|\Phi\rangle\!\rangle_{AA'}$ and $\mathbb{P}_k^{(A)}$, all of them being equivalent from the perspective of security analysis.

Given this outline, we now perform explicit construction of the entangled state in Alice's hands, satisfying both Eq.s (6.6) and (6.8) [162, 180, 223]. We start from the eigenvalue decomposition of the state ρ in (6.3), namely $\rho = \sum_j \lambda_j |\phi_j\rangle\langle\phi_j|$, $\lambda_j \geq 0$, and consider the particular purification obtained by the Schmidt decomposition:

$$\begin{aligned} |\Phi\rangle\!\rangle_{AA'} &\equiv \sum_j \sqrt{\lambda_j}\, |\phi_j^*\rangle_A\, |\phi_j\rangle_{A'} \\ &= \sum_j \sqrt{\lambda_j}\, |\phi_j^*\rangle_A \left(\sum_{n=0}^{\infty} \langle n|\phi_j\rangle |n\rangle_{A'} \right) \\ &= \sum_{n=0}^{\infty} \left(\sum_j \sqrt{\lambda_j}\, |\phi_j^*\rangle_A \langle\phi_j^*| \right) |n\rangle_A |n\rangle_{A'} \\ &= \left[(\rho^*)^{1/2} \otimes \mathbb{1} \right] |\mathrm{EPR}\rangle\!\rangle_{AA'} , \end{aligned} \tag{6.7}$$

where we introduced the Fock basis $\{|n\rangle\}_n$, such that $\langle n|\phi_j\rangle = \langle\phi_j^*|n\rangle$, and the EPR state $|\mathrm{EPR}\rangle\!\rangle = \sum_{n=0}^{\infty} |n\rangle|n\rangle$, corresponding to a (un-normalizable) two-mode squeezed vacuum state with infinite amount of squeezing. The $*$ in Eq. (6.7), denoting complex conjugation, only represents a technical detail of small practical relevance. In fact, the main constellation schemes employed in optical communications, e.g. phase-shift keying and quadrature-amplitude modulation, exhibit symmetry with respect to complex conjugation, and one typically has $|\phi_j^*\rangle = |\phi_j\rangle$ and $\rho^* = \rho$.

The state (6.7) is pure and normalized, and satisfies the physical request (6.6). Moreover, it provides a symmetric configuration between the two subsystems A and A', as performing partial trace over mode A' yields:

$$\mathrm{Tr}_{A'} \left[|\Phi\rangle\!\rangle_{AA'} \langle\!\langle\Phi| \right] = \sum_k p_A(\alpha_k) |\alpha_k^*\rangle_A \langle\alpha_k^*| = \rho_A^* . \tag{6.8}$$

In turn, the overall state on mode A has the same mean energy as that on A', i.e. $\bar{n}_A = \bar{n}_{A'} = \bar{n}$, see Eq. (6.4), and, beside complex conjugation, it describes the same statistical ensemble being injected into the channel towards Bob.

We now prove that this purification can be brought back to the expression (6.5). To this aim, we define the projective measurement $\mathbb{P}_k^{(A)}$ associated with $|\Phi\rangle\!\rangle_{AA'}$ by introducing the measurement vectors [223]:

$$|\psi_k\rangle \equiv \sqrt{p_A(\alpha_k)}\, (\rho^*)^{-1/2}\, |\alpha_k^*\rangle , \tag{6.9}$$

where, in general, $(\rho^*)^{-1/2}$ represents the square-root Moore-Penrose pseudo-inverse of ρ^*, accounting for the case in which ρ gets finite rank, thus being not invertible. In particular, this implies that $\rho^*(\rho^*)^{-1} = \mathbb{P}_{\mathcal{S}^*}$, $\mathbb{P}_{\mathcal{S}^*}$ being the projector onto the subspace $\mathcal{S}^*$ spanned by the conjugated constellation states $\{|\alpha_k^*\rangle\}_k$.

Eq. (6.9) implies the equivalence between states (6.7) and (6.5), as their overlap $\mathcal{O}_{AA'}$

is equal to:

$$\begin{aligned}\mathcal{O}_{AA'} &= \left\{\sum_k \sqrt{p_A(\alpha_k)}\langle\psi_k|\langle\alpha_k|\right\}\left\{[(\rho^*)^{1/2}\otimes\mathbb{1}]\sum_{n=0}^{\infty}|n\rangle|n\rangle\right\}\\ &= \sum_{kn} p_A(\alpha_k)\langle\alpha_k^*|\langle\alpha_k|\left[(\rho^*)^{-1/2}\otimes\mathbb{1}\right]\left[(\rho^*)^{1/2}\otimes\mathbb{1}\right]|n\rangle|n\rangle\\ &= \sum_{kn} p_A(\alpha_k)\langle\alpha_k^*|\langle\alpha_k|(\mathbb{P}_{\mathcal{S}^*}\otimes\mathbb{1})|n\rangle|n\rangle\\ &= \sum_n\langle n|\left(\sum_k p_A(\alpha_k)|\alpha_k\rangle\langle\alpha_k|\right)|n\rangle = \mathrm{Tr}[\rho] = 1\,,\end{aligned} \tag{6.10}$$

where we used the properties $\langle\alpha_k^*|n\rangle = \langle n|\alpha_k\rangle$ and $\mathbb{P}_{\mathcal{S}^*}|\alpha_k^*\rangle = |\alpha_k^*\rangle$.

Finally, in order to complete the EB construction, we need to prove that the measurement vectors $\mathbb{M} = \{|\psi_k\rangle : k\in\mathcal{K}\}$ form indeed an orthonormal system in the subspace $\mathcal{S}^*$, such that the associated measurement $\mathbb{P}_k^{(A)}$ is projective. The completeness relation follows directly from (6.9):

$$\begin{aligned}\sum_k|\psi_k\rangle\langle\psi_k| &= \sum_k p_A(\alpha_k)(\rho^*)^{-1/2}|\alpha_k^*\rangle\langle\alpha_k^*|(\rho^*)^{-1/2}\\ &= (\rho^*)^{-1/2}\rho\,(\rho^*)^{-1/2} = \mathbb{P}_{\mathcal{S}^*}\,,\end{aligned} \tag{6.11}$$

On the contrary, the obtain the orthogonality condition $\langle\psi_j|\psi_k\rangle = \delta_{jk}$, we proceed as follows. At first, we compute the reduced (not normalized) state $|\chi_j\rangle_{A'}$ obtained after projecting the state $|\Phi\rangle\!\rangle_{AA'}$ in (6.7) onto $|\psi_j\rangle_A$, that yields the coherent state $|\alpha_j\rangle_{A'}$:

$$\begin{aligned}|\chi_j\rangle_{A'} &= {}_A\langle\psi_j|\Phi\rangle\!\rangle_{AA'}\\ &= \sqrt{p_A(\alpha_j)}\sum_n{}_A\langle\alpha_j^*|\left[(\rho^*)^{-1/2}\otimes\mathbb{1}\right]\left[(\rho^*)^{1/2}\otimes\mathbb{1}\right]|n\rangle_A|n\rangle_{A'}\\ &= \sqrt{p_A(\alpha_j)}\sum_n{}_A\langle\alpha_j^*|\,\mathbb{P}_{\mathcal{S}^*}|n\rangle_A|n\rangle_{A'}\\ &= \sqrt{p_A(\alpha_j)}\sum_n\langle n|\alpha_j\rangle|n\rangle_{A'} = \sqrt{p_A(\alpha_j)}|\alpha_j\rangle_{A'}\,.\end{aligned} \tag{6.12}$$

On the other hand, from (6.5) we get $|\chi_j\rangle_{A'} = \sum_k\sqrt{p_A(\alpha_k)}\langle\psi_j|\psi_k\rangle|\alpha_k\rangle_{A'}$, being equivalent to Eq. (6.12) iff $\langle\psi_j|\psi_k\rangle = \delta_{jk}$, thus proving the measurement vectors to form a complete orthonormal set.

Bearing this in mind, the overall state ρ_{AB} shared by Alice and Bob after propagation through the noisy channel can be written as:

$$\rho_{AB} = \left(\hat{\mathbb{1}}_A\otimes\mathcal{N}\right)\left[|\Phi\rangle\!\rangle_{AA'}\langle\!\langle\Phi|\right], \tag{6.13}$$

where, now, the CP map $\mathcal{N}$ acts on mode A', being transformed into B. In turn, the conditional output statistics at Bob's side is obtained as $p_{B|A}(x|\alpha_k) = \mathrm{Tr}[\rho_{AB}\,\mathbb{P}_k^{(A)}\otimes\Pi_x^{(B)}]$.

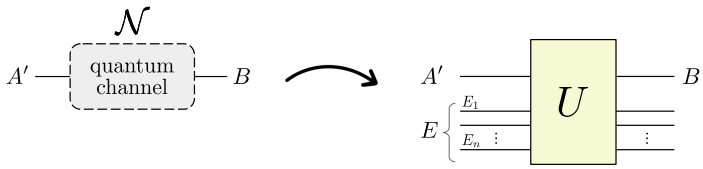


Figure 6.2.3: Unitary dilation of the channel noisy map $\mathcal{N}$, obtained according to Kraus theorem. It is described by a set of additional modes $E = (E_1, \dots, E_n)$, $n > 1$, coupled to the signal mode A' via a suitable joint unitary operation U.

6.2.3 Addressing physical layer security

As discussed along the previous lines, regardless the adopted version of the protocol, in CVQKD Alice and Bob have only access to the input ensemble $\{p_A(\alpha_k), |\alpha_k\rangle\}_k$ and the output statistics $p_{B|A}(x|\alpha_k)$, $k \in \mathcal{K}$, and $p_B(x)$. However, these quantities are not sufficient to perform full characterization of the untrusted channel $\mathcal{N}$, which remains only partially known, being, in general, described in terms of few relevant parameters to be estimated during the channel evaluation stage. As an example, in fiber-optic practical realizations (which will provide the main case study in this thesis) the quantum channel is typically described by means of a thermal-loss channel with transmissivity

$$T = 10^{-\kappa d/10}\,, \tag{6.14}$$

where d is the transmission distance in kilometers and $\kappa = 0.2$ dB/km is typical loss rate for fibers at telecom wavelength (1550 nm) [38, 191, 192, 236, 237]; and with the excess noise $\epsilon \geq 0$, introduced by realistic defects in the experimental apparatus, being of the order of $10^{-3} \div 10^{-2}$ shot-noise units [191, 192]. In particular, the excess noise is introduced both at the modulation stage, thanks to imperfect generation of the signals; during propagation, by non-idealities of the fiber support; and in the detection apparatus, e.g. arising from electronic noise, phase-mismatch between signal and local oscillator in the presence of homodyne and DH measurement, ... Equivalently, this effect can be also modeled in terms of equivalent number of thermal photons; that is by assuming a single-mode thermal bath interfering with the encoded signal mode, such that the mean photon number at the receiver's side is equal to

$$\bar{n}_{\rm rec} = T\bar{n} + \bar{n}_{\rm b}\,, \tag{6.15}$$

where $\bar{n}$ is the mean energy at transmitter, reported in (6.4), whereas $\bar{n}_{\rm b} = T\epsilon/2$ is the number of background photons added to the signal mode, resulting in excess noise equal to ϵ. We precise that the adoption of the excess noise as a figure of merit is typical in fiber-optic communications, whilst the description in terms of equivalent background photons is more common for free-space channels [206, 220].

Given these considerations, an eavesdropper may exploit Alice and Bob's incomplete knowledge to his favor, and manipulate the channel in suitable way to extract the largest amount of information without being detected by the two trusted parties. In fact, the noisy map $\mathcal{N}$ is, in general, not unique, namely, there exists different CP maps that lead to the same local statistics at the sender's and receiver's side. According to Kraus theorem, each of these maps is associated with a different unitary dilation, described by a set of additional modes $E = (E_1, \dots, E_n)$, for some $n > 1$, coupled to A' via a suitable joint unitary operation U, as schematized in Fig. 6.2.3. Then, Eve may optimize her

strategy and choose the unitary dilation that provides her with the maximum amount of information compatible with both the fundamental limits imposed by quantum mechanics and the local statistics probed by Alice and Bob, thus being completely undetected by them.

Accordingly, to address security of the protocol, we should first answer to the question: *How much is the channel untrusted?* Indeed, different assumptions on the setup would lead to different security levels, corresponding to more or less constraints on Eve's action. In light of this, we identify three main different security frameworks:

- *Unconditional security*: the channel is completely untrusted, thus Eve performs arbitrary channel manipulation, i.e. her attack implements the most-informative unitary dilation among those that preserve the local statistics at Alice and Bob's sides, without any further constraint.

- *Trusted-device scenario*: there is some level of trust in the equipment, e.g. trusted detection losses and noise. This implies that only few additional modes $(E_1, \dots, E_m)$ in $\mathbf{E}$, with $m < n$, are at Eve's disposal, whilst the remaining $n - m$ are assumed to be under Alice and Bob's control, thus reducing the set of possible eavesdropping strategies.

- *Quantum wiretap channel*: in this case, Alice and Bob hold characterization of the quantum channel, obtained thanks to either reasonable assumptions or prior information, therefore they have access to a specific noise map $\mathcal{N}$. This also establishes the channel connecting Alice to Eve in terms of the unitary dilation of $\mathcal{N}$, therefore arbitrary channel manipulation by Eve is not allowed [238, 239].

The two latest scenarios provide examples of restricted eavesdropping, being also referred in literature with the terms *practical security* or *conditional security*, as opposed to the unconditional approach. Here below we will firstly focus on the unconditional security analysis, whilst the features of restricted eavesdropping will be addressed in Chapter 7.

6.2.3.1 Unconditional security

In the unconditional security framework, Eve is unrestricted; therefore, the most powerful attack that Eve may launch is the so-called *purification attack*, where she is assumed to "purify" the state ρ_{AB} in Eq. (6.13). That is, she has full access to the unitary dilation of the noise map $\mathcal{N}$ depicted in Fig. 6.2.3, and controls all the additional modes E. Therefore, the tripartite system ABE is closed and isolated, and the state of system is a pure state $|\Psi\rangle_{ABE}$ such that $\rho_{AB} = \mathrm{Tr}_E[|\Psi\rangle_{ABE}\langle\Psi|]$ [222]. This allows to explicitly evaluate the Holevo information $\chi(B;E) = S(E) - S(E|B)$, namely the maximum amount of information extractable by Eve, where $S(E) = \mathsf{S}[\rho_E]$ is the von Neumann entropy of Eve's overall state ρ_E, and $S(E|B) = \sum_x p_B(x)\mathsf{S}[\rho_{E|x}]$, where $\rho_{E|x}$ is the conditional Eve's state related to Bob's measurement outcome x, obtained with probability $p_B(x)$.

In fact, we consider the Schmidt decomposition of the (pure) state of ABE:

$$|\Psi\rangle_{ABE} = \sum_s \sqrt{\lambda_s}\,|\varphi_s\rangle_{AB} \otimes |\varsigma_s\rangle_E\,, \tag{6.16}$$

$\lambda_s \geq 0$, and obtain the quantum states of the reduced subsystems AB and E as:

$$\rho_{AB} = \mathrm{Tr}_E \left[|\Psi\rangle_{ABE}\langle\Psi| \right] = \sum_s \lambda_s |\varphi_s\rangle_{AB}\langle\varphi_s| \,,$$
$$\rho_E = \mathrm{Tr}_{AB} \left[|\Psi\rangle_{ABE}\langle\Psi| \right] = \sum_s \lambda_s |\varsigma_s\rangle_{E}\langle\varsigma_s| \,, \tag{6.17}$$

respectively, being diagonal in the Schmidt bases [27, 222]. As a consequence, they have the same von Neumann entropy, equal to:

$$S(E) = S(AB) = -\sum_s \lambda_s \log_2 \lambda_s \,, \tag{6.18}$$

where $S(AB) = \mathsf{S}[\rho_{AB}]$.

Analogously, when Bob performs a 1-rank measurement $\Pi_x = |\pi_x\rangle_B\langle\pi_x|$, retrieving outcome x with probability $p_B(x)$, the joint conditional state of modes AE is pure and equal to $|\Xi\rangle\!\rangle_{AE|x} = {}_B\langle\pi_x|\Psi\rangle_{ABE}/\sqrt{p_B(x)}$, therefore the two reduced conditional states on modes A and E, obtaining after partial trace, are isentropic: we have $\mathsf{S}[\rho_{A|x}] = \mathsf{S}[\rho_{E|x}]$. In turn, the average conditional entropy $S(E|B) = \sum_x p_B(x)\mathsf{S}[\rho_{E|x}]$ and $S(A|B) = \sum_x p_B(x)\mathsf{S}[\rho_{A|x}]$ are equal, i.e. $S(E|B) = S(A|B)$. We note that the choice of a 1-rank measurement is not too restrictive, as in practical realizations one often deals with homodyne or DH detection. We conclude that, for a given channel map $\mathcal{N}$,

$$\begin{aligned} \chi(B;E) &= S(E) - S(E|B) \\ &= S(AB) - S(A|B) \,, \end{aligned} \tag{6.19}$$

completely characterizing Eve's information in terms of the state ρ_{AB} shared by Alice and Bob and reported in (6.13). However, in the unconditional security approach, we remind that Alice and Bob do not perform characterization state ρ_{AB}, but have only limited information on it, arising from the statistics $p_A(\alpha_k)$, $p_{B|A}(x|\alpha_k)$, and $p_B(x)$, respectively. Accordingly, there exists different states ρ_{AB}, or, equivalently, different channel CP maps $\mathcal{N}$, leading to the same statistics, and the KGR is obtained by performing optimization over all the possible CP maps that preserve these local statistics at Alice's and Bob's side, namely:

$$K_{\mathrm{DW}} = \beta I(A;B) - \sup_{\mathcal{N}:A'\to B} \chi(B;E) \,, \tag{6.20}$$

referred to as the *Devetak-Winter bound* (DW) [240], where $\beta \leq 1$ is the reconciliation efficiency.

6.3 The GG02 protocol

We now introduce the GG02 protocol, being the first seminal CVQKD protocol, proposed by Grosshans and Grangier in 2002 and proving the benchmark for all the subsequent progress in the field [14, 175–177].

The scheme of the protocol in its PM version is reported in Fig. 6.3.1(a). Here, Alice implements Gaussian modulation of coherent states; that is, in each repetition of the protocol, she generates a coherent state $|x_A + iy_A\rangle$, where the variables $z = x_A, y_A$ are

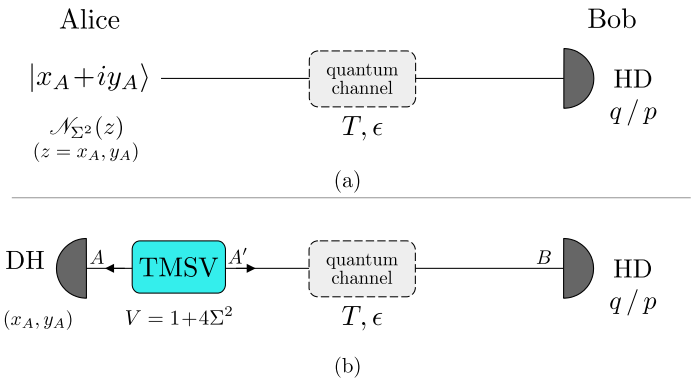


Figure 6.3.1: Scheme of the GG02 protocol both in the PM (a) and EB version (b). In the PM protocol, Alice generates a random coherent state $|x_A + iy_A\rangle$, where the amplitudes $z = x_A, y_A$ are drawn from a normal distribution $\mathcal{N}_{\Sigma^2}(z)$ with variance Σ^2. Instead, in the EB scheme the signal generation is obtained by performing DH detection on the first branch of a TMSV with modulation variance $V = 1 + 4\Sigma^2$; when she retrieves the outcome (x_A, y_A), the second arm is projected onto a coherent state with amplitude proportional to $x_A + iy_A$.

(independently) sampled from the normal distribution:

$$\mathcal{N}_{\Sigma^2}(z) = \frac{e^{-z^2/(2\Sigma^2)}}{\sqrt{2\pi\Sigma^2}}\,, \qquad z = x_A, y_A\,, \tag{6.21}$$

with zero mean and variance $\Sigma^2 \geq 0$, such that the probability of preparing a coherent state with amplitude $x_A + iy_A$ reads $p_A(x_A, y_A) = \mathcal{N}_{\Sigma^2}(x_A)\mathcal{N}_{\Sigma^2}(y_A)$. The overall statistical mixture generated by Alice then reads:

$$\begin{aligned}\rho &= \int_{\mathbb{R}^2} dx_A dy_A\, p_A(x_A, y_A)\, |x_A + iy_A\rangle\langle x_A + iy_A| \\ &= \frac{1}{1+2\Sigma^2} \sum_{n=0}^{\infty} \left(\frac{2\Sigma^2}{1+2\Sigma^2}\right)^n |n\rangle\langle n| \\ &= \nu^{\rm th}(2\Sigma^2)\,,\end{aligned} \tag{6.22}$$

corresponding to a thermal state with $\bar{n} = 2\Sigma^2$ mean photons. The encoded signals are then injected into the untrusted quantum channel, described as a thermal-loss channel with transmissivity $T \leq 1$ and excess noise $\epsilon \geq 0$, until to reach Bob, who performs Gaussian detection on his received pulses, either homodyne detection of a random quadrature chosen between q and p, as in the original proposal [14], or DH detection, as in the no-switching scheme proposed in [200]. In the following we will follow the original proposal and, thanks to the symmetry of the modulation scheme with respect to both quadratures, we safely assume that Bob always homodynes quadrature q. The DH protocol leads to analogous results. Given this considerations, the conditional probability that Bob obtains outcome x_B, measuring q, when Alice sent the state $|x_A + iy_A\rangle$ reads:

$$p_{B|A}(x_B|x_A) = \frac{\exp\left[-(x_B - 2\sqrt{T}x_A)^2/(2(1+T\epsilon))\right]}{\sqrt{2\pi(1+T\epsilon)}}\,, \tag{6.23}$$

expressed in shot-noise units (SNU), which will be always considered thereafter. As we can see, $p_{B|A}(x_B|x_A)$ is independent of y_A. Accordingly, the overall distribution probed by Bob reads:

$$\begin{aligned} p_B(x_B) &= \int_{\mathbb{R}} dx_A \, \mathcal{N}_{\Sigma^2}(x_A) \, p_{B|A}(x_B|x_A) \\ &= \frac{\exp\left[-x_B^2/(2\Sigma_B^2)\right]}{\sqrt{2\pi\Sigma_B^2}} \end{aligned} \tag{6.24}$$

where $\Sigma_B^2 = 1 + T(4\Sigma^2 + \epsilon) = 1 + T(2\bar{n} + \epsilon)$. We underline that all the probed statistics, corresponding to Alice's modulation and Bob's detection, are Gaussian: an important property that will be useful for the security analysis. Given the probability distributions (6.21), (6.23), and (6.24), we evaluate the mutual information by recalling that the Shannon entropy of a Gaussian distribution $\mathcal{G}(\mu, \sigma^2)$ with mean μ and variance σ^2 is equal to $\mathsf{H}[\mathcal{G}(\mu, \sigma^2)] = \log_2(2\pi e\sigma^2)/2$. In turn, we get:

$$\begin{aligned} I_{\mathrm{GG}}(A;B) &= H(B) - H(B|A) \\ &= \frac{1}{2}\log_2\left(1 + \frac{2T\bar{n}}{1+T\epsilon}\right), \end{aligned} \tag{6.25}$$

which coincides with the Shannon capacity for the signal-to-noise ratio (SNR):

$$\mathrm{SNR} = \frac{2T\bar{n}}{1+T\epsilon}, \tag{6.26}$$

whose numerator represents the mean signal power, proportional to the mean number of photons at the receiver's side, while the denominator provides the added noise on quadratures in SNU, equal to $1 + T\epsilon$.

Equivalently, we design the EB version of the protocol, by considering a purification of state (6.22), provided by the two-mode squeezed vacuum state (TMSV):

$$|\mathrm{TMSV}\rangle\!\rangle_{AA'} = \sqrt{1-\lambda^2}\sum_{n=0}^{\infty}\lambda^n|n\rangle|n\rangle, \tag{6.27}$$

where $\lambda = \sqrt{(V-1)/(V+1)}$, $V = 1+2\bar{n} = 1+4\Sigma^2$ being the modulation variance [176, 222]. Then, Alice performs DH measurement on mode A, described as a 1-rank projection onto the coherent state $|\alpha\rangle_A$, where $\alpha = x_A + iy_A$; when she obtains the outcomes (x_A, y_A), the branch A' is projected onto a coherent state, as

$${}_A\langle\alpha|\mathrm{TMSV}\rangle\!\rangle_{AA'} \propto |\lambda\,\alpha\rangle_{A'}. \tag{6.28}$$

This guarantees the equivalence with the PM scheme, provided that Alice rescales her outcomes by a constant factor λ. The scheme of the EB protocol is displayed in Fig. 6.3.1(b).

6.3.1 Unconditional security

To assess unconditional security, we underline that in the GG02 protocol all the statistics probed by Alice and Bob are Gaussian. As a consequence, the quantum channel has also to be Gaussian; otherwise some non-Gaussianity introduced throughout signal propagation would be registered at the receiver's side. This imposes a constraint on the possible

eavesdropping strategies by Eve, being limited to implement a Gaussian purification attack; making it straightforward to compute the DW (6.20), as no optimization over all channel maps $\mathcal{N}$ yielding Alice's and Bob's statistics is required.

Then, approaching the problem in the EB description, we start by considering the covariance matrix (CM) of Alice's TMSV state, namely:

$$\boldsymbol{\sigma}_{AA'} = \begin{pmatrix} V\,\mathbb{1}_2 & Z\,\boldsymbol{\sigma}_z \\ Z\,\boldsymbol{\sigma}_z & V\,\mathbb{1}_2 \end{pmatrix}, \tag{6.29}$$

where $Z = \sqrt{V^2-1}$, $\mathbb{1}_2$ is a 2×2 identity matrix and $\boldsymbol{\sigma}_z$ is the Pauli z-matrix [31, 33]. Thereafter, mode A' is injected into the thermal-loss channel, with associated transmissivity $T \leq 1$ and thermal noise $\bar{n}_T = T\epsilon/(2(1-T))$, described via a Gaussian completely positive (CP) map associated with the matrices [31]:

$$X_{\rm TL} = \sqrt{T}\,\mathbb{1}_2 \quad \text{and} \quad Y_{\rm TL} = (1-T)(1+2\bar{n}_T)\mathbb{1}_2\,. \tag{6.30}$$

Ultimately, the state ρ_{AB} shared by Alice and Bob is a Gaussian state with zero first moments and CM $\boldsymbol{\sigma}_{AB} = (\mathbb{1}_2 \oplus X_{\rm TL})\boldsymbol{\sigma}_{AA'}(\mathbb{1}_2 \oplus X_{\rm TL})^{\intercal} + (\mathbf{0} \oplus Y_{\rm TL})$, $\mathbf{0}$ being the null 2×2 matrix. Straightforward calculations lead to:

$$\boldsymbol{\sigma}_{AB} = \begin{pmatrix} \boldsymbol{\sigma}_A & \boldsymbol{\sigma}_Z \\ \boldsymbol{\sigma}_Z^{\intercal} & \boldsymbol{\sigma}_B \end{pmatrix} = \begin{pmatrix} V\,\mathbb{1}_2 & \sqrt{T}Z\,\boldsymbol{\sigma}_z \\ \sqrt{T}Z\,\boldsymbol{\sigma}_z & T(V+\chi)\,\mathbb{1}_2 \end{pmatrix}, \tag{6.31}$$

where

$$\chi = \frac{1-T}{T} + \epsilon \tag{6.32}$$

provides the total added noise on quadratures, due to both the vacuum and the thermal excess noise contributions.

We also note that Eq. (6.25) can be re-derived as follows. Alice and Bob performs Gaussian detection on their local modes, namely DH and homodyne of q, being associated with the CMs:

$$\boldsymbol{\sigma}_A^{(\rm m)} = \mathbb{1}_2 \quad \text{and} \quad \boldsymbol{\sigma}_B^{(\rm m)} = \lim_{z\to 0}\begin{pmatrix} z & 0 \\ 0 & z^{-1} \end{pmatrix}, \tag{6.33}$$

respectively. In turn, the mutual information between Alice and Bob is obtained directly from (6.31) as:

$$I_{\rm GG}(A;B) = \frac{1}{2}\log_2\left\{\frac{\det\left[\boldsymbol{\sigma}_A + \boldsymbol{\sigma}_A^{(\rm m)}\right]\det\left[\boldsymbol{\sigma}_B + \boldsymbol{\sigma}_B^{(\rm m)}\right]}{\det\left[\boldsymbol{\sigma}_{AB} + (\boldsymbol{\sigma}_A^{(\rm m)} \oplus \boldsymbol{\sigma}_B^{(\rm m)})\right]}\right\} \tag{6.34}$$

$$= \frac{1}{2}\log_2\left[1 + \frac{T(V-1)}{1+T\epsilon}\right]. \tag{6.35}$$

Furthermore, the Holevo information $\chi(B;E) = S(AB) - S(A|B)$ can be also retrieved from the CM (6.31), by exploiting the tools of the Gaussian formalism. In fact, the von Neumann entropy of the (Gaussian) state ρ_{AB} depends only on its CM and reads:

$$S(AB) = h\left(\frac{\mathrm{d}_1 - 1}{2}\right) + h\left(\frac{\mathrm{d}_2 - 1}{2}\right), \tag{6.36}$$

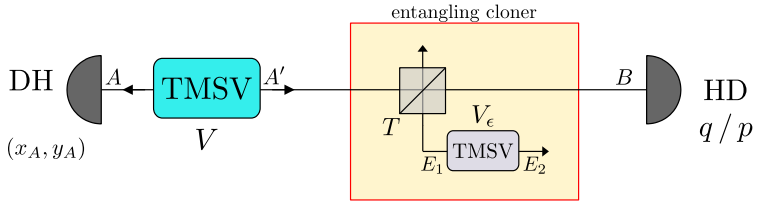


Figure 6.3.2: Schematic description of the entangling cloner attack, performed in the GG02 protocol. Eve replaces the quantum channel by a lossless channel where she inserts a beam splitter with transmissivity T. To mimic the presence of the excess noise, she generates a TMSV with variance $V_\epsilon = 1 + 2\bar{n}_T$ on two modes $\boldsymbol{E} = (E_1, E_2)$ and lets Alice's signal mode A' interfere with E_1 at the beam splitter. Then, she keeps the reflected beam for herself while sending the transmitted one to Bob. This scheme allows her to be undetected from Alice and Bob, as performing partial trace over modes $\boldsymbol{E}$ yields a thermal-loss channel CP map.

where

$$h(x) = (x+1)\log_2(x+1) - x\log_2 x\,, \tag{6.37}$$

and

$$\mathrm{d}_{1(2)} = \sqrt{\frac{\Delta \pm \sqrt{\Delta^2 - 4I_4}}{2}}\,, \tag{6.38}$$

being the symplectic eigenvalues of $\boldsymbol{\sigma}_{AB}$, with $I_{1(2)} = \det(\boldsymbol{\sigma}_{A(B)})$, $I_3 = \det(\boldsymbol{\sigma}_Z)$, $I_4 = \det(\boldsymbol{\sigma}_{AB})$ and $\Delta = I_1 + I_2 + 2I_3$. Moreover, the conditional state of Alice $\rho_{A|x_B}$ given Bob's outcome x_B is still a Gaussian state with CM:

$$\boldsymbol{\sigma}_{A|B} = \boldsymbol{\sigma}_A - \boldsymbol{\sigma}_Z\left[\boldsymbol{\sigma}_B + \boldsymbol{\sigma}_B^{(\mathrm{m})}\right]^{-1}\boldsymbol{\sigma}_Z^{\mathsf{T}} \tag{6.39}$$

$$= \begin{pmatrix} V - \frac{V^2-1}{V+\chi} & 0 \\ 0 & V \end{pmatrix}, \tag{6.40}$$

being independent of x_B, thus $S(A|B) = h((\mathrm{d}_3 - 1)/2)$, where $d_3 = \sqrt{\det(\boldsymbol{\sigma}_{A|B})}$. Accordingly, Eve's Holevo information writes:

$$\chi_{\mathrm{GG}}(B;E) = h\left(\frac{\mathrm{d}_1 - 1}{2}\right) + h\left(\frac{\mathrm{d}_2 - 1}{2}\right) - h\left(\frac{\mathrm{d}_3 - 1}{2}\right)\,. \tag{6.41}$$

As demonstrated in [222], the optimal purification eavesdropping strategy is practically implemented by the so-called *entangling cloner attack*, introduced by Weedbrook *et al.* in [241] and displayed in Fig. 6.3.2. It represents an active eavesdropping strategy, allowing Eve to mimic the effect of the channel losses and excess noise. In more detail, Eve replaces the quantum channel by a lossless channel where she inserts a beam splitter with transmissivity T. She prepares a TMSV with variance $V_\epsilon = 1+2\bar{n}_T = 1+T\epsilon/(1-T)$ on two modes $\boldsymbol{E} = (E_1, E_2)$ and lets Alice's signal mode A' interfere with E_1 at the beam splitter. Then, she keeps the reflected beam for herself while sending the transmitted one to Bob. In this way, when Alice generates a coherent state $|x_A + iy_A\rangle$, Bob will receive a

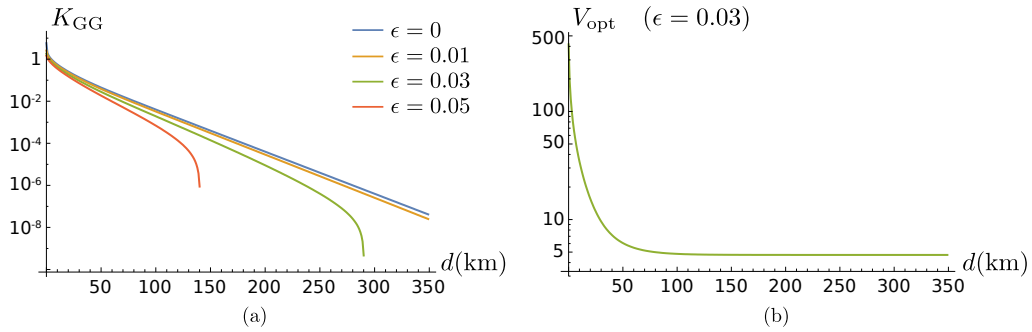


Figure 6.3.3: (a) Log plot of the KGR $K_{\rm GG}$ as a function of the transmission distance d in km for different values of the excess noise. For $\epsilon > 0$ there exists a maximum transmission distance $d_{\max}$ after which the KGR drops to 0. (b) Log plot of the optimized modulation variance $V_{\rm opt}$ for the GG02 protocol as a function of d for $\epsilon = 0.03$. In both the pictures we set the reconciliation efficiency $\beta = 0.95$ and the loss rate $\kappa = 0.2$ dB/km.

displaced thermal state, with displacement amplitude $\sqrt{T}(x_A + iy_A)$ and mean number of thermal photons equal to $T\epsilon/2$, leading to the same results of a thermal-loss channel with parameters (T, ϵ) *in the absence of eavesdropper*. Thereby, the entangling cloner attack allows Eve to hide herself behind the channel losses and noise, being completely undetected by Alice and Bob.

Given this considerations, we obtain the KGR associated with the GG02 scheme as

$$K_{\rm GG} = \max_{V} \Big\{ \beta I_{\rm GG}(A;B) - \chi_{\rm GG}(B;E) \Big\}, \tag{6.42}$$

where we perform optimization over the modulation variance V for fixed realistic values of reconciliation efficiency $\beta = 0.95$, loss rate $\kappa = 0.2$ dB/km, and channel excess noise ϵ [162, 210, 223].

Plots of the resulting KGR as a function of the transmission distance d in km is reported in Fig. 6.3.3(a). As demonstrated in [14, 177, 222], in the absence of excess noise, $\epsilon = 0$, and for unit reconciliation efficiency $\beta = 1$, the KGR is $K_{\rm GG} > 0$ for all $d \geq 0$, allowing to share secret keys at arbitrary large distances. Otherwise, as we can see from the plot, when $\epsilon > 0$, $K_{\rm GG}$ is positive up to a maximum transmission distance $d_{\max}$, i.e. $K_{\rm GG} > 0$ for $d \leq d_{\max}$, after which the KGR drops to 0 and no secure communication is possible. The resulting maximum transmission distance $d_{\max}$ is then a function of both the excess noise ϵ and the reconciliation efficiency β, i.e. $d_{\max} = d_{\max}(\epsilon, \beta)$. In particular, for $\beta = 0.95$ and $\epsilon = 0.03$ ($\epsilon = 0.05$), we have $d_{\max} \approx 290$ km ($d_{\max} \approx 140$ km).

For completeness, in Fig. 6.3.3(b), we also show the optimized input modulation $V_{\rm opt}$, being a decreasing function of d, that, differently from the KGR, is only weakly dependent on the excess noise value ϵ.

Finally, another relevant figure of merit to evaluate the performance of the protocol is the maximum tolerable excess noise $\epsilon_{\max}$, being a decreasing function of the transmission distance d, as depicted in Fig. 6.3.4. It represents the maximum value of ϵ for which the KGR is positive. That is, at the distance d the KGR is positive as long as $\epsilon < \epsilon_{\max}$.

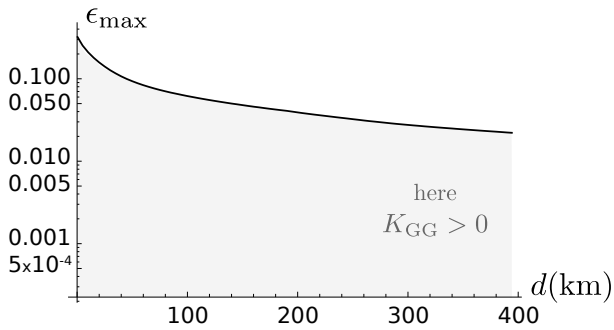


Figure 6.3.4: Log plot of the maximum tolerable excess noise $\epsilon_{\max}$ for the GG02 protocol as a function of the distance d in km. The shaded area, corresponding with the undergraph of $\epsilon_{\max}$, represents the region where $K_{\rm GG} > 0$. We set the reconciliation efficiency $\beta = 0.95$.

6.4 The optimality of Gaussian attacks

The GG02 protocol provides the cornerstone example of CVQKD, representing the benchmark for all other proposals of possible protocols. Moreover, its security analysis can be easily carried out, since the protocol involves only Gaussian resources: a particular feature that, indirectly, constrains Eve to implement Gaussian attacks, i.e. the entangling cloner. However, in more general schemes, non-Gaussian elements may be introduced, e.g. non-Gaussian modulation of coherent states at Alice's side, or non-Gaussian channels, in which case the statistics probed by Alice and Bob are not sufficient to characterize the quantum state ρ_{AB} shared by them in the EB protocol, making it hard to compute the DW. In fact, in these conditions, the DW should be evaluated by optimization over all possible channel quantum CP maps compatible with the probed statistics.

A convenient solution is to look for simpler suitable bounds, upper bounding Eve's Holevo information and, accordingly, providing a lower bound on the DW, and a sufficient condition to establish unconditional security. Following this outline, a fundamental result is the so-called "*optimality of Gaussian attacks*" theorem, being independently proved in 2006 with different methods by both Navascués *et al.* [178] and García-Patrón and Cerf [179, 180]. In particular, provided Bob's measurement to be Gaussian, the theorem establish an upper bound on Eve's information by the Holevo information of the Gaussian state having the same first and second momenta of the quantum state ρ_{AB} in (6.13). The resort to Gaussian formalism leads to a simple lower bound on the DW, being useful to assess security in protocols adopting either non-Gaussian modulation by Alice or propagation through non-Gaussian channels.

Here, we prove the theorem following Navascués approach [178], which exploits the extremality properties of Gaussian states and operations. On the contrary, the equivalent proof developed by García-Patrón and Cerf in [179, 180] involves theorems from functional analysis, being more technical, and, therefore, it is hard to provide a physical interpretation.

To begin with, in the following subsection we derive some fundamental results that will be exploited throughout the proof.

6.4.1 Theoretical framework

Let us now consider an arbitrary quantum state ϱ of a physical system A, being a quantum operator over a Hilbert space $\mathcal{H}$, and let $F : \mathcal{B}(\mathcal{H}) \to \mathbb{C}$ be a functional over the set of Hermitian operators $\mathcal{B}(\mathcal{H})$. We now introduce the state $\varrho_{\rm G}$ as the Gaussian state having the same first moments and CM as ϱ. If F is the value of some quantity computed for state ϱ and $F_{\rm G}$ the corresponding value related to state $\varrho_{\rm G}$, we define the difference:

$$\Delta F \equiv F_{\rm G} - F \,. \tag{6.43}$$

To prove the optimality of Gaussian attacks it is useful to state the following lemmas. The first lemma involves the average conditional entropy.

Lemma 6.1. *Let $\{\Pi_x\}_x$ be a positive-operator valued measurement (POVM) performed on a system A and associated with a classical register X, such that $\Pi_x = M_x^\dagger M_x$ and $\sum_x \Pi_x = \hat{\mathbb{1}}$. Let $p(x) = \mathrm{Tr}[\varrho \Pi_x]$ and $\varrho_{|x} = M_x \varrho M_x^\dagger / p(x)$ be the probability of retrieving outcome x and the corresponding conditional state of A, respectively. Then, the average conditional entropy $S(A|X) = \sum_x p(x) S(\varrho_{|x})$ is equal to:*

$$S(A|X) = S(\overline{AX}) - H(X) \,, \tag{6.44}$$

where $S(\overline{AX})$ is the von Neumann entropy of the state

$$R_{AX} = \sum_x p(x) \varrho_{|x} \otimes |x\rangle\langle x| \,, \tag{6.45}$$

$|x\rangle$ being the (classical) state of register X associated with outcome x, and $H(X) = -\sum_x p(x) \times \log_2 p(x)$ is the Shannon entropy of the distribution $p(x)$.

Proof. To prove Eq. (6.44), we should compute the von Neumann entropy of state R_{AX}, namely $S(\overline{AX}) = -\,\mathrm{Tr}\,[R_{AX} \log_2 R_{AX}]$. To begin with, we evaluate the operator

$$\mathcal{R} = \log_2 R_{AX} = \log_2 \left(\sum_x \widetilde{\varrho}_{|x} \otimes |x\rangle\langle x| \right) . \tag{6.46}$$

with $\widetilde{\varrho}_{|x} = p(x) \varrho_{|x}$. For given x, we consider the spectral decomposition $\widetilde{\varrho}_{|x}$, equal to $\widetilde{\varrho}_{|x} = \sum_j \lambda_j(x) |\phi_j(x)\rangle\langle\phi_j(x)|$, with $\lambda_j(x) \geq 0$ and $\{|\phi_j(x)\rangle\}_j$ being a complete orthonormal system. Then, state R_{AX} becomes:

$$R_{AX} = \sum_x \sum_j \lambda_j(x) |\phi_j(x)\rangle\langle\phi_j(x)| \otimes |x\rangle\langle x| \,. \tag{6.47}$$

We note that Eq. (6.47) corresponds to the spectral decomposition of R_{AX}, provided a suitable reordering of the indices j and x. Therefore, we straightforwardly obtain the spectral decomposition of $\mathcal{R}$ as:

$$\begin{aligned} \mathcal{R} &= \sum_x \underbrace{\sum_j \log_2 \left(\lambda_j(x)\right) |\phi_j(x)\rangle\langle\phi_j(x)|}_{\equiv \log \widetilde{\varrho}_{|x}} \otimes |x\rangle\langle x| \\ &= \sum_x \log_2 \widetilde{\varrho}_{|x} \otimes |x\rangle\langle x| \,. \end{aligned} \tag{6.48}$$

As a consequence, the von Neumann entropy $S(\overline{AX})$ is equal to:

$$\begin{aligned} S(\overline{AX}) &= -\operatorname{Tr}\left[R_{AX}\log_2 R_{AX}\right] \\ &= -\operatorname{Tr}_{AX}\left\{\left(\sum_y p(y)\varrho_{|y}\otimes|y\rangle\langle y|\right)\left[\sum_x \log_2\left(p(x)\varrho_{|x}\right)\otimes|x\rangle\langle x|\right]\right\}, \end{aligned} \tag{6.49}$$

where the trace is performed over both systems A and X. At first, we perform partial trace over X, obtaining:

$$\begin{aligned} S(\overline{AX}) &= -\sum_x\sum_y p(y)\operatorname{Tr}_A\left\{\varrho_{|y}\log_2\left(p(x)\varrho_{|x}\right)|\langle y|x\rangle|^2\right\} \\ &= -\sum_x p(x)\operatorname{Tr}_A\left\{\varrho_{|x}\log_2\left(p(x)\varrho_{|x}\right)\right\} \\ &= -\sum_x p(x)\operatorname{Tr}_A\{\varrho_{|x}\left(\log_2 p(x)+\log_2\varrho_{|x}\right)\} \\ &= -\sum_x p(x)\log_2 p(x)\underbrace{\operatorname{Tr}_A\{\varrho_{|x}\}}_{=1} - \sum_x p(x)\underbrace{\operatorname{Tr}_A\{\varrho_{|x}\log_2\varrho_{|x}\}}_{=S[\varrho_{|x}]} \\ &= H(X)+S(A|X), \end{aligned} \tag{6.50}$$

$H(X)$ being the Shannon entropy of $p(x)$. In turn, we have $S(A|X)=S(\overline{AX})-H(X)$. Moreover, in the second line we used the property $\langle x|y\rangle=\delta_{xy}$, being valid since the register states are classical and, thus, distinguishable. □

The second lemma introduces the relation between $\Delta S(A)$, namely, the difference between the von Neumann entropies of $\varrho_{\rm G}$ and ϱ, see Eq. (6.43), and their relative entropy.

Lemma 6.2. *For any quantum state ϱ of a system A, we have*

$$\Delta S(A)=S(\varrho\parallel\varrho_{\rm G}) \quad \textit{and} \quad S(\varrho\parallel\varrho_{\rm G})\geq 0, \tag{6.51}$$

where $S(\varrho\parallel\varrho_{\rm G})=\operatorname{Tr}[\varrho\log_2\varrho]-\operatorname{Tr}[\varrho\log_2\varrho_{\rm G}]$ is the relative von Neumann entropy.

Proof. We re-express the quantity $\Delta S(A)=S_{\rm G}(A)-S(A)=-\operatorname{Tr}[\varrho_{\rm G}\log\varrho_{\rm G}]+\operatorname{Tr}[\varrho\log\varrho]$ as $\Delta S(A)=S(\varrho\parallel\varrho_{\rm G})+\Delta$, where

$$\Delta=\operatorname{Tr}[(\varrho-\varrho_{\rm G})\log_2\varrho_{\rm G}]. \tag{6.52}$$

We remind that any n-mode Gaussian state can be written as a Gibbs state in the quadrature vector operators $\hat{\mathbf{r}}=(q_1,p_1,q_2,p_2,\ldots,q_n,p_n)^{\mathsf{T}}$. That is, $\varrho_{\rm G}=\exp(-\zeta\hat{\mathbb{H}})/\mathcal{Z}$, with $\zeta>0$, $\mathcal{Z}=\operatorname{Tr}[\exp(-\zeta\hat{\mathbb{H}})]$, and $\hat{\mathbb{H}}=\hat{\mathbf{r}}^{\mathsf{T}}\mathbf{d}+\hat{\mathbf{r}}^{\mathsf{T}}\mathbb{H}\hat{\mathbf{r}}/2$, for some displacement vector $\mathbf{d}\in\mathbb{R}^{2n}$ and $2n\times 2n$ symmetric matrix $\mathbb{H}\in\operatorname{Sym}(2n)$ [31]. In turn, we have $\log_2\varrho_{\rm G}=-\log_2\mathcal{Z}-\zeta\hat{\mathbb{H}}$, being a polynomial operator of the second order in the canonical variables $\{q_k,p_k\}_k$. This, together with the fact that, by construction, ϱ and $\varrho_{\rm G}$ share the same CM, leads to $\Delta=\operatorname{Tr}[(\varrho-\varrho_{\rm G})\log_2\varrho_{\rm G}]=0$. Ultimately, we have $\Delta S(A)=S(\varrho\parallel\varrho_{\rm G})$. □

We remark that, since the relative entropy is a non-negative quantity, Lemma 6.2 implies that the state of maximal entropy for fixed first moments and CM is Gaussian.

With analogous methods the lemma can be also proved for probability distributions $p(x)$, $x \in \mathcal{X}$. That is:

$$\Delta H(X) = H(p \parallel p_{\mathrm{G}}) \geq 0\,, \tag{6.53}$$

where $p_{\mathrm{G}}(x)$ is the Gaussian distribution having the same FM and CM as $p(x)$, and $H(p \parallel p_{\mathrm{G}}) = \sum_x p(x) \log_2 \left(p(x)/p_{\mathrm{G}}(x)\right)$ is the Shannon relative entropy [242].

Finally, the last lemma follows from the monotonicity of quantum relative entropy, firstly proved by Lindblad [26, 243].

Lemma 6.3. *For any Gaussian CPTP map $\mathcal{E}_{\mathrm{G}}$ acting the system A, one has:*

$$\Delta S(A) \geq \Delta S\big(\mathcal{E}_{\mathrm{G}}(A)\big)\,, \tag{6.54}$$

and $\Delta S(A) = \Delta S\big(\mathcal{E}_{\mathrm{G}}(A)\big)$ iff the state of A is Gaussian.

Proof. Lemma 6.3 follows from the monotonicity of the quantum relative entropy: that is, for any two states ϱ_1 and ϱ_2 and any quantum CP map $\mathcal{E}$, we have:

$$S(\varrho_1 \parallel \varrho_2) \geq S\left(\mathcal{E}(\varrho_1) \parallel \mathcal{E}(\varrho_2)\right)\,. \tag{6.55}$$

If $\mathcal{E} = \mathcal{E}_{\mathrm{G}}$ is a Gaussian map and ϱ is an arbitrary quantum state of system A, the choices $\varrho_1 = \varrho$ and $\varrho_2 = \varrho_{\mathrm{G}}$, together with Lemma 6.2, imply that:

$$\Delta S(A) \geq S\left(\mathcal{E}_{\mathrm{G}}(\varrho) \parallel \mathcal{E}_{\mathrm{G}}(\varrho_{\mathrm{G}})\right)\,. \tag{6.56}$$

To conclude the proof, we should demonstrate that the state $\Xi' = \mathcal{E}_{\mathrm{G}}(\varrho_{\mathrm{G}})$ is indeed the Gaussian state associated with $\Xi = \mathcal{E}_{\mathrm{G}}(\varrho)$, that is $\Xi_{\mathrm{G}} = \Xi'$. To this aim, we approach the problem in the Heisenberg picture and consider the input-output relations associated with $\mathcal{E}_{\mathrm{G}}$. At first, we remind that any open Gaussian dynamics can be retrieved from a Gaussian interaction with a Gaussian environment, having null first moments and CM $\boldsymbol{\sigma}_E$, and being thereafter traced out [31]. In turn, if $\hat{\mathbf{r}}_{\mathrm{in(out)}}$ are the input (output) quadrature operators of the channel, we have:

$$\hat{\mathbf{r}}_{\mathrm{out}} = \mathsf{X}\,\hat{\mathbf{r}}_{\mathrm{in}} + M\hat{\mathbf{r}}_E \quad \text{and} \quad \mathsf{Y} = M\boldsymbol{\sigma}_E M^{\mathsf{T}} \tag{6.57}$$

where $\hat{\mathbf{r}}_E$ is the quadrature vector operator of the environmental modes, and X and Y are the matrices describing the evolution of first and second momenta under $\mathcal{E}_{\mathrm{G}}$, see Sec. 2.3.1 [31]. Given these considerations, we evaluate the first moments and CM of state Ξ as: Then, the first moments and CM of state Ξ read:

$$\mathbf{R}_{\Xi} = \langle \hat{\mathbf{r}}_{\mathrm{out}} \rangle = \mathsf{X}\,\mathbf{R}_{\varrho}\,, \tag{6.58a}$$

$$\boldsymbol{\sigma}_{\Xi} = \frac{1}{2}\langle \{\hat{\mathbf{r}}_{\mathrm{out}}, \hat{\mathbf{r}}_{\mathrm{out}}^{\mathsf{T}}\}\rangle - \mathbf{R}_{\Xi}\mathbf{R}_{\Xi}^{\mathsf{T}} = \mathsf{X}\boldsymbol{\sigma}_{\varrho}\mathsf{X}^{\mathsf{T}} + \mathsf{Y}\,, \tag{6.58b}$$

where $\mathbf{R}_{\varrho}$ and $\boldsymbol{\sigma}_{\varrho}$ are the first moments and CM of the input state ϱ. Analogous results can be obtained for state Ξ', provided the substitution $\varrho \to \varrho_{\mathrm{G}}$. However, by construction $\mathbf{R}_{\varrho_{\mathrm{G}}} = \mathbf{R}_{\varrho}$ and $\boldsymbol{\sigma}_{\varrho_{\mathrm{G}}} = \boldsymbol{\sigma}_{\varrho}$, thus, we conclude that $\Xi_{\mathrm{G}} = \Xi'$. □

6.4.2 Proving Gaussian optimality

The preliminary results derived above allow us to rephrase the scheme of a general CVQKD protocol in more precise fashion, as schematized in Fig. 6.4.1. We start from

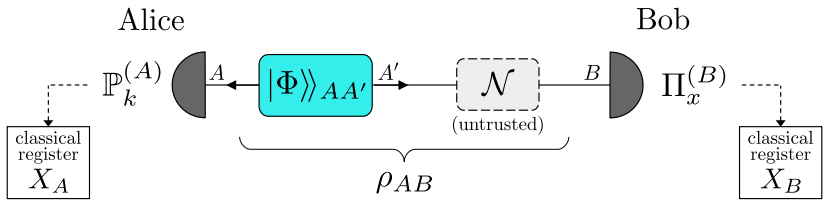


Figure 6.4.1: Extended scheme of the EB version of a general CVQKD protocol, adopted for the proof of the optimality of Gaussian attacks. Differently than Fig. 6.2.2, we now expand the protocol description and include the two classical registers $X_{A(B)}$ in which Alice and Bob store the results of the quantum measurement performed on the first and second branch of the state $\rho_{AB} = (\hat{\mathbb{1}}_A \otimes \mathcal{N})[|\Phi\rangle\!\rangle_{AA'}\langle\!\langle\Phi|]$, respectively.

the EB protocol depicted in Fig. 6.2.2, and widely discussed in Sec.s 6.2.2 and 6.2.3.1, in which Alice holds an entangled pure state $|\Phi\rangle\!\rangle_{AA'}$ and sends branch A' to Bob, such that the two parties eventually share the state ρ_{AB} in Eq. (6.13). Then, following Lemma 6.1, we construct an extended scheme of the previous EB picture, in which the classical outcomes of Alice's and Bob's measurements are stored in a classical register $X_{A(B)}$, respectively. This description provides explicit modeling of the quantum-to-classical decoding induced by the performed quantum measurements but, as a matter of fact, it only represents a technicality that does not change the amount of information shared by the parties. Within this approach, we rewrite the mutual information shared by Alice and Bob as $I(A;B) = H(X_A) + H(X_B) - H(X_AX_B)$, where $H(\cdot)$ is the Shannon entropy associated with the classical variables $X_{A(B)}$. Similarly, the Holevo information shared by Bob and Eve becomes $\chi(B;E) = S(E) - S(E|X_B)$, where $S(E)$ is the von Neumann entropy of the overall state in Eve's hands, and $S(E|X_B)$ is the average conditional entropy of Eve related to Bob's measurement outcomes, being stored in register X_B.

We are now ready prove the Gaussian optimality theorem.

Theorem 6.1. (Optimality of Gaussian attacks) *Provided Bob's measurement to be Gaussian, for any state ρ_{AB}, the Holevo information $\chi(B;E)$ is upper bounded by:*

$$\chi(B;E) \leq \chi_{\mathrm{G}}(B;E)\,, \tag{6.59}$$

where $\chi_{\mathrm{G}}(B;E)$ is the Holevo information computed for the Gaussian state having the same CM as ρ_{AB}.

Proof. At first, following the purification argument adopted in Eq. (6.19), we re-express Eve's information as $\chi(B;E) = S(E) - S(E|X_B) = S(AB) - S(AB|X_B)$. To prove the theorem, we focus on the quantity $\Delta\chi(B;E)$, see (6.43). Then, we have:

$$\begin{aligned}\Delta\chi(B;E) &= \chi_{\mathrm{G}}(B;E) - \chi(B;E)\\ &= \Delta S(AB) - \Delta S(AB|X_B)\\ &= \Delta S(AB) - \Delta S\left(\overline{ABX_B}\right) + \Delta H(X_B)\end{aligned} \tag{6.60}$$

where we used Lemma 6.1 to get the last equality. Since the map $AB \to \overline{ABX_B}$ is a Gaussian CP map, as Bob's detection is Gaussian, Lemma 6.3 implies:

$$\Delta S(AB) - \Delta S\left(\overline{ABX_B}\right) + \Delta H(X_B) \geq \Delta H(X_B)\,, \tag{6.61}$$

and, finally, exploiting Lemma 6.2 we find $\Delta H(X_B) \geq 0$, or, summarizing the previous relations, $\chi_{\mathrm{G}}(B;E) \geq \chi(B;E)$, that proves the theorem. □

As a consequence, Eq. (6.71) provides a lower bound on the DW:

$$K = \beta I(A;B) - \chi_{\rm G}(B;E) \geq K_{\rm DW}\,, \tag{6.62}$$

where $I(A;B)$ is the (exact) mutual information between Alice and Bob, whereas $\chi_{\rm G}(B;E)$ is the Holevo information retrieved in a virtual EB protocol where Alice and Bob share a Gaussian state with the CM $\boldsymbol{\sigma}_{AB}$ of state ρ_{AB}. The evaluation $\boldsymbol{\sigma}_{AB}$ is based on the amount of knowledge that Alice and Bob have on the channel. In particular, we identify two main scenarios, corresponding to the assumption of a linear or nonlinear channel.

Linear channel. The channel $\mathcal{N}: A' \to B$ is linear if described by the following input-output relations of the quadrature operators in Heisenberg picture,

$$q_B = \sqrt{T} q_{A'} + q_{\rm b} \qquad \text{and} \qquad p_B = \sqrt{T} p_{A'} + p_{\rm b}\,, \tag{6.63}$$

where $q_{\rm b}$ and $p_{\rm b}$ are the quadrature operators of some additional background noise modes, uncorrelated with the signal mode, such that $\langle q_{\rm b}\rangle = \langle p_{\rm b}\rangle = 0$, and $\langle q_{\rm b}^2\rangle = \langle p_{\rm b}^2\rangle = 1 - T + T\epsilon$. In this case, $\boldsymbol{\sigma}_{AB}$ can be expressed as a function of the CM $\boldsymbol{\sigma}_{AA'}$ of the state $|\Phi\rangle\!\rangle_{AA'}$ generated by Alice, see Eq. (6.5), that reads:

$$\boldsymbol{\sigma}_{AA'} = \begin{pmatrix} V\,\mathbb{1}_2 & Z\,\boldsymbol{\sigma}_z \\ Z\,\boldsymbol{\sigma}_z & V\,\mathbb{1}_2 \end{pmatrix}\,, \tag{6.64}$$

where:

$$V = 1 + 2\bar{n} \qquad \text{and} \qquad Z = \frac{1}{2}\langle\!\langle \Phi | (q_A q_{A'} - p_A p_{A'}) | \Phi \rangle\!\rangle\,, \tag{6.65}$$

in which $\bar{n} = \sum_k p_A(\alpha_k)|\alpha_k|^2$ is the mean number of photons per symbol, and $\boldsymbol{\sigma}_z$ is the Pauli z-matrix. The correlation term Z can be also expressed as a function of the average quantum state generated by Alice, equal to $\rho = \sum_k p_A(\alpha_k)|\alpha_k\rangle\langle\alpha_k|$, see Eq. (6.3), as:

$$Z = 2\,{\rm Tr}\left[\rho^{1/2} a\, \rho^{1/2} a^\dagger\right]\,, \tag{6.66}$$

where a and $a^\dagger$ are the creation and annihilation operators, respectively [223]. Then, thanks to (6.63), we obtain $\boldsymbol{\sigma}_{AB}$ as:

$$\boldsymbol{\sigma}_{AB} = \begin{pmatrix} V\,\mathbb{1}_2 & \sqrt{T}\,Z\,\boldsymbol{\sigma}_z \\ \sqrt{T}\,Z\,\boldsymbol{\sigma}_z & T\,(V+\chi)\,\mathbb{1}_2 \end{pmatrix}\,, \qquad \text{for a linear channel}\,. \tag{6.67}$$

Nonlinear channel. The linear channel provides a simple model to describe beam propagation in optical media, e.g. fibers, being often adopted in classical communications. However, from the CVQKD perspective, it may represent a too restrictive condition. In fact, if the channel from Alice to Bob is linear, we implicitly assume to know all the statistical moments of Bob's output state, whereas the quantities evaluated in a realistic CVQKD protocol are only the first and second moments of Bob's conditional state when Alice sends state k, and the second moment of Bob's overall state, as discussed in Sec. 6.2. For these reasons, it is also worth to investigate the more general case of an arbitrary $\mathcal{N}: A' \to B$, being associated with a nonlinear input-output relation. This

scenario has been addressed in detail by Denys *et al.* in [223]. Now, the CM $\boldsymbol{\sigma}_{AB}$ gets the different expression:

$$\boldsymbol{\sigma}_{AB} = \begin{pmatrix} V\,\mathbb{1}_2 & \widetilde{Z}\,\boldsymbol{\sigma}_z \\ \widetilde{Z}\,\boldsymbol{\sigma}_z & T\,(V+\chi)\,\mathbb{1}_2 \end{pmatrix}, \qquad \text{for a nonlinear channel}. \tag{6.68}$$

where the off-diagonal block terms $\widetilde{Z}$ satisfy:

$$\widetilde{Z} \geq 2\sqrt{T}\,\mathrm{Tr}\left[\rho^{1/2} a\,\rho^{1/2} a^\dagger\right] - \sqrt{2T\epsilon w}\,, \tag{6.69}$$

in which we introduce the quantity:

$$w = \sum_k p_A(\alpha_k)\left[\langle\alpha_k|a_\rho^\dagger a_\rho|\alpha_k\rangle - |\langle\alpha_k|a_\rho|\alpha_k\rangle|^2\right], \tag{6.70}$$

with $a_\rho = \rho^{1/2} a\,\rho^{-1/2}$. To assess unconditional security, one can either perform numerical calculation of $\widetilde{Z}$ [164, 168], or take the right hand side of (6.69) as a lower bound to the CM $\boldsymbol{\sigma}_{AB}$ and evaluate the corresponding KGR [223].

6.4.3 Final remarks and comments

Remarkably, we underline that referring to Theorem 6.1 as the "optimality of Gaussian attacks" theorem is rather misleading. The theorem merely states that we may safely assess security of a CVQKD protocol by considering the Gaussian state associated with the unknown state ρ_{AB} actually shared by Alice and Bob. Therefore, it does not provide identification of the most powerful attack at Eve's disposal, which, in general, is non Gaussian. In fact, the bound (6.71) can be saturated iff ρ_{AB} itself is a Gaussian state, in which case we retrieve the usual GG02 protocol, where the optimal eavesdropping coincides with a Gaussian attack, i.e. the entangling cloner [222]. On the contrary, in all other protocols, the bound is not attainable, and the optimal attack is no longer Gaussian.

Finally, we note that Eq. (6.62) requires to evaluate the exact mutual information $I(A;B)$ shared by the two parties, whose numerical calculation should be preferably approached in the PM picture. However, with analogous techniques, a simpler Gaussian bound on $I(A;B)$ can be obtained in the presence of Gaussian modulation at Alice's side. In this case, the following theorem holds.

Theorem 6.2. *If Bob's measurement is Gaussian and Alice employs Gaussian modulation, for any state ρ_{AB}, the mutual information $I(A;B)$ is lower bounded by:*

$$I(A;B) \geq I_{\mathrm{G}}(A;B)\,, \tag{6.71}$$

where $I_{\mathrm{G}}(A;B)$ is the mutual information computed for the Gaussian state having the same CM as ρ_{AB}, see Eq. (6.34) .

Proof. Starting from the expression $I(A;B) = H(X_A) + H(X_B) - H(X_A X_B)$, we evaluate the quantity $\Delta I(A;B)$, see (6.43):

$$\begin{aligned} \Delta I(A;B) &= I_{\mathrm{G}}(A;B) - I(A;B) \\ &= \Delta H(X_A) + \Delta H(X_B) - \Delta H(X_A X_B) \\ &\leq \Delta H(X_A)\,, \end{aligned} \tag{6.72}$$

where we used Lemma 6.3 as the map $X_A X_B \to X_B$, corresponding to averaging over the (Gaussian) random variable X_A, is Gaussian. Then, since Alice implements Gaussian modulation, we have $\Delta H(X_A) \equiv 0$, concluding the proof. □

Theorem 6.2 implies that the KGR of a Gaussian-modulated protocol with Gaussian detection is lower bounded by that of an all-Gaussian protocol where Alice and Bob share the Gaussian state with CM $\boldsymbol{\sigma}_{AB}$, namely:

$$K' = \beta I_{\rm G}(A;B) - \chi_{\rm G}(B;E) \geq K \geq K_{\rm DW}\,, \tag{6.73}$$

which provides a lower bound to (6.62), that avoids the exact numerical computation of the mutual information $I(A;B)$. In particular, the present bound is applicable to CVQKD schemes over non-Gaussian channels.

6.5 Discrete modulation protocols

Despite its simplicity, the GG02 scheme discussed in the previous sections raises important issues about its practical implementation with the state-of-the-art technologies in optical communications, especially regarding the continuous modulation of the coherent pulses. In fact, although justified on a theoretical level, Gaussian modulation involves several practical difficulties, and, so far, its application is limited to short-distance communications [244–246]. The main drawback lies in the error correction stage needed for the reconciliation process, being implemented via suitable codes originally designed for discrete variables, that perform worse in the presence of Gaussian modulation [162, 180, 246]. In fact, as discussed in Sec. 6.3, to perform GG02 in the long-distance regime, the protocol should operate at low values of modulation energy, corresponding to few mean photons per time slot, see Fig. 6.3.3(b); thus, accordingly, we should consider low values of SNR. On the other hand, reconciliation of Gaussian variables, even with the most advanced error correction codes, e.g. turbo codes [13] or LDPC codes [247], can be efficiently performed only in the high SNR regime, whereas the common techniques, e.g. the slice reconciliation method [248], even if assisted by LDPC, leads to low reconciliation efficiency if the SNR is too low [162, 180, 210].

To date, the problem of obtaining good reconciliation efficiencies at low SNR is still open; therefore a possible solution is to design CVQKD protocols employing discrete modulation formats of appropriate order. In this way, the dataset in Alice's and Bob's hands would be the same of a classical communication scheme based on discrete signaling and additive white Gaussian noise channel, for which there exists more efficient codes working in the low SNR regime, e.g. multi-edge type LDPC codes [249].

For these reasons, CVQKD employing discrete modulation has been recently addressed in literature, with the intent of adopting a feasible modulation technique being as close as possible to the Gaussian modulation limit [162, 164, 165, 167, 223, 225–229, 231–235, 250–252]. To this aim, in the following we address two paradigmatic formats, namely, phase-shift keying (PSK), a well known stratgey in literature, and quadrature amplitude modulation (QAM), here investigated for the first time in the context of unconditionally secure CVQKD.

6.5.1 Phase-shift keying (PSK)

The first discrete modulation protocol was proposed in 2009 by Leverrier and Grangier [162], involving the *phase-shift keying* (PSK) format already presented in Sec. 5.5. The choice of PSK modulation is mainly due for twofold reason. Firstly, a well known result in classical communication theory is that PSK constellations, of proper order $M \geq 2$, approximate the Shannon capacity, achieved by Gaussian modulation, in the low-energy regime [53, 253]; thus making it worth of interest to assess their relevance also

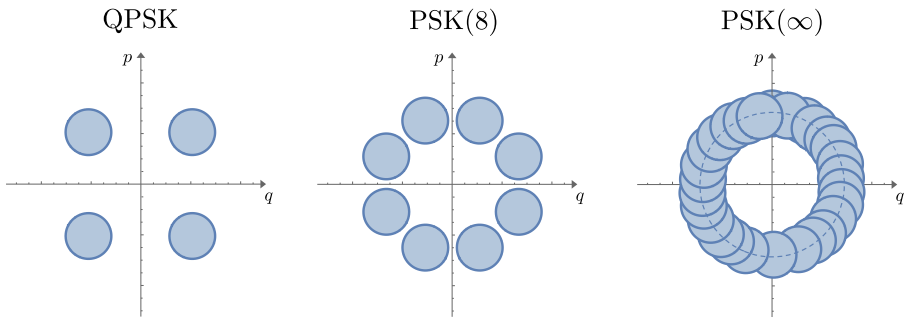


Figure 6.5.1: Phase space representation of several PSK(M) constellations, with different $M > 1$. The case PSK(4) is also referred to as quadrature phase-shift keying (QPSK). We also note that, in the limit $M \gg 1$, we approach the PSK(∞), or continuous phase-shift keying, modulation, in which the constellation is composed of infinitely many coherent states with the same amplitude $\alpha > 0$, and different phase, getting continuous values in the range $\phi \in [0, 2\pi)$.

for CVQKD. Secondly, from a practical point of view, PSK(M) protocols represent the simplest hybrid schemes, combining both the physical implementation of GG02, and the practicality of discrete modulation protocols, for which the error correction stage, occurring during reconciliation, is much simpler to perform.

Given these considerations, in the presence of PSK(M) modulation, Alice randomly prepares a coherent state drawn from the constellation of the M states $\{|\alpha_k\rangle\}_k$, with:

$$|\alpha_k\rangle = |\alpha\, e^{i\pi(2k+1)/M}\rangle\,, \qquad k = 0, \dots, M-1\,, \tag{6.74}$$

where $\alpha \geq 0$, generated with equal a priori probabilities $p_A(\alpha_k) = 1/M$ [19, 51]. We remind that the case $M = 4$ is also referred to as quadrature phase-shift keying (QPSK). The phase space representation of PSK(M) constellations is reported in Fig. 6.5.1 for the typical values $M = 4, 8$ commonly employed in optical communications.

Accordingly, the overall quantum state generated at Alice's side is equal to:

$$\rho = \frac{1}{M}\sum_{k=0}^{M-1} |\alpha_k\rangle\langle\alpha_k| = \sum_{k=0}^{M-1} \lambda_k |\phi_k\rangle\langle\phi_k|\,, \tag{6.75}$$

whose right hand side provides its spectral decomposition, associated with eigenvalues:

$$\lambda_k = e^{-\alpha^2}\sum_{n=0}^{\infty}\frac{\alpha^{2(nM+k)}}{(nM+k)!} = \frac{e^{-\alpha^2}}{M}\sum_{j=0}^{M-1} e^{-i\frac{2\pi}{M}jk}\exp(\alpha^2 e^{i\frac{2\pi}{M}j})\,, \tag{6.76}$$

and eigenstates:

$$|\phi_k\rangle = \frac{e^{-\alpha^2/2}}{\sqrt{\lambda_k}}\sum_{n=0}^{\infty}\frac{\alpha^{nM+k}}{\sqrt{(nM+k)!}}\,|nM+k\rangle\,, \tag{6.77}$$

expanded in the Fock basis. As an example, for the QPSK case we have:

$$\lambda_{0(2)} = \frac{e^{-\alpha^2}}{2}\Big[\cosh(\alpha^2) \pm \cos(\alpha^2)\Big]\,,$$

$$\lambda_{1(3)} = \frac{e^{-\alpha^2}}{2}\Big[\sinh(\alpha^2) \pm \sin(\alpha^2)\Big]\,. \tag{6.78}$$

After signal modulation, Alice injects the pulses into the unstrusted quantum channel, associated with transmissivity $T \leq 1$ and excess noise $\epsilon \geq 0$; finally, Bob collects the output signals and performs Gaussian detection. Here, we consider the case of homodyne detection, and, without loss of generality, assume that quadrature q is measured. In turn, when Alice sends state $|\alpha_k\rangle$, Bob's conditional probability of obtaining the outcome x_B is equal to:

$$p_{B|A}(x_B|\alpha_k) = \frac{\exp\left\{-\left[x_B - 2\sqrt{T}\alpha\cos\left(\frac{\pi(2k+1)}{M}\right)\right]^2 / \left(2(1+T\epsilon)\right)\right\}}{\sqrt{2\pi(1+T\epsilon)}}\,, \tag{6.79}$$

whose corresponding Shannon entropy gets the analytic expression

$$\begin{aligned}\mathsf{H}\left[p_{B|A}(x_B|\alpha_k)\right] &= \int_{\mathbb{R}} dx_B\, p_{B|A}(x_B|\alpha_k)\log_2 p_{B|A}(x_B|\alpha_k) \\ &= \frac{1}{2}\log_2\left[2\pi e(1+T\epsilon)\right],\end{aligned} \tag{6.80}$$

being independent of the signal amplitude. Instead, Bob's overall homodyne distribution reads:

$$p_B(x_B) = \frac{1}{M}\sum_{k=0}^{M-1} p_{B|A}(x_B|\alpha_k)\,. \tag{6.81}$$

In turn, we obtain the mutual information shared by the two parties as:

$$I_{AB}(\alpha^2) = H_B - \frac{1}{2}\log_2\left[2\pi e(1+T\epsilon)\right], \tag{6.82}$$

where H_B is the Shannon entropy of $p_B(x_B)$, to be evaluated numerically.

We now prove unconditional security of the PSK(M) protocol, by invoking the optimality of Gaussian attacks presented in the previous section. That is, we consider the EB description, where Alice and Bob share the non-Gaussian state ρ_{AB} in (6.13), and provide an upper bound to the actual Holevo infomation shared between Bob and Eve by the Holevo information obtained in the associated EB Gaussian protocol, where Alice and Bob share the Gaussian state with the same CM as ρ_{AB}, equal to $\boldsymbol{\sigma}_{AB}$. Moreover, here we adopt the linear channel assumption, as in the original proposal [162], and, thanks to Eq. (6.67), we get:

$$\boldsymbol{\sigma}_{AB} = \begin{pmatrix} \boldsymbol{\sigma}_A & \boldsymbol{\sigma}_Z \\ \boldsymbol{\sigma}_Z^{\mathsf{T}} & \boldsymbol{\sigma}_B \end{pmatrix} = \begin{pmatrix} V\,\mathbb{1}_2 & \sqrt{T}\,Z_M\,\boldsymbol{\sigma}_z \\ \sqrt{T}\,Z_M\,\boldsymbol{\sigma}_z & T\,(V+\chi)\,\mathbb{1}_2 \end{pmatrix}, \tag{6.83}$$

$V = 1 + 2\alpha^2$ being the modulation variance, $\chi = (1-T)/T + \epsilon$, and with the correlation $Z_M = 2\,\mathrm{Tr}[\rho^{1/2} a\,\rho^{1/2} a^\dagger]$, see Eq. (6.66). To explicitly compute it, we exploit Eq. (6.75) and note that:

$$\langle\phi_j|\alpha_k\rangle = \sqrt{\lambda_j}e^{i\frac{2\pi}{M}jk} \quad \text{and} \quad a\,|\phi_k\rangle = \alpha\,\lambda_{(k-1)\bmod M}^{1/2}\lambda_k^{-1/2}|\phi_{(k-1)\bmod M}\rangle\,. \tag{6.84}$$

Straightforward calculations lead to [162, 180, 223]:

$$Z_M = 2\alpha^2\sum_{k=0}^{M-1}\frac{\lambda_k^{3/2}}{\lambda_{k+1}^{1/2}}\,. \tag{6.85}$$

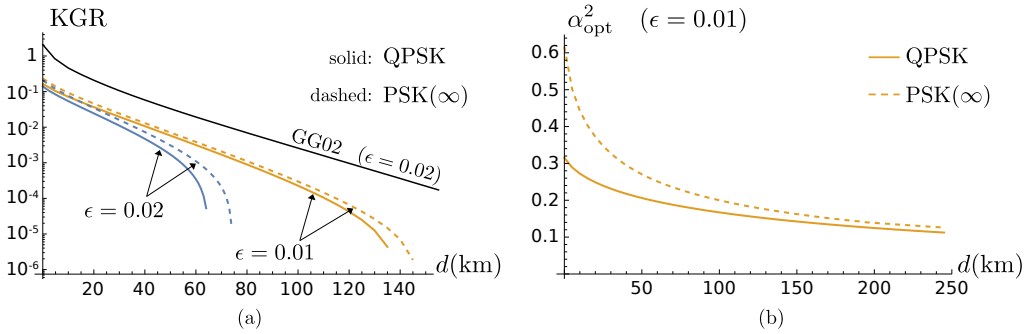


Figure 6.5.2: (a) Log plot of the optimized KGR K as a function of the transmission distance d in km for QPSK (solid lines) and PSK(∞) (dashed lines) and different values of the excess noise. The black line corresponds to the KGR $K_{\rm GG}$ of the GG02 protocol for $\epsilon = 0.02$. As we can see, $K < K_{\rm GG}$, proving PSK(M) modulation to be strongly suboptimal with respect to Gaussian modulation. (b) Plot of the optimized modulation energy $\alpha^2_{\rm opt}$ as a function of d for QPSK (solid line) and PSK(∞) (dashed line) and $\epsilon = 0.01$. In both the pictures we set the reconciliation efficiency $\beta = 0.95$ and the loss rate $\kappa = 0.2$ dB/km.

Then, we obtain the Holevo information as:

$$\chi_{BE}(\alpha^2) = h\left(\frac{\mathrm{d}_1 - 1}{2}\right) + h\left(\frac{\mathrm{d}_2 - 1}{2}\right) - h\left(\frac{\mathrm{d}_3 - 1}{2}\right), \tag{6.86}$$

with the h function in Eq. (8.40), $\mathrm{d}_{1(2)}$ being the symplectic eigenvalues of $\boldsymbol{\sigma}_{AB}$, and $d_3 = \sqrt{\det(\boldsymbol{\sigma}_{A|B})}$, where:

$$\boldsymbol{\sigma}_{A|B} = \boldsymbol{\sigma}_A - \boldsymbol{\sigma}_Z\left[\boldsymbol{\sigma}_B + \boldsymbol{\sigma}_B^{(\mathrm{m})}\right]^{-1}\boldsymbol{\sigma}_Z^{\mathsf{T}}, \tag{6.87}$$

in which

$$\boldsymbol{\sigma}_B^{(\mathrm{m})} = \lim_{z\to 0}\begin{pmatrix} z & 0 \\ 0 & z^{-1}\end{pmatrix} \tag{6.88}$$

is the 2×2 CM associated with homodyne detection. Ultimately, the KGR reads:

$$K(\alpha^2) = \beta I_{AB}(\alpha^2) - \chi_{BE}(\alpha^2), \tag{6.89}$$

$\beta \leq 1$ being the reconciliation efficiency, where we highlighted the dependence on the modulation energy α^2. Since we are interested in determining the highest achievable key rate as a function of the transmission distance d, we perform optimization over α^2 and obtain:

$$K = \max_{\alpha^2} K(\alpha^2), \tag{6.90}$$

together with the distance-dependent optimized mean energy $\alpha^2_{\rm opt}$.

In Fig. 6.5.2(a) we report plots of the optimized KGR K as a function of the transmission distance d for the QPSK case, i.e. $M = 4$, and different channel excess noise ϵ. Similarly to the GG02 protocol, the KGR is positive up to a maximum transmission distance $d_{\max}$ decreasing with the excess noise ϵ. However, as we can see, for a given excess

noise, we have $K < K_{\rm GG}$, and both the values of KGR and maximum distance of the PSK(M) protocol are much lower than the corresponding ones achieved by the GG02. This is a ineludible consequence both of the type of constellation employed and the values of the resulting optimized mean energy $\alpha^2_{\rm opt}$, reported in Fig. 6.5.2(b). In fact, at given energy α^2, the mutual information $I_{AB}(\alpha^2)$ is close to that shared in GG02, equal to (6.25) and coinciding with the Shannon capacity, only in the range $\alpha^2 \lesssim 10^{-1}$. In this regime, the correlation term Z_M of the CM (6.83) is $Z_M \lesssim Z_{\rm GG}$, where $Z_{\rm GG} = \sqrt{V^2-1}$ is the off diagonal CM term of the TSMV state employed in GG02, and, accordingly, also $\chi_{BE}(\alpha^2)$ is close to the Holevo information achieved by the Gaussian modulation protocol. On the contrary, in high-energy regime, the overlap between the PSK encoded states vanishes and $I_{AB}(\alpha^2)$ saturates to the maximum possible entropy of the constellation, equal to $\log_2(M)$. In turn, for high α^2, the encoded symbols are more "distinguishable", allowing Eve to retrieve more information, and making the KGR (6.89) deviate from the GG02 limit and drop below 0. The tradeoff between these two energy regimes leads to optimized values of the modulation energy comprised between $0.2 \leq \alpha^2_{\rm opt} \leq 0.6$, being at least one order of magnitude lower than those achieved by GG02. This, ultimately, leads to lower values of optimized KGR and makes PSK modulation strongly suboptimal with respect to Gaussian modulation.

Further improvements may be obtained by increasing the modulation order M, e.g. considering the PSK(8) protocol proposed by Becir *et al.* [232], for which both the optimized energy and key rate are larger. In light of this, the best performance of PSK modulation is achieved in the limit $M \gg 1$, where we approach the PSK(∞), or continuous phase-shift keying, modulation. Now, the constellation is composed of an infinite number of coherent pulses in the form $|\alpha_\phi\rangle = |\alpha e^{i\phi}\rangle$, with the same amplitude $\alpha > 0$ and different phase, getting continuous values in the range $\phi \in [0, 2\pi)$, and being chosen with a priori probability $p_A(\alpha_\phi) = 1/2\pi$, see Fig. 6.5.1 [254]. Then, the average state at Alice's side is the phase-averaged (PHAV) state [255]:

$$\rho_{\rm PHAV} = \frac{1}{2\pi}\int_0^{2\pi} d\phi\, |\alpha e^{i\phi}\rangle\langle \alpha e^{i\phi}| = e^{-\alpha^2}\sum_{n=0}^{\infty}\frac{\alpha^{2n}}{n!}|n\rangle\langle n|\,, \tag{6.91}$$

corresponding to a Poisson-distributed ensemble of Fock states $\{|n\rangle\}_n$, while the correlation term Z_M in the CM (6.83) becomes:

$$Z_\infty = 2e^{-\alpha^2}\sum_{n=0}^{\infty}\frac{\sqrt{n+1}}{n!}\alpha^{2n+1} \quad \text{for PSK}(\infty)\text{ modulation,} \tag{6.92}$$

where the (convergent) series has to be evaluated numerically. Accordingly, we follow the same procedure above outlined, and compute the optimized KGR and modulation energy, plotted in Fig. 6.5.2(a) and (b), respectively. As we can see, PSK(∞) induces an enhancement both in the KGR and the maximum transmission distance with respect to QPSK, being more accentuated for higher values of excess noise ϵ. However, as we can see, the gap with respect to GG02 is not closed, thus the sole phase modulation, even of infinitely many coherent states, is not sufficient to approach the peformance Gaussian modulation protocol. Furthermore, we note that numerical calculations prove that PSK(8) is sufficient to well approximate the continuous phase-shift keying limit.

Finally, we compute the maximum tolerable excess noise $\epsilon_{\rm max}$ for both the QPSK and PSK(∞) protocols, depicted in Fig. 6.5.3, and compared to the maximum tolerable noise $\epsilon^{\rm (GG)}_{\rm max}$ of GG02. As expected, we have $\epsilon_{\rm max} < \epsilon^{\rm (GG)}_{\rm max}$, consistently with the previous discussion.

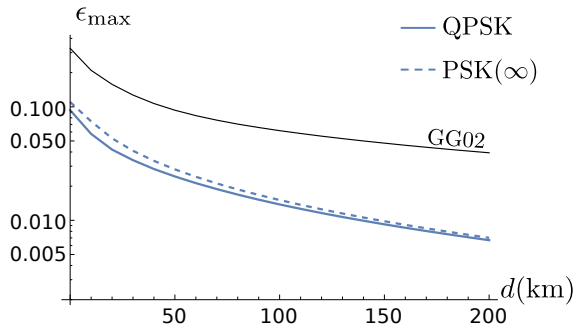


Figure 6.5.3: Log plot of the maximum tolerable excess noise $\epsilon_{\max}$ for the QPSK (solid line) and PSK(∞) (dashed line) protocols as a function of the distance d in km. The black line corresponds to the maximum tolerable noise $\epsilon_{\max}^{(\mathrm{GG})}$ of GG02. As we see, PSK(M) protocol are much less tolerant to the channel excess noise than the Gaussian modulation protocol. We set the reconciliation efficiency $\beta = 0.95$.

6.5.2 Quadrature amplitude modulation (QAM)

Despite their practicality for the error correction procedure, in the previous subsection we showed that, for a given reconciliation efficiency $\beta \leq 1$, PSK(M) protocols are strongly suboptimal with respect to GG02, in terms of both KGR and maximum tolerable excess noise. Therefore, we may look for other suitable discrete modulation formats, that, in principle, could close the gap with the Gaussian modulation protocol, and still provide efficient reconciliation.

Recently, quadrature amplitude modulation (QAM) of a regular grid of signals has been proposed as a promising solution [223, 225, 226]. In fact, differently from PSK, QAM constellations may employ a non-uniform discrete probability distribution of the symbols that approximates better the Gaussian one, thus obtaining a higher KGR closer to GG02. To implement this non-uniform sampling, probabilistic amplitude shaping (PAS) is a practical coded modulation scheme that combines QAM, probabilistic constellation shaping, and forward error correction (FEC) to closely approach optimal channel capacity [256–258]. PAS uses a distribution matcher to map uniformly distributed information bits on QAM symbols with the desired target distribution [259–261]. In particular, a Maxwell–Boltzmann target distribution is considered, which maximizes the source entropy for a given discrete constellation and mean energy per symbol [262] (in practice, lower-energy symbols are used more often than higher-energy symbols, reducing the energy required to achieve a certain information rate).

In more detail, the QAM format adopted by Alice works as follows [51, 263]. Alice generates a coherent state $|\alpha_{x_A,y_A}\rangle = |x_A + iy_A\rangle$, where each couple (x_A, y_A) is drawn from the finite set $\mathcal{A} = \Lambda \times \Lambda$, where

$$\Lambda = \left\{ n\Delta \ : \ n = -\frac{M-1}{2}, \ldots, \frac{M-1}{2} \right\} \tag{6.93}$$

contains $M = 2^k$ points, for some $k \in \mathbb{N}$. The points in Λ are placed at distance $\Delta \geq 0$ between one another, $\Delta \in \mathbb{R}$ being a parameter that determines the mean energy per symbol, which is hence referred to indifferently as *scaling factor* or *symbol spacing* [263]. In turn, the resulting constellation consists in a square lattice of $M \times M$ coherent states, centered in $(2\sigma_0 x_A, 2\sigma_0 y_A)$ and with pace $2\sigma_0\Delta$, σ_0^2 being the shot noise variance, de-

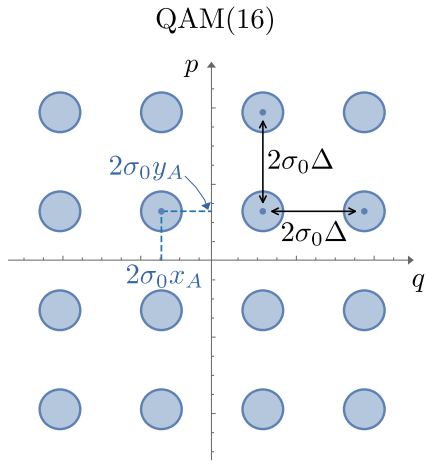


Figure 6.5.4: Phase space representation of the QAM(M^2) constellation, with $M = 4$, composed of a regular grid of $M \times M$ coherent states, centered in $(2\sigma_0 x_A, 2\sigma_0 y_A)$ and with pace $2\sigma_0\Delta$, σ_0^2 being the shot noise variance.

picted in Fig. 6.5.4 for the relevant case of $M^2 = 16$ symbols. As before, we will consider shot noise units (SNU), fixing $\sigma_0^2 = 1$ in the rest of the analysis. Unlike PSK, now the pulses encoded by Alice are associated with different mean energies $|\alpha_{x_A,y_A}|^2$, therefore different probability distributions may be investigated to sample the alphabet $\mathcal{A}$. In particular, here we discuss two alternative possibilities. The former, referred to as case I, is the uniform distribution:

$$\mathcal{P}(z) = \frac{1}{M}\,, \quad z = x_A, y_A\,, \qquad \text{(case I)}\,, \tag{6.94}$$

commonly exploited in classical communications [263] and quantum state-discrimination schemes [51]. The latter, case II, is the Maxwell–Boltzmann (MB) distribution: [53, 262]

$$\mathcal{M}_\xi(z) = \frac{e^{-\xi z^2}}{Z}\,, \quad z = x_A, y_A\,, \qquad \text{(case II)}\,, \tag{6.95}$$

$Z = \sum_z e^{-\xi z^2}$ being the normalization constant, that depends on the free parameter ξ, referred to as the *inverse temperature*. The MB represents the maximum-entropy distribution for a discrete random variable with given variance (mean energy) [53] and, for a sufficiently large QAM constellation, it has been shown to closely approach the Shannon capacity of the AWGN channel [256]. For this reason, it provides a good candidate to also enhance discrete modulation CVQKD, closing the gap between the PSK(M) and the GG02 protocols. We also note that in the limit $\xi \to \infty$, only the lowest-energy level of the MB have non-zero probability, so that the resulting constellation tends to a simple QAM(4), i.e. with $M = 2$, being equivalent to QPSK. On the other hand, for $\xi = 0$, all the levels of the MB distribution have the same probability, and we retrieve the uniform modulation adopted in case I.

We start the security analysis by considering case I. At first, we determine the value of the symbol spacing $\Delta^{(\mathrm{I})}$ from the mean energy $\bar{n}$ of the constellation. The overall state

generated by Alice is:

$$\rho^{(\mathrm{I})} = \frac{1}{M^2} \sum_{x_A \in \Lambda} \sum_{y_A \in \Lambda} |x_A + iy_A\rangle\langle x_A + iy_A| \,, \tag{6.96}$$

its mean energy being equal to $\bar{n} = 2/M \sum_{x_A} x_A^2 = 2\Delta^2/M \sum_{n=-(M-1)/2}^{(M+1)/2} n^2$, which can be inverted to obtain:

$$\Delta^{(\mathrm{I})} = \sqrt{\frac{6\bar{n}}{M^2 - 1}} \,. \tag{6.97}$$

Accordingly, the mean energy $\bar{n}$ provides a free parameter in Alice's hands to properly adjust the size of the QAM constellation. Thereafter, once the signals have been generated, Alice injects them into the quantum channel of parameters (T, ϵ). Bob receives them and performs homodyne detection, associated with the mutual information:

$$I_{AB}^{(\mathrm{I})}(\bar{n}) = H_B^{(\mathrm{I})} - \frac{1}{2} \log_2 \Big[2\pi e (1 + T\epsilon) \Big] \,, \tag{6.98}$$

where $H_B^{(\mathrm{I})}$ is the Shannon entropy of Bob's overall distribution:

$$p_B^{(\mathrm{I})}(x_B) = \frac{1}{M} \sum_{x_A} p_{B|A}(x_B|x_A) \,, \tag{6.99}$$

with

$$p_{B|A}(x_B|x_A) = \frac{\exp\Big[-(x_B - 2\sqrt{T}x_A)^2/(2(1 + T\epsilon)) \Big]}{\sqrt{2\pi(1 + T\epsilon)}} \,. \tag{6.100}$$

Instead, the Holevo information $\chi_{BE}^{(\mathrm{I})}(\bar{n})$ is computed thanks to the optimality of Gaussian attacks. We exploit Eq. (6.86) and the CM (6.83), where, now, the correlation term Z_M should be changed into:

$$Z^{(\mathrm{I})} = 2 \,\mathrm{Tr} \Big\{ \big[\rho^{(\mathrm{I})}\big]^{1/2} a \, \big[\rho^{(\mathrm{I})}\big]^{1/2} a^\dagger \Big\} \,, \tag{6.101}$$

to be evaluated numerically from the quantum state (6.96). The resulting KGR then reads:

$$K^{(\mathrm{I})} = \max_{\bar{n}} \Big[\beta I_{AB}^{(\mathrm{I})}(\bar{n}) - \chi_{BE}^{(\mathrm{I})}(\bar{n}) \Big] \,, \tag{6.102}$$

together with the optimized energy $\bar{n}_{\mathrm{opt}}^{(\mathrm{I})}$.

On the contrary, in case II, the modulation stage is associated with two free parameters: the constellation energy $\bar{n}$ and the inverse temperature ξ. Now, the statistical operator at Alice's side becomes:

$$\rho^{(\mathrm{II})} = \sum_{x_A, y_A} \mathcal{M}_\xi(x_A) \mathcal{M}_\xi(y_A) \, |x_A + iy_A\rangle\langle x_A + iy_A| \,, \tag{6.103}$$

therefore we have:

$$\bar{n} = 2 \sum_{x_A} \mathcal{M}_\xi(x_A) \, x_A^2 = 2\Delta^2 \sum_{n=-\frac{M-1}{2}}^{\frac{M+1}{2}} \mathcal{M}_\xi(n\Delta) \, n^2 \,, \tag{6.104}$$

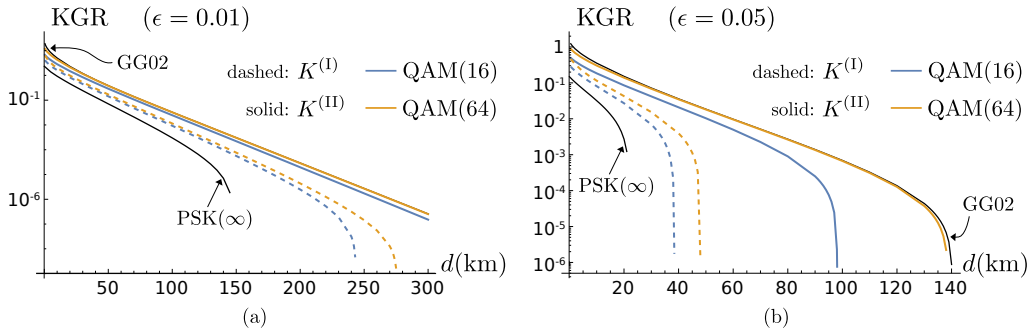


Figure 6.5.5: Log plot of the optimized KGRs $K^{(\mathrm{p})}$, $\mathrm{p} = \mathrm{I}, \mathrm{II}$, as a function of the transmission distance d in km for $\epsilon = 0.01$ (a) and $\epsilon = 0.05$ (b). As we can see, QAM modulation outperforms the results obtained for PSK(M) protocols for all M, both in the presence of uniform and MB sampling. Moreover, when QAM is further assisted by PAS, namely in case II, by increasing the number of symbols M, we progressively close the existing gap between the PSK and the Gaussian modulation. In both the pictures we set the reconciliation efficiency $\beta = 0.95$ and the loss rate $\kappa = 0.2$ dB/km.

to be inverted numerically, and whose corresponding solution $\Delta^{(\mathrm{II})}(\xi)$ exhibits an implicit dependence also on ξ, making the spacing dependent on both the energy and the inverse temperature. The mutual information shared by Alice and Bob becomes:

$$I_{AB}^{(\mathrm{II})}(\bar{n}, \xi) = H_B^{(\mathrm{II})} - \frac{1}{2} \log_2 \left[2\pi e (1 + T\epsilon) \right], \tag{6.105}$$

where $H_B^{(\mathrm{II})}$ is the Shannon entropy of the distribution:

$$p_B^{(\mathrm{II})}(x_B) = \sum_{x_A} \mathcal{M}_\xi(x_A)\, p_{B|A}(x_B|x_A)\,, \tag{6.106}$$

whereas the Holevo information $\chi_{BE}^{(\mathrm{II})}(\bar{n}, \xi)$ is computed by Eq. (6.86) and the CM (6.83), with the correlation term:

$$Z^{(\mathrm{II})} = 2\,\mathrm{Tr}\left\{ \left[\rho^{(\mathrm{II})}\right]^{1/2} a \left[\rho^{(\mathrm{II})}\right]^{1/2} a^\dagger \right\}. \tag{6.107}$$

The obtained KGR is equal to:

$$K^{(\mathrm{II})} = \max_{\bar{n},\xi} \left[\beta I_{AB}^{(\mathrm{II})}(\bar{n}, \xi) - \chi_{BE}^{(\mathrm{II})}(\bar{n}, \xi) \right], \tag{6.108}$$

with the optimized energy $\bar{n}_{\mathrm{opt}}^{(\mathrm{II})}$ and inverse temperature ξ_{opt}.

Plots of $K^{(\mathrm{p})}$, $\mathrm{p} = \mathrm{I}, \mathrm{II}$, are reported in Fig. 6.5.5 as a function of the transmission distance d with excess noise $\epsilon = 0.01$ (a) and $\epsilon = 0.05$ (b), for the relevant constellations QAM(16) and QAM(32), corresponding to $M = 4, 8$, respectively. As we can see, QAM modulation provides a preferable choice over PSK, beating the PSK(∞) protocol for both cases $\mathrm{p} = \mathrm{I}, \mathrm{II}$, and leading to higher KGR and larger maximum transmission distance. The MB sampling outperforms the uniform one, as $K^{(\mathrm{II})} \geq K^{(\mathrm{I})}$, and, remarkably, its corresponding KGR is also able to approach the GG02 scheme for a large enough number of symbols M. In particular, the QAM(32) constellation is able to well approximate the

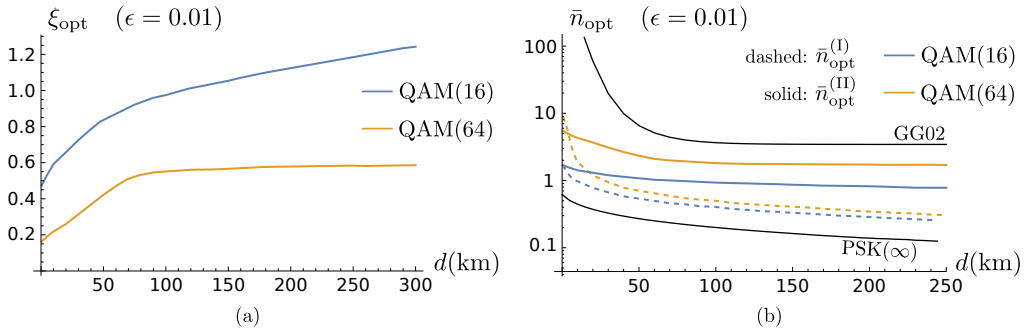


Figure 6.5.6: Plot of the optimized parameters $\xi_{\rm opt}$ (a) and $\bar{n}_{\rm opt}$ (b) for cases $\mathrm{p} = \mathrm{I}, \mathrm{II}$, as a function of the transmission distance d in km. In both the pictures we set the values $\epsilon = 0.01$, $\beta = 0.95$, and $\kappa = 0.2$ dB/km.

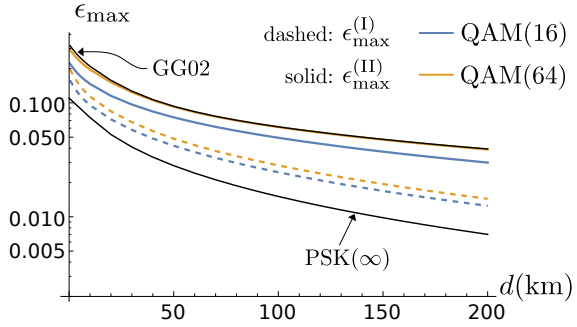


Figure 6.5.7: Log plot of the maximum tolerable excess noise $\epsilon_{\rm max}$ for the QAM protocols in cases $\mathrm{p} = \mathrm{I}, \mathrm{II}$, together with the maximum tolerable noises of the PSK(∞) and GG02 protocol. Consistently with the previous results, QAM modulation closes the gap with respect to GG02, especially when assisted by PAS. We set the reconciliation efficiency $\beta = 0.95$.

results of GG02 for excess noises $\epsilon \leq 0.05$. In turn, PAS proves itself as a crucial factor to combine both the practical necessity of discrete modulation formats and the possibility to obtain high values of key rate.

The enhancement brought by PAS is due to a nontrivial optimization of the MB distribution, as emerges by considering the optimized inverse temperature $\xi_{\rm opt}$, reported in Fig. 6.5.6(a). In fact, $\xi_{\rm opt}$ an increasing function of the transmission distance such that $0 < \xi_{\rm opt} < \infty$; thus, we do not retrieve neither the QPSK nor the uniform modulation limit, and the best-working performance of the protocol is achieved by exploiting the full cardinality of the constellation, in which the lower-energy symbols are more likely than the higher-energy ones. Moreover, $\xi_{\rm opt}$ saturates for large d and is a decreasing function of M. For the sake of completeness, in Fig. 6.5.6(b) we report the optimized energy $\bar{n}^{(\rm p)}_{\rm opt}$, $\mathrm{p} = \mathrm{I}, \mathrm{II}$, which is a decreasing function of the distance and saturates as d increases. As one may expect, increasing the size of the constellation increases also $\bar{n}^{(\rm p)}_{\rm opt}$, until to reach the value of the GG02 scheme. Moreover, for large d we have $\bar{n}^{(\rm II)}_{\rm opt} \geq \bar{n}^{(\rm I)}_{\rm opt}$, and the MB reaches its maximum KGR for higher energies.

Finally, we compute the maximum tolerable excess noise $\epsilon^{(\rm p)}_{\rm max}$, $\mathrm{p} = \mathrm{I}, \mathrm{II}$, plotted in

Fig. 6.5.7, and compared to the maximum tolerable noise of both the PSK(∞) and the GG02 protocols. Consistently with the former analysis, we have $\epsilon_{\max}^{(\mathrm{II})} \geq \epsilon_{\max}^{(\mathrm{I})}$, and, in both the cases, the maximum tolerable noise is larger than that of PSK(∞). Remarkably, by increasing the modulation order M, the QAM constellation assisted by PAS closes the gap with respect to GG02.

CHAPTER 7

CVQKD in the presence of restricted eavesdropping

In this Chapter, we study the two other main security frameworks presented in the previous one, namely the trusted-device scenario and the wiretap channel assumption. They both provide examples of restricted eavesdropping, in which the eavesdropper, Eve, cannot perform arbitrary channel manipulation, unlike the unconditional security case.

In more detail, in the trusted-device scenario we assume a composite quantum channel, given by the composition of two subsequent noisy maps, of which only one is actually controlled by Eve. This scenario models the realistic case of noisy detection at the receiver's side, where we may safely assume that detection noise and losses are simply lost to the environment and cannot be intercepted by Eve, who, instead, controls both the losses and noise acquired during signal transmission. On the contrary, the wiretap channel provides an example of specific eavesdropping. Indeed, the term wiretap channel refers to a quantum channel from Alice to Bob being completely characterized in terms of its unitary dilation; accordingly, if we consider the ancillary environmental modes to be controlled by Eve, the wiretap channel not only described signal propagation from both Alice to Bob, but also determines the quantum map Alice $\rightarrow$ Eve, ultimately identifying a particular eavesdropping strategy.

The Chapter is organized as follows. In Sec. 7.1, we study the trusted-device scenario: we extend the validity of the optimality of Gaussian attacks to this framework, and compute the corresponding KGR for the QPSK protocol, as a paradigmatic example. Subsequently, in Sec. 7.2 we introduce the wiretap channel description and perform the associated CVQKD security analysis. Ultimately, we compute the KGR for the QPSK protocol, comparing the obtained results under both the unconditional security and wiretap channel assumptions.

7.1 The trusted-device scenario

As widely discussed in the previous Chapter, the traditional security proofs for CVQKD have been established under unconditional security. This implicitly assumes the presence of an omnipotent eavesdropper having full access to the quantum channel connecting Alice and Bob, namely being able to both collect all the lost photons and control the noise acquired during the propagation [222]. Within this framework, security has been firstly guaranteed by the optimality of Gaussian attacks, providing a lower bound to DW, while, more recently, an almost exact calculation of DW have been achieved by a sophisticated approach based on SDP [164–166].

In realistic conditions, however, Bob will also experience further noise due to non-idealities in his measurement device, which may not be directly accessible to Eve. Therefore, it is justified to address physical layer security under different frameworks, consid-

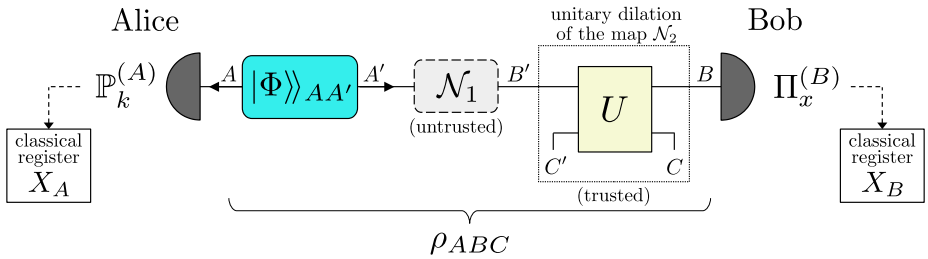


Figure 7.1.1: Extended scheme of the EB version of a CVQKD protocol in the presence of trusted devices. Alice prepares the state $|\Phi\rangle\!\rangle_{AA'}$ and injects mode A' into the quantum channel. The noisy evolution is composed of the two CP maps $\mathcal{N}_1$ (untrusted) and $\mathcal{N}_2$ (trusted). Thereafter, Bob performs a Gaussian measurement $\{\Pi_x^{(B)}\}_x$, storing the obtained outcomes in a classical register X_B.

ering different degrees of trust for each setup component. In particular, we retrieve unconditional security if all components are completely untrusted, whereas when some of the setup elements (e.g. detection losses and noise) are trusted, we deal with the *trusted-device scenario* [22, 220, 264]. This latter scenario includes also loss-compensation strategies, e.g. exploiting phase-insensitive amplifiers to perform signal restoration before detection [12], being noisy operations that are useless under the unconditional security approach, but whose application, if trusted, may be beneficial [22, 193].

To date, security in the trusted scenario has been carried out only for Gaussian protocols, where the optimal eavesdropping strategy is again realized by entangling cloner attack [22, 264], leaving the problem open for more general schemes, e.g. involving discrete modulation. The first obstacle in this direction is to identify the optimal attack that Eve may launch. In fact, while in the existing unconditional security proofs Eve's information is computed by a purification ansatz, see Sec. 6.2.3.1, this argument does not hold anymore in the case of some lack of information on Eve's side, that, now, cannot purify the whole state shared among the parties. This makes the security analysis nontrivial, as the framework presented in both [178–180] and [164–166] cannot be applied straightforwardly.

To this aim, in the following we extend for the first time the validity of Gaussian attacks optimality for general CVQKD protocols in the presence of trusted devices. In particular, we prove that, provided Bob's measurement to be Gaussian, the information extracted by Eve is upper bounded by the Holevo information of the Gaussian state having the same first and second momenta of the quantum state shared between Alice, Bob and the trusted parties. The results of this section are original.

7.1.1 Extending the optimality of Gaussian attacks

To investigate security, we adopt the EB framework depicted in Fig. 7.1.1. We model the noisy evolution as a composition of two distinct CP maps $\mathcal{N}_1$ and $\mathcal{N}_2$, describing the quantum channel under Eve's control and the further losses and noise, respectively. As a matter of fact, $\mathcal{N}_1$ is untrusted, whilst $\mathcal{N}_2$ could be assumed to be trusted, and here we assume it is.

Overall, the signal prepared by Alice on mode A' experiences the subsequent evolutions $\mathcal{N}_1$ and $\mathcal{N}_2$ and reaches Bob, who implements a 1-rank Gaussian measurement $\{\Pi_x^{(B)}\}_x$ and stores the outcomes x in a classical register X_B. We denote by B' and B

the output modes retrieved after the maps $\mathcal{N}_1$ and $\mathcal{N}_2$, respectively (see Fig. 7.1.1). Since $\mathcal{N}_2$ is trusted, we have access to its unitary dilation guaranteed by Kraus theorem, that is a set of n trusted ancillary modes $C' = (C'_1, \dots, C'_n)$ and a unitary operation U coupling modes B' and C' [23]. The output ancillary modes after U are referred to as C. Ultimately, Alice and Bob share the state ρ_{ABC} of modes ABC.

Given this scenario, the optimal eavesdropping strategy is the "purification attack" as proved in [222, 264], where the eavesdropper is assumed to "purify" the state ρ_{ABC}. Then, Eve has access to the unitary dilation of $\mathcal{N}_1$: the state of the global (closed and isolated) system of modes $ABCE$ can be written as a pure state $|\Psi\rangle_{ABCE}$ such that $\rho_{ABC} = \mathrm{Tr}_E\left[|\Psi\rangle_{ABCE}\langle\Psi|\right]$. In turn, thanks to the property of von Neumann entropy [21, 222, 264], the Holevo information between Bob and Eve becomes $\chi(B;E) = S(ABC) - S(ABC|X_B)$, depending only on ρ_{ABC}.

Starting from these considerations, the extension of the optimality of Gaussian attacks becomes straightforward. In fact, we now prove that, for any state ρ_{ABC}:

$$\chi(B;E) \leq \chi_{\mathrm{G}}(B;E)\,, \tag{7.1}$$

where $\chi_{\mathrm{G}}(B;E)$ is the Holevo information computed for the $(n+2)$-mode Gaussian state having the same CM as ρ_{ABC}. To this aim, we exploit the results derived in framework presented in Sec. 6.4.1 and evaluate the quantity $\Delta\chi(B;E)$, see Eq. (6.43), whose positivity confirms Gaussian optimality. Indeed:

$$\begin{aligned}\Delta\chi(B;E) &= \chi_{\mathrm{G}}(B;E) - \chi(B;E)\\ &= \Delta S(ABC) - \Delta S(ABC|X_B)\\ &= \Delta S(ABC) - \Delta S\left(\overline{ABCX_B}\right) + \Delta H(X_B)\end{aligned} \tag{7.2}$$

where we used Lemma 6.1 to get the last equality. Since the map $ABC \to \overline{ABCX_B}$ is Gaussian, as Bob's detection is Gaussian, Lemma 6.3 implies:

$$\Delta S(ABC) - \Delta S\left(\overline{ABCX_B}\right) + \Delta H(X_B) \geq \Delta H(X_B)\,, \tag{7.3}$$

and, finally, exploiting Lemma 6.2 we get $\Delta H(X_B) \geq 0$.

As for the unconditional security framework, Eq. (7.1) bounds the maximum amount of information that Eve may extract during the protocol, leading to a lower bound of the KGR achievable by Alice and Bob. Remarkably, this bound can be saturated iff ρ_{ABC} itself is a Gaussian state, in which case the optimal eavesdropping coincides with an entangling cloner attack [222, 264]. Moreover, if also the map $\mathcal{N}_2$ were untrusted, we would retrieve the standard proof of Gaussian optimality under unconditional security by tracing out modes C and computing the CM of $\rho_{AB} = \mathrm{Tr}_C[\rho_{ABC}]$.

The calculation of the CM $\boldsymbol{\sigma}_{ABC}$ associated with ρ_{ABC} is further simplified under some realistic assumptions. First of all, if the map $\mathcal{N}_2$ is Gaussian, it suffices to compute the CMs $\boldsymbol{\sigma}_{AB'}$ and $\boldsymbol{\sigma}_{C'}$ of the states of AB' and C', respectively, and:

$$\boldsymbol{\sigma}_{ABC} = (\mathbb{1}_2 \oplus S)\,\boldsymbol{\sigma}_{AB'} \oplus \boldsymbol{\sigma}_{C'}\,(\mathbb{1}_2 \oplus S)^{\mathsf{T}}\,, \tag{7.4}$$

where $\oplus$ denotes direct sum, $\mathbb{1}_2$ is the 2×2 identity matrix and S is the symplectic matrix associated with the unitary operator U in Fig. 7.1.1 [31, 33]. Furthermore, if the channel $\mathcal{N}_1$ is linear and characterized by a transmissivity $0 \leq T_{\mathrm{ch}} \leq 1$ and excess noise at the transmitter $\epsilon_{\mathrm{ch}} \geq 0$, such that the total added noise is $\chi_{\mathrm{ch}} = (1 - T_{\mathrm{ch}})/T_{\mathrm{ch}} + \epsilon_{\mathrm{ch}}$, the CM $\boldsymbol{\sigma}_{AB'}$ reads:

$$\boldsymbol{\sigma}_{AB'} = \begin{pmatrix} V\,\mathbb{1}_2 & \sqrt{T_{\mathrm{ch}}}\,Z\,\boldsymbol{\sigma}_z \\ \sqrt{T_{\mathrm{ch}}}\,Z\,\boldsymbol{\sigma}_z & T_{\mathrm{ch}}\,(V+\chi_{\mathrm{ch}})\,\mathbb{1}_2 \end{pmatrix}, \tag{7.5}$$

where $V = 1 + 2\bar{n}$, $\bar{n} = \sum_k p_A(\alpha_k)|\alpha_k|^2$ being the mean number of photons per symbol and $Z = \langle\langle \Phi|(q_A q_{A'} - p_A p_{A'})|\Phi\rangle\rangle/2 = 2\,\mathrm{Tr}[\rho^{1/2} a\, \rho^{1/2} a^\dagger]$, in which $\rho = \sum_k p_A(\alpha_k)|\alpha_k\rangle\langle\alpha_k|$ is overall quantum state at Alice's side, see Eq. (6.66). In the more general case of an arbitrary $\mathcal{N}_1$, we should consider the bound in Eq. (6.69) for the off-diagonal block terms of $\boldsymbol{\sigma}_{AB'}$, as discussed in Sec. 6.4.

The present extension of the Gaussian optimality theorem provides a cornerstone to prove security under restricted eavesdropping in wider scenarios. First of all, it guarantees a sufficient condition to assess security in non-Gaussian protocols with Gaussian measurements, e.g. involving discrete modulation or non-Gaussian channels [21, 35, 250]. Thereafter, it provides a scalable approach that may be extended to composite quantum channels, such as multi-span links [22, 265, 266], free-space settings with multiple noise sources [205, 220, 267, 268], or trusted preparation noise [264, 269]. In fact, if the channel connecting Alice and Bob is modeled by a sequence of $M \geq 2$ CP maps $\mathcal{N}_j$, $j = 1, \ldots, M$, of which only $m < M$ are trusted, we bound Eve's Holevo information from the CM of the state of the quantum system composed of Alice, Bob and the ancillary modes associated with the m maps. Moreover, by increasing m, the modes under Eve's control are progressively reduced and the KGR increases accordingly. As a final remark, we note that the philosophy adopted here can be also embedded into the SDP approach of [165, 166], where, now, the quantum state shared between Alice, Bob and the trusted parties should be considered to perform the convex optimization algorithm.

7.1.2 A case study: the QPSK protocol

We now apply the optimality of Gaussian attacks to a paradigmatic example: the quadrature phase-shift keying (QPSK) protocol originally proposed in [162]. As discussed in Sec. 6.5.1, in the QPSK protocol Alice samples one of the four coherent states $|\alpha_k\rangle = |\alpha e^{i\pi(2k+1)/4}\rangle$, generated with equal a priori probability $p_A(\alpha_k) = 1/4$. The signal is then injected into the untrusted channel $\mathcal{N}_1$, assumed to be a linear channel with parameters $(T_{\mathrm{ch}}, \epsilon_{\mathrm{ch}})$, until to reach Bob, who implements homodyne detection of either quadrature q_B or p_B.

We perform the security analysis by considering trusted noisy detection at Bob's side, including non-unit quantum efficiency $\eta \leq 1$ and nonzero electronic noise. In this case, the map $\mathcal{N}_2$ describes detection noise, modeled as a thermal-loss (Gaussian) channel, where detection losses are described as a beam splitter with transmissivity η, and the electronic noise is a thermal noise arising from a two-mode squeezed state (TMSV) on two ancillary modes $C' = (C'_1, C'_2)$, whose first branch C'_1 is injected into the auxiliary port of the previous beam splitter [192, 193, 220, 269]. The TMSV has $\bar{n}_{\mathrm{d}} = \eta T_{\mathrm{ch}} \epsilon_{\mathrm{d}}/[2(1-\eta)]$ mean photons, $\epsilon_{\mathrm{d}} \geq 0$ being the detection excess noise. In turn, state $\rho_{C'}$ is a Gaussian state with CM:

$$\boldsymbol{\sigma}_{C'} = \begin{pmatrix} V_{\mathrm{d}}\, \mathbb{1}_2 & Z_{\mathrm{d}}\, \boldsymbol{\sigma}_z \\ Z_{\mathrm{d}}\, \boldsymbol{\sigma}_z & V_{\mathrm{d}}\, \mathbb{1}_2 \end{pmatrix}, \tag{7.6}$$

where $V_{\mathrm{d}} = 1 + 2\bar{n}_{\mathrm{d}}$ and $Z_{\mathrm{d}} = \sqrt{V_{\mathrm{d}}^2 - 1}$ [192]. The global channel, given by the subsequent applications of $\mathcal{N}_1$ and $\mathcal{N}_2$, is then associated with a total transmissivity $T_{\mathrm{tot}} = \eta T_{\mathrm{ch}}$ and excess noise $\epsilon_{\mathrm{tot}} = \epsilon_{\mathrm{ch}} + \epsilon_{\mathrm{d}}$ [220, 264].

To address physical layer security, we identify three scenarios associated with different trust levels at the *detection*:

- trusted losses and noise (tL; tN);
- trusted losses and untrusted noise (tL; uN);

- untrusted losses and noise (uL; uN).

The latter scenario falls under the unconditional security framework. In all the cases the lower bound on the KGR is computed as

$$K^{(\mathrm{sL;sN})} = \max_{\alpha^2} \left[\beta I_{AB}(\alpha^2) - \chi_{BE}^{(\mathrm{sL;sN})}(\alpha^2) \right] , \qquad \mathrm{s} = \mathrm{t}, \mathrm{u} \, , \tag{7.7}$$

where $\beta \leq 1$ is the reconciliation efficiency, $I_{AB}(\alpha^2)$ is the exact mutual information shared between Alice and Bob in Eq. (6.82), while $\chi_{BE}^{(\mathrm{sL;sN})}(\alpha^2)$ is the Gaussian bound over Eve's Holevo infomation, to be computed in different ways according to the scenario under investigation. For case (tL; tN), both modes C' are trusted, therefore $\chi_{BE}^{(\mathrm{sL;sN})}(\alpha^2)$ is retrieved from the 8×8 CM $\boldsymbol{\sigma}_{ABC}$ in Eq. (7.4), with the symplectic matrix S_η of the detection-losses beam splitter, namely:

$$S_\eta = \begin{pmatrix} \sqrt{\eta}\, \mathbb{1}_2 & \sqrt{1-\eta}\, \mathbb{1}_2 \\ -\sqrt{1-\eta}\, \mathbb{1}_2 & \sqrt{\eta}\, \mathbb{1}_2 \end{pmatrix} , \tag{7.8}$$

and the CMs $\boldsymbol{\sigma}_{C'}$ in (7.6) and $\boldsymbol{\sigma}_{AB'}$ in (7.5), with the choice of parameters $V = 1 + 2\alpha^2$ and

$$Z = 2\alpha^2 \sum_{k=0}^{3} \frac{\lambda_k^{3/2}}{\lambda_{k+1}^{1/2}} , \tag{7.9}$$

with $\lambda_{0,2} = e^{-\alpha^2}[\cosh(\alpha^2) \pm \cos(\alpha^2)]/2$, and $\lambda_{1,3} = e^{-\alpha^2}[\sinh(\alpha^2) \pm \sin(\alpha^2)]/2$ [162, 180]. The von Neumann entropy of the Gaussian state associated with $\boldsymbol{\sigma}_{ABC}$ is then retrieved by Eq. (2.44). On the contrary, for case (tL; uN) detection noise is untrusted, therefore the mode C_2 shall be assumed under Eve's control and the Holevo information $\chi_{BE}^{(\mathrm{sL;sN})}(\alpha^2)$ is computed from the 6×6 CM $\boldsymbol{\sigma}_{ABC_1}$ of state $\rho_{ABC_1} = \mathrm{Tr}_{C_2}[\rho_{ABC}]$, obtained by selecting the sub-blocks of $\boldsymbol{\sigma}_{ABC}$ associated with modes ABC_1. Similarly, for case (uL; uN) both modes C are untrusted, therefore $\chi_{BE}^{(\mathrm{sL;sN})}(\alpha^2)$ is obtained with the unconditional security approach, by considering the state $\rho_{AB} = \mathrm{Tr}_C[\rho_{ABC}]$ and its associated 4×4 CM $\boldsymbol{\sigma}_{AB}$.

The three resulting KGRs are reported in Fig. 7.1.2(a) as a function of the transmission distance d, for the realistic values of quantum efficiency $\eta = 0.7$ and detection noise $\epsilon_{\mathrm{d}} = 0.01$ [220], and channel excess noise $\epsilon_{\mathrm{ch}} = 0.01$. In all cases, the modulation variance V has been optimized to maximize the key rate value. As we see, $K^{(\mathrm{uL;uN})} \leq K^{(\mathrm{tL;uN})} \leq K^{(\mathrm{tL;tN})}$ and in the trusted-device scenario both the KGR and the maximum transmission distance are increased. In particular, a crucial role is played by the presence of trusted detection excess noise. ndeed, the detection noise accounts for both electronic noise of realistic measurement devices and phase mismatch introduced by an imperfect LO in the homodyne setup [192, 220], being typically larger than the channel excess noise, $\epsilon_{\mathrm{d}} \gtrsim \epsilon_{\mathrm{ch}}$. Therefore, a trusted ϵ_{d} guarantees a huge increase in the transmission distances reached by the protocol.

Furthermore, in the presence of trusted detector we observe the "fighting noise with noise" effect. That is, as displayed in Fig. 7.1.2(b), for cases (tL; uN) and (tL; tN) and large channel excess noise ϵ_{ch}, trusted losses and noise *increase* the key rate with respect to the lossless detection scheme [264, 270, 271]. It happens when the values of η and ϵ_{d} decrease Eve's information more than the mutual information $I_{AB}(\alpha^2)$, resulting in a higher KGR. While this effect is fragile against detection noise for case (tL; uN), it shows more robustness for case (tL; tN) even for large ϵ_{d}.

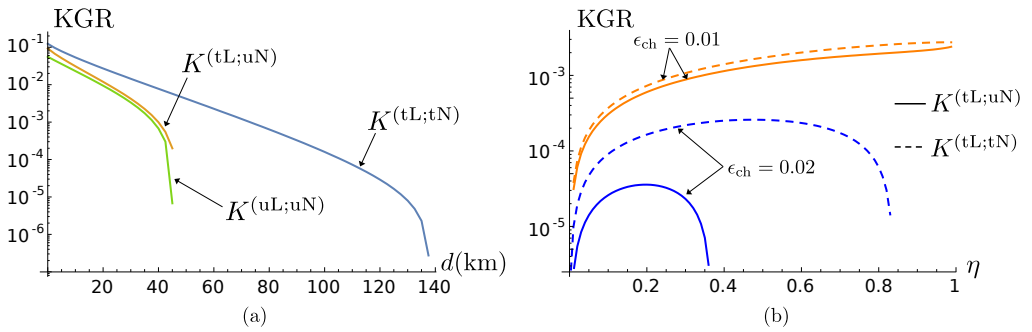


Figure 7.1.2: (a) Log plot of the optimized KGRs of the QPSK protocol $K^{(\mathrm{sL;sN})}$, $\mathrm{s} = \mathrm{t}, \mathrm{u}$, as a function of the transmission distance d in km, for the realistic parameters $\eta = 0.7$, $\epsilon_{\mathrm{d}} = 0.01$, and $\epsilon_{\mathrm{ch}} = 0.01$ [220]. (b) Log plots of the optimized KGRs $K^{(\mathrm{tL;uN})}$ and $K^{(\mathrm{tL;tN})}$, as a function of the quantum efficiency η for fixed transmission distance $d = 60$ km and detection noise $\epsilon_{\mathrm{d}} = 0.001$, and different channel excess noise ϵ_{ch}. For large ϵ_{ch}, there is an increase in the KGR in the trusted-device scenario. In both the pictures we set the reconciliation efficiency $\beta = 0.95$ and the loss rate $\kappa = 0.2$ dB/km.

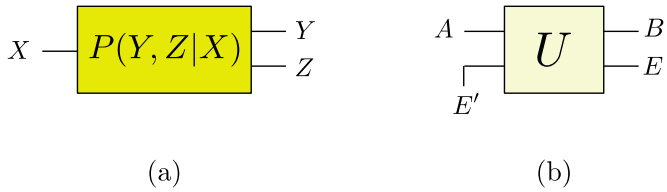


Figure 7.2.1: Schematic representation of a classical (a) and quantum (b) wiretap channel.

7.2 The wiretap channel

Finally, we discuss the last proposed security framework and address secret-key distillation in the presence of a wiretap channel. Generally speaking, the concept of wiretap channel has been first introduced by Wyner in 1975 in the context of classical communications [272]. He addressed the problem of reliable transmission of classical information over a memory-less channel being wiretapped at the receiver's side, in which the wiretapper views the channel output by a second (separately parameterized) memory-less channel. In turn, in classical information theory, the wiretap channel is completely characterized by the conditional probability distribution $P(Y, Z|X)$ between the sender, described by a classical random variable X, the legitimate receiver Y, *and* the wiretapper Z, see Fig. 7.2.1(a).

Moving to the quantum realm, the wiretap scenario involves a quantum channel $\mathcal{N} : A \to B$ between the sender, holding a quantum system A, and the receiver B, *in the presence* of a third malicious party, namely the eavesdropper Eve, E, that wiretaps the channel output by a second quantum channel $A' \to E$. Accordingly, the quantum wiretap channel, shown in Fig. 7.2.1(b), is formally described by the unitary dilation U of the CP map $\mathcal{N}$ guaranteed by Kraus theorem. The transformation $U : AE' \to BE$ couples Alice's system A to an ancillary quantum system E', leading, at the output, to a joint correlated system BE. We assume that Eve controls the input system E', being

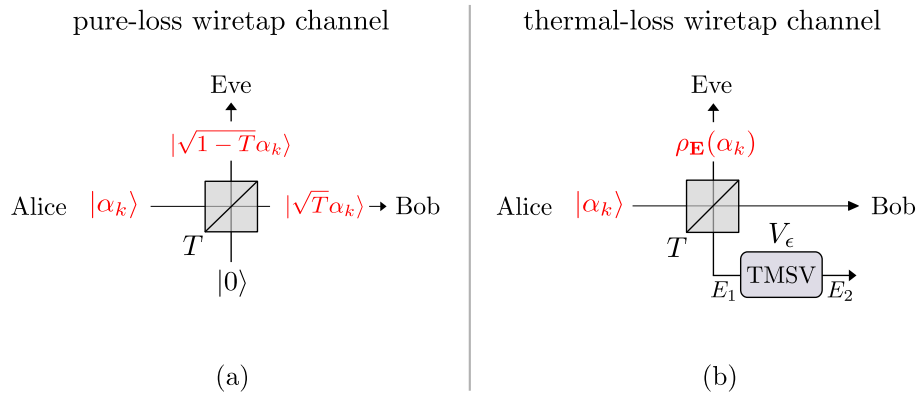


Figure 7.2.2: Scheme of the PM CVQKD protocol in the presence of a pure-loss (a) and thermal-loss (b) wiretap channel. In the former case, Eve only collects the fraction of the signals lost during the propagation through the channel, whereas in the latter, she performs an entangling-cloner attack: that is she injects one arm of a TMSV into the channel beam splitter, retrieving the final output state.

prepared in a state statistically independent of A, such that, at the output, subsystem B is sent to Bob, while she keeps subsystem E for herself. Furthermore, from the perspective of CVQKD, the wiretap channel description implies that the action of the eavesdropper is known, as the unitary U is specified, and, unlike the unconditional security case, no arbitrary channel manipulation is allowed. This captures the realistic idea that Eve is not omnipotent and cannot perform any quantum operation, but is partially limited to implement realistic attacks compatible with the state-of-the-art technologies [238, 239].

The wiretap channels associated with the usual CVQKD protocols over either pure-loss and thermal-loss channels, are depicted in Fig. 7.2.2(a) and (b), respectively, where, now, the prepare and measure (PM) approach provides the natural framework to adopt, as the unitary dilation of the channel map is known [238, 239, 264]. In both the cases, transmission losses are described by a beam splitter dynamics of suitable transmissivity $T = 10^{-\kappa d/10}$, where κ is the photon loss rate of the link. In the pure-loss case, the auxiliary port of the beam splitter is left in the vacuum, and Eve performs passive eavesdropping: that is she only collects the reflected fraction of the encoded signals. On the contrary, in the latter case, she also generates the channel excess noise acquired by the pulses, thus implementing active eavesdropping. We model this effect via the entangling cloner scheme, see Fig. 6.3.2. In more detail, Eve locally prepares a TMSV with variance $V_\epsilon = 1 + T\epsilon/(1-T)$ on two modes $\mathbf{E} = (E_1, E_2)$, and makes branch E_1 interfere with the pulse sent by Alice; ultimately, she collects the output reflected state. Physically, this implies that Eve is limited to implement a Gaussian attack, in which she both collects all the lost photons and hides behind the channel excess noise.

We conclude that, in general, performing CVQKD over a quantum wiretap channel yields a higher KGR than the unconditional security scenario, as we are considering a particular Gaussian unitary dilation of the noisy map $\mathcal{N} : A \to B$. On the contrary, the GG02 protocol provides a special case where the two approaches lead to same KGR, given that the optimal attack is known, and equal to the entangling-cloner.

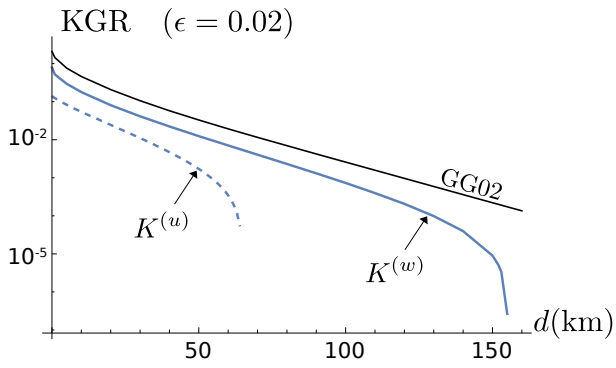


Figure 7.2.3: Log plot of the optimized KGR $K^{(w)}$ of the QPSK protocol over a wiretap channel, as a function of the transmission distance d in km, compared to both the KGR $K^{(u)}$ of the QPSK protocol under unconditional security and the GG02 protocol. We set the reconciliation efficiency $\beta = 0.95$, the loss rate $\kappa = 0.2$ dB/km and the excess noise $\epsilon = 0.02$.

7.2.1 The QPSK protocol over a wiretap channel

As a paradigmatic example, we now compute the KGR for the QPSK protocol, introduced in Sec. 6.5.1, in the presence of a thermal-loss wiretap channel. According to the previous discussions, when performing the entangling-cloner attack, Eve is undetected by Alice and Bob, who then share the same mutual information $I_{AB}(\alpha^2)$ in Eq. (6.82). The difference with respect to the unconditional security approach lies in the amount of information achievable by Eve. In fact, since the wiretap channel represents a particular unitary dilation, we expect Eve to have access to the Holevo information $\chi^{(w)}_{BE}(\alpha^2)$, being lower than that in Eq. (6.86).

However, in the present case, the computation of $\chi^{(w)}_{BE}(\alpha^2)$ is not straightforward and requires the advanced tools of Gaussian formalism summarized in Sec. 2.2.2. In particular, we adopt the PM description depicted in Fig. 7.2.2(b), noting that, if Alice samples the coherent state $|\alpha_k\rangle = |\alpha e^{i\pi(2k+1)/4}\rangle$, $k = 0, \ldots, 3$, both Eve's overall and conditional states $\rho_{\mathbf{E}}(\alpha_k)$ and $\rho_{\mathbf{E}|x_B}(\alpha_k)$, respectively, are Gaussian states. In more detail, in a thermal-loss wiretap channel, Eve generates a TMSV state with variance $V_\epsilon = 1 + T\epsilon/(1-T)$, with zero first moment (FM) vector, $\mathbf{r}^{(0)}_{\mathbf{E}} = 0$, and CM

$$\boldsymbol{\sigma}^{(0)}_{\mathbf{E}} = \begin{pmatrix} V_\epsilon \, \mathbb{1}_2 & Z_\epsilon \, \boldsymbol{\sigma}_z \\ Z_\epsilon \, \boldsymbol{\sigma}_z & V_\epsilon \, \mathbb{1}_2 \end{pmatrix}, \tag{7.10}$$

with $Z_\epsilon = \sqrt{V_\epsilon^2 - 1}$ and $\boldsymbol{\sigma}_z$ being the Pauli z-matrix. Moreover, if Alice samples a state with amplitude α_k, she gets a single-mode Gaussian state with FM $\mathbf{r}^{(0)}_A = 2\alpha\,[\cos((2k+1)\pi/4), \sin((2k+1)\pi/4)]$ and CM $\boldsymbol{\sigma}^{(0)}_A = \mathbb{1}_2$. Thereafter, Alice's pulse interferes at the channel beam splitter with Eve's mode E_1, resulting in a tripartite Gaussian state $\rho_{A\mathbf{E}}(\alpha_k)$ characterized by FM and CM equal to

$$\mathbf{r}_{A\mathbf{E}} = S\left(\mathbf{r}^{(0)}_A \oplus \mathbf{r}^{(0)}_{\mathbf{E}}\right) \qquad \text{and} \qquad \boldsymbol{\sigma}_{A\mathbf{E}} = S\left(\boldsymbol{\sigma}^{(0)}_A \oplus \boldsymbol{\sigma}^{(0)}_{\mathbf{E}}\right) S^{\mathsf{T}}, \tag{7.11}$$

with $S = S_{\rm BS} \oplus \mathbb{1}_2$ and

$$S_{\rm BS} = \begin{pmatrix} \sqrt{T}\,\mathbb{1}_2 & \sqrt{1-T}\,\mathbb{1}_2 \\ -\sqrt{1-T}\,\mathbb{1}_2 & \sqrt{T}\,\mathbb{1}_2 \end{pmatrix} \tag{7.12}$$

being the symplectic matrix associated with the beam splitter operation. From (7.11) we straightforwardly derive both Eve's overall state $\rho_{\mathbf{E}}(\alpha_k)$ and conditional state after Bob's homodyne measurement $\rho_{\mathbf{E}|x_B}(\alpha_k)$ [31, 33]. In turn, the overall quantum states at Eve's sides read:

$$\rho_{\mathbf{E}} = \frac{1}{4}\sum_{k=0}^{3} \rho_{\mathbf{E}}(\alpha_k)\,, \tag{7.13a}$$

$$\rho_{\mathbf{E}|x_B} = \frac{1}{4p_B(x_B)}\sum_{k=0}^{3} p_{B|A}(x_B|\alpha_k)\,\rho_{\mathbf{E}|x_B}(\alpha_k)\,, \tag{7.13b}$$

with the probability distributions in (6.79) and (6.81). Ultimately, we obtain the Holevo information as:

$$\chi_{BE}^{(w)}(\alpha^2) = S\big[\rho_{\mathbf{E}}\big] - \int dx_B\, p_B(x_B)\, S\big[\rho_{\mathbf{E}|x_B}\big]\,, \tag{7.14}$$

that can be computed numerically by suitably expanding states (7.13) onto the Fock basis [37]. The resulting KGR then reads:

$$K^{(w)} = \max_{\alpha^2}\Big[\beta I_{AB}(\alpha^2) - \chi_{BE}^{(w)}(\alpha^2)\Big]\,, \tag{7.15}$$

optimized over the input modulation energy.

Plot of $K^{(w)}$ is reported in Fig 7.2.3 as a function of the transmission distance d in km for $\epsilon = 0.02$, compared to the KGR $K^{(u)}$ of the QPSK protocol under unconditional security in Eq. (6.90). As expected, we have $K^{(w)} \geq K^{(u)}$, and the wiretap channel assumption leads to higher values of key rate and maximum transmission distance. Incidentally, we also note that the gap between $K^{(w)}$ and $K^{(u)}$ provides a measure of the non-Gaussianity of the protocol, as the entangling cloner scheme embedded in the wiretap model provides the optimal eavesdropping strategy for a Gaussian protocol. In turn, we expect the separation between the two key rates to be progressively reduced when considering modulation formats of increasing order than better approximate Gaussian modulation, e.g. QAM.

CHAPTER 8

Optical amplification for long-distance CVQKD

The previous Chapter showed that one of the crucial limitations of CVQKD is provided by the channel losses and noises, that both reduce the amount of extractable secure bits, i.e. the KGR, and introduce a maximum transmission distance, after which the KGR drops to 0. Accordingly, a challenging strategy to enhance CVQKD in the long-distance regime is to adopt optical amplification techniques to perform signal restoration after transmission, or, equivalently, loss mitigation. However, optical amplifiers are limited in the quantum regime, and deterministic noiseless amplification is untenable without the introduction of excess noise of quantum origin. In turn, optical amplification has to be described in terms of CP maps, and amplifiers are commonly divided into two main classes: conventional amplifiers and probabilistic noiseless linear amplifiers (NLAs). With the first tem, we refer to either phase-insensitive amplifiers (PIAs), performing noisy signal amplification by two-mode squeezing, with the ineludible introduction of thermal noise on both the field quadratures, and phase-sensitive amplifiers (PSAs), namely single-mode squeezing operations that noiselessly amplify a single field quadrature at the expense of the conjugate one. On the other hand, NLAs are probabilistic heralded schemes that perform noiseless amplification by coupling the signal mode to an ancillary system, being measured thereafter. Amplification is successful with a given probability, provided that a particular outcome is retrieved from the measurement of the ancillary system. Given this scenario, in this Chapter we address the role of optical amplification in CVQKD protocols, assessing the potentiality and limitations of each type of amplifiers.

The Chapter is organized as follows. In Sec.s 8.1 and 8.2 we introduce the problems of long-distance CVQKD and optical amplification at the quantum limit, respectively. Thereafter, we study the application of both conventional amplifiers and NLAs within the context of CVQKD. In particular, in Sec. 8.3, we discuss the role of PIAs and PSAs arranged in a multi-span configuration, addressing security under both the unconditional security framework and the trusted-device scenario, where only a single span of the link is untrusted. Then, in Sec. 8.4 we analyze NLA-assisted CVQKD under unconditional security, by considering both the application of an ideal NLA and feasible physical NLAs, that is quantum scissors (QS) and single-photon catalysis (SPC).

8.1 The problem of long-distance CVQKD

As widely discussed in the previous Chapters, CVQKD makes a sender and a receiver share a common secure key in the presence of an untrusted channel up to a maximum transmission distance $d_{\max}$, at which the key generation rate (KGR) vanishes. The value of $d_{\max}$ depends on several factors, such as the channel characteristics, e.g. the loss rate

and the amount of thermal excess noise [191], the non-unit reconciliation efficiency [210], the presence of finite-size effects [252] and the degree of trust of the channel, conditioning the amount of information at the eavesdropper's disposal [206, 220]. In turn, all these limitations crucially affect the KGR and prevent long-distance communication in practical realizations. As an example, we note that the first implementation of CVQKD at telecom wavelength has been achieved in 2007 by Lodewyck *et al.* [192], reaching the maximum distance of ≈ 25 km. Since then, in 2013 and 2016 the maximum transmission distance has been increased to 80 km [237] and 100 km [273], respectively. More recently, thanks to the exploitation of ultra-low-losses fibers, CVQKD has been established up to distances ranging from 100 to 200 km [274–277]. In contrast, the performance of realistic DVQKD, implemented by the so-called decoy states [188, 189, 278], is much more robust, reaching distances from 15 to 100 km in the early 2000s [279–282], until the record transmission distance of 421 km achieved by Zbinden *et al.* with ultra-low-loss fibers [283].

A challenging task to face those CVQKD issues is to embed strategies in the original protocols allowing to increase as much as possible the maximum transmission distance. In principle, we may follow two different approaches, aiming at either reducing the amount of channel losses or mitigating the impact of excess noise. In this Chapter, we focus on the first scenario and consider the role of the optical amplifiers, introduced in the following section, to perform signal restoration after transmission, with the intent of increasing the effective transmissivity of the channel. In more detail, in the following we take the GG02 protocol, presented in Sec. 6.3, as a benchmark, and design an improved scheme assisted by two different classes of amplifiers:

- at first, we adopt conventional optical amplifiers, namely phase-insensitive (PIAs) and phase-sensitive amplifiers (PSAs), in a multi-span configuration, where the untrusted channel is composed of many regenerative stations interspersed with lossy links. In this case, we investigate security under both the unconditional and the trusted-device frameworks;

- thereafter, we discuss a more intriguing solution provided by heralded noiseless linear amplifiers (NLAs), being probabilistic operations that amplify signals without additional noise, provided that a particular outcome is retrieved from the measurement of some ancillary modes. We consider noiseless amplification at the receiver's side and, for the sake of simplicity, we only address unconditional security, comparing both ideal and physical feasible examples of NLAs.

8.2 Amplification of optical signals

The problem of optical amplification is one of the relevant issues in quantum communications. In fact, since the development of masers in the 1950's, it has been realized that active optical media, e.g. laser systems without cavity, can be effectively used to amplify the power of a laser beam without converting it into an electrical signal [284]. For this reason, optical amplifiers can be exploited as optical repeaters for signal restoration in long distance fiber-optic communication networks, as well as front-end devices for optical receivers, in which a weak optical signal is amplified before detection. The range of possible applications makes it fundamental to assess the ultimate quantum-mechanical limitations of these devices, which has been firstly analyzed by Caves in [12].

Ideally, at the quantum limit, we would like an optical amplifier to be described by a quantum operation that, when a coherent state $|\alpha\rangle$ is considered at the input, produces

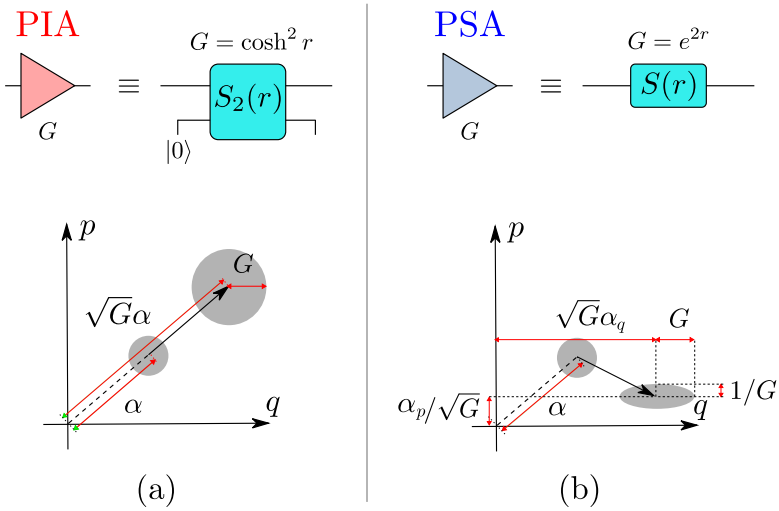


Figure 8.2.1: Schemes of the phase-insensitive amplifier (PIA) (a) and phase-sensitive amplifier (PSA) (b). In both the cases the amplification power gain G is related to the squeezing parameter r. The PIA applies the same amplification to both quadratures and introduces additional noise while PSA amplifies one of the quadratures and deamplifies the second rescaling the variances accordingly as seen on the example for a coherent state with amplitude $\alpha = \alpha_q + i\alpha_p$.

as output another coherent state with amplitude $g\alpha$, for a given real (amplitude) gain $g \geq 1$. Accordingly, $G = g^2$ represents the amplifier power gain [285]. This suggests the following input-output relation between the input radiation mode a, $[a, a^\dagger] = 1$, and the output mode $a_{\rm out}$:

$$a_{\rm out} = g\, a\,, \tag{8.1}$$

that, however, violates the canonical commutation rule:

$$[a_{\rm out}, a_{\rm out}^\dagger] = g^2\, [a, a^\dagger] = G \neq 1\,. \tag{8.2}$$

We conclude that the present transformation does not represent a physical operation, and a unitary description of optical amplification is untenable. In turn, we should recast the problem within the framework of quantum CP maps, in which case two different approaches are possible, involving either deterministic maps or heralded non-deterministic (non-unitary) transformations.

8.2.1 Phase-insensitive and phase-sensitive amplifiers

From the perspective of deterministic CP maps, the usual conclusion is that an additional noise operator should be added to the input-output relation (8.1) in order to preserve the commutation rule. That is, we introduce an ancillary optical mode b prepared in the vacuum state $|0\rangle$, such that $[b, b^\dagger] = 1$ and $[a, b] = 0$, and consider the following transformation:

$$a_{\rm out} = g\, a + \sqrt{g^2 - 1}\, b^\dagger\,, \tag{8.3}$$

that, now, satisfies $[a_{\rm out}, a_{\rm out}^\dagger] = 1$. Then, we conclude that linear amplification is an intrinsically noisy process, amplifying not only the signal power but also its noise level.

Indeed, if mode a is excited in the coherent state $|\alpha\rangle$, the expectation values and variances on the two output quadratures become

$$\langle q_{\rm out}\rangle = 2\sigma_0 g\,{\rm Re}(\alpha) \qquad \text{and} \qquad \langle p_{\rm out}\rangle = 2\sigma_0 g\,{\rm Im}(\alpha)\,, \tag{8.4a}$$

$$\Delta^2 q = \Delta^2 p = (2g^2-1)\sigma_0^2 = \sigma_0^2 + N_g\,, \tag{8.4b}$$

respectively, thus introducing an excess noise equal to $N_g = 2(g^2-1)\sigma_0^2$ on both quadratures, that turns the pure state $|\alpha\rangle$ into a mixed state.

From a practical point of view, the transformation (8.3) may be realized by the phase-insensitive amplifier (PIA) depicted in Fig. 8.2.1(a). It is implemented by coupling the signal mode a together with an ancillary mode b excited in the vacuum $|0\rangle$ and performing a two-mode squeezing operation, namely

$$S_2(r) = \exp\left[r\,(a^\dagger b^\dagger - ab)\right], \tag{8.5}$$

$r \geq 0$ being the squeezing parameter [31, 284]. The original input mode is then transformed into $a_{\rm out} = \sqrt{G}\,a + \sqrt{G-1}\,b^\dagger$, with $G = \cosh^2 r$, thus retrieving the result of Eq. (8.3). Thereafter, we trace over mode b, ending up with an amplified signal but at the expense of introducing a further ineludible noise equal to $G-1$ on both quadratures variances.

Given these considerations, PIAs are of particular interest for systems working at high powers, whereas their application at the quantum level is more limited due to the introduced excess noise [12]. The issue of noise may be circumvented by employing phase-sensitive amplifiers (PSAs), see Figure 8.2.1(b), implemented via a unitary single-mode squeezing operation

$$S(r) = \exp\left\{\frac{r}{2}\left[(a^\dagger)^2 - a^2\right]\right\}, \tag{8.6}$$

$r \geq 0$ [31, 284]. The PSA amplifies the quadrature q by a factor $\sqrt{G} = \exp(r) \geq 1$ at the expense of squeezing, i.e. de-amplifying, quadrature p by $1/\sqrt{G} \leq 1$. Consequently, the quadrature variances are also amplified and de-amplified by G and $1/G$, respectively. Crucially, the input commutation relations between the quadratures are preserved without introducing any further noise.

8.2.2 Noiseless linear amplifiers

Even if conventional amplifiers, namely PIAs and PSAs, can efficiently perform restoration of classical signals, their application at the quantum limit is more limited. Indeed, both PIAs and PSAs introduce partial distortions of the original signal, by introducing either thermal noise on both quadratures or phase-sensitive effects, respectively. Therefore, we may look for a more sophisticated solution, that produces noiseless linear amplification, albeit in probabilistic fashion. In fact, in principle, the input-output relation (8.1) can be realized by a non-deterministic (non-unitary) transformation $\mathcal{T}$, such that $\mathcal{T}|\alpha\rangle = \gamma|g\alpha\rangle$, for some constant $\gamma \in \mathbb{C}$. In particular, Eq. (8.1) is retrieved with the choice $\mathcal{T} = g^{\hat{n}}$, $\hat{n} = a^\dagger a$ being the photon-number operator of the input radiation mode, where $\mathcal{T}$ is a non-unitary unbounded operator. In turn, we have:

$$\mathcal{T}|\alpha\rangle = e^{-|\alpha|^2/2}\sum_{n=0}^{\infty}\frac{\alpha^n}{\sqrt{n!}}\,g^n|n\rangle = \gamma|g\alpha\rangle\,, \tag{8.7}$$

for the constant $\gamma = \exp[(g^2-1)|\alpha|^2/2]$. Given this consideration, we define an ideal noiseless linear amplifier (NLA) as the device implementing the CP map:

$$\mathcal{E}_{\rm id}(\rho) = P_{\rm id}\,\frac{\mathcal{T}\rho\,\mathcal{T}^\dagger}{{\rm Tr}[\mathcal{T}\rho\,\mathcal{T}^\dagger]} + (1-P_{\rm id})|0\rangle\langle 0|\,. \tag{8.8}$$

That is, we assume that an heralding signal identifies which state is produced in every run of the device, such that noiseless linear amplification of the input signal is achieved with probability $P_{\rm id} \leq 1$, whereas, in the opposite case, the output state is left into the vacuum. We also note that the success probability $P_{\rm id} \leq 1$ is not equal to the trace of the post-selected state $\mathcal{T}\,\rho\,\mathcal{T}^\dagger$, since $\mathcal{T}$ is unbounded. The map $\mathcal{E}_{\rm id}$ describes a physical operation, provided that the distinguishability of the amplified states is not increased on average [285, 286]; that is, the map must not decrease the fidelity $\mathcal{F}$ between any two input quantum states [27, 287]. In turn, for all states ρ we should have:

$$\mathcal{F}\left(\rho, |0\rangle\langle 0|\right) \leq \mathcal{F}\left(\mathcal{E}_{\rm id}(\rho), |0\rangle\langle 0|\right)\,, \tag{8.9}$$

where we exploited the property $\mathcal{E}_{\rm id}(|0\rangle\langle 0|) = |0\rangle\langle 0|$. In the presence of a coherent input $\rho = |\alpha\rangle\langle\alpha|$, this imposes a constraint on the success probability, namely [286]:

$$P_{\rm id} \leq \frac{1-e^{-|\alpha|^2}}{1-e^{-g^2|\alpha|^2}}\,. \tag{8.10}$$

In summary, provided $P_{\rm id}$ to satisfy this bound, we have an heralded probabilistic device that increases the amplitude of a coherent state retaining the initial amount of noise.

Nevertheless, to date, the unitary dilation of $\mathcal{E}_{\rm id}$, that should provide its exact experimental implementation, is still unknown. Therefore, the task is to design feasible physical NLAs, that approximate the map (8.8), at least in the limit of weak amplitudes [285, 288–296]. Here, we present two relevant examples, the quantum scissors (QS) and the single-photon catalysis (SPC).

Quantum scissors (QS). The first implementation of a physical NLA has been proposed by Ralph and Lund in [285] via the QS scheme schematized in Fig. 8.2.2(a).

In the QS scheme, the incoming signal mode a, impinges at a balanced beam splitter with the first arm of the two-mode single-photon entangled state:

$$|\varphi\rangle\!\rangle_{bc} = \sqrt{\tau}\,|10\rangle\!\rangle_{bc} + \sqrt{1-\tau}\,|01\rangle\!\rangle_{bc}\,, \tag{8.11}$$

obtained by mixing a single photon with the vacuum at a beam splitter with transmissivity τ, as depicted in Fig. 8.2.2(a). If mode a is excited in the coherent state $|\alpha\rangle$, the tripartite state at the output reads:

$$\begin{aligned}|\Psi\rangle_{abc} &= U_{ab}\,D_a(\alpha)\left[\sqrt{\tau}b^\dagger + \sqrt{1-\tau}c^\dagger\right]|000\rangle \\ &= \sqrt{\frac{\tau}{2}}D_a\left(\frac{\alpha}{\sqrt{2}}\right)D_b\left(-\frac{\alpha}{\sqrt{2}}\right)\left(|01\rangle_{ab} + |10\rangle_{ab}\right)|0\rangle_c \\ &\quad + \sqrt{1-\tau}\left|\frac{\alpha}{\sqrt{2}}\right\rangle_a\left|-\frac{\alpha}{\sqrt{2}}\right\rangle_b|1\rangle_c\,,\end{aligned} \tag{8.12}$$

where $D_{a(b)}(\cdot)$ is the displacement operator on mode $a(b)$ and U_{ab} is the beam splitter operator acting on modes a and b.

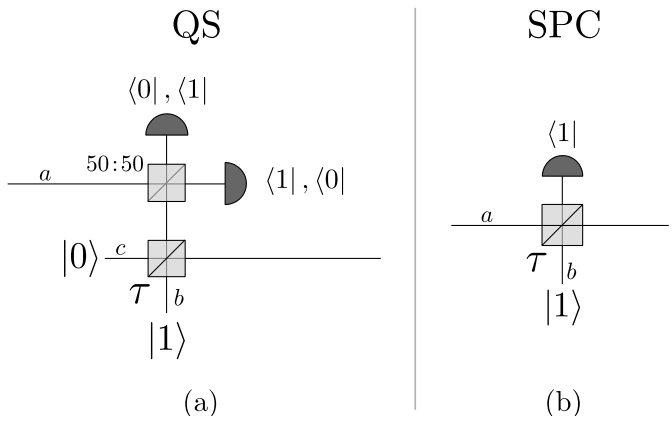


Figure 8.2.2: Schematic representation of the quantum scissors (QS) (a) and the single-photon catalyis (SPC) (b). In the QS scheme, a single photon is mixed with the vacuum at a beam splitter with transmissivity τ. One of the output branches then impinges at a balanced beam splitter with the incoming signal, after which double conditional photo-detection is performed. Noiseless amplification is achieved when one of the two detectors reveals a single photon. Instead, in the SPC process a single photon interferes directly with the incoming signal at a beam splitter with transmissivity τ and then a single photon is retrieved at the end.

Thereafter, we perform conditional photodetection on both the output modes a and b: when one of the two detectors retrieves a single photon, the output mode c is projected onto the (not normalized) quantum state:

$$|\psi\rangle = e^{-|\alpha|^2/2}\sqrt{\frac{\tau}{2}}\left[|0\rangle_c \pm \sqrt{\frac{1-\tau}{\tau}}\alpha\,|1\rangle_c\right], \tag{8.13}$$

where the "+" and "−" solutions are obtained by projection onto $\Pi_{10} = |10\rangle\!\rangle_{ab}\langle\!\langle 10|$ and $\Pi_{01} = |01\rangle\!\rangle_{ab}\langle\!\langle 01|$, respectively. In particular, for weak amplitude coherent states, i.e. $|\alpha|^2 \ll 1$, we have $|\psi\rangle \approx |g\alpha\rangle$ for the gain:

$$g = \sqrt{\frac{1-\tau}{\tau}}, \tag{8.14}$$

being larger than 1 for $\tau \leq 1/2$. Hence, the action of the QS is to truncate the coherent state expansion up to the first order and simultaneously amplify the coherent amplitude. Finally, the success probability is is given by twice the norm of $|\psi\rangle$, as NLA is successful when both the pairs of outcomes $(0,1)$ and $(1,0)$ are retrieved, leading to:

$$P_{\rm QS} = 2e^{-|\alpha|^2}\frac{\tau}{2}\left[1+g^2|\alpha|^2\right] \approx \tau e^{(g^2-1)|\alpha|^2}. \tag{8.15}$$

Experimental demonstrations of the QS scheme have also been achieved by means of linear optics, parametric-down-conversion-based single-photon source, and single-photon detection [297–299].

Single photon catalysis (SPC). It has been recently proved in [292] that also SPC provides a candidate to implement noiseless amplification. As depicted in Fig. 8.2.2(b), in

the SPC scheme a single ancillary mode b, excited in the single-photon state $|1\rangle$, impinges with the incoming signal at a beam splitter with transmissivity τ. Thereafter, photodetection is implemented on the reflected branch, conditioning on $\Pi_1 = |1\rangle\langle 1|$.

In turn, the reduced conditional dynamics for the signal mode a is described by the Kraus operator:

$$M_1 = {}_b\langle 1|U_{ab}|1\rangle_b = \left[1-(1-\tau)aa^\dagger\right] \frac{e^{\ln(\sqrt{\tau})a^\dagger a}}{\sqrt{\tau}}\,, \tag{8.16}$$

$U_{ab} = \exp[\arccos(\sqrt{\tau})\ (a^\dagger b - ab^\dagger)]$ being the beam splitter operator acting on modes a and b. When a weak coherent state $|\alpha\rangle \approx |0\rangle + \alpha|1\rangle$, $|\alpha|^2 \ll 1$, is considered at the input, we obtain:

$$|\psi\rangle = M_1|\alpha\rangle \approx \sqrt{\tau}\left[|0\rangle - \frac{1-2\tau}{\sqrt{\tau}}\alpha\,|1\rangle\right] \approx \sqrt{\tau}\,|e^{i\pi}g\alpha\rangle\,, \tag{8.17}$$

that approximates an amplified coherent state with a π phase shift and gain:

$$g = \frac{1-2\tau}{\sqrt{\tau}}\,, \tag{8.18}$$

such that $g \geq 1$ for $\tau \leq 1/4$.

Moreover, the SPC setup has been experimentally realized in [300, 301] with the intent of generating nonclassical states of light, whilst its application for noiseless amplification has not been practically tested to date. However, we note that, differently from QS, in the SPC process a single photon interferes directly with the incoming signal; therefore, SPC provides a simpler scheme and may represent a feasible alternative to QS for experimental NLA realizations.

8.3 CVQKD with phase-insensitive and phase-sensitive amplifiers

Starting from the discussions of the previous section, we now address for the first time the application of optical amplifiers as a possible resource to mitigate the losses impact in CVQKD schemes. The results obtained in the following sections are original. Here, we start from the case of PIAs and PSAs, arranged in multi-span configuration.

8.3.1 Multi-span links

To compensate transmission losses and restore the signal, a first natural option is to employ conventional optical amplifiers [12, 284, 302] and consider a multi-span link, that is, a periodic array of amplifiers connected by many independent thermal-loss channels. To date, this configuration have been investigated with the intent of increasing channel capacity for information transmission [265, 266, 303, 304], showing that both PIAs [265] and PSAs [266] induce an exponential enhancement of the ultimate capacity being more appreciable for short-distance communication. In contrast, in the context of CVQKD the role of optical amplifiers has been investigated to compensate for detection imperfections [193], raising the question on their possible application to the channel losses mitigation task. In fact, multi-span links provide a simple and versatile solution for practical implementations, unlike many other solutions. As an example, an alternative choice would be instead to insert classical-like repeaters after each span and establish keys separately between neighboring nodes. At the quantum limit, a classical repeater

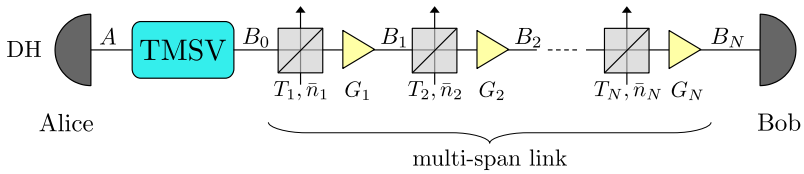


Figure 8.3.1: Scheme of CVQKD in the presence of a multi-span link. A two mode squeezed vacuum state (TMSV) is distributed between Alice and Bob. Alice performs a double homodyne (DH) measurement on her mode, whereas the mode sent to Bob travels through a thermal-loss channel modeled by a series of M beam splitters with transmissivities T_j and added mean thermal number of photons $\bar{n}_j$. To counteract losses, the signal mode B_j after each span is amplified by either PIA or PSA with power gain G_j. Finally, Bob performs a measurement which we assume to be either case I: a random homodyne detection of quadratures q/p, or homodyne detection of either q, IIa, or p, IIb.

would be described as an intercept-resend system, performing double homodyne detection on the received signal and preparing a coherent pulse with amplitude equal to the obtained outcome. Due to the probabilistic nature of quantum measurements, the overall effect of such intercept-resend strategy would be the introduction of an excess thermal noise, similar to the case of PIA. In principle, establishing keys between subsequent nodes would significantly reduce the impact of channel losses at the cost of introducing additional excesss noise due to probabilistic nature of the quadrature measurement. However, from a practical point of view, this configuration would be unfeasible in real networks, as classical-repeater nodes are expensive and, thus, cannot be placed at every few kilometers. A further solution may be the adoption of quantum repeaters [305–307], which represent an intriguing strategy from a theoretical point of view, but rather an unpractical one with current state-of-the-art technology. In fact, quantum repeaters for CV systems employ probabilistic noiseless linear amplifiers as a fundamental building block, and, thus, require the presence of a quantum memory, not yet available with the current optical communication technologies and far from a direct large-scale implementation [308, 309]. Thus, employing either classical or quantum repeaters can lead to a much higher key rate at the cost of making infrastructure complicated and expensive. On the contrary, optical amplifiers like PIA and PSA are much cheaper and manageable than repeaters and provide a feasible tool to enhance communication between the nodes.

Given these considerations, the scheme of CVQKD over multi-span links is depicted in Fig. 8.3.1. In particular, we start from the GG02 scheme in its entanglement-based version: that is, Alice has a two-mode squeezed vacuum state (TMSV) with variance $V > 1$, namely

$$|\mathrm{TMSV}\rangle\rangle = \sqrt{1-\lambda^2}\sum_{n=0}^{\infty}\lambda^n|n\rangle|n\rangle\,, \tag{8.19}$$

where $\lambda = \sqrt{(V-1)/(V+1)}$ and $|n\rangle$ being the Fock state with n photons [39]. She injects the second branch into the quantum channel while performing double homodyne (DH) detection on the remaining mode, such that the conditional state sent to Bob is a coherent state. Ultimately, Bob performs a homodyne measurement on the received pulses, which in the former version of GG02 consists of a random homodyne detection of either q or p quadratures [14, 177].

Unlike in the standard GG02 protocol, now, the quantum channel consists of a multi-span link with M spans alternated by optical amplifiers. Each span $j = 1, \dots, M$ is modeled as an independent thermal-loss channel with transmissivity $T_j \leq 1$ and excess noise $\epsilon_j \geq 0$. More precisely, the optical mode entering the j-th link is mixed at a beam splitter with transmissivity T_j with a thermal state having $\bar{n}_j = T_j \epsilon_j / [2(1 - T_j)]$ mean number of photons [39]. Thereafter, the radiation undergoes optical amplification, either phase-insensitive or phase-sensitive, before being injected into the $(j + 1)$-th span. For simplicity, here we assume both identical and equally spaced amplifiers, such that all spans have the same transmissivity $T_j = T$, added thermal noise $\bar{n}_j = \bar{n}_T$ and amplification power gain $G_j = G$. Note, however, that this choice may not be the optimal arrangement [265]. Then, if the total transmission distance is d, two neighboring amplifiers are spaced by d/M and we have

$$T = 10^{-\kappa d/(10M)}, \tag{8.20}$$

$\kappa = 0.2$ dB/km being the typical loss rate of standard optical fibers [38, 191, 192]. Moreover, we assume the added thermal photons in each span to be equal to

$$\bar{n}_T = \frac{T^M \epsilon}{2(1 - T^M)}. \tag{8.21}$$

With these choices, in the absence of optical amplification, that is $G = 1$, we retrieve the standard GG02 scenario, that is a single-span thermal-loss channel with total transmissivity $T_{\rm n} = T^M$ and added noise $\chi_{\rm n} = (1 - T_{\rm n})/T_{\rm n} + \epsilon$, $\epsilon \geq 0$ being the total excess noise [177, 222].

Starting from the scheme in Fig. 8.3.1, we address three different cases, differing from one another by both the employed amplifier and the measurement implemented by Bob:

- Case I: PIA link and random homodyne detection of quadratures q/p,
- Case IIa: PSA link and homodyne detection of quadrature q, namely the anti-squeezed quadrature,
- Case IIb: PSA link and homodyne detection of quadrature p, namely the squeezed quadrature.

We note that the presence of a PSA link makes the channel phase-sensitive, thus differentiating the behavior of quadratures q and p. Therefore, in the presence of PSAs Bob may perform homodyne detection of a single quadrature for those experimental runs dedicated to key extraction, while homodyning both q and p for the channel evaluation stage, in order to fully characterize the quantum channel [222]. We also remark the important difference between PIA and PSA: the former is a noisy operation requiring the introduction of an additional light mode lost to the environment which, in principle, can be intercepted by a malicious party, whereas the latter amplification scenario assumes unitary evolution which does not leak any information, thus being always trusted.

In the following, we compute the KGR for all three cases under both unconditional security and the trusted device scenarios, in which we assume trusted amplifiers and only a single untrusted span $0 \leq k \leq M$. To perform the analysis, we adopt the notation introduced in Fig. 8.3.1. At first Alice has two optical modes A and B_0 excited in a TMSV state. Then, the mode B_0 is injected into the sequence of M spans. We denote by B_j the optical mode coming out from the j-th span and subsequently amplified by the j-th amplifier. Finally, we refer to the last output mode as $B = B_M$. We start by computing

the mutual information shared between Alice and Bob, addressing the cases I and IIp, $\mathrm{p} = \mathrm{a}, \mathrm{b}$, separately. The whole analysis is carried out following the Gaussian formalism.

In fact, a thermal-loss channel with transmissivity $T \leq 1$ and thermal noise $\bar{n}_T$ is described via a Gaussian completely positive (CP) map associated with the matrices [31]:

$$X_{\mathrm{TL}} = \sqrt{T}\,\mathbb{1}_2 \quad \text{and} \quad Y_{\mathrm{TL}} = (1-T)(1+2\bar{n}_T)\mathbb{1}_2\,, \tag{8.22}$$

$\mathbb{1}_2$ being the 2×2 identity matrix.

As regards optical amplification, PIA are descripted by the Gaussian CP map [31]:

$$X_{\mathrm{PIA}} = \sqrt{G}\,\mathbb{1}_2 \quad \text{and} \quad Y_{\mathrm{PIA}} = (G-1)\mathbb{1}_2\,, \tag{8.23}$$

$G \geq 1$ being the amplification power gain, whilst PSA are unitary maps, thus completely described by the symplectic matrix [33]:

$$S_{\mathrm{PSA}} = \begin{pmatrix} G^{1/2} & 0 \\ 0 & G^{-1/2} \end{pmatrix}. \tag{8.24}$$

Thus, for case I, namely in the presence of a PIA link, each span is given by the composition of the two Gaussian CP maps described by Eqs. (8.22) and (8.23), resulting in a overall Gaussian CP map defined by the matrices:

$$\begin{aligned} X^{(\mathrm{I})} &= X_{\mathrm{PIA}} X_{\mathrm{TL}} = \sqrt{GT}\,\mathbb{1}_2\,, \\ Y^{(\mathrm{I})} &= X_{\mathrm{PIA}} Y_{\mathrm{TL}} X_{\mathrm{PIA}}^{\intercal} + Y_{\mathrm{PIA}} \\ &= \left[G(1-T)(1+2\bar{n}_T) + (G-1)\right]\,\mathbb{1}_2\,. \end{aligned} \tag{8.25}$$

Otherwise, for case II, namely PSA link, each span is the composition of the CP map (8.22) and the symplectic evolution (8.24), resulting in the overall Gaussian CP map associated with $X^{(\mathrm{II})} = S_{\mathrm{PSA}} X_{\mathrm{TL}}$ and $Y^{(\mathrm{II})} = S_{\mathrm{PSA}} Y_{\mathrm{TL}} S_{\mathrm{PSA}}^{\intercal}$, namely:

$$X^{(\mathrm{II})} = \begin{pmatrix} \sqrt{GT} & 0 \\ 0 & \sqrt{G^{-1}T} \end{pmatrix}, \tag{8.26}$$

and

$$Y^{(\mathrm{II})} = \begin{pmatrix} G(1-T)(1+2\bar{n}_T) & 0 \\ 0 & G^{-1}(1-T)(1+2\bar{n}_T) \end{pmatrix}. \tag{8.27}$$

Case I **: PIA link** The initial state before injection into the channel is a TMSV in modes A and B_0, completely characterized by its covariance matrix (CM)

$$\boldsymbol{\sigma}_{AB_0} = \begin{pmatrix} V\,\mathbb{1}_2 & Z\,\boldsymbol{\sigma}_z \\ Z\,\boldsymbol{\sigma}_z & V\,\mathbb{1}_2 \end{pmatrix}, \tag{8.28}$$

where $Z = \sqrt{V^2-1}$, and $\boldsymbol{\sigma}_z$ is the Pauli z-matrix.

The mode B_0 is injected into the noisy channel, which may be modeled via a sequence of Gaussian CP maps. More specifically, each node is described by a Gaussian CP map (8.23), such that the bipartite state on modes AB_j after the j-th span is a Gaussian state with associated CM $\boldsymbol{\sigma}^{(\mathrm{I})}_{AB_j} = (\mathbb{1}_2 \oplus X^{(\mathrm{I})})\boldsymbol{\sigma}^{(\mathrm{I})}_{AB_{j-1}}(\mathbb{1}_2 \oplus X^{(\mathrm{I})})^{\intercal} + (\mathbf{0} \oplus Y^{(\mathrm{I})})$, $\mathbf{0}$ being the null 2×2 matrix.

Accordingly, after M nodes applying PIA the state shared between Alice and Bob is still Gaussian with CM

$$\boldsymbol{\sigma}_{AB}^{(\mathrm{I})} = \begin{pmatrix} \boldsymbol{\sigma}_{A}^{(\mathrm{I})} & \boldsymbol{\sigma}_{Z}^{(\mathrm{I})} \\ \boldsymbol{\sigma}_{Z}^{(\mathrm{I})\mathsf{T}} & \boldsymbol{\sigma}_{B}^{(\mathrm{I})} \end{pmatrix} = \begin{pmatrix} a^{(M)}\,\mathbb{1}_2 & z^{(M)}\boldsymbol{\sigma}_z \\ z^{(M)}\boldsymbol{\sigma}_z & b^{(M)}\,\mathbb{1}_2 \end{pmatrix}, \tag{8.29}$$

where

$$a^{(M)} = V\,, \tag{8.30a}$$

$$b^{(M)} = T^{(M)}\Big[V + \chi^{(M)}\Big]\,, \tag{8.30b}$$

$$z^{(M)} = \sqrt{T^{(M)}}\,Z\,, \tag{8.30c}$$

and

$$T^{(M)} = (GT)^M\,, \tag{8.31a}$$

$$\chi^{(M)} = \frac{1}{(GT)^{M-1}}\frac{1-(GT)^M}{1-GT}\Big[\chi + \chi_G\Big]\,, \tag{8.31b}$$

$\chi = (1-T)(1+2\bar{n}_T)/T$ being the added noise introduced after the passage though a single span due to the channel thermal noise, while $\chi_G = (G-1)/(GT)$ is the added noise due to the PIA. Consequently, compared to the scenario in the absence of amplifiers, the PIA link is equivalent to a thermal-loss channel with increased transmissivity $T^{(M)} \geq T_{\mathrm{n}}$, but also increased added noise $\chi^{(M)} \geq \chi_{\mathrm{n}}$.

After transmission, Alice performs DH detection on her mode, associated with the CM $\boldsymbol{\sigma}_{\mathrm{DH}} = \mathbb{1}_2$, while Bob implements a homodyne detection of either quadrature q or p, referred to as sub-cases a and b, and described by the CMs

$$\boldsymbol{\sigma}_{\mathrm{a}} = \lim_{z\to 0}\begin{pmatrix} z & 0 \\ 0 & z^{-1} \end{pmatrix} \quad \text{and} \quad \boldsymbol{\sigma}_{\mathrm{b}} = \lim_{z\to \infty}\begin{pmatrix} z & 0 \\ 0 & z^{-1} \end{pmatrix}, \tag{8.32}$$

respectively. Due to the symmetry of (8.29), the resulting statistics for both quadrtures are identical, therefore, we can safely assume that Bob always measures the quadrature q. In turn, the mutual information between Alice and Bob may be obtained directly from (8.29) as:

$$I_{AB}^{(\mathrm{I})}(V,G) = \frac{1}{2}\log_2\left\{\frac{\det\left[\boldsymbol{\sigma}_{A}^{(\mathrm{I})} + \boldsymbol{\sigma}_{\mathrm{DH}}\right]\det\left[\boldsymbol{\sigma}_{B}^{(\mathrm{I})} + \boldsymbol{\sigma}_{\mathrm{a}}\right]}{\det\left[\boldsymbol{\sigma}_{AB}^{(\mathrm{I})} + (\boldsymbol{\sigma}_{\mathrm{DH}} \oplus \boldsymbol{\sigma}_{\mathrm{a}})\right]}\right\}, \tag{8.33}$$

where we highlighted the dependence on the free parameters V and G.

Case II **: PSA link** For cases IIp, $\mathrm{p} = \mathrm{a}, \mathrm{b}$, we follow analogous procedure as in the previous subsection. Now, each node is modeled by a Gaussian CP map (8.26). The shared state on modes AB_j has CM $\boldsymbol{\sigma}_{AB_j}^{(\mathrm{II})} = (\mathbb{1}_2 \oplus X^{(\mathrm{II})})\boldsymbol{\sigma}_{AB_{j-1}}^{(\mathrm{II})}(\mathbb{1}_2 \oplus X^{(\mathrm{II})})^{\mathsf{T}} + (\mathbf{0} \oplus Y^{(\mathrm{II})})$, thus ultimately we obtain the CM of the state shared between Alice and Bob as:

$$\boldsymbol{\sigma}_{AB}^{(\mathrm{II})} = \begin{pmatrix} \boldsymbol{\sigma}_{A}^{(\mathrm{II})} & \boldsymbol{\sigma}_{Z}^{(\mathrm{II})} \\ \boldsymbol{\sigma}_{Z}^{(\mathrm{II})\mathsf{T}} & \boldsymbol{\sigma}_{B}^{(\mathrm{II})} \end{pmatrix} = \begin{pmatrix} a^{(M)} & 0 & z_1^{(M)} & 0 \\ 0 & a^{(M)} & 0 & -z_2^{(M)} \\ z_1^{(M)} & 0 & b_1^{(M)} & 0 \\ 0 & -z_2^{(M)} & 0 & b_2^{(M)} \end{pmatrix}, \tag{8.34}$$

where

$$b_{1(2)}^{(M)} = T_{1(2)}^{(M)}\left[V + \chi_{1(2)}^{(M)}\right], \tag{8.35a}$$

$$z_{1(2)}^{(M)} = \sqrt{T_{1(2)}^{(M)}}\, Z\,, \tag{8.35b}$$

and

$$T_1^{(M)} = (GT)^M\,, \qquad T_2^{(M)} = (G^{-1}T)^M\,, \tag{8.36a}$$

$$\chi_1^{(M)} = \frac{1}{(GT)^{M-1}}\frac{1-(GT)^M}{1-GT}\chi\,, \tag{8.36b}$$

$$\chi_2^{(M)} = \frac{1}{(G^{-1}T)^{M-1}}\frac{1-(G^{-1}T)^M}{1-G^{-1}T}\chi\,, \tag{8.36c}$$

with $\chi = (1-T)(1+2\bar{n}_T)/T$.

Unlike case I, the PSA link is a phase-sensitive channel. Indeed, in the presence of PSA, quadrature q exhibits an increased transmissivity $T_1^{(M)} \geq T_{\rm n}$ and reduced added noise $\chi_1^{(M)} \leq \chi_{\rm n}$, whereas quadrature p shows a reduced transmissivity $T_2^{(M)} \leq T_{\rm n}$ with increased added noise $\chi_2^{(M)} \geq \chi_{\rm n}$. As we discuss in the following, under appropriate conditions this allows Bob to hide behind the increased noise to reduce the amount of information intercepted by an eventual eavesdropper. The mutual information for the two sub-cases $\mathrm{p} = \mathrm{a}, \mathrm{b}$ then reads:

$$I_{AB}^{(\mathrm{IIp})}(V,G) = \frac{1}{2}\log_2\left\{\frac{\det\left[\boldsymbol{\sigma}_A^{(\mathrm{II})} + \boldsymbol{\sigma}_{\rm DH}\right]\det\left[\boldsymbol{\sigma}_B^{(\mathrm{II})} + \boldsymbol{\sigma}_{\rm p}\right]}{\det\left[\boldsymbol{\sigma}_{AB}^{(\mathrm{II})} + (\boldsymbol{\sigma}_{\rm DH} \oplus \boldsymbol{\sigma}_{\rm p})\right]}\right\}. \tag{8.37}$$

In the next subsections, we will perform a security analysis of the above protocols by considering both the cases of unconditional security, where the entire channel is untrusted, and conditional security, assuming that only a single span is untrusted and may be intercepted by Eve. In both scenarios, we take as a benchmark the security of the associated protocol in the absence of optical amplifiers, referred to as the "no-amplifier protocol", in which we assume Bob to perform a random homodyne measurement of either quadrature q or p as in GG02. The results of the standard no-amplifier protocol can be retrieved from both cases I and II by fixing $G = 1$.

8.3.2 Unconditional security

At first, we analyze the performance of the discussed protocol under the unconditional security approach, where the whole transmission line is supposed to be attacked by Eve. In this framework, all elements of the multi-span link are assumed to be untrusted and the most powerful attack is the so-called purification attack [177, 222]. That is, Eve intercepts all the lost photons, and collects modes associated with the channel noise and purifies the final state shared between Alice and Bob, such that the tripartite system ABE is pure [222]. Under these conditions employing PIAs is useless because Eve would have access also to their purification, and extract more information with respect to the no-amplifier protocol. In contrast, case II is still worth of interest due to the unitarity of phase-sensitive amplification.

Considering reverse reconciliation [177, 222], for the cases IIp, $\mathrm{p} = \mathrm{a}, \mathrm{b}$, the KGR is given by

$$K_u^{(\mathrm{IIp})}(V,G) = \beta I_{AB}^{(\mathrm{IIp})}(V,G) - \chi_{BE}^{(\mathrm{IIp})}(V,G)\,, \tag{8.38}$$

where $\beta \leq 1$ is the reconciliation efficiency and $\chi_{BE}^{(\mathrm{IIp})}(V,G) = S_E - S_{E|B}^{(\mathrm{p})}$ is the Holevo information between Bob and Eve, S_E and $S_{E|B}^{(\mathrm{p})}$ being the Von Neumann entropies of Eve's overall state and Eve's conditional state after Bob's measurement, respectively. Due to the purification attack and the fact that Bob's measurement is represented by a 1-rank operator, we have $S_E = S_{AB}$ and $S_{E|B}^{(\mathrm{p})} = S_{A|B}^{(\mathrm{p})}$, where S_{AB} and $S_{A|B}^{(\mathrm{p})}$ are the Von Neumann entropies of Alice and Bob's bipartite state and Alice's conditional state, respectively. These two latter quantities can be retrieved from the CM (8.34), leading to:

$$\chi_{BE}^{(\mathrm{IIp})}(V,G) = h\left(\frac{\mathrm{d}_1 - 1}{2}\right) + h\left(\frac{\mathrm{d}_2 - 1}{2}\right) - h\left(\frac{\mathrm{d}_3^{(\mathrm{p})} - 1}{2}\right)\,, \tag{8.39}$$

where

$$h(x) = (x+1)\log_2(x+1) - x\log_2 x\,, \tag{8.40}$$

d_1 and d_2 are the symplectic eigenvalues of (8.34) and $\mathrm{d}_3^{(\mathrm{p})} = \sqrt{\det\left[\boldsymbol{\sigma}_{A|B}^{(\mathrm{IIp})}\right]}$, with

$$\boldsymbol{\sigma}_{A|B}^{(\mathrm{IIp})} = \boldsymbol{\sigma}_A^{(\mathrm{II})} - \boldsymbol{\sigma}_Z^{(\mathrm{II})}\left[\boldsymbol{\sigma}_B^{(\mathrm{II})} + \boldsymbol{\sigma}_{\mathrm{p}}\right]^{-1}\boldsymbol{\sigma}_Z^{(\mathrm{II})\mathsf{T}}\,. \tag{8.41}$$

In particular, we have:

$$\mathrm{d}_3^{(\mathrm{a(b)})} = V\sqrt{1 - \frac{Z^2}{V\left[V + \chi_{1(2)}^{(M)}\right]}}\,. \tag{8.42}$$

Finally, we perform optimization over the free parameters - modulation variance V and power gain G, obtaining

$$K_u^{(\mathrm{IIp})} = \max_{V,G} K_u^{(\mathrm{IIp})}(V,G)\,, \qquad (\mathrm{p} = \mathrm{a}, \mathrm{b})\,, \tag{8.43}$$

subject to the set of constraints $b_1^{(j)} \leq V$, see Eq. (8.35a), i.e.

$$T_1^{(j)}\left[V + \chi_1^{(j)}\right] \leq V\,, \quad (j = 1, \ldots, M)\,, \tag{8.44}$$

assuring that throughout the channel the squeezing operation does not amplify the variances of the quadratures, proportional to the total optical power, over their input values [265, 266]. This conditions arises from a physical requirement that realistic optical fibers cannot support propagation of pulses with arbitrarily high energy without damaging the optical infrastructure or the emergence of unwanted nonlinear effects. Therefore, it is reasonable to impose a condition on the gain of the PSA, such that energy of the amplified signal after each span is not larger than the input one.

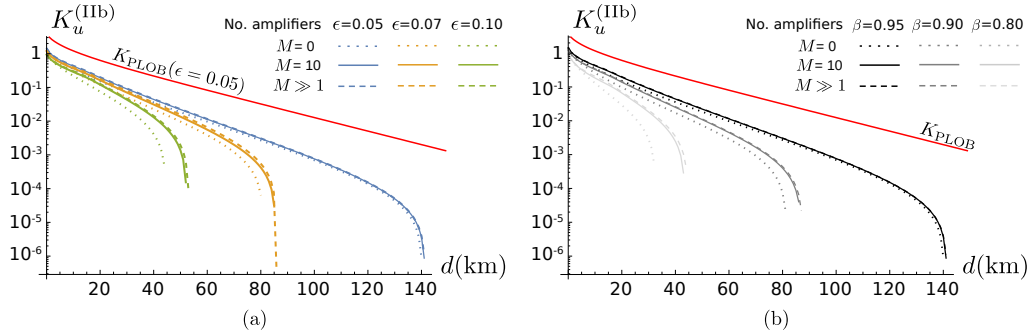


Figure 8.3.2: (a) Log plot of $K_u^{(\mathrm{IIb})}$ as a function of the transmission link length d for different level of external noise and number of amplifiers M, with fixed reconciliation efficiency $\beta = 0.95$. (b) Log plot of $K_u^{(\mathrm{IIb})}$ as a function of d for different values of reconciliation efficiency and number of amplifiers M, with fixed channel excess noise $\epsilon = 0.05$. The enhancement introduced by PSAs is accentuated for lower β. The case $M = 0$ refers to the no-amplifier protocol. The pink shaded area represents KGR greater than the PLOB bound, computed for $\epsilon = 0.05$.

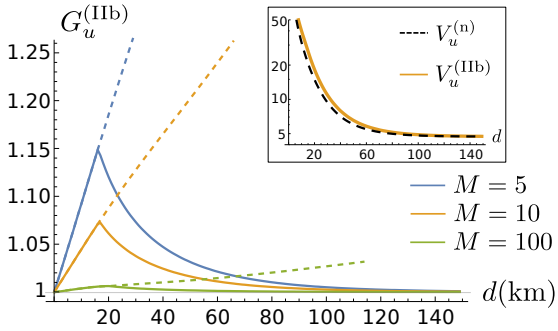


Figure 8.3.3: Plot of the optimized amplifier power gain $G_u^{(\mathrm{IIb})}$ as a function of link length d for different number of amplifiers M. The dashed lines represent the maximum attainable gain $G_{\max}^{(\mathrm{II})}$ computed with the optimized modulation $V_u^{(\mathrm{IIb})}$, presented in the inset. We set $\epsilon = 0.05$ and $\beta = 0.95$.

Furthermore, since we assume all amplifiers to be characterized by the same gain , it suffices to verify condition (8.44) for $j = 1$, satisfied if $b_1^{(1)} \leq V$, namely

$$G \leq G_{\max}^{(\mathrm{II})} \equiv \frac{V}{1 + T(V + \epsilon - 1)} \,. \tag{8.45}$$

In this security paradigm, the no-amplifier protocol is described by a single-span quantum channel with transmissivity T_{n} and added noise χ_{n}, which coincides with the GG02 protocol. The benchmark key rate $K_u^{(\mathrm{n})}$ is obtained by optimizing the unamplified KGR over the modulation variance V:

$$K_u^{(\mathrm{n})} = \max_V K_u^{(\mathrm{IIp})}(V, G = 1) \,. \tag{8.46}$$

The obtained numerical results suggest that the optimized gain for case IIa is equal to $G_u^{(\mathrm{IIa})} \equiv 1$ for all d, therefore $K_u^{(\mathrm{IIa})} \equiv K_u^{(\mathrm{n})}$ and measuring the anti-squeezed quadrature q does not increase the key rate of the discussed protocol. On the contrary, the case IIb improves the security for large values of excess noise ϵ, as depicted in Fig. 8.3.2(a). In this case, PSA links offer a higher KGR and, remarkably, increase the achievable maximum transmission distance, although the enhancement is relevant only for large excess noise, namely $\epsilon \gtrsim 0.05$ [225, 226]. Furthermore, as shown in Fig. 8.3.2(b), at fixed excess noise ϵ, the KGR increase induced by PSAs becomes larger for lower values of the reconciliation efficiency β. For the sake of completeness, in Fig. 8.3.2 we also show the Pirandola–Laurenza–Ottaviani–Banchi (PLOB) bound [310]:

$$K_{\mathrm{PLOB}} = -\log_2 \left[(1 - T_{\mathrm{n}})T_{\mathrm{n}}^{\bar{n}_T}\right] - h(\bar{n}_T) \,, \tag{8.47}$$

which represents the maximum KGR achievable with the considered repeaterless thermal-loss channel.

The optimized gain $G_u^{(\mathrm{IIb})}$ obtained from the maximization procedure is plotted in Fig. 8.3.3. For small link lengths d, constraint (8.45) leads to $G_u^{(\mathrm{IIb})} = G_{\max}^{(\mathrm{II})}$ and the gain increases with link length, whereas for larger d it becomes a decreasing function approaching 1 asymptotically. Moreover, $G_u^{(\mathrm{IIb})}$ decreases with the number of spans M, as expected. Finally, the optimized modulation $V_u^{(\mathrm{IIb})}$ is a decreasing function of the link length such that $V_u^{(\mathrm{IIb})} \geq V_u^{(\mathrm{n})}$, where $V_u^{(\mathrm{n})}$ is the optimized modulation of the no-amplifier protocol.

The physical explanation of the previous results is the following. When measuring the squeezed quadrature p, Bob observes a higher added noise with respect to the standard protocol, that is, $\chi_2^{(M)} \geq \chi_{\mathrm{n}}$, and a reduced effective transmissivity $T_2^{(M)} \leq T_{\mathrm{n}}$, as depicted in Fig. 8.3.4. In turn, the mutual information between Alice and Bob is reduced, but at the same time also Eve's Holevo information is reduced since the conditional entropy $S_{E|B}^{(\mathrm{b})}$ becomes larger, according to (8.42). The tradeoff between the two types of information leads to the the existence of an optimized gain for which the Holevo information is reduced more than the mutual information, eventually resulting in a higher KGR obtained by "hiding" behind the noise.

In light of this, the advantage introduced by PSAs shall increase with the number of spans M. In particular, we may obtain the maximum increase in KGR in the continuous-amplification limit, $M \gg 1$. Since $T^M = T_{\mathrm{n}}$ is fixed, in this limit, up to a leading order in M, we have that $T \approx 1$, $1 - T \approx -\ln T = -(\ln T_{\mathrm{n}})/M$ and $G^M = G_\infty$. Consequently, the effective transmissivities and added noises read

$$T_1^{(\infty)} = G_\infty T_{\mathrm{n}} \,, \qquad T_2^{(\infty)} = G_\infty^{-1} T_{\mathrm{n}} \,, \tag{8.48}$$

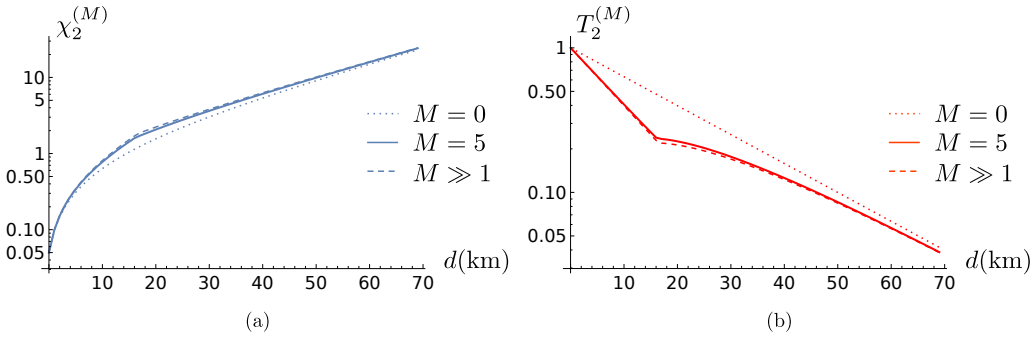


Figure 8.3.4: Plot of the added noise $\chi_2^{(M)}$ (a) and the effective link transmission $T_2^{(M)}$ (b) as a function of link length d for different number of amplifiers M for $\epsilon = 0.05$ and $\beta = 0.95$. The case $M = 0$ refers to the no-amplifier protocol.

while the effective added noise $\chi_1^{(M)}$ on quadrature q becomes:

$$\begin{aligned}\chi_1^{(\infty)} &= \lim_{M\to\infty}\left\{\frac{1}{G_\infty T_\mathrm{n}}\frac{1-G_\infty T_\mathrm{n}}{1-(G_\infty T_\mathrm{n})^{1/M}}\frac{1-T}{T}(1+2\bar{n}_T)\right\}\\ &= \frac{1}{G_\infty T_\mathrm{n}}\left[-\frac{1-G_\infty T_\mathrm{n}}{\ln(G_\infty T_\mathrm{n})/M}\right]\left[-\frac{\ln T_\mathrm{n}}{M}\right](1+2\bar{n}_T)\\ &= \frac{1-G_\infty T_\mathrm{n}}{G_\infty T_\mathrm{n}}\frac{\ln T_\mathrm{n}}{\ln(G_\infty T_\mathrm{n})}(1+2\bar{n}_T)\,,\end{aligned} \tag{8.49}$$

where we also adopted the Taylor expansion $1 - x^{1/M} = -\ln x/M + O(1/M^2)$, holding for $M \gg 1$. With analogous method, we obatin:

$$\chi_2^{(\infty)} = \frac{1-T_\mathrm{n}/G_\infty}{T_\mathrm{n}/G_\infty}\frac{\ln T_\mathrm{n}}{\ln(T_\mathrm{n}/G_\infty)}(1+2\bar{n}_T)\,, \tag{8.50}$$

and we obtain the KGR by (8.43). These channel parameters, calculated for the resulting optimized gain G_∞, are plotted in Fig. 8.3.4. Note also that even a few spans allow one to approach the continuous amplification limit.

Finally, we calculate the maximum tolerable excess noise $\epsilon_{\max}^{(\mathrm{IIb})}$ as a function of the transmission distance, reported in Fig. 8.3.5. It represents the maximum acceptable amount of noise to maintain a positive KGR. Consistently with the previous results, the exploitation of PSAs increases the maximum tolerable excess noise with respect to the no-amplifier scheme in the metropolitan-distance regime, as $\epsilon_{\max}^{(\mathrm{IIb})} \geq \epsilon_{\max}^{(\mathrm{n})}$. As expected, the advantage introduced increases with the number of nodes.

8.3.3 Trusted-device scenario

We now discuss the second instance under investigation, namely the restricted eavesdropping case. In this scenario we assume Eve to attack only a single span of the link, whilst all the remaining ones as well as the employed amplifiers are considered to be trusted, thus letting our analysis to belong to the conditional security framework. In turn, only a fraction $1/M$ of the whole fiber link is untrusted. The scheme for the eavesdropping strategy under investigation is depicted in Fig. 8.3.6. Across the whole channel, only the k-th link, $k = 1, \ldots, M$, is untrusted and may be attacked via entangling

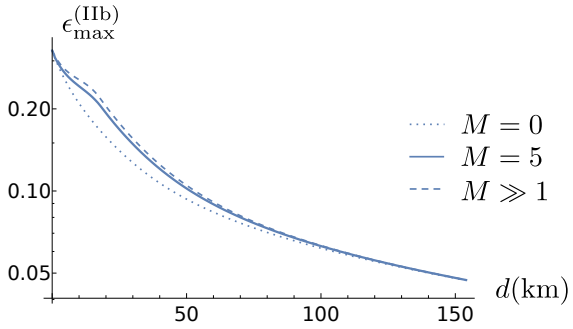


Figure 8.3.5: Plot of the maximum tolerable noise $\epsilon_{\max}^{(\mathrm{IIb})}$ as a function of the link length d for different number of amplifiers M and $\beta = 0.95$. The case $M = 0$ refers to the no-amplifier protocol.

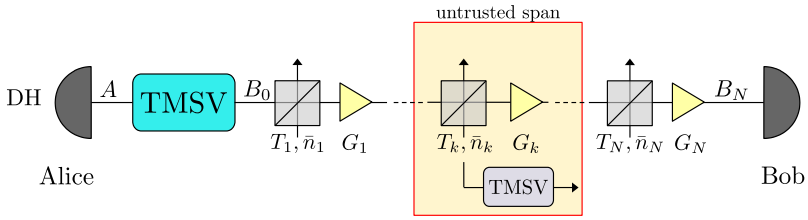


Figure 8.3.6: Scheme of the CVQKD protocol under restricted eavesdropping. All the amplifiers are trusted and Eve is allowed to attack only the k-th span, $k = 1, \ldots, M$, via active eavesdropping, that is by injecting one arm of a TMSV state into the span, hiding herself behind the introduced excess noise.

cloner attack by Eve [222, 239], performing active eavesdropping. That is, Eve hides herself behind the thermal noise $\bar{n}_k = \bar{n}_T$, equal to (8.21), by generating a TMSV state with variance $V_\epsilon = 1 + 2\bar{n}_T$ on two modes $\boldsymbol{E} = (E_1, E_2)$ and injecting mode E_1 into the second input port of the beam splitter modeling the k-th span, retrieving the reflected output state. In this way she gets undetected by Alice and Bob, as performing partial trace over modes $\boldsymbol{E}$ introduces an additive thermal noise with exactly $\bar{n}_T$ mean number of photons. In order to perform the security analysis under the above paradigm we shall compute the quantum state in Eve's possession after the entangling cloner attack. We proceed as follows, starting with the case I.

Since all nodes $j = 1, \ldots, k-1$ are trusted, the quantum state shared by Alice and Bob injected into the k-th span is in the form (8.29), namely:

$$\boldsymbol{\sigma}^{(\mathrm{I})}_{AB_{k-1}} = \begin{pmatrix} a^{(k-1)}\,\mathbb{1}_2 & z^{(k-1)}\,\boldsymbol{\sigma}_z \\ z^{(k-1)}\,\boldsymbol{\sigma}_z & b^{(k-1)}\,\mathbb{1}_2 \end{pmatrix} . \tag{8.51}$$

Instead, the CM of Eve's initial TMSV state reads:

$$\boldsymbol{\sigma}_{\boldsymbol{E}} = \begin{pmatrix} V_\epsilon\,\mathbb{1}_2 & Z_\epsilon\,\boldsymbol{\sigma}_z \\ Z_\epsilon\,\boldsymbol{\sigma}_z & V_\epsilon\,\mathbb{1}_2 \end{pmatrix} , \tag{8.52}$$

with $Z_\epsilon = \sqrt{V_\epsilon^2 - 1}$. After the interference at the beam splitter, the joint quantum state of Alice, Bob and Eve is described by the CM:

$$\boldsymbol{\sigma}^{(\mathrm{I})}_{AB_k\boldsymbol{E}} = S \left(\boldsymbol{\sigma}^{(\mathrm{I})}_{AB_{k-1}} \oplus \boldsymbol{\sigma}_{\boldsymbol{E}} \right) S^{\mathsf{T}} , \tag{8.53}$$

where

$$S = \mathbb{1}_2 \oplus S_{\mathrm{BS}} \oplus \mathbb{1}_2 , \tag{8.54}$$

and

$$S_{\mathrm{BS}} = \begin{pmatrix} \sqrt{T}\,\mathbb{1}_2 & \sqrt{1-T}\,\mathbb{1}_2 \\ -\sqrt{1-T}\,\mathbb{1}_2 & \sqrt{T}\,\mathbb{1}_2 \end{pmatrix} \tag{8.55}$$

is the symplectic matrix associated with the beam splitter operation [31, 33].

Thereafter, we let the transmitted signal pass through the remaining $M - k$ spans, applying the techniques described in 8.3.1. Ultimately, the tripartite joint state after the channel is associated with the CM:

$$\boldsymbol{\sigma}^{(\mathrm{I})}_{AB\boldsymbol{E}} = \begin{pmatrix} \boldsymbol{\sigma}^{(\mathrm{I})}_{AB} & \boldsymbol{\sigma}^{(\mathrm{I})}_{C} \\ \boldsymbol{\sigma}^{(\mathrm{I})\mathsf{T}}_{C} & \boldsymbol{\sigma}^{(\mathrm{I})}_{\boldsymbol{E}} \end{pmatrix} , \tag{8.56}$$

with the $\boldsymbol{\sigma}^{(\mathrm{I})}_{AB}$ in Equation (8.29) and

$$\boldsymbol{\sigma}^{(\mathrm{I})}_{\boldsymbol{E}} = \begin{pmatrix} \left[(1-T) b^{(k-1)} + T V_\epsilon \right] \mathbb{1}_2 & \sqrt{T} Z_\epsilon\,\boldsymbol{\sigma}_z \\ \sqrt{T} Z_\epsilon\,\boldsymbol{\sigma}_z & V_\epsilon\,\mathbb{1}_2 \end{pmatrix} , \tag{8.57}$$

$$\boldsymbol{\sigma}^{(\mathrm{I})}_{C} = \begin{pmatrix} \boldsymbol{\sigma}^{(\mathrm{I})}_{A\boldsymbol{E}} \\ \hline \boldsymbol{\sigma}^{(\mathrm{I})}_{B\boldsymbol{E}} \end{pmatrix} = \left(\begin{array}{cc} c^{(1)}\,\boldsymbol{\sigma}_z & \mathbf{0} \\ \hline c^{(2)}\,\mathbb{1}_2 & c^{(3)}\,\boldsymbol{\sigma}_z \end{array}\right) , \tag{8.58}$$

being the CM of Eve's overall state and the correlation matrix between Alice and Bob and Eve, respectively, with

$$c^{(1)} = -\sqrt{1-T}\, z^{(k-1)}\,, \tag{8.59}$$

$$c^{(2)} = \sqrt{(GT)^{M-k+1}(1-T)}\left[V_\epsilon - b^{(k-1)}\right], \tag{8.60}$$

$$c^{(3)} = \sqrt{(GT)^{M-k}G(1-T)}\, Z_\epsilon\,. \tag{8.61}$$

Subsequently, after Bob's measurement Eve is left with the conditional state associated with:

$$\boldsymbol{\sigma}^{(\mathrm{I})}_{\boldsymbol{E}|B} = \boldsymbol{\sigma}^{(\mathrm{I})}_{\boldsymbol{E}} - \boldsymbol{\sigma}^{(\mathrm{I})\mathsf{T}}_{B\boldsymbol{E}}\left[\boldsymbol{\sigma}^{(\mathrm{I})}_{B} + \boldsymbol{\sigma}_{\mathrm{a}}\right]^{-1}\boldsymbol{\sigma}^{(\mathrm{I})}_{B\boldsymbol{E}}\,. \tag{8.62}$$

Similarly as in the unconditional security case, the KGR resulting from the present conditional security analysis is given by the difference between the appropriately rescaled Alice and Bob's mutual information $I^{(\mathrm{I})}_{AB}(V,G)$ and the Holevo information between Eve and Bob $\chi^{(\mathrm{I})}_{BE}(V,G)$:

$$K^{(\mathrm{I})}_c(V,G) = \beta I^{(\mathrm{I})}_{AB}(V,G) - \chi^{(\mathrm{I})}_{BE}(V,G)\,, \tag{8.63}$$

where β denotes the reconciliation efficiency. The Holevo information can be written as

$$\chi^{(\mathrm{I})}_{BE}(V,G) = S^{(\mathrm{I})}_E - S^{(\mathrm{I})}_{E|B} = h(\mathrm{d}^{(\mathrm{I})}_1) + h(\mathrm{d}^{(\mathrm{I})}_2) - h(\mathrm{d}^{(\mathrm{I})}_3) - h(\mathrm{d}^{(\mathrm{I})}_4)\,, \tag{8.64}$$

where $h(x)$ is the function in (8.40) and $\mathrm{d}^{(\mathrm{I})}_{1(2)}$ and $\mathrm{d}^{(\mathrm{I})}_{3(4)}$ are symplectic eigenvalues of the CMs (8.57) and (8.62), respectively. The resulting optimized KGR is equal to:

$$K^{(\mathrm{I})}_c = \max_{V,G} K^{(\mathrm{I})}_c(V,G)\,, \tag{8.65}$$

subject to the constraints of maximum power in the link $T^{(j)}[V+\chi^{(j)}] \leq V$ for all $j = 1,\ldots,M$, or, equivalently,

$$G \leq G^{(\mathrm{I})}_{\max} \equiv \frac{1+V}{2+T(V+\epsilon-1)}\,. \tag{8.66}$$

The same procedure may be followed to derive the key rate of case II, identifying the corresponding CMs $\boldsymbol{\sigma}^{(\mathrm{II})}_{\boldsymbol{E}}$ and $\boldsymbol{\sigma}^{(\mathrm{IIp})}_{\boldsymbol{E}|B}$, $\mathrm{p} = \mathrm{a},\mathrm{b}$, the latter depending on the particular quadrature measured by Bob. Now, the joint state of the three parties is associated with the CM:

$$\boldsymbol{\sigma}^{(\mathrm{II})}_{AB\boldsymbol{E}} = \begin{pmatrix} \boldsymbol{\sigma}^{(\mathrm{II})}_{AB} & \boldsymbol{\sigma}^{(\mathrm{II})}_{C} \\ \boldsymbol{\sigma}^{(\mathrm{II})\mathsf{T}}_{C} & \boldsymbol{\sigma}^{(\mathrm{II})}_{\boldsymbol{E}} \end{pmatrix}, \tag{8.67}$$

with the $\boldsymbol{\sigma}_{AB}^{(\mathrm{II})}$ in Equation (8.34) and

$$\boldsymbol{\sigma}_{\boldsymbol{E}}^{(\mathrm{II})} = \begin{pmatrix} e_1 & 0 & \sqrt{T}Z_\epsilon & 0 \\ 0 & e_2 & 0 & -\sqrt{T}Z_\epsilon \\ \sqrt{T}Z_\epsilon & 0 & V_\epsilon & 0 \\ 0 & -\sqrt{T}Z_\epsilon & 0 & V_\epsilon \end{pmatrix}, \tag{8.68}$$

$$\boldsymbol{\sigma}_{C}^{(\mathrm{II})} = \begin{pmatrix} \boldsymbol{\sigma}_{A\boldsymbol{E}}^{(\mathrm{II})} \\ \hline \boldsymbol{\sigma}_{B\boldsymbol{E}}^{(\mathrm{II})} \end{pmatrix} = \left(\begin{array}{cccc} c_1^{(1)} & 0 & 0 & 0 \\ 0 & -c_2^{(1)} & 0 & 0 \\ \hline c_1^{(2)} & 0 & c_1^{(3)} & 0 \\ 0 & c_2^{(2)} & 0 & -c_2^{(3)} \end{array}\right), \tag{8.69}$$

with

$$e_{1(2)} = \left[(1-T)b_{1(2)}^{(k-1)} + TV_\epsilon\right], \tag{8.70a}$$

$$c_{1(2)}^{(1)} = -\sqrt{1-T}\, z_{1(2)}^{(k-1)}, \tag{8.70b}$$

$$c_1^{(2)} = \sqrt{(GT)^{M-k+1}(1-T)}\left[V_\epsilon - b_1^{(k-1)}\right], \tag{8.70c}$$

$$c_2^{(2)} = \sqrt{(G^{-1}T)^{M-k+1}(1-T)}\left[V_\epsilon - b_2^{(k-1)}\right], \tag{8.70d}$$

$$c_1^{(3)} = \sqrt{(GT)^{M-k}G(1-T)}\, Z_\epsilon, \tag{8.70e}$$

$$c_2^{(3)} = \sqrt{(G^{-1}T)^{M-k}G^{-1}(1-T)}\, Z_\epsilon. \tag{8.70f}$$

Finally, Eve's conditional CM reads:

$$\boldsymbol{\sigma}_{\boldsymbol{E}|B}^{(\mathrm{IIp})} = \boldsymbol{\sigma}_{\boldsymbol{E}}^{(\mathrm{II})} - \boldsymbol{\sigma}_{B\boldsymbol{E}}^{(\mathrm{II})\mathsf{T}}\left[\boldsymbol{\sigma}_{B}^{(\mathrm{II})} + \boldsymbol{\sigma}_{\mathrm{p}}\right]^{-1}\boldsymbol{\sigma}_{B\boldsymbol{E}}^{(\mathrm{II})}, \qquad \mathrm{p} = \mathrm{a}, \mathrm{b}. \tag{8.71}$$

The corresponding KGR can be written as:

$$K_c^{(\mathrm{IIp})}(V,G) = \beta I_{AB}^{(\mathrm{IIp})}(V,G) - \chi_{BE}^{(\mathrm{IIp})}(V,G), \qquad \mathrm{p} = \mathrm{a}, \mathrm{b}, \tag{8.72}$$

with the mutual information $I_{AB}^{(\mathrm{IIp})}(V,G)$ given in (8.37) and the Holevo information equal to

$$\begin{aligned} \chi_{BE}^{(\mathrm{IIp})}(V,G) &= S_E^{(\mathrm{II})} - S_{E|B}^{(\mathrm{IIp})} \\ &= h(\mathrm{d}_1^{(\mathrm{II})}) + h(\mathrm{d}_2^{(\mathrm{II})}) - h(\mathrm{d}_3^{(\mathrm{IIp})}) - h(\mathrm{d}_4^{(\mathrm{IIp})}), \end{aligned} \tag{8.73}$$

$\mathrm{d}_{1(2)}^{(\mathrm{II})}$ and $\mathrm{d}_{3(4)}^{(\mathrm{IIp})}$ being the symplectic eigenvalues of $\boldsymbol{\sigma}_{\boldsymbol{E}}^{(\mathrm{II})}$ and $\boldsymbol{\sigma}_{\boldsymbol{E}|B}^{(\mathrm{IIp})}$, respectively. Finally, one obtains

$$K_c^{(\mathrm{IIp})} = \max_{V,G} K_c^{(\mathrm{IIp})}(V,G), \tag{8.74}$$

subject to the constraint (8.45). Differently from Section 8.3.2, in this scenario the no-amplifier protocol is equivalent to the case of a wiretap channel under restricted eavesdropping, in which Eve has access only to a portion $1/M$ of the fiber link [239]. That is, we may model the channel as an asymmetric three-span channel composed of three beam splitters with effective transmissivities $T_l = T^{k-1}$, $T_k = T$ and $T_r = T^{M-k}$, and thermal noise $\bar{n}_l = \bar{n}_k = \bar{n}_r = \bar{n}_T$, respectively, in which only the central span is attacked by Eve via entangling-cloner attack. The benchmark key rate $K_c^{(\mathrm{n})}$ is then equal to:

$$K_c^{(\mathrm{n})} = \max_V K_c^{(\mathrm{I})}(V, G = 1)\,. \tag{8.75}$$

In the following, we show the obtained results, by comparing directly cases I and IIa, in which the amplified quadrature is probed by Bob and, thereafter, by discussing case IIb, where Bob detects the de-amplified quadrature.

8.3.3.1 Cases I and IIa : measuring the amplified quadrature

For both the discussed cases I and II, plots of the KGR $K_c^{(\mathrm{q})}$, $\mathrm{q} = \mathrm{I}, \mathrm{IIa}$, are presented in Figure 8.3.7 for links with $M = 5$ (a) or $M = 10$ (b) amplifiers and different positions $k = 1, \ldots, N$ of the untrusted span, and compared to $K_c^{(\mathrm{n})}$ for no-amplifier protocol. We underline that the results for $M = 5$ and $M = 10$ can be only qualitatively compared, as we keep the assumption that only one span is untrusted and, in turn, by increasing M Eve becomes more and more restricted.

In general, one can observe that, when Bob measures the amplified quadrature, both PIAs and PSAs improve the KGR with respect to the no-amplifier protocol only if Eve attacks one of the first spans of the fiber-link. The case $k = 1$, where the first span is the untrusted one, represents the best-case scenario, where the key rate is increased by several orders of magnitude. Indeed, in this scenario the signal intercepted by Eve has not been amplified yet. Thus, Eve's overall state, described by the CM $\boldsymbol{\sigma}_{\boldsymbol{E}}^{(\mathrm{q})}$, is independent of the gain G and the only effect of amplification is the reduction of the conditional entropy $S_{E|B}^{(\mathrm{q})}$ appearing in the Holevo information Eqs. (8.64) and (8.73). On the other hand, for $k \geq 2$, amplifying Bob's received signal also increases Eve's overall entropy $S_E^{(\mathrm{q})}$. In turn, the benefits of optical amplification are more and more reduced with increasing k. To better quantify this effect, we compute the ratio:

$$\mathcal{R}^{(\mathrm{q})} = \frac{K_c^{(\mathrm{q})}}{K_c^{(\mathrm{n})}}\,, \qquad \mathrm{q} = \mathrm{I}, \mathrm{IIa}\,, \tag{8.76}$$

which is presented in Figure 8.3.7(c-d). All ratios are initially equal to 1 up to a threshold distance, that is, $\mathcal{R}^{(\mathrm{q})} = 1$ if $d \leq d_{\min}^{(\mathrm{q})}$, thereafter for $k \geq 2$ they reach a maximum and then decrease towards an asymptotic value. Moreover, the key ratio $\mathcal{R}^{(\mathrm{q})}$ decreases with increasing k and there exists a threshold value k_{th} such that for $k \geq k_{\mathrm{th}}^{(\mathrm{q})}$ we have $\mathcal{R}^{(\mathrm{q})} \equiv 1$. Therefore, if Eve attacks a span located further, $k \geq k_{\mathrm{th}}^{(\mathrm{q})}$, employing signal amplification is no longer beneficial. For link parameters values $\kappa = 0.2\,\mathrm{dB/km}$, $\epsilon = 0.05$ and $\beta = 0.95$ one obtains $k_{\mathrm{th}}^{(\mathrm{I})} = 2$ and $k_{\mathrm{th}}^{(\mathrm{IIa})} = 3$ for $M = 5$, while for $M = 10$ one gets $k_{\mathrm{th}}^{(\mathrm{I})} = 5$ and $k_{\mathrm{th}}^{(\mathrm{IIa})} = 8$. Importantly, note that the performance of PIA links is always lower than PSA ones, as $\mathcal{R}^{(\mathrm{I})} \leq \mathcal{R}^{(\mathrm{IIa})}$, $d_{\min}^{(\mathrm{I})} \leq d_{\min}^{(\mathrm{IIa})}$ and $k_{\mathrm{th}}^{(\mathrm{I})} \leq k_{\mathrm{th}}^{(\mathrm{IIa})}$. This is a direct consequence of the additional noise introduced by the phase-insensitive amplification process.

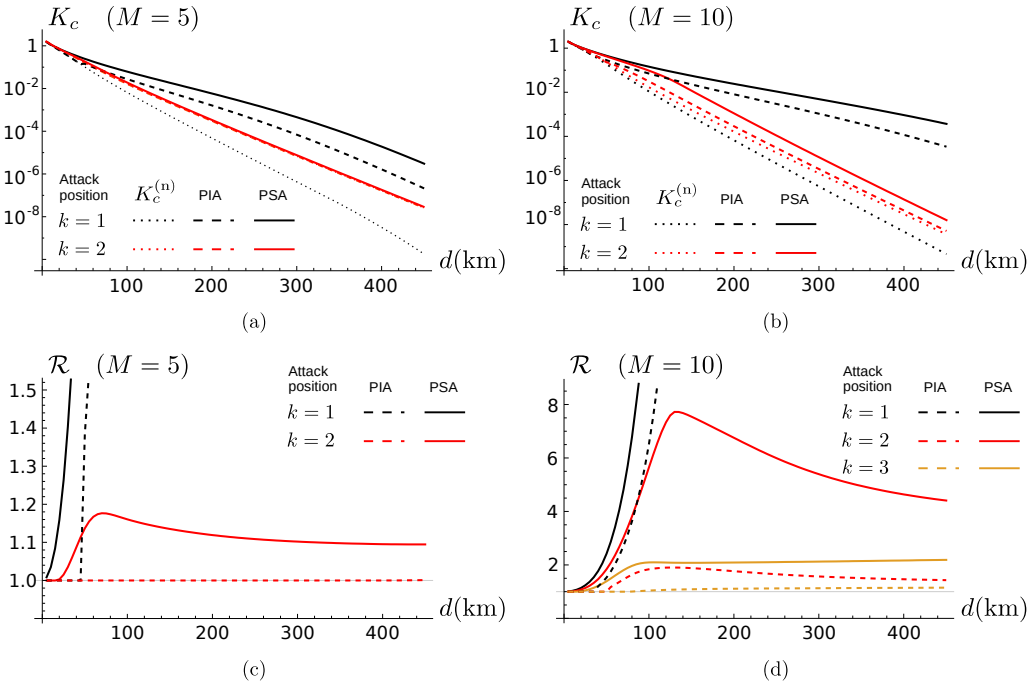


Figure 8.3.7: Plot of the optimized KGR K_c and key ratio $\mathcal{R}$ for cases I and IIa as a function of the transmission link length d for different locations of the eavesdropper for $M = 5$ (a) and (c) and $M = 10$ (b) and (d), respectively. We set $\epsilon = 0.05$ and $\beta = 0.95$.

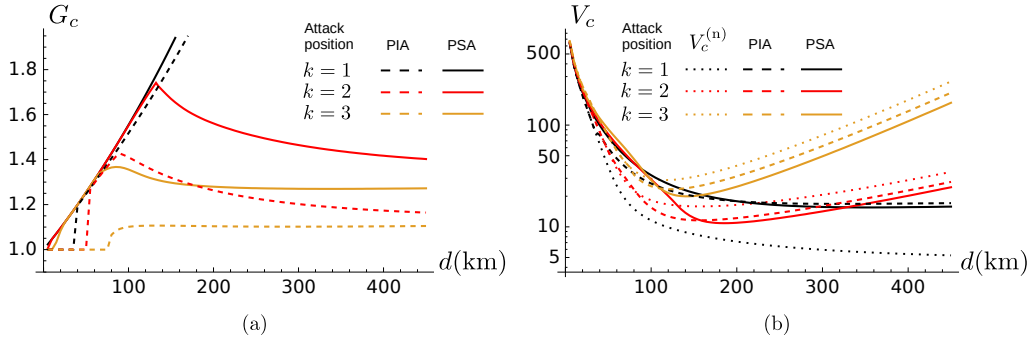


Figure 8.3.8: Optimal amplifier power gain (a) and modulation (b) for cases I and IIa as a function of the link length d for different locations of the untrusted span k for $M = 10$, $\epsilon = 0.05$ and $\beta = 0.95$.

The optimized gain $G_c^{(\mathrm{q})}$ and modulation $V_c^{(\mathrm{q})}$, $\mathrm{q} = \mathrm{I}, \mathrm{IIa}$, are depicted in Figure 8.3.8 (a) and (b), respectively. Consistent with the results from the previous paragraph, it is optimal to not amplify the signal, i.e. $G_c^{(\mathrm{q})} = 1$, for short distances $d \leq d_{\min}^{(\mathrm{q})}$. For longer link lengths the optimal gain initially increases with d, following constraints (8.45) and (8.66), and then ultimately decreases towards an asymptotic value. The optimal gain $G_c^{(\mathrm{q})}$ also decreases with k, similarly to the key ratio. On the other hand, the behavior of optimal modulation $V_c^{(\mathrm{q})}$ is quite peculiar. For $k = 1$ it is a monotonous decreasing function of the transmission distance d, as obtained in Section 8.3.2. The presence of optical amplifiers increases the modulation value with respect to the no-amplifier protocol, as $V_c^{(\mathrm{q})} \geq V_c^{(\mathrm{n})}$. On the contrary, when $k \geq 2$ the situation is completely different and in the long-distance regime the optimized modulation turns out to be an increasing function of d. In fact, if Eve attacks one of the last spans of the communication link she intercepts a weak pulse, therefore it is possible to safely increase the input modulation variance without preventing secure communication between Alice and Bob.

When the amplified quadrature is measured, the effective transmissivity probed by Bob, namely $T^{(M)}$ and $T_1^{(M)}$ for cases I and IIa respectively, is larger with respect to the no-amplifier protocol, $T^{(M)}, T_1^{(M)} \geq T_{\mathrm{n}}$. This leads to an increase of both mutual information between Alice and Bob, and, at the same time, Holevo information on Eve's side. This is because for $k \geq 2$ she also receives an amplified signal. In turn, when performing optimization over the free parameters, there emerges a tradeoff between these two types of information, resulting in the key rates shown in Figure 8.3.7. In particular, for short-distance communication, $d \leq d_{\min}^{(\mathrm{q})}$, one obtains that optical amplification is useless, $G_c^{(\mathrm{q})} = 1$. The difference between cases I and IIa is due to the different impact of the added noise. In fact, for case IIa the added noise is rescaled with respect to the no-amplifier protocol, $\chi_1^{(M)} \leq \chi_{\mathrm{n}}$, whilst for case I the noise is increased because of the additive contribution χ_G due to phase-insensitive amplification, $\chi^{(M)} \geq \chi_{\mathrm{n}}$. In the latter case the (incoherent) added contribution χ_G detriments the mutual information between Alice and Bob, being less than its counterpart of case IIa. Ultimately, this leads to a reduced performance of PIA links with respect to PSA ones.

8.3.3.2 Case IIb : measuring the de-amplified quadrature

The KGR $K_c^{(\mathrm{IIb})}$ for the Bob's measurement of the de-amplified quadrature, IIb, is depicted in Figure 8.3.9 for links with $M = 5$ (a) or $M = 10$ (b) amplifiers and different positions $k = 1, \ldots, M$ of the untrusted span, together with the key ratio

$$\mathcal{R}^{(\mathrm{IIb})} = \frac{K_c^{(\mathrm{IIb})}}{K_c^{(\mathrm{n})}} \,. \tag{8.77}$$

The scenario is reversed with respect to the previous cases. Indeed, when Bob probes the squeezed (i.e. de-amplified) quadrature, PSA links improve the resulting KGR if Eve attacks one of the last spans of the channel. The best-case scenario is provided by $k = M$, in which the KGR increases by more than an order of magnitude. Consequently, and in contrast to the results from Section 8.3.3.1, one observes enhancement in the key ratio $\mathcal{R}^{(\mathrm{IIb})}$ with increasing k. In this scenario the PSA becomes useless if Eve attacks the first span for all M, namely $\mathcal{R}^{(\mathrm{IIb})} \equiv 1$, since in this case she intercepts the pulse before all amplifiers and therefore, de-amplifying the signal only reduces the mutual information between Alice and Bob, maintaining a higher Holevo information at Eve's side. On the

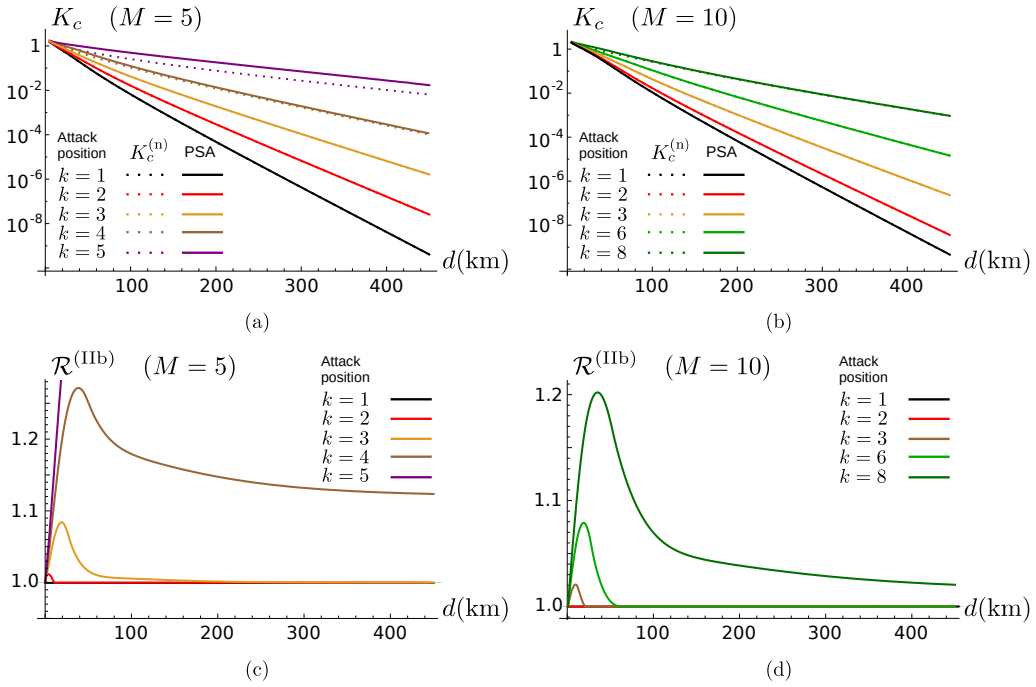


Figure 8.3.9: Plot of the optimized KGR and key ratio $\mathcal{R}^{(\mathrm{IIb})}$ for case IIb as a function of the transmission link length d for different locations of the eavesdropper for $M = 5$ (a) and (c) and $M = 10$ (b) and (d), respectively. We set $\epsilon = 0.05$ and $\beta = 0.95$.

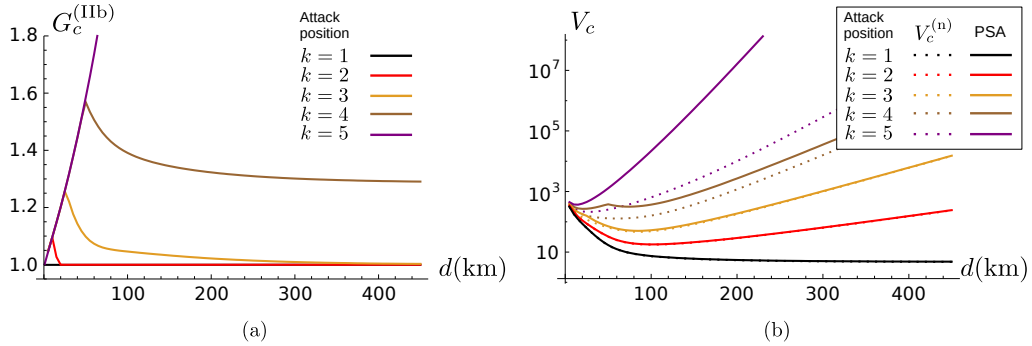


Figure 8.3.10: Optimal amplifier power gain (a) and modulation (b) for case IIb as a function of the link length d for different locations of the untrusted span k for $M = 10$, $\epsilon = 0.05$ and $\beta = 0.95$.

other hand, for $k \geq 2$, de-amplifying Bob's signal also reduces Eve's extracted information, thus leading to $\mathcal{R}^{(\mathrm{IIb})} \geq 1$. In particular, there exists a threshold attack location $k_{\mathrm{th}}^{(\mathrm{IIb})}$ such that for $k \leq k_{\mathrm{th}}^{(\mathrm{IIb})}$ one has $\mathcal{R}^{(\mathrm{IIb})} \equiv 1$, being equal to $k_{\mathrm{th}}^{(\mathrm{IIb})} = 1$ for $M = 5$ and $k_{\mathrm{th}}^{(\mathrm{IIb})} = 2$ for $M = 10$. For eavesdropping performed on a span located further within the link $k \geq k_{\mathrm{th}}^{(\mathrm{IIb})}$ all key ratios exhibit a maximum and then decrease towards an asymptotic value, equal to 1 for locations closer to the threshold value or greater than 1 for those placed further, implying an improvement of security in the long-distance regime brought by the PSA link.

We note that the absence of PSA advantage for $k = 1$ does not stand in contradiction with its existence in the unconditional security framework discussed in Section 8.3.2, where Eve is assumed to collect the reflected pulses from all spans. This is because de-amplification reduces the accessible information contained in the signals lost after the second span, eventually resulting in a enhancement of the KGR.

In Figure 8.3.10(a) and (b), one can see the optimized gain $G_c^{(\mathrm{IIb})}$ and modulation $V_c^{(\mathrm{IIb})}$, respectively. We see that amplification is not beneficial, $G_c^{(\mathrm{IIb})} \equiv 1$, for eavesdropping performed on initial spans $k \leq k_{\mathrm{th}}^{(\mathrm{IIb})}$, whereas for attacks on latter spans the optimal gain increases with the link length following constraint (8.45), until finally decreasing towards an asymptotic value. In accordance with the previous results, one needs to employ the stronger optimal amplification the further the eavesdropped span is located. The optimized modulation increases with respect to the no-amplifier protocol $V_c^{(\mathrm{IIb})} \geq V_c^{(\mathrm{n})}$. Similarly to the results obtained in Section 8.3.3.1, it is a decreasing function of the link length if the attack is performed on the first span, whilst it becomes non-monotonous for $k \geq 2$, increasing in the long-distance regime.

The physical meaning of these results is analogous to these obtained in Section 8.3.2. Indeed, the case IIb is associated with a reduced transmissivity with respect to the no-amplifier protocol, $T_2^{(M)} \leq T_{\mathrm{n}}$, and amplified added noise $\chi_2^{(M)} \geq \chi_{\mathrm{n}}$. Therefore, for $k \geq 2$ by employing PSAs Bob accepts to reduce the extracted mutual information, in order to increase the conditional entropy $S_{E|B}^{(\mathrm{IIb})}$, resulting in a lower Holevo information between Eve and himself. The tradeoff between these two quantities is such that for $k \geq k_{\mathrm{th}}^{(\mathrm{IIb})}$ one has $G_c^{(\mathrm{IIb})} \geq 1$ and PSA links increase the obtained KGR.

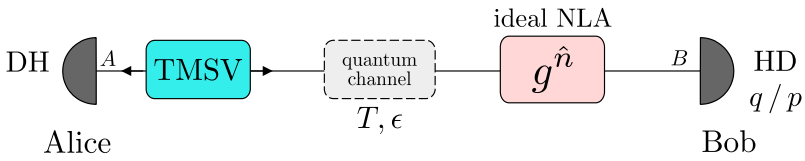


Figure 8.4.1: Scheme of the CVQKD protocol assisted by the ideal NLA proposed in [287]. Alice performs double homodyne (DH) detection on the first branch of a TMSV state with variance $V > 1$ to perform coherent state generation. The second one is then injected into the thermal-loss channel to Bob, who implements the ideal NLA operation $g^{\hat{n}}$ to amplify his signal, before performing homodyne (HD) detection.

8.4 CVQKD with noiseless linear amplifiers

As outlined in the previous section, conventional amplifiers based on parametric down conversion have a relatively limited impact of CVQKD in the presence of unconditional security, whereas they prove themselves more powerful under restricted eavesdropping, when only few parts of the fiber links are untrusted. An intriguing solution to overcome this fundamental limitation is provided by heralded noiseless linear amplification at the receiver's side. Indeed, in 2012 Blandino *et al.* showed that an ideal probabilistic NLA with amplitude gain g leads to an increase in the maximum transmission distance proportional to $\log g$ [287]. Nevertheless, any realistic physical NLA can only approximate the ideal amplifier for low-amplitude optical signals [285, 288–296]. To avoid this drawback, measurement-based NLAs, performing virtual amplification based on classical data post-selection, have also been proposed [311–313]. However, the low success probabilities of these operations [314, 315] make physical NLAs still worth of investigation. Recently, CVQKD employing quantum scissors (QS) [285] has been addressed, allowing to achieve long-distance secure communication for sufficiently low channel excess noise [35, 250]. To the same goal, also single-photon catalysis (SPC) has been investigated [292, 316].

In the following, we firstly present the unconditional security analysis for the GG02 protocol assisted by the ideal NLA proposed by Blandino *et al.*. Thereafter, we investigate security in the presence of feasible physical NLAs, realized via either the quantum scissors (QS) or the single-photon catalysis (SPC) scheme, in which we consider the simplified realistic scenario where photo-detection is replaced by on-off detection, see Sec. 8.2.2. Moreover, we distinguish two alternative cases. In the former, we fix the NLA gain g and show that also physical NLAs increase the maximum transmission distance by the same amount $\ln g$ as the ideal amplifier. In the latter, we assume g to be a free parameter and optimize its value, obtaining that both physical and ideal NLAs achieve arbitrary long-distance CVQKD. For the physical amplifiers, we also discuss the robustness in the presence of a quantum detection efficiency $\eta \leq 1$, showing that the detection efficiency only rescales the KGR without preventing long-distance communication.

8.4.1 Ideal NLA

To begin with, we consider a GG02 scheme in which Bob employs an ideal NLA to amplify his received signal, as depicted in Fig. 8.4.1. That is, Alice prepares a two-mode squeezed vacuum (TMSV) state with modulation variance $V > 1$ and injects one mode

into a thermal-loss channel with transmissivity $T \leq 1$ and excess noise $\epsilon \geq 0$, with corresponding added noise $\chi = (1-T)/T + \epsilon$. Thereafter, Bob implements an ideal NLA with gain $g > 1$ on his received pulse, before performing a Gaussian measurement, here assumed to be homodyne (HD) detection. As discussed in Sec. 8.2.2, the ideal NLA is a non-deterministic operation described by the self-adjoint operator $g^{\hat{n}}$, $\hat{n}$ being the photon-number operator of the optical mode undergoing amplification, therefore it preserves Gaussianity [285, 287]. Therefore the protocol in Fig. 8.4.1 is equivalent to a GG02 scheme where Alice and Bob share a Gaussian state with covariance matrix (CM):

$$\boldsymbol{\sigma}_{AB}^{(\mathrm{id})} = \begin{pmatrix} V_{\mathrm{id}}\, \mathbb{1}_2 & \sqrt{T_{\mathrm{id}}} Z_{\mathrm{id}}\, \boldsymbol{\sigma}_z \\ \sqrt{T_{\mathrm{id}}} Z_{\mathrm{id}}\, \boldsymbol{\sigma}_z & T_{\mathrm{id}}(V_{\mathrm{id}} + \chi_{\mathrm{id}})\, \mathbb{1}_2 \end{pmatrix}, \tag{8.78}$$

with $\chi_{\mathrm{id}} = (1 - T_{\mathrm{id}})/T_{\mathrm{id}} + \epsilon$, $Z_{\mathrm{id}} = \sqrt{V_{\mathrm{id}}^2 - 1}$, and the effective channel parameters, explicitly derived in App. A.3:

$$V_{\mathrm{id}} = V + \frac{T(g^2-1)Z^2}{2 - T(g^2-1)(V - 1 + \epsilon)}, \tag{8.79a}$$

$$T_{\mathrm{id}} = \frac{g^2 T}{1 + T(g^2-1)[1 + T\epsilon(g^2-1)(2-\epsilon)/4 - \epsilon]}, \tag{8.79b}$$

$$\epsilon_{\mathrm{id}} = \epsilon + (g^2 - 1)\frac{T\epsilon(2-\epsilon)}{2}, \tag{8.79c}$$

provided that:

$$g \leq \sqrt{1 + \frac{2}{T(V + \epsilon - 1)}}. \tag{8.80}$$

Without the last condition on the gain an unphysical un-normalizable state is obtained [285, 287]. Equivalently, for a fixed gain Eq. (8.80) corresponds to a threshold of the transmissivity, namely:

$$T \leq T_{\mathrm{th}} \equiv \frac{2}{(g^2-1)(V + \epsilon - 1)}, \tag{8.81}$$

preventing the use of the NLA protocol for distances $d \leq d_{\mathrm{th}}^{(\mathrm{id})} = (-10 \log_{10} T_{\mathrm{th}})/\kappa$. For $d > d_{\mathrm{th}}^{(\mathrm{id})}$, employing the ideal NLA is equivalent to considering an effective channel of increased transmissivity $T_{\mathrm{id}} \geq T$. The resulting KGR then reads:

$$\widetilde{K}_{\mathrm{id}}(V, g) = P_{\mathrm{id}}(V, g)\left[\beta I_{AB}^{(\mathrm{id})}(V, g) - \chi_{BE}^{(\mathrm{id})}(V, g)\right], \tag{8.82}$$

where $P_{\mathrm{id}}(V, g)$ is the success probability of the NLA, $\beta \leq 1$ is the reconciliation efficiency, whereas $I_{AB}^{(\mathrm{id})}(V, g)$ and $\chi_{BE}^{(\mathrm{id})}(V, g)$ are computed from Eq.s (6.34) and (6.41), respectively, with the modified parameters (8.79). As demonstrated in App. A.3, the success NLA probability is bounded by $P_{\mathrm{id}}(V, g) \leq 1/g^2$, therefore from now on we consider as a benchmark the KGR:

$$K_{\mathrm{id}}(V, g) = \frac{1}{g^2}\left[\beta I_{AB}^{(\mathrm{id})}(V, g) - \chi_{BE}^{(\mathrm{id})}(V, g)\right]. \tag{8.83}$$

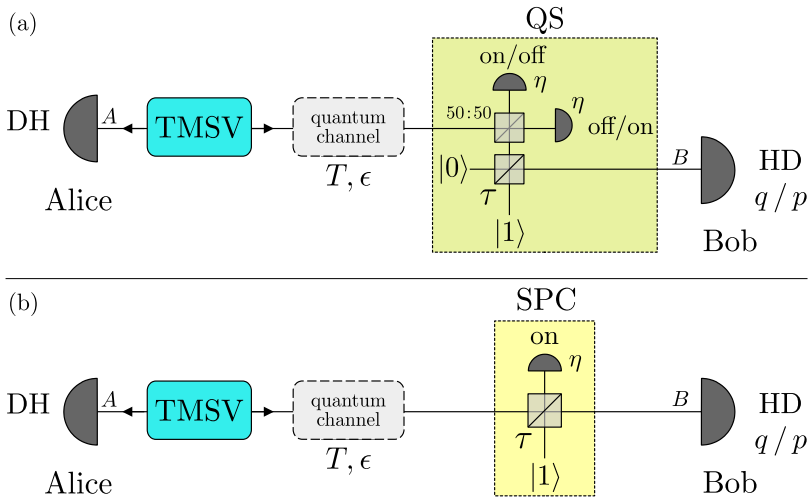


Figure 8.4.2: Scheme of the CVQKD protocol assisted by the two physical NLAs discussed in the paper. (a) Strategy based on quantum scissors (QS); (b) strategy based on single-photon catalysis (SPC).

The KGR (8.83) depends on the two free parameters V and g that can be optimized. As discussed in the following, the choice of the gain g will be a crucial task. Hence, we will discuss two separate cases. In the former case we assume a fixed g and optimize only the modulation variance, obtaining the KGR:

$$K_{\rm id}(g) = \max_{V} K_{\rm id}(V, g)\,, \tag{8.84}$$

and the corresponding distance-dependent modulation $V_{\rm opt}^{\rm (id)}(g)$. In the latter case the optimization involves also the gain, obtaining:

$$K_{\rm id} = \max_{V,g} K_{\rm id}(V, g)\,, \tag{8.85}$$

and the associated parameters $V_{\rm opt}^{\rm (id)}$ and $g_{\rm opt}^{\rm (id)}$. For the sake of clarity, we will review the obtained results in Sec. 8.4.3 together with the physical NLA-assisted strategies under investigation.

8.4.2 Physical NLAs: QS and SPC

Now, we consider the more realistic scenario in which Bob employs a physical NLA, realized via either QS or SPC and employing on-off detection rather than photon counting.

In the QS scheme proposed in [35], see Fig. 8.4.2(a), Bob prepares two ancillary modes in the Fock states $|1\rangle$ and $|0\rangle$, respectively. He mixes them at a beam splitter with transmissivity τ and lets the reflected signal interfere at a balanced beam splitter with the pulse received by Alice. Then, he performs conditional on-off detection on both the output branches (see App. A.4 for details), corresponding to the positive-operator-valued measurement (POVM) $\{\Pi_{\rm off}, \Pi_{\rm on} = \mathbb{1} - \Pi_{\rm off}\}$, where:

$$\Pi_{\rm off} = \sum_{k=0}^{\infty} (1-\eta)^k |k\rangle\langle k|\,, \tag{8.86}$$

and $\eta \leq 1$ is the detection quantum efficiency. If one of the two detectors gives the outcome "on", Bob performs homodyne detection on the post-selected output state. The value of τ fixes the gain associated with the NLA, that for low-amplitude coherent signals reads $g = \sqrt{(1-\tau)/\tau}$ [285]. Thus, to achieve the gain g we set the transmissivity equal to:

$$\tau_{\rm QS}(g) = \frac{1}{1+g^2}\,. \tag{8.87}$$

On the contrary, in the SPC scheme, reported in Fig. 8.4.2(b), Bob has a single ancillary mode excited in $|1\rangle$ impinging at a beam splitter with transmissivity τ with the pulse received by Alice. He performs on-off detection on the reflected branch, conditioning on outcome "on", and homodynes the post-selected state. The associated gain is $g = (1-2\tau)/\sqrt{\tau}$ [292], which can be inverted to find the transmissivity as a function of the gain,

$$\tau_{\rm SPC}(g) = \frac{1}{8}\left(4+g^2-g\sqrt{8+g^2}\right). \tag{8.88}$$

In both the cases, after the NLA Alice and Bob share a non-Gaussian state $\rho_{AB}^{(\rm p)}$, $\rm p = QS, SPC$. However, since Bob's measurement is Gaussian, the security analysis of the NLA-assisted protocol can be based on the optimality of Gaussian attacks discussed in Sec. 6.4, which, in this scenario, maximize the amount of information extractable by Eve. Moreover, since also Alice's DH detection is Gaussian, we further consider the Gaussian lower bound on the mutual information, and, in turn, obtain a lower bound of the exact KGR as:

$$K_{\rm p}(V,g) = P_{\rm p}(V,g)\left[\beta I_{AB}^{(\rm p)}(V,g) - \chi_{BE}^{(\rm p)}(V,g)\right], \tag{8.89}$$

where $P_{\rm p}(V,g)$ is the success probability associated with the p-th NLA and $I_{AB}^{(\rm p)}(V,g)$ and $\chi_{BE}^{(\rm p)}(V,g)$ are the mutual information and the Holevo information, respectively, both computed for a Gaussian state having the same CM of $\rho_{AB}^{(\rm p)}$. The condition $K_{\rm p}(V,g) \geq 0$ provides a sufficient condition to guarantee secure communication. Nevertheless, our results are in good agreement with other exact numerical approaches [35], proving the bound (8.89) to be tight, especially in the long-distance regime $\kappa d \gg 1$.

Thus, in our approach it suffices to compute the CM $\boldsymbol{\sigma}_{AB}^{(\rm p)}$ associated with $\rho_{AB}^{(\rm p)}$ to perform the security analysis. Straightforward calculations lead to:

$$\boldsymbol{\sigma}_{AB}^{(\rm p)} = \begin{pmatrix} V_{\rm p}(V,g)\,\mathbb{1}_2 & Z_{\rm p}(V,g)\,\boldsymbol{\sigma}_z \\ Z_{\rm p}(V,g)\,\boldsymbol{\sigma}_z & W_{\rm p}(V,g)\,\mathbb{1}_2 \end{pmatrix}, \tag{8.90}$$

as derived in App. A.4. The expressions of $P_{\rm p}(V,g)$, $V_{\rm p}(V,g)$, $W_{\rm p}(V,g)$ and $Z_{\rm p}(V,g)$ are clumsy and thus only reported in App. A.4. We compute the mutual information and the Holevo information following the procedure described in Sec. 6.3 by substituting $\boldsymbol{\sigma}_{AB} \to \boldsymbol{\sigma}_{AB}^{(\rm p)}$ and optimize Eq. (8.89) over the free parameters, obtaining the KGRs

$$K_{\rm p}(g) = \max_{V} K_{\rm p}(V,g)\,, \qquad {\rm p} = {\rm QS, SPC}\,, \tag{8.91}$$

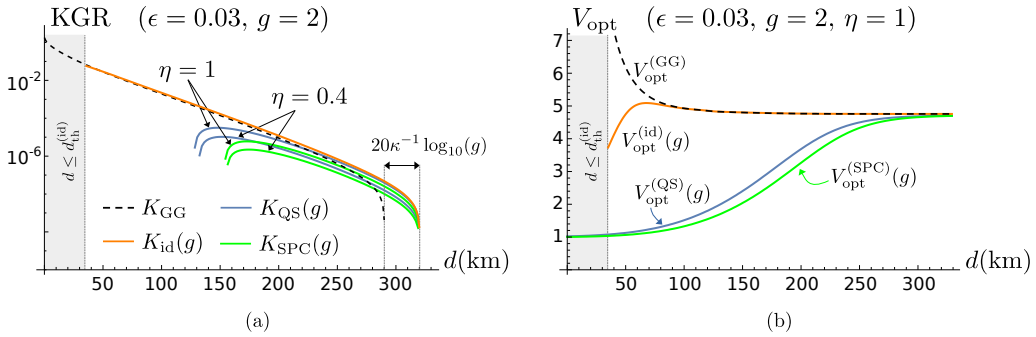


Figure 8.4.3: (a) Log plot of the KGRs $K_{\rm p}(g)$ for different values of the quantum efficiency η and $K_{\rm id}(g)$ as functions of the distance d in km. The dashed line is the KGR of the original protocol. (Bottom) Plot of the optimized (input) modulations $V_{\rm opt}^{\rm (p)}(g)$ and $V_{\rm opt}^{\rm (id)}(g)$ as a function of the distance d in km for $\epsilon = 0.03$. In both the plots, the shaded region represents the regime $d \leq d_{\rm th}^{\rm (id)}$, where ideal NLAs generate an unphysical un-normalizable state (see the text for details). We set $\beta = 0.95$, $\epsilon = 0.03$ and $g = 2$.

for a fixed g, together with the corresponding modulation $V_{\rm opt}^{\rm (p)}(g)$, and

$$K_{\rm p} = \max_{V,g} K_{\rm p}(V,g)\,, \qquad {\rm p} = {\rm QS}, {\rm SPC}\,, \tag{8.92}$$

if g can be optimized too, with the associated optimized parameters $V_{\rm opt}^{\rm (p)}$ and $g_{\rm opt}^{\rm (p)}$.

We note that in the SPC scheme there always exists a local maximum for $\tau = 1$, in which case the SPC performs as the identity operator, allowing to retrieve the results of the original GG02 protocol. However, for a more fair comparison with the QS, in the optimization procedure we have neglected this point and restricted maximization over the interval $0 \leq \tau \leq 1/2$ for which the corresponding gain is $g \geq 0$, as shown in App. A.4.

8.4.3 Unconditional security for the NLA-assisted protocols

We now compare the KGRs of all the schemes under investigation, for the two cases of fixed or optimized gain.

8.4.3.1 KGR with fixed gain g

For a fixed g, the optimized KGRs are depicted in Fig. 8.4.3(a) for $\epsilon > 0$. As emerges from the plot, NLAs are fundamental in the long-distance regime, as for large d all the NLA-assisted protocols beat the KGR $K_{\rm GG}$ of the original protocol. The ideal NLA increases the maximum transmission distance by the amount $(20\log_{10} g)/\kappa$, since for $T \ll 1$ the effective transmissivity in Eq. (8.79) is $T_{\rm id} \approx g^2 T$ [287]. Remarkably, also the physical NLA-assisted protocols achieve the same maximum transmission distance. Moreover, the presence of inefficient conditional detection reduces the value of the KGRs, still maintaining the same increase in distance even for the realistic values of practical CVQKD systems where $0.4 \leq \eta \leq 0.6$ [191, 192].

In fact, by expanding the CM (8.90) in the long-distance regime where $T \ll 1$ up to

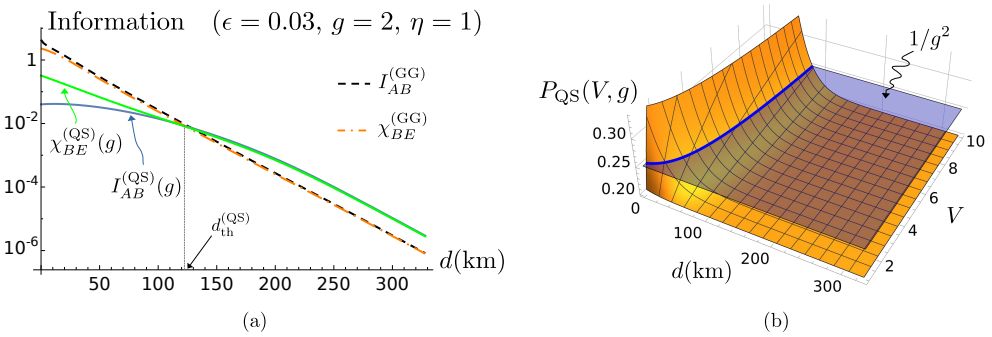


Figure 8.4.4: (a) Log plot of $I_{AB}^{(\mathrm{QS})}(g)$ and $\chi_{BE}^{(\mathrm{QS})}(g)$ (solid lines) and $I_{AB}^{(\mathrm{GG})}$ (dashed line) and $\chi_{BE}^{(\mathrm{GG})}$ (dash-dotted line) as a function of the distance d in km. (b) Plot of the success probability $P_{\mathrm{QS}}(V,g)$ as a function of the distance d and the modulation variance V. The horizontal plane refers to the value $1/g^2$: when $P_{\mathrm{QS}}(V,g) > 1/g^2$, the QS do not perform noiseless amplification. In both the pictures we set $\beta = 0.95$, $\epsilon = 0.03$, $g = 2$ and $\eta = 1$.

the first order in T, we have:

$$V_{\mathrm{p}}(V,g) = V + O(T)\,, \tag{8.93a}$$

$$W_{\mathrm{p}}(V,g) = g^2 T(V+\chi) + O(T^2)\,, \tag{8.93b}$$

$$Z_{\mathrm{p}}(V,g) = \sqrt{g^2 T}\, Z + O(T^{3/2})\,, \qquad \mathrm{p} = \mathrm{QS}, \mathrm{SPC}\,, \tag{8.93c}$$

corresponding to the CM of a GG02 scheme with transmissivity g^2T, consistently with the ideal case. The success probabilities read :

$$P_{\mathrm{p}}(V,g) \approx P_{\mathrm{p}}(g) = \eta \tau_{\mathrm{p}}(g)\,, \tag{8.94}$$

and, being $P_{\mathrm{SPC}}(g) \leq P_{\mathrm{QS}}(g)$, we have $K_{\mathrm{SPC}}(g) \leq K_{\mathrm{QS}}(g)$. In turn, a quantum efficiency $\eta \leq 1$ only reduces the success probability and rescales the KGR, without preventing long-distance secure communication. For completeness, we report the (input) optimized modulations in Fig. 8.4.3(b). Despite the different behaviour at small distances, for large d all the protocols converge to the same asymptotic value, not depending on ϵ. Numerical calculations have also shown that $V_{\mathrm{opt}}^{(\mathrm{p})}(g)$ does not depend on the quantum efficiency.

We note that in the short-distance regime, where $T \approx 1$ or, equivalently, $\kappa d \ll 1$, both the physical NLAs are useless, since we obtain negative KGR up to a threshold distance $d_{\mathrm{th}}^{(\mathrm{p})}$, $\mathrm{p} = \mathrm{QS}, \mathrm{SPC}$. In this regime, the CM (8.90) cannot be recast in the GG02 form of Eq. (6.31), and, as displayed in Fig. 8.4.4(a) for the QS case, both the mutual information $I_{AB}^{(\mathrm{p})}(g) = I_{AB}^{(\mathrm{p})}(V_{\mathrm{opt}}^{(\mathrm{p})}(g), g)$ and the Holevo information $\chi_{BE}^{(\mathrm{p})}(g) = \chi_{BE}^{(\mathrm{p})}(V_{\mathrm{opt}}^{(\mathrm{p})}(g), g)$ are lower than their GG02 counterparts $I_{AB}^{(\mathrm{GG})}$ and $\chi_{BE}^{(\mathrm{GG})}$, respectively. Moreover, for $\epsilon > 0$ we have $I_{AB}^{(\mathrm{p})}(g) \leq \chi_{BE}^{(\mathrm{p})}(g)$, leading to a negative KGR which inhibits secure communication. This effect may be understood by considering the success probability $P_{\mathrm{p}}(V,g)$ of the proposed physical NLAs, plotted in Fig. 8.4.4(b) for the QS case. Analogous considerations hold for SPC. When $P_{\mathrm{p}}(V,g) > 1/g^2$ the p scheme does not implement a true NLA [35, 287], and the amplification process introduces a unavoidable noise on the quadrature variances, becoming a further resource for Eve's attack. Accordingly, for $\kappa d \ll 1$ the optimization procedure leads to low modulation variances $V_{\mathrm{opt}}^{(\mathrm{p})}(g) \approx 1$, resulting in

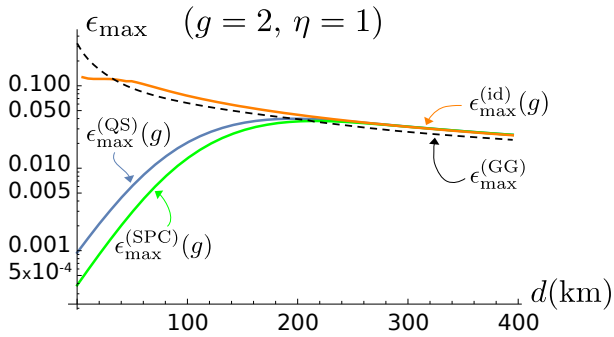


Figure 8.4.5: Log plot of the maximum tolerable excess noise $\epsilon_{\max}^{(\mathrm{id})}(g)$ and $\epsilon_{\max}^{(\mathrm{p})}(g)$, $\mathrm{p} = \mathrm{QS}, \mathrm{SPC}$, as a function of the distance d in km. The black dashed line corresponds to the $\epsilon_{\max}^{(\mathrm{GG})}$ of the original protocol. We set $\beta = 0.95$ and $\eta = 1$.

a lower mutual information with respect to the GG02 scheme and in a negative KGR. On the other hand, for $\kappa d \gg 1$, $V_{\mathrm{opt}}^{(\mathrm{p})} \approx V_{\mathrm{opt}}^{(\mathrm{GG})}$ and both $I_{AB}^{(\mathrm{p})}$ and $\chi_{BE}^{(\mathrm{p})}$ outperform the GG02 protocol. In turn, between the short- and long-distance regimes, we identify the threshold distance such that $K_{\mathrm{p}}(g) \geq 0$ for $d \leq d_{\mathrm{th}}^{(\mathrm{p})}$.

Finally, in Fig. 8.4.5 we plot the maximum tolerable excess noise (MTEN) $\epsilon_{\max}$ as a function of the distance d: it represents the maximum value of ϵ still leading to a positive KGR. For the original protocol, $\epsilon_{\max}^{(\mathrm{GG})}$ is a decreasing function of d. The behaviour is rather different for the NLA-assisted protocols. In the presence of ideal NLA the MTEN $\epsilon_{\max}^{(\mathrm{id})}(g)$ for $d \lesssim 40$ km is lower than the original protocol due to the limitation imposed by (8.80). However, for larger distances we have $\epsilon_{\max}^{(\mathrm{id})}(g) > \epsilon_{\max}^{(\mathrm{GG})}$. On the contrary, the MTEN associated with the physical NLAs, namely $\epsilon_{\max}^{(\mathrm{p})}(g)$, is not a monotonous function of d: it is an increasing function of d approaching $\epsilon_{\max}^{(\mathrm{id})}$. A quantum efficiency $\eta \leq 1$ does not affect the value of $\epsilon_{\max}^{(\mathrm{p})}$, consistently with the previous discussions. As a consequence, for fixed g, in the long-distance regime the physical NLAs guarantee the same performance of the ideal NLA.

8.4.3.2 KGR with optimized gain g

The situation is rather different if we can also optimize the gain g associated with the NLAs, as reported in Fig. 8.4.6(a). Firstly, in the short-distance regime the physical NLAs still exhibits a threshold distance to obtain a positive KGR, differently from the ideal amplifier. Secondly, all the NLA-assisted protocols allow to reach arbitrary large distances, but the ideal amplifier outperforms the physical ones. As before, a quantum efficiency still rescales the KGR. However, differently from Sec. 8.4.3.1, in the long distance regime $\kappa d \gg 1$, K_{QS} and K_{SPC} are almost identical, proving SPC as a feasible alternative to QS. We also remark that in the long-distance regime both K_{id} and K_{p}, $\mathrm{p} = \mathrm{QS}, \mathrm{SPC}$, are proportional to the PLOB bound:

$$K_{\mathrm{PLOB}} = -\log_2\left[(1-T)T^{\bar{n}_T}\right] - h(\bar{n}_T)\,, \tag{8.95}$$

with $\bar{n}_T = T\epsilon/(2(1-T))$ and the h function in Eq. (8.40), thus resulting in nearly optimal strategies.

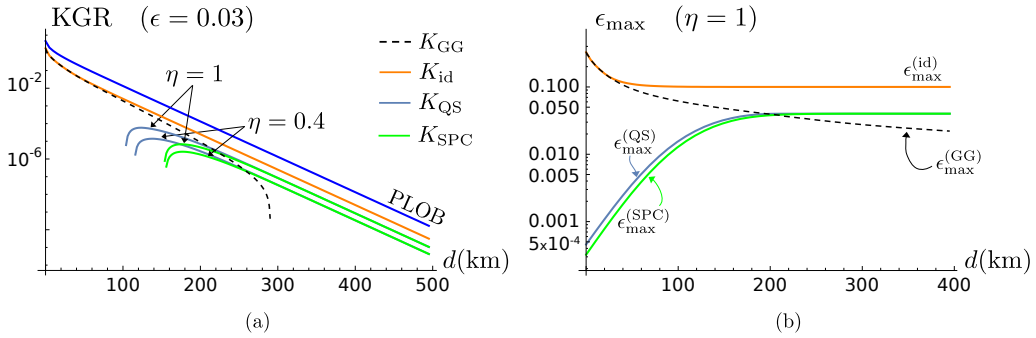


Figure 8.4.6: (a) Log plot of the KGRs $K_{\rm p}$, ${\rm p} = {\rm QS}, {\rm SPC}$, and $K_{\rm id}$ as a function of the distance d in km, for different values of the quantum efficiency η and $\epsilon = 0.03$ and with optimized gain g. The dashed line is the KGR of the original protocol and the upper line is the PLOB bound (8.47). (b) Log plot of the maximum tolerable excess noises $\epsilon_{\rm max}^{\rm (id)}$ and $\epsilon_{\rm max}^{\rm (p)}$, ${\rm p} = {\rm QS}, {\rm SPC}$, as a function of the distance d in km, for $\eta = 1$. $\epsilon_{\rm max}^{\rm (GG)}$ corresponds to the maximum tolerable excess noise of the original protocol. In both the pictures we set $\beta = 0.95$.

Furthermore, in Fig. 8.4.7(a) and (b) we report the optimized parameters $V_{\rm opt}^{\rm (p)}$ and $g_{\rm opt}^{\rm (p)}$, respectively. The modulation $V_{\rm opt}^{\rm (p)}$ has a different behavior with respect to Sec. 8.4.3.1, being an ϵ-dependent growing function of d. On the contrary, the modulations of the original and the ideal NLA-assisted protocols are decreasing functions of d converging to an asymptotic value not depending on ϵ, as for the case of fixed g. Instead, the optimized gains $g_{\rm opt}^{\rm (id)}$ and $g_{\rm opt}^{\rm (p)}$ grow exponentially with d in the long-distance regime. However, if $\epsilon = 0$ this exponential scaling is not reached yet for the physical NLAs within the considered range of distances $d \leq 500\,{\rm km}$.

Finally, in Fig. 8.4.6(b) we plot the MTENs as a function of d. Differently from Sec. 8.4.3.1, the MTEN associated with the physical NLAs, namely $\epsilon_{\rm max}^{\rm (p)}$, do not achieve the performance of the ideal one, $\epsilon_{\rm max}^{\rm (id)}$. Actually, both these MTENs outperform the original protocol and saturate to a value ϵ_∞ as $\kappa d \gg 1$. However, the saturation value of the physical NLAs, namely $\epsilon_\infty^{\rm (p)} \approx 0.04$, is lower than the ideal NLA one, that is $\epsilon_\infty^{\rm (id)} \approx 0.1$, see Fig. 8.4.6(b). The numerical results also show that a quantum efficiency $\eta \leq 1$ does not affect the value of $\epsilon_\infty^{\rm (p)}$, consistently with the previous findings.

The difference between ideal and physical NLAs emerges by expanding the CM (8.90) in the long-distance regime $T \ll 1$ up to the first order, keeping all the contributions of $O(g^2 T)$, due to the fact that $g_{\rm opt}^{\rm (p)} \gg 1$, and neglecting the other terms:

$$V_{\rm p}(V,g) \approx V + \delta V_{\rm p}\,, \tag{8.96a}$$

$$W_{\rm p}(V,g) \approx T_{\rm p}\big[V_{\rm p}(V,g) + \chi_{\rm p}\big]\,, \tag{8.96b}$$

$$Z_{\rm p}(V,g) \approx \frac{T_{\rm p}}{\sqrt{g^2 T}}\, Z\,, \qquad {\rm p} = {\rm QS}, {\rm SPC}\,, \tag{8.96c}$$

where $\delta V_{\rm p} = T_{\rm p} Z^2/2$. $T_{\rm p}$ represents the effective transmissivity

$$T_{\rm p} = \frac{g^2\, T}{1 + g^2 T (V + \epsilon - 1)/2}\,, \tag{8.97}$$

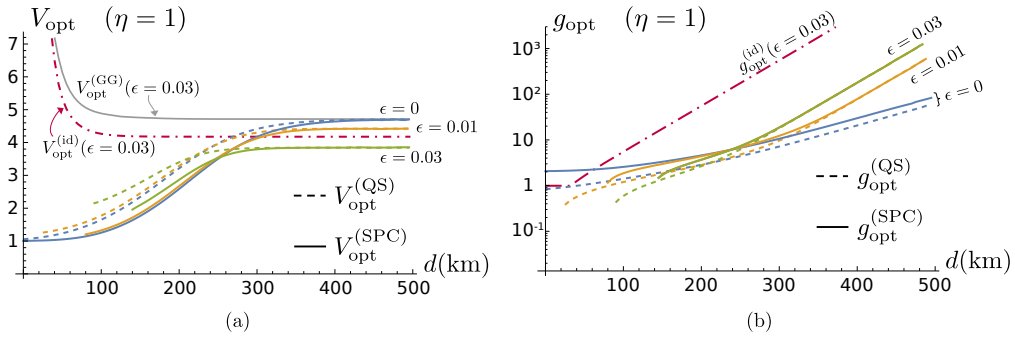


Figure 8.4.7: (a) Plot of $V_{\rm opt}^{(\rm p)}$, $\rm p = QS, SPC$, as a function of the distance d in km, for different values of excess noise ϵ. The upper gray and the dash-dotted lines represent the optimized modulation for the original and the ideal NLA-assisted protocols, respectively, for $\epsilon = 0.03$. (b) Log plot of $g_{\rm opt}^{(\rm p)}$, $\rm p = QS, SPC$, as a function of the distance d in km, for different values of excess noise ϵ. The plots have been performed only for the distances such that $K_{\rm p} > 0$, $\rm p = QS, SPC$. We set $\beta = 0.95$ and $\eta = 1$.

while $\chi_{\rm p} = (1 - T_{\rm p})/T_{\rm p} + \epsilon_{\rm p}$, with the effective excess noise

$$\epsilon_{\rm p} = \epsilon - \delta V_{\rm p} \,. \tag{8.98}$$

Employing a physical NLA is then equivalent to considering an effective channel of higher transmissivity $T_{\rm p} \geq T$ and lower excess noise $\epsilon_{\rm p} \leq \epsilon$. Nevertheless, the correspondence with a GG02 protocol does not occur anymore, as the correlation term $Z_{\rm p}(V, g)$ does not coincide with the one expected for a GG02 scheme, namely,

$$Z_{\rm p}^{(\rm GG)}(V, g) = \sqrt{T_{\rm p}\left[V_{\rm p}(V, g)^2 - 1\right]} \,, \tag{8.99}$$

but rather:

$$Z_{\rm p}(V, g) \leq Z_{\rm p}^{(\rm GG)}(V, g) \,, \tag{8.100}$$

as depicted in Fig. 8.4.8(a). We have $Z_{\rm p}(V, g) \approx Z_{\rm p}^{(\rm GG)}(V, g)$ only if $g^2 T \ll 1$. As a consequence, the analogy with the ideal-NLA assisted protocol in Eq. (8.79) is broken.

Now, the optimization procedure described above leads to exponential gains $g_{\rm opt}^{(\rm id)}$ and $g_{\rm opt}^{(\rm p)}$ for the ideal and physical NLAs, respectively, such that the product $g^2 T$ is kept constant for $\kappa d \gg 1$. Consequently, the effective transmissivities $T_{\rm id}$ and $T_{\rm p}$ saturate, as shown in Fig. 8.4.8(b). In turn, also the mutual information and the Holevo information saturate and the corresponding KGRs (8.85) and (8.92) turn out to be proportional only to the success probability of the NLAs, namely:

$$K_{\rm id} \propto \frac{1}{\left(g_{\rm opt}^{(\rm id)}\right)^2} \propto T \,, \tag{8.101}$$

and

$$K_{\rm p} \propto P_{\rm p} \approx \frac{\eta T}{2 T_{\rm p}} \left[1 + T_{\rm p}(V_{\rm p} + \chi_{\rm p})\right] , \tag{8.102}$$

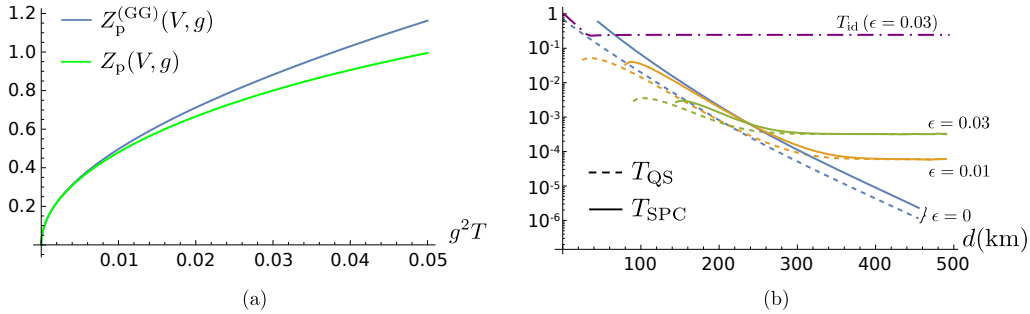


Figure 8.4.8: (a) Plot of $Z_{\rm p}(V,g)$ and $Z_{\rm p}^{(\rm GG)}(V,g)$, $\rm p = QS, SPC$, as a function of g^2T for $\epsilon = 0.03$ and $V = 4$. (b) Log plot of the effective transmissivity $T_{\rm p}$, $\rm p = QS, SPC$, as a function of the distance d in km, for different values of excess noise ϵ. The plot have been performed only for the distances such that $K_{\rm p} > 0$. In both the pictures we set $\beta = 0.95$ and $\eta = 1$.

with $P_{\rm p} = P_{\rm p}\big(V_{\rm opt}^{(\rm p)}, g_{\rm opt}^{(\rm p)}\big)$ and $V_{\rm p} = V_{\rm p}\big(V_{\rm opt}^{(\rm p)}, g_{\rm opt}^{(\rm p)}\big)$, decreasing linearly with T and thus guaranteeing $K_{\rm p} > 0$ for $\kappa d \gg 1$. The same linear scaling is achieved by the PLOB bound if $T \ll 1$:

$$K_{\rm PLOB} \approx T \left\{ \frac{2 - \epsilon[1 - \ln(\epsilon/2)]}{2 \ln 2} \right\}, \tag{8.103}$$

which proves both all the NLA-assisted protocols to be nearly optimal. Furthermore, as in Sec. 8.4.3.1 a quantum efficiency $\eta \leq 1$ only rescales the KGR and does not introduce any maximum transmission distance.

Moreover, the saturation value of $T_{\rm p}$ determines the difference between ideal and physical NLAs. Indeed, if $\epsilon_{\rm p}$ is small we have $T_{\rm p} \ll 1$ and the physical NLA-assisted protocols approximate a GG02 protocol with the effective channel parameters $T_{\rm p}$ and $\epsilon_{\rm p}$. By increasing the excess noise further, we have $T_{\rm p} \not\ll 1$ and $Z_{\rm p}(V,g) \leq Z_{\rm p}^{(\rm GG)}(V,g)$, the state shared between Alice and Bob is less correlated and the protocol deviates more and more from GG02. This implies the reduced asymptotic maximum tolerable excess noise with respect to the ideal case.

CHAPTER 9

Enhancing CVQKD by non-Gaussian measurements

In this last Chapter, we proceed beyond the Gaussian CVQKD previously discussed, and make a first step towards the design of fully non-Gaussian protocols. As a matter of fact, to date, all the proposed CVQKD schemes always assume Gaussian detection at the receiver, for both practical and theoretical reasons, whereas it has recently been proved that the secret key capacity provided by the PLOB bound, introduced in the previous Chapter, is achieved by a non-Gaussian measurement [317]. Therefore, non-Gaussian CVQKD represents a new challenging topic, with unexplored potentialities. On the other hand, addressing security of protocols that do not exploit Gaussian detection is a nontrivial task, as, in this case, the Gaussian optimality theorem is no longer applicable, and more complex analyses have to be carried out, e.g. based on the semidefinite programming approach recently proposed by Lin *et al.* [165, 166]. In turn, all these considerations make non-Gaussian CVQKD both an attractive and unclear field of research.

In this Chapter we propose an example of CVQKD employing non-Gaussian detection. By drawing inspiration on the results of quantum state discrimination theory presented in Chapter 5, we design an optimized state-discrimination receiver for the QPSK protocol, referred to as the key-rate optimized receiver (KOR) [19]. For the sake of simplicity, we analyze security under a pure-loss wiretap channel, and compare the resulting KGR with that obtained from conventional double-homodyne detection, showing an enhancement in the metropolitan-network distance regime. We also consider the performance of a feasible scheme, namely the quaternary displacement feed-forward receiver (QDFFRE), obtaining an increase in the KGR with respect to Gaussian detection up to a maximum transmission distance.

The structure of the Chapter is the following. In Sec. 9.1 we discuss the issues and the state of the art in non-Gaussian CVQKD. Thereafter, in Sec. 9.2 we perform explicit construction of the KOR for the QPSK protocol, discussing its security under the wiretap channel assumption, also comparing its performance with the QDFFRE. The results of the whole Chapter are original.

9.1 Towards non-Gaussian CVQKD

As we outlined throughout the previous Chapters, several CVQKD protocols have been proposed in literature, employing either Gaussian modulation of coherent states [14, 175–177, 200] or discrete modulation formats [162, 164, 165, 168, 223, 231, 232, 235, 302, 318–320]. All these schemes share a common feature: they assume Gaussian detection at Bob's side, either homodyne or double homodyne (DH). This is mainly due for a twofold reason. The former, more practical, is that quadrature detection provides a simple and feasible solution for experimental implementations being large-scale applicable, as it is commonly adopted in the state-of-the-art communication systems at telecom

wavelength [191–193]. The latter, more theoretical, is that Gaussian detection guarantees unconditional security proofs, thanks to the resort to the optimality of Gaussian attacks [178–180], whilst, only recently, a tight lower bound to the Devetak-Winter (DW) bound, not invoking Gaussian optimality, has been obtained [165]. However, the fundamental limitations of Gaussian CVQKD have been recently established in [317], proving a gap between the key generation rate (KGR) achievable with Gaussian operations and the secret-key channel capacity provided by the PLOB bound. In turn, non-Gaussianity becomes necessary to enhance quantum secure communications and close the gap with respect to the PLOB bound.

These results suggest non-Gaussian measurements as a potential resource for CVQKD, also considering that in many other frameworks, they often outperform Gaussian ones. For instance, in the transmission of classical information, the classical capacity of a lossy bosonic channel is enhanced, in particular energy regimes, by resorting to photon-number resolving (PNR) detection [64–66] and weak-field homodyne measurement [52]. Furthermore, in quantum state discrimination, the quantum receivers associated with the standard quantum limit (SQL), based on Gaussian detection, do not achieve the minimum decision error probability, as widely discussed in Chapters 4 and 5. Nevertheless, addressing unconditional security of a CVQKD scheme employing non-Gaussian measurements is an open problem since the Gaussian optimality theorem does not hold anymore, and the DW bound can only be directly evaluated with the advanced methods presented in [165]. Therefore, to date, the main results in the field of non-Gaussian key distribution have been limited to restricted eavesdropping settings. In particular, Cattaneo *et al.* showed that weak-field homodyne detection enhances a Gaussian modulation protocol, in the presence of a quantum pure-loss wiretap channel under both individual and collective attacks, with higher increase in the KGR for high channel transmissivity, corresponding to short-distance communications [321].

Following the same philosophy, we now extend the analysis in this direction and address a complementary problem, namely to design an optimized state-discrimination receiver for discrete modulation CVQKD, by exploiting the characterization outlined in Chapter 5. In fact, in the present literature, only the receivers achieving the SQL have been investigated for CVQKD [163], leaving the open problem of designing a genuine quantum receiver maximizing the KGR of a M-ary protocol. This also raises the question about the compatibility between optimum discrimination and maximum secret-key distillation, that is whether or not the POVM minimizing the decision error probability coincides with that maximizing the KGR.

In light of this, in the following we consider a quadrature phase-shift keying (QPSK) protocol employing a quantum discrimination receiver in place of Gaussian detection and show that, in particular conditions, it is possible to theoretically design a suitable measurement outperforming the conventional quadrature detection schemes. Moreover, as in [321], we investigate security under a quantum wiretap channel, where Eve may only collect the lost fraction of the encoded signals without performing arbitrary channel manipulation.

9.2 The QPSK protocol with state-discrimination receivers

Here, we investigate the potentiality of state-discrimination receivers for secure quantum communications and propose a new quantum receiver, the *key-rate optimized receiver* (KOR), for CVQKD protocols employing discrete modulation. In particular, we consider a QPSK protocol in which Bob implements the KOR rather than a Gaussian measurement [19]. We compute the KGR under the wiretap channel assumption and, for the

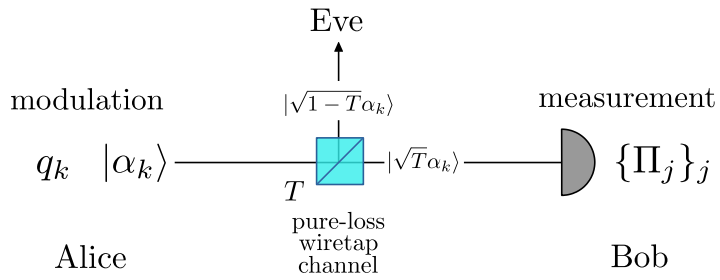


Figure 9.2.1: Scheme of the QPSK protocol employing state-discrimination receivers. Alice generates one of the coherent states $|\alpha_k\rangle$, $k = 0, \ldots, M-1$, with uniform probability $q_k = 1/M$ and sends it via the quantum wiretap channel to Bob, who performs the finite-valued POVM $\{\Pi_j\}_j$, $j = 0, \ldots, M-1$.

sake of simplicity, we consider a pure-loss channel, in order to deal with discrimination of pure states at Bob's side. This latter assumption depicts a simplified scenario, providing a cornerstone fostering more advanced developments. However, it is still worth of investigation for a twofold reason. At first, in the recent literature there has been a revived interest in passive eavesdropping strategies [322–327]. Secondly, passive eavesdropping can be used as the first stepping stone to identify scenarios where a potential advantage of quantum receivers may be substantial, even in the possible presence of nonzero excess noise. Starting from the general structure of quantum receivers derived in Sec.s 5.2.1 and 5.3.1.2, we design the KOR to maximize the KGR of the addressed protocol and compare it with the pretty good measurement (PGM), being the POVM minimizing the decision error probability for discrimination, showing that both these non-Gaussian measurements improve the KGR in the metropolitan-network distance regime with respect to the conventional Gaussian measurement scheme. Finally, we also investigate the performance of some feasible quantum receivers, by considering the quaternary displacement feed-forward receiver (QDFFRE) introduced in Sec. 5.5.3.

Given this outline, the protocol under investigation is reported in Fig. 9.2.1. The sender, Alice, employs the QPSK modulation, that is she generates one of the $M = 4$ coherent states:

$$|\alpha_k\rangle = |\alpha\, e^{i\pi(2k+1)/M}\rangle\,, \qquad k = 0, \ldots, M-1\,, \tag{9.1}$$

where $\alpha \geq 0$, sampled with equal a priori probabilities $q_k = 1/M$. We remind that the QPSK constellation satisfies the geometrically uniform symmetry (GUS) for the phase-shift symmetry operator $S_\theta = \exp(-i\,\theta\,\hat{n})$, with $\theta = 2\pi/M$ and $\hat{n}$ being the photon-number quantum operator [51]. After the modulation stage, Alice injects the signals into an untrusted pure-loss wiretap channel with transmissivity:

$$T = 10^{-\kappa d/10}\,, \tag{9.2}$$

d being the transmission distance (expressed in km) and $\kappa = 0.2$ dB/km is the loss rate of common fibers at telecom wavelength [38, 191, 192, 236, 237]. Then, the transmitted fraction $|\alpha_k^{(t)}\rangle = |\sqrt{T}\alpha_k\rangle$ reaches the receiver, Bob, whereas the eavesdropper, Eve, receives the reflected part $|\alpha_k^{(r)}\rangle = |\sqrt{1-T}\alpha_k\rangle$. Ultimately, Bob, probes the rescaled constellation $\{|\alpha_k^{(t)}\rangle\}_k$ via a state-discrimination receiver, namely, a finite-valued POVM $\{\Pi_j\}_j$, $j = 0, \ldots, M-1$, defined in the M-dimensional subspace $\mathcal{S}$ spanned by the transmitted

pulses and satisfying the properties described in Sec. 5.2. Actually, we note that, to form a truly identity-resolving set, the POVM elements $\{\Pi_j\}_j$, should be complemented with an $(M+1)$-th inconclusive element $\Pi_M = \hat{\mathbb{1}} - \mathbb{P}_{\mathcal{S}}$, $\mathbb{P}_{\mathcal{S}}$ being the projection operator onto subspace $\mathcal{S}$. However, for the case under investigation, Π_M is irrelevant, and we will neglect it in the following. This would not be true anymore in the presence of a channel excess noise; thus, registering a zero probability for this additional outcome may provide a useful way to check the reasonableness of the pure-loss hypothesis in a realistic implementation of the proposed protocol.

Provided these two assumptions, in the following we construct the optimized POVM that describes the KOR, and show it to bring advantages in some particular regimes.

9.2.1 Construction of the key-rate optimized receiver

In our protocol Bob should employ an optimized POVM to perform discrimination among the transmitted pulses, described by the state vector $\Gamma = (|\alpha_0^{(t)}\rangle, \ldots, |\alpha_{M-1}^{(t)}\rangle)$ and the Gram matrix:

$$G = \left(\langle \alpha_l^{(t)} | \alpha_k^{(t)} \rangle\right)_{l,k=0,\ldots,M-1}, \tag{9.3}$$

see Sec. 5.2.1, in which the overlap $G_{lk} = \langle \alpha_l^{(t)} | \alpha_k^{(t)} \rangle$ reads [31]:

$$\begin{aligned} G_{lk} &= \exp\left\{-\frac{1}{2}\left|\alpha_k^{(t)} - \alpha_l^{(t)}\right|^2 + \frac{1}{2}\left[\alpha_k^{(t)}\left(\alpha_l^{(t)}\right)^* - \left(\alpha_k^{(t)}\right)^* \alpha_l^{(t)}\right]\right\} \\ &= \exp\left(-T\alpha^2\left\{1 - \cos\left[\frac{2\pi}{M}(k-l)\right]\right\} + i\,T\alpha^2 \sin\left[\frac{2\pi}{M}(k-l)\right]\right). \end{aligned} \tag{9.4}$$

The constellation of transmitted pulses maintains the GUS for the phase-shift operator S_θ, thus the set of measurement vectors $\mathbb{M} = \{|\mu_j\rangle\}_j$, $j = 0, \ldots, M-1$, with $\mathbb{M} = \Gamma A$, also satisfies the GUS, and the corresponding matrix A is in the form (5.58), according to the results of Sec. 5.3.1.2. That is, $A \equiv A_{\boldsymbol{\phi}} = \mathbb{U}\,\Lambda_A^{(\boldsymbol{\phi})}\,\mathbb{U}^\dagger$, $\mathbb{U}$ being the inverse discrete Fourier transform matrix and

$$\Lambda_A^{(\boldsymbol{\phi})} = \mathrm{diag}\left(\left\{\lambda_j^{(\boldsymbol{\phi})}\right\}_{j=0,\ldots,M-1}\right), \tag{9.5}$$

where:

$$\lambda_j^{(\boldsymbol{\phi})} = e^{i\phi_j} g_j^{-1/2}, \tag{9.6}$$

$\{g_j\}_j$ being the eigenvalues of the Gram matrix (9.3) and $\boldsymbol{\phi}$ being the array of phases fully characterizing the receiver. Given this structure, the KOR is obtained by optimizing the phase array $\boldsymbol{\phi}$ to maximize the KGR, and is described by the optimized "reference" measurement vector:

$$|\mu_0^{(\boldsymbol{\phi})}\rangle = \sum_{k=0}^{M-1} (A_{\boldsymbol{\phi}})_{k0} \left|\alpha_k^{(t)}\right\rangle \tag{9.7}$$

$$= e^{-T\alpha^2/2} \sum_{n=0}^{\infty} \frac{\left(\sqrt{T}\alpha_0\right)^n}{\sqrt{n!}} \lambda_{(n-1) \bmod M}^{(\boldsymbol{\phi})} |n\rangle, \tag{9.8}$$

where $a \bmod b$ is the modulo operation, returning the reminder of the division a/b, $a, b \in \mathbb{Z}$, and $\{|n\rangle\}_n$ is the photon-number basis. In turn, the other measurement vectors are obtained as $|\mu_j^{(\boldsymbol{\phi})}\rangle = (S_\theta)^j |\mu_0^{(\boldsymbol{\phi})}\rangle$, $j = 0, \ldots, M-1$.

Given the previous considerations, we compute the KGR of the discussed protocol, considering a reverse reconciliation scenario [14, 175, 176]. Moreover, for the sake of simplicity, we perform the asymptotic key-rate calculation, where the channel parameters are known with no uncertainty. Under this paradigm, for a generic state-discrimination receiver described by the phase vector $\boldsymbol{\phi}$, the KGR reads:

$$K(\boldsymbol{\phi}, \alpha^2) = \beta I_{AB}(\boldsymbol{\phi}, \alpha^2) - \chi_{BE}(\boldsymbol{\phi}, \alpha^2)\,, \tag{9.9}$$

where I_{AB} and χ_{BE} are the mutual information between Alice and Bob and the Holevo information [55] between Bob and Eve, respectively, and $\beta \leq 1$ is the reconciliation efficiency [162, 231].

The mutual information reads:

$$I_{AB}(\boldsymbol{\phi}, \alpha^2) = H\left[p_B^{(\boldsymbol{\phi})}(j)\right] - \frac{1}{M}\sum_{k=0}^{M-1} H\left[p_{B|\alpha_k}^{(\boldsymbol{\phi})}(j)\right]\,, \tag{9.10}$$

where

$$p_{B|\alpha_k}^{(\boldsymbol{\phi})}(j) = \left\langle \sqrt{T}\alpha_k \left|\Pi_j\right| \sqrt{T}\alpha_k \right\rangle = \left| \left(A_{\boldsymbol{\phi}}^\dagger G\right)_{kj} \right|^2\,, \tag{9.11}$$

and

$$p_B^{(\boldsymbol{\phi})}(j) = \frac{1}{M}\sum_{k=0}^{M-1} p_{B|\alpha_k}^{(\boldsymbol{\phi})}(j)\,, \tag{9.12}$$

are the conditional and overall probabilities of Bob's detection associated with outcome $j = 0, \ldots, M-1$, respectively, and $H[p(x)] = -\sum_x p(x)\log_2 p(x)$ is the Shannon entropy of the probability distribution $p(x)$.

To compute the Holevo information shared between Bob and Eve, that is the maximum amount of information accessible to Eve, we approach the problem in the prepare-&-measure picture [14, 175, 222] and obtain:

$$\chi_{BE}(\boldsymbol{\phi}, \alpha^2) = S\left[\rho_E\right] - \sum_{j=0}^{M-1} p_B^{(\boldsymbol{\phi})}(j)\, S\left[\rho_{E|j}^{(\boldsymbol{\phi})}\right]\,, \tag{9.13}$$

where $\rho_{E|j}^{(\boldsymbol{\phi})}$ and ρ_E are the conditional and overall Eve's state, respectively, $p_B^{(\boldsymbol{\phi})}(j)$ is Bob's probability distribution (9.12) and $S[\rho] = -\operatorname{Tr}[\rho\log_2\rho]$ represents the von Neumann entropy associated with state ρ. These two states may be retrieved from the joint state of Bob and Eve after the channel, that is:

$$\begin{aligned}\rho_{BE} &= U_{\mathrm{BS}}(T)\,\rho_A \otimes |0\rangle\langle 0|\, U_{\mathrm{BS}}(T)^\dagger \\ &= \frac{1}{M}\sum_{k=0}^{M-1} \left|\alpha_k^{(t)}\right\rangle\left\langle\alpha_k^{(t)}\right| \otimes \left|\alpha_k^{(r)}\right\rangle\left\langle\alpha_k^{(r)}\right|\,,\end{aligned} \tag{9.14}$$

where $\rho_A = \sum_k q_k |\alpha_k\rangle\langle\alpha_k|$ is Alice's overall state, $|0\rangle$ is the vacuum state and $U_{\rm BS}(T)$ is unitary operator associated with a beam splitter with transmissivity T [39], as displayed in Fig. 9.2.1. In turn, we have:

$$\rho_E = {\rm Tr}_B\left[\rho_{BE}\right] = \frac{1}{M}\sum_{k=0}^{M-1}\left|\sqrt{1-T}\alpha_k\right\rangle\left\langle\sqrt{1-T}\alpha_k\right|\,, \tag{9.15}$$

and

$$\begin{aligned}\rho_{E|j}^{(\boldsymbol{\phi})} &= \frac{1}{p_B^{(\boldsymbol{\phi})}(j)}\,{\rm Tr}_B\left[\rho_{BE}\,\Pi_j\otimes\hat{\mathbb{1}}_E\right]\\ &= \frac{1}{Mp_B^{(\boldsymbol{\phi})}(j)}\sum_{k=0}^{M-1}p_{B|\alpha_k}^{(\boldsymbol{\phi})}(j)\,\left|\sqrt{1-T}\alpha_k\right\rangle\left\langle\sqrt{1-T}\alpha_k\right|\,,\end{aligned} \tag{9.16}$$

${\rm Tr}_B$ being the partial trace over Bob's mode and $\hat{\mathbb{1}}_E$ being the identity operator over Eve's mode. Finally, the von Neumann entropy of states (9.15) and (9.16) may be computed as follows. Both of them are expressed in the form:

$$\varrho = \sum_{k=0}^{M-1} c_k\,|\alpha_k^{(r)}\rangle\langle\alpha_k^{(r)}|\,, \tag{9.17}$$

for some coefficients $c_k\in\mathbb{C}$. To compute the associated entropy we need to diagonalize (9.17). If $|\psi\rangle$ is the eigenvector of ϱ associated with eigenvalue ω, we have $|\psi\rangle = \sum_m b_m|\alpha_m^{(r)}\rangle$ and the following chain of equations holds:

$$\begin{aligned}&\varrho|\psi\rangle = \omega|\psi\rangle\\ &\left(\sum_k c_k|\alpha_k^{(r)}\rangle\langle\alpha_k^{(r)}|\right)\sum_m b_m|\alpha_m^{(r)}\rangle = \omega\sum_s b_s|\alpha_s^{(r)}\rangle\\ &\sum_k c_k\left(\sum_m \mathbb{G}_{km}b_m\right)|\alpha_k^{(r)}\rangle = \omega\sum_s b_s|\alpha_s^{(r)}\rangle\,,\end{aligned} \tag{9.18}$$

where $\mathbb{G}_{km} = \langle\alpha_k^{(r)}|\alpha_m^{(r)}\rangle$.

As a consequence, we obtain the set of equations:

$$\omega\,b_k = c_k\left(\sum_{m=0}^{M-1}\mathbb{G}_{km}b_m\right),\quad k=0,\ldots,M-1\,, \tag{9.19}$$

or, equivalently,

$$\left(\frac{\omega}{c_k}-1\right)b_k - \sum_{m\neq k}\mathbb{G}_{km}b_m = 0\,. \tag{9.20}$$

This defines the homogeneous linear system $M\mathbf{b}=0$, where $\mathbf{b}=(b_0,\ldots,b_{M-1})$ and

$$M = \begin{pmatrix}\frac{\omega}{c_0}-1 & -\mathbb{G}_{01} & -\mathbb{G}_{02} & -\mathbb{G}_{03}\\ -\mathbb{G}_{10} & \frac{\omega}{c_1}-1 & -\mathbb{G}_{12} & -\mathbb{G}_{13}\\ -\mathbb{G}_{20} & -\mathbb{G}_{21} & \frac{\omega}{c_2}-1 & -\mathbb{G}_{23}\\ -\mathbb{G}_{30} & -\mathbb{G}_{31} & -\mathbb{G}_{32} & \frac{\omega}{c_3}-1\end{pmatrix}. \tag{9.21}$$

The equation $M\mathbf{b} = 0$ always admits a trivial solution $\mathbf{b} = 0$, therefore to obtain a nonzero eigenvector we shall impose the condition $\det M = 0$. This provides us with the four eigenvalues $\{\omega_j\}_j$ and the corresponding von Neumann entropy $S[\varrho] = -\sum_j \omega_j \log_2 \omega_j$. For state ρ_E in (9.15), for which $c_k = M^{-1}$, the equation $\det M = 0$ may be solved analytically, leading to:

$$\omega_{0(1)} = \frac{e^{-(1-T)\alpha^2}}{2}\left\{\cosh\left[(1-T)\alpha^2\right] \pm \cos\left[(1-T)\alpha^2\right]\right\},$$

$$\omega_{2(3)} = \frac{e^{-(1-T)\alpha^2}}{2}\left\{\sinh\left[(1-T)\alpha^2\right] \pm \left|\sin\left[(1-T)\alpha^2\right]\right|\right\}. \tag{9.22}$$

In our analysis, we are interested in the maximum achievable KGR as a function of the transmission distance d, therefore, in the end we will perform optimization over the free parameters, namely the phases $\boldsymbol{\phi}$ and the constellation energy α^2. The final, optimized, KGR is therefore equal to

$$K_{\mathrm{KOR}} = \max_{\boldsymbol{\phi},\,\alpha^2} K(\boldsymbol{\phi},\,\alpha^2)\,, \tag{9.23}$$

with the optimized phases and modulation energy denoted by $\boldsymbol{\phi}_{\mathrm{KOR}} = (0, \phi_1^{(\mathrm{KOR})}, \ldots, \phi_{M-1}^{(\mathrm{KOR})})$ and α^2_{KOR}, reminding that, thanks to the GUS, we may set $\phi_0^{(\mathrm{KOR})} = 0$. As a consequence, we define the KOR via Eq. (5.58), as the quantum receiver associated with the optimized phase vector $\boldsymbol{\phi}_{\mathrm{KOR}}$. Furthermore, we compare the performance of the KOR with that associated with the PGM, defined via Eq. (5.58) with the choice $\boldsymbol{\phi}_{\mathrm{PGM}} = \mathbf{0}$, for which the optimized KGR reads:

$$K_{\mathrm{PGM}} = \max_{\alpha^2} K(\boldsymbol{\phi} = \mathbf{0},\,\alpha^2)\,, \tag{9.24}$$

with the optimized energy α^2_{PGM}. The results obtained for the above two receivers are discussed in the following section, where we compare both KGRs with the key rate of the DH protocol in order to highlight the advantages brought by the two non-Gaussian measurements.

The DH protocol is analogous to the one discussed above and employs DH detection at Bob's side, that is, a measurement of both field quadratures q and p, retrieving a pair of real outcomes $\mathbf{x} = (x_B, y_B) \in \mathbb{R}^2$. We underline that, while both the KOR and the PGM are described in terms of a finite-valued POVM with M possible outcomes, in the presence of heterodyne detection we have a continuous-variable measurement. Therefore, in this case Bob's conditional probability reads:

$$p^{(\mathrm{DH})}_{B|\alpha_k}(\mathbf{x}) = \frac{1}{4\pi\sigma_0^2}\exp\left\{-\left[x_B - 2\sigma_0\sqrt{T}\,\mathrm{Re}\,(\alpha_k)\right]^2/(4\sigma_0^2)\right\}\times$$
$$\exp\left\{-\left[y_B - 2\sigma_0\sqrt{T}\,\mathrm{Im}\,(\alpha_k)\right]^2/(4\sigma_0^2)\right\}, \tag{9.25}$$

σ_0^2 being the shot-noise variance [39], which from now on will be taken equal to 1, performing calculations in shot-noise units (SNU). Similarly to (9.10), the obtained mutual information is given by:

$$I^{(\mathrm{DH})}_{AB}(\alpha^2) = H\left[p^{(\mathrm{DH})}_B(\mathbf{x})\right] - \frac{1}{M}\sum_{k=0}^{M-1} H\left[p^{(\mathrm{DH})}_{B|\alpha_k}(\mathbf{x})\right], \tag{9.26}$$

with $p_B^{(\mathrm{DH})}(\mathbf{x}) = M^{-1}\sum_k p_{B|\alpha_k}^{(\mathrm{DH})}(\mathbf{x})$. Instead, the Holevo information becomes:

$$\chi_{BE}(\alpha^2) = S\left[\rho_E\right] - \int_{\mathbb{R}^2} d^2\mathbf{x}\; p_{B|\alpha_k}^{(\mathrm{DH})}(\mathbf{x})\; S\left[\rho_{E|\mathbf{x}}\right]\,, \tag{9.27}$$

with ρ_E given in (9.15) and

$$\rho_{E|\mathbf{x}} = \frac{1}{M p_B^{(\mathrm{DH})}(\mathbf{x})}\;\sum_{k=0}^{M-1} p_{B|\alpha_k}^{(\mathrm{DH})}(\mathbf{x})\;\left|\sqrt{1-T}\alpha_k\right\rangle\left\langle\sqrt{1-T}\alpha_k\right|\,. \tag{9.28}$$

The integration in (9.27) can been performed numerically by exploiting the Simpson's rule [328]. Finally, the resulting KGR is obtained as

$$K_{\mathrm{DH}} = \max_{\alpha^2}\left[\beta I_{AB}^{(\mathrm{DH})}(\alpha^2) - \chi_{BE}^{(\mathrm{DH})}(\alpha^2)\right]\,, \tag{9.29}$$

with the optimized modulation energy α^2_{DH}.

As a final remark, towards a realistic implementation of the present protocol, we underline that both the KOR and the PGM may not represent appropriate POVMs for the channel evaluation stage. Indeed, assuming that the channel properties do not change, Alice and Bob must estimate the channel parameters, which in the present case is limited to the sole transmissivity T. However, unlike homodyne and DH detection, in principle the designed POVM $\{\Pi_j\}_j$ does not guarantee full channel characterization. This problem may be circumvented, at least for the asymptotic key rate calculation, by performing Gaussian detection on a small fraction of the exchanged pulses and reserving it for the channel estimation stage, whilst exploiting the non-Gaussian receiver only for the key extraction. On the contrary, in the presence of a finite-size scenario, Alice and Bob estimate the channel transmissivity T with a finite uncertainty ΔT, thus leaving more space for Eve's intervention. Therefore, they employ a conservative strategy and compute the KGR by considering a lower value of the transmissivity, namely $T - \Delta T$. However, the main effect of this lower effective transmissivity is to reduce the range of distances for which the state-discrimination receivers outperforms the heterodyne protocol. Furthermore, the dataset for the key extraction is also finite, resulting in a lower KGR with respect to the asymptotic case.

Results. We now compare the results derived previously. In Fig. 9.2.2(a) we plot the KGRs (9.23), (9.24) and (9.29) as a function of the transmission distance d, expressed in km. The reconciliation efficiency is fixed to $\beta = 0.95$ [191, 192, 223]. We see that both PGM and KOR beat the DH protocol, that is $K_{\mathrm{p}} \geq K_{\mathrm{DH}}$, $\mathrm{p} = \mathrm{PGM}, \mathrm{KOR}$. The improvement in the KGR is more relevant for metropolitan-network distances, in particular for $d \leq 100$ km, whereas for larger ones both K_{KOR} and K_{PGM} approach K_{DH} and achieve the same asymptotic scaling. To quantify this improvement we compute the ratio

$$\mathcal{R}_{\mathrm{p}} = \frac{K_{\mathrm{p}}}{K_{\mathrm{DH}}}\,, \qquad \mathrm{p} = \mathrm{PGM}, \mathrm{KOR}\,, \tag{9.30}$$

reported in Fig. 9.2.2(b). Both the ratios exhibit peaks for $d \leq 40$ km and then decrease towards 1 in the long-distance regime, but the behaviour is rather different between the two cases. In fact, $\mathcal{R}_{\mathrm{PGM}}$ achieves a single maximum at ≈ 5 km, increasing the KGR with respect to K_{DH} by more than 42%, and then decays monotonously to 1. On the contrary, K_{KOR} is not a monotonic function of the transmission distance and, in turn,

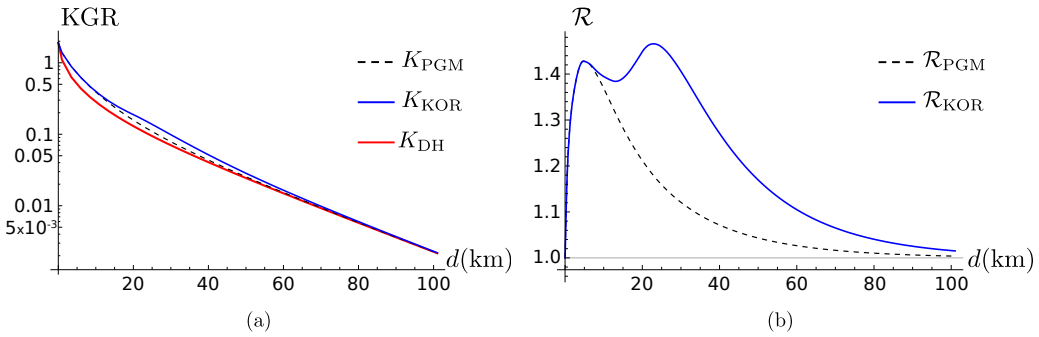


Figure 9.2.2: (a) Log plot of $K_{\rm p}$, $\rm p = PGM, KOR$, compared to $K_{\rm DH}$, as a function of the transmission distance d in km. (b) Plot of the ratio $\mathcal{R}_{\rm p}$, $\rm p = PGM, KOR$, as a function of the transmission distance d. State-discrimination receivers improve the KGR with respect to the DH protocol in the regime $d \leq 100$ km. In both pictures we set $\beta = 0.95$.

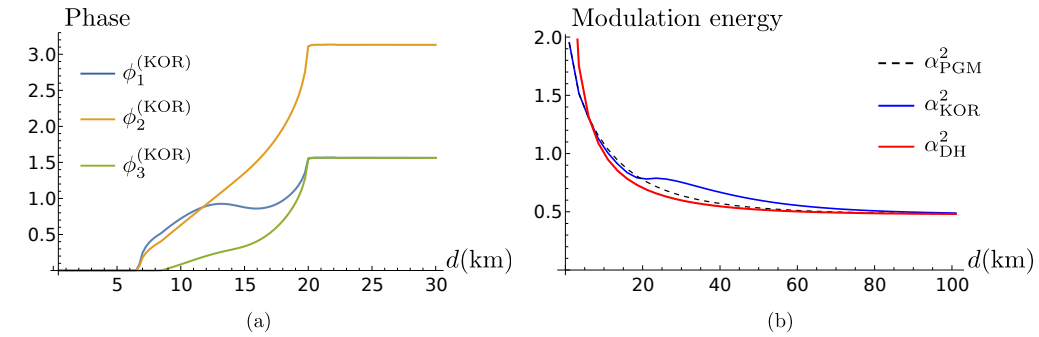


Figure 9.2.3: (a) Plot of the optimized phases $\phi_j^{(\rm KOR)}$, $j = 1, \ldots, 3$, as a function of the transmission distance d in km. We recall that $\phi_0^{(\rm KOR)} = 0$. (b) Plot of the optimized modulation energies $\alpha^2_{\rm p}$, $\rm p = PGM, KOR$, and $\alpha^2_{\rm DH}$, as a function of the transmission distance d. In both pictures we set $\beta = 0.95$.

the associated ratio exhibits two separated peaks. The KOR coincides with the PGM up to its first maximum, that is $\mathcal{R}_{\rm KOR} = \mathcal{R}_{\rm PGM}$ for $d \lesssim 7$ km, while for larger d we have $\mathcal{R}_{\rm KOR} \geq \mathcal{R}_{\rm PGM}$. Thereafter, $\mathcal{R}_{\rm KOR}$ reaches a local minimum and then achieves a second maximum at ≈ 23 km, with $\approx 47\%$ increase in the KGR. Ultimately, the curve decreases to 1, approaching the DH protocol together with $\mathcal{R}_{\rm PGM}$.

The behavior of $K_{\rm KOR}$ is a consequence of the resulting optimized phases $\phi_j^{(\rm KOR)}$, depicted in Fig. 9.2.3(a). We recall that $\phi_0^{(\rm KOR)} = 0$ by definition. For $d \lesssim 7$ km we have $\boldsymbol{\phi}_{\rm KOR} = \mathbf{0}$ and the optimized receiver is identical to the PGM, whereas for larger distances the optimized phases are nonzero and $\mathcal{R}_{\rm KOR} \geq \mathcal{R}_{\rm PGM}$. Interestingly, for $d \gtrsim 20$ km the optimized phase tuple becomes distance-independent and reads $\boldsymbol{\phi}_{\rm KOR} = (0, \pi/2, \pi, \pi/2)$. This choice allows to reach the second maximum in Fig. 9.2.2(b), after which the KOR approaches the DH protocol. For completeness, Fig. 9.2.3(b) reports also the optimized energies $\alpha^2_{\rm p}$, $\rm p = PGM, KOR$, and $\alpha^2_{\rm DH}$. All curves converge to 0.5 average number of photons in the long-distance regime but, differently from the other cases, $\alpha^2_{\rm KOR}$ shows the same non-monotonic trend of $K_{\rm KOR}$.

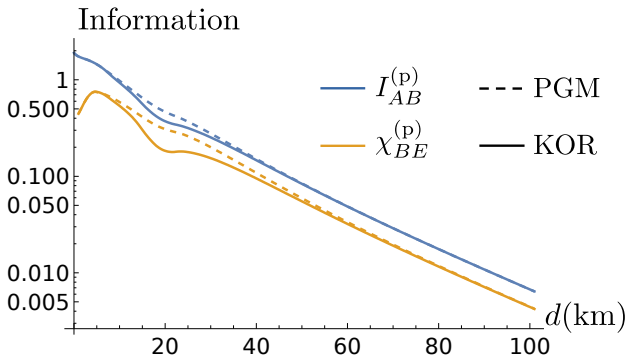


Figure 9.2.4: Log plot of $I_{AB}^{(\mathrm{p})}$ and $\chi_{BE}^{(\mathrm{p})}$, $\mathrm{p} = \mathrm{PGM}, \mathrm{KOR}$, as a function of the transmission distance d in km. Both the quantities are computed with the optimized parameters α_{p}^2 and $\boldsymbol{\phi}_{\mathrm{KOR}}$ (for the KOR). We set $\beta = 0.95$.

The previous results prove non-Gaussian receivers as a potential tool for improving the key rate of the QPSK protocol, at least in the present restricted eavesdropping scenario. Remarkably, they also highlight that the discrete-valued POVM minimizing the error probability, namely the PGM, does not coincide with the discrete-valued POVM maximizing the KGR, namely the KOR. The reason becomes evident when comparing separately the mutual and the Holevo information appearing in the KGR (9.9). In Fig. 9.2.4 we plot the quantities $I_{AB}^{(\mathrm{p})}$ and $\chi_{BE}^{(\mathrm{p})}$, $\mathrm{p} = \mathrm{PGM}, \mathrm{KOR}$, computed with the same optimized energy and phases previously obtained and depicted in Fig. 9.2.3 As we can see, in the metropolitan-network distance regime the optimized receiver is associated with a reduced mutual information with respect to the PGM but, at the same time, reducing the mutual information induces also a reduction of the Holevo information extractable by Eve, thus resulting in a higher KGR. As a consequence, differently from the state-discrimination scenario, in CVQKD there emerges a tradeoff between the goal of increasing the information accessible to Bob and the necessity of making the encoded symbols less "distinguishable" to weaken Eve's attack.

In light of this, we may interpret the physical meaning of the optimized phases as follows. For small transmission distances $\kappa d \ll 1$, Eve's intercepted signals are too weak to give her sufficient knowledge on which symbol was sent and the two different goals of reducing the error probability and maximizing the KGR are compatible, therefore the KOR coincides with the PGM. On the contrary, for larger d the compatibility does not hold anymore, and Bob has to sacrifice part of his potential information and to reduce the mutual information shared with Alice to the detriment of the eavesdropper.

The discussed tradeoff may be qualitatively appreciated by comparing the phase-space representations of the PGM and the KOR effects. More in detail, we consider the two reference measurement vectors $|\mu_0\rangle_{\mathrm{p}}$, $\mathrm{p} = \mathrm{PGM}, \mathrm{KOR}$, computed from (9.7) with the phases $\boldsymbol{\phi} = \mathbf{0}$ and $\boldsymbol{\phi} = (0, \pi/2, \pi, \pi/2)$, respectively, and compute the associated Wigner function:

$$W^{(\mathrm{p})}(q,p) = \frac{1}{2\pi} \sum_{n=0}^{\infty} (-1)^n \, \langle n | D^{\dagger}(\zeta) \, \rho_{\mathrm{p}} \, D(\zeta) | n \rangle \,, \quad \mathrm{p} = \mathrm{PGM}, \mathrm{KOR} \,, \tag{9.31}$$

where $\zeta = (q + ip)/2$ expressed in SNU, $\rho_{\mathrm{p}} = |\mu_0\rangle_{\mathrm{p}\,\mathrm{p}}\langle\mu_0|$ and $D(\zeta)$ is the displacement operator [31, 39]. The contour plots of $W^{(\mathrm{p})}(q,p)$ are depicted in Fig. 9.2.5 for $\alpha^2 = 1$

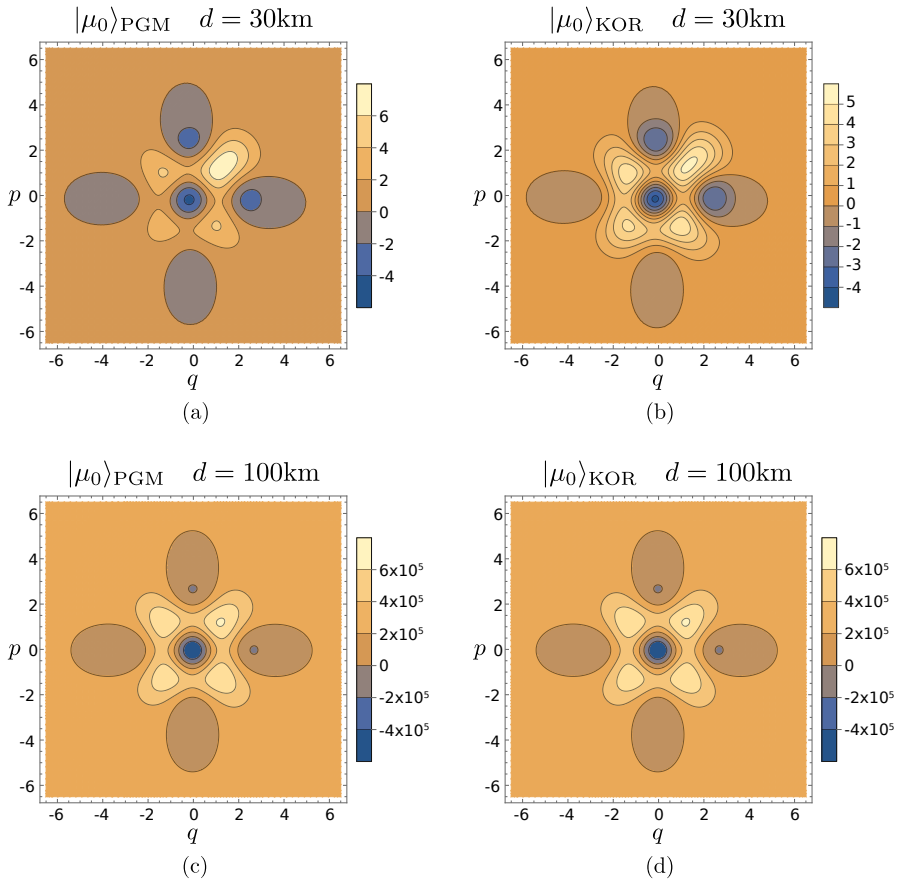


Figure 9.2.5: Contour plot of the Wigner functions $W^{(\mathrm{p})}(q,p)$ of the reference measurement vectors $|\mu_0\rangle_{\mathrm{p}}$, $\mathrm{p} = \mathrm{PGM}, \mathrm{KOR}$, for either $d = 30$ km (a-b) or $d = 100$ km (c-d). We set $\alpha^2 = 1$ and $\boldsymbol{\phi} = \mathbf{0}$ and $\boldsymbol{\phi} = (0, \pi/2, \pi, \pi/2)$ for the PGM and the optimized receiver, respectively.

and two different transmission distances $d = 30$ km and $d = 100$ km. If $d = 30$ km, that is for metropolitan-network distances, there is a qualitative difference between the two compared cases, see Fig.s 9.2.5(a) and 9.2.5(b). Both Wigner functions exhibit four peaks, corresponding to the four transmitted states $|\alpha_k^{(t)}\rangle$. However, $W^{(\mathrm{PGM})}(q,p)$ is well concentrated around state $|\alpha_0^{(t)}\rangle$, while $W^{(\mathrm{KOR})}(q,p)$ is more delocalized over the four states and the peaks are less distinguishable. This implies a reduced distinguishability of the states and, in turn, a reduced mutual information $I_{AB}^{(\mathrm{KOR})}$. On the contrary, when the distance is larger, e.g. $d = 100$ km, the transmitted states are weak coherent states with a greater overlap between one another. As a consequence, $W^{(\mathrm{p})}(q,p)$ for respective receivers are equally delocalized over the four peaks and the differences between PGM and KOR become negligible; see Fig.s 9.2.5(c) and 9.2.5(d). In turn, the associated KGRs converge to the same value, corresponding also to the rate of the DH protocol, as depicted in Fig. 9.2.2. Furthermore, in all cases we observe a Wigner-negativity, proving both $|\mu_0\rangle_{\mathrm{p}}$ to be non-classical (as well as non-Gaussian) states at all distances [31, 36, 39].

9.2.2 Employing feasible receivers

Even though both PGM and KOR discussed in the previous sections have shown interesting potentialities for CVQKD, from a practical point of view there is no clear idea on their experimental implementation. In fact, as discussed in Sec. 5.5, in the presence of QSPK designing a feasible optimum receiver is an open problem. In contrast, different suboptimal receivers have been proposed, ranging from feedback ones, like the Bondurant receiver, to displacement-photon counting schemes, either without feed-forward, e.g. the quaternary displacement receiver (QDRE), or employing it, like the quaternary displacement feed-forward receiver (QDFFRE) [17, 83, 92, 109, 110, 149, 154]. Therefore, it is worth of interest to investigate also the performance of these receivers for CVQKD. Here, in particular, we focus on the QDFFRE proposed by Izumi *et al.* in [109] and presented in Sec. 5.5.3.

In particular, when Bob adopts the QDFFRE in the protocol of Fig. 9.2.1, he probes

the conditional probabilities reported in Eq. (5.136), namely:

$$p^{(N)}_{B|\alpha_k}(0) = p_0^N \,, \tag{9.32a}$$

$$p^{(N)}_{B|\alpha_k}(1) = \sum_{t=0}^{N-2} p_k^t\,(1-p_k)\,p^{N-1-t}_{(k-1)\bmod M} + \frac{p_k^{N-1}(1-p_k)}{3} \,, \tag{9.32b}$$

$$\begin{aligned} p^{(N)}_{B|\alpha_k}(2) = &\sum_{t=0}^{N-3}\sum_{s=0}^{N-3-t} p_k^t\,(1-p_k)\,p^s_{(k-1)\bmod M}\,(1-p_{(k-1)\bmod M})\times \\ &p^{N-2-t-s}_{(k-2)\bmod M} + \sum_{t=0}^{N-2} p_k^t\,(1-p_k)\,\frac{p^{N-2-t}_{(k-1)\bmod M}(1-p_{(k-1)\bmod M})}{2} \\ &+ \frac{p_k^{N-1}(1-p_k)}{3} \,, \end{aligned} \tag{9.32c}$$

$$\begin{aligned} p^{(N)}_{B|\alpha_k}(3) = &\sum_{t=0}^{N-3}\sum_{s=0}^{N-3-t}\sum_{u=0}^{N-3-t-s} p_k^t\,(1-p_k)\,p^s_{(k-1)\bmod M}\times \\ &(1-p_{(k-1)\bmod M})\,p^u_{(k-2)\bmod M}\,(1-p_{(k-2)\bmod M})\,p^{N-3-t-s-u}_{(k-3)\bmod M} \\ &+ \sum_{t=0}^{N-2} p_k^t\,(1-p_k)\,\frac{p^{N-2-t}_{(k-1)\bmod M}(1-p_{(k-1)\bmod M})}{2} \\ &+ \frac{p_k^{N-1}(1-p_k)}{3} \,, \end{aligned} \tag{9.32d}$$

where, now, $p_0 = 1$, $p_1 = p_3 = \exp(-2T\alpha^2/N)$, and $p_2 = \exp(-4T\alpha^2/N)$, as Bob receives only the transmitted fraction of Alice's signals. Instead, the overall Bob's probability reads $p^{(N)}_B(j) = M^{-1}\sum_{k=0}^{M-1} p^{(N)}_{B|\alpha_k}(j)$, $j = 0, \ldots, M-1$.

To compute the KGR $K_{\rm QDF}(N;\alpha^2)$ associated with the QDFFRE, we exploit Eq.s (9.9), (9.10) and (9.13), provided the substitutions $p^{(\boldsymbol{\phi})}_{B|\alpha_k} \to p^{(N)}_{B|\alpha_k}$ and $p^{(\boldsymbol{\phi})}_{B} \to p^{(N)}_{B}$, and optimize over the modulation energy, obtaining:

$$K_{\rm QDF}(N) = \max_{\alpha^2} K_{\rm QDF}(N;\alpha^2) \,. \tag{9.33}$$

Moreover, we also compute the ratio with respect to the DH protocol, namely,

$$\mathcal{R}_{\rm QDF}(N) = \frac{K_{\rm QDF}(N)}{K_{\rm DH}} \,, \tag{9.34}$$

reported in Fig. 9.2.6(a) for different number of copies N. Unlike the PGM and the KOR, the QDFFRE outperforms the DH protocol only up to a maximum transmission distance $d_{\max}(N)$ whose value increases with N. Afterwards, we have $K_{\rm QDF}(N) \leq K_{\rm DH}$ and, in turn, $\mathcal{R}_{\rm QDF}(N)$ saturates to an asymptotic value ≤ 1. The best performance is achieved in the limit of infinite copies, $N \gg 1$, where the receiver approximates the type-I Bondurant receiver, see Sec. 5.5.3, obtaining a maximum increase in the KGR of about $\lesssim 20\%$ and $d_{\max}(N) \lesssim 25$ km.

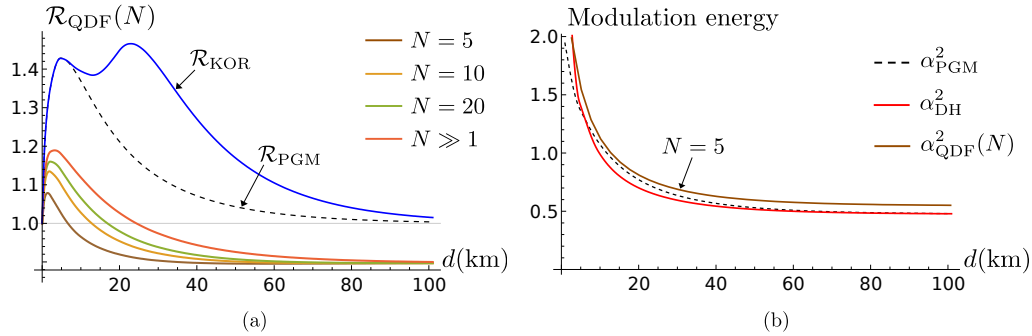


Figure 9.2.6: (a) Plot of the ratio $\mathcal{R}_{\rm QDF}(N)$ as a function of the transmission distance d in km. Differently from both PGM and KOR, the QDFFRE improves the KGR with respect to the DH protocol only up to a maximum distance $d_{\max}(N)$, increasing with the number of copies N. (b) Plot of the optimized modulation energies $\alpha^2_{\rm QDF}(N)$, $\alpha^2_{\rm PGM}$, and $\alpha^2_{\rm DH}$, as a function of the transmission distance d. In both pictures we set $\beta = 0.95$.

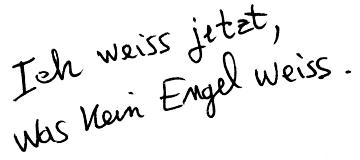
This behaviour is a direct consequence of the optimized modulation $\alpha^2_{\rm QDF}(N)$, reported in Fig. 9.2.6(b). In fact, $\alpha^2_{\rm QDF}(N)$ is a decreasing function of d, which in the long-distance regime, $\kappa d \gg 1$, reaches an asymptotic value $\gtrsim 0.5$. Numerical calculations also show this asymptote to be independent of the number of copies N. In these conditions, Bob receives a signal with $T\alpha^2_{\rm QDF}(N) \ll 0.5$ mean photons, for which the QDFFRE does not beat the SQL, achieved by DH discrimination (see, for instance, Fig. 5.5.7). In turn, even the KGR of the CVQKD protocol is lower than the corresponding heterodyne protocol. On the other hand, for $\kappa d \ll 1$, the optimized modulation is of few photons, the QDFFRE outperforms the SQL and we observe an increase also in the KGR.

In conclusion, despite its feasibility, the present displacement feed-forward scheme is not optimal for CVQKD, just as it is not optimal for coherent state discrimination. Nevertheless, it still provides an improvement of the resulting key rate in the short-distance regime, being a candidate for experimental realizations of the present protocol.

Conclusions

CHAPTER 10

Concluding remarks and future perspectives



- Damiel, *Der Himmel über Berlin*
(directed by Wim Wenders)

In this PhD thesis we have addressed some relevant aspects of quantum communications theory in continuous variable systems, with particular reference to quantum optical platforms. The field has gained much interest in time, for a twofold reason. On the one hand, quantum effects determine the ultimate limits of the transmission of classical information over optical communication links, being of particular relevance for protocols operated at low signal powers, e.g. near-space or deep-space communications. On the other hand, quantum features, like superposition, entanglement, teleportation, and Heisenberg's uncertainty relations, can be effectively exploited as a resource to design novel protocols and algorithms, and convey information in more efficient fashion. It is the case of quantum computation and quantum key distribution (QKD), where the superposition principle and the ultimate quantum noise due to commutation rules are crucial to efficiently solve hard computation problems and to distill random secure keys with unconditional security, respectively, thus overcoming the limitations of the corresponding classical schemes.

In particular, throughout the thesis, we focused ourselves on two main topics, namely quantum state discrimination and continuous variable (CV) QKD, providing a comprehensive theoretical analysis, together with an eye to possible practical implementations being compatible with the state-of-art technologies in optical telecommunications. We both addressed the general aspects of the theory and proposed new receivers and protocols that can be feasibly experimentally demonstrated, discussing also their robustness with respect to the relevant realistic inefficiencies occurring in practice.

To begin with, we dealt with the problem of quantum state discrimination. In Chapter 4, we introduced the fundamental aspects of the theory, whose task is to perform conclusive decision among a set of non-orthogonal quantum states. The very laws of quantum mechanics forbid exact discrimination, making every quantum receiver associated with a nonzero decision error probability, therefore the task is to identify the optimum receiver achieving the lowest possible error probability. Subsequently, we focused on the binary discrimination scenario, for which Helstrom's theory provides a full characterization of the optimum receiver. Then, we addressed binary discrimination of coherent states of radiation, that represents one of the fundamental problems in optical communication schemes, and consider a binary phase-shhift keying (BPSK) encoding. Remarkably, we proposed new hybrid receivers, based on the combination of weak-field homodyne detection and conditional displacement-photon counting, that outperform conventional detection schemes, based on quadrature detection, providing a genuine quantum advantage, and closing the gap with the Helstrom bound.

In Chapter 5, we widened our analysis to multilevel systems, studying discrimination of a constellation of M quantum states, with $M \geq 2$. In this case, the decision task can be recast into a convex optimization problem, and advanced linear algebra tools lead to characterization of the optimum receiver. Nevertheless, an explicit construction of this optimum quantum measurement is obtained only in the particular case of pure-state discrimination and geometrically uniform symmetry (GUS). Ultimately, we addressed M-ary discrimination of coherent states, considering quadrature phase-shift keying (QPSK) constellations, as a natural generalization of the previously considered BPSK encoding.

Then, our interest turned to CVQKD. In Chapter 6, we presented the basic tools of QKD, and discussed the main characteristics of CV protocols, where coherent states with randomly modulated amplitude are transmitted from a sender (Alice) to a receiver (Bob), communicating by an untrusted noisy quantum channel. Given this scenario, the protocol is considered secure as long as the information shared by Alice and Bob is larger than the one that can be extracted by a possible eavesdropper (Eve), leading to a nonzero key generation rate (KGR). Furthermore, we outlined the different security framework under which the analysis may be conducted, namely unconditional security, trusted-device scenario and wiretap channel. In this Chapter, we focused only on the unconditional security approach, and provide security proof for the GG02 protocol, based on Gaussian modulation of coherent states, as well as discrete-modulation protocols, employing both PSK and quadrature amplitude modulation (QAM), that provide a feasible alternative being easier to implement into practice. To this aim, we proved the fundamental theorem on the "optimality of Gaussian attacks", establishing a manageable lower bound to the KGR of protocols employing Gaussian detection.

Thereafter, in Chapter 7 we studied the two remaining security frameworks, that provide examples of restricted eavesdropping, in which we pose realistic limitations to the possible attacks that Eve may launch. In the trusted-device scenario, we included detection losses and noise in the theoretical description, assuming them to be simply lost to the environment and not intercepted by Eve, who, instead, controls both the losses and noise acquired during signal transmission. Remarkably, we extended the validity of optimality of Gaussian attacks to this scenario, thus determining a useful result to assess security in all the cases of partial lack of information at Eve's sides. Then, we addressed the wiretap channel description, that provides an example of a particular eavesdropping strategy, where Eve's action is completely characterized and specified. In both the scenarios, we computed the KGR for the QPSK protocol, comparing the results with the unconditional security approach, and obtaining an increase in the distilllable key rate.

In Chapter 8, we investigated the potentialities of optical amplifiers to perform loss mitigation of the quantum channel and enhance CVQKD. We established the quantum limits of amplification, introducing both conventional amplifiers, phase-insensitive (PIAs) and phase-sensitive amplifiers (PSAs), as well as probabilistic noiseless linear amplifiers (NLAs), studying their application for CVQKD in the Gaussian modulation format.

Finally, in Chapter 9, we merged the acquired knowledge of the two main Parts of the thesis, and designed an optimized state-discrimination receiver, the key-rate optimized receiver (KOR), for the QPSK CVQKD protocol, providing a first step towards non-Gaussian CVQKD. We assessed security under a pure-loss wiretap channel, and obtain an enhancement of the KGR with respect to the conventional protocol in the metropolitan-network distance regime. Furthermore, we also consider the performance of displacement receivers for CVQKD, as a benchmark example of a feasible scheme, obtaining an increase in the KGR up to a maximum transmission distance.

10.1 Future directions and outlooks

The results obtained in the thesis provide a detailed analysis of the current state of the art in the fields of both quantum state discrimination and CVQKD, and present innovative solutions to enhance the existing communication protocols by means of improved quantum receivers and advanced stragies for transmission losses mitigation. Furthermore, they identify the limits of quantum communications in realistic conditions, e.g. imperfect detection, non-Gaussian noise, imperfect signal modulation, ..., paving the way for new applications, from both a theoretical and experimental point of view. A brief overview of possible further developments is presented in the following.

10.1.1 Novelties in coherent states discrimination

Within quantum decision theory, one of the relevant results of this thesis is the proposal of hybrid receivers, namely the hybrid near-optimum (HYNORE) and the hybrid feed-forward (HFFRE) receivers, to enhance BPSK discrimination of coherent states [16–18]. These hybrid schemes exploit the photon-number resolving (PNR) technologies, gaining fast progresses in the latest years [329–331], to suitably combine the homodyne like and displacement setups, thus jointly probing the wave-like and particle-like properties of optical fields. In particular, in hybrid receivers the incoming signal is split at a beam splitter of variable transmissivity, and the reflected beam undergoes homodyne like detection, whose outcome determines a conditioned displacement operation on the transmitted beam: accordingly, we obtain a reduced error probability with respect to the standard displacement receivers.

Interestingly, the present philosophy offers a powerful approach to improve quantum receivers also for quaternary and M-ary phase-shift-keying discrimination [109, 149, 153, 154], where displacement feed-forward schemes are less powerful and may benefit even more from a suitable combination with weak-field measurements. In particular, two possible paths can be pursued. On the one hand, a fundamental problem is to assess the most efficient usage of PNR detectors to improve the maximum a posteriori probability (MAP) decision strategy. In the presence of multiple state discrimination, the capability to resolve individual photons promises a powerful enhancement for displacement feed-forward schemes, as the outcomes of PNR detection yield more information about the incoming signals than on-off detection. In fact, the encoded pulses are associated with Poisson statistics with different rates, thereby the number of registered clicks

gives indirect information on which was the probed signal, instead of the simple acceptance/rejection of the nulled hypothesis occurring with on-off strategies. In turn, a proper extension of the MAP criterion may lead to significant enhancements of the feed-forward rules, possibly closing the gap with the type II Bondurant receiver. On the other hand, given a displacement-PNR setup, we may also claim whether or not hybrid setups combining either weak-field homodyne or double weak-field homodyne detection, being the natural extension of the HYNORE, are able to further reduce the error probability, especially in the low-energy limit where non-optimized displacement schemes do not outperform the standard quantum limit.

10.1.2 Progresses in CVQKD

As regards the CVQKD analysis presented in this work, different problems can be addressed to obtain innovative solutions.

First of all, in the thesis we widely discussed about the practical limitation of Gaussian modulation, and address discrete modulation protocols as a more practical solution, highlighting the tradeoff between increased practicality of the setup and reduced amount of KGR to be achieved. In particular, PSK modulation proved itself as the simplest scheme for a realistic implementation, whereas QAM yielded a better tradeoff between the modulator complexity and the resulting KGR, allowing to close the gap with respect to GG02. A further solution within this topic may be offered by amplitude phase-shift keying (APSK) modulation, where both the amplitude and the phase of a carrier field are modulated to generate a multiple-ring constellation geometry in the phase space. APSK is becoming the emerging modulation format for deep-space communications, and it guarantees high information rates and energy efficiency with respect to competitive schemes, being also able to reach the Gaussian modulation capacity as the constellation size grows to infinity [332–337]. Accordingly, it candidates itself as a powerful scheme also for CVQKD applications, especially in the presence of smaller constellations with few symbols.

A second relevant issue in CVQKD is represented by channel loss mitigation, that can be partially addressed by the exploitation of optical amplifiers. In particular, we proved NLAs to provide an effective solution to achieve long-distance key distribution, being also robust against a reduced detection quantum efficiency. In turn, these results open new perspectives for the applications of NLAs in realistic conditions for both one-way communication and end-to-end communication over quantum repeater chains [305–307], with the ultimate goal of increasing the KGR up to the quantum channel secure-key capacity established in [306]. On the other hand, conventional amplifiers provide a simpler choice for large-scale applications in the framework of conditional security CVQKD. In particular, the advantage given by PSA, being a phase-sensitive operation, may be potentially further boosted by employing modulation of squeezed states [199, 201–205, 338].

Finally, in the last Chapter we made a first step towards the analysis of CVQKD with non-Gaussian measurements, suggesting suitable non-Gaussian receivers as a resource to increase the achievable key rate. Differently from conventional CVQKD protocols, this field still provides unclear and attractive open problems, fostering new research with a possibly higher potential impact. Given this premise, our results, obtained under a (restrictive) pure-loss wiretap channel assumption, leave many points as open problems. At first, the extension of the present analysis to the more realistic case of a thermal-loss channel remains a challenging task. In fact, in the presence of thermal mixed states, designing the receiver achieving the minimum error probability is non-trivial. The general

structure of quantum receivers exploited to the design the KOR does not hold anymore, as the $M \geq 2$ mixed states now span the whole infinite dimensional Hilbert space. Moreover, from the perspective of quantum communications, the optimum receiver achieving the minimum error probability can only be obtained numerically via linear convex semidefinite programming [51]. As a consequence, the search of the KOR could only be obtained via a brute-force functional optimization over all possible POVMs, being a non-linear and non-convex problem. Secondly, the sketch of an unconditional security proof may be designed, identifying which is the optimal Eve's attack. To do so, we should optimize over all the possible attacks compatible with Alice and Bob's statistics, retrieving the Devetak-Winter bound by extending the methods of [165, 166]. Indeed, the question whether or not protocols employing non-Gaussian measurement guarantee higher security than Gaussian ones is an interesting open problem. Finally, we should investigate the scalability of the present scheme with discrete modulation formats of higher order, like PSK schemes with $M \geq 4$ states or QAM constellations, in which the GUS is not satisfied anymore [20, 223, 225, 226].

Appendices

List of Appendices

A.1 The maximum a posteriori probability criterion

The maximum a posteriori probability (MAP) criterion represents a strategy based on Bayesian inference to improve the decision rule of a displacement-photon counting discrimination scheme [16, 92]. Here, we consider as a paradigmatic example the displacement-PNR (DPNR) receiver presented in Sec. 4.3.1 and, for the sake of simplicity, we address the case of binary coherent-state discrimination. That is, we discriminate between the two coherent states $|\alpha_k\rangle = |e^{ik\pi}\alpha\rangle$, $k = 0, 1$, $\alpha > 0$, generated with equal *a priori* probabilities $q_k = 1/2$.

In all displacement receivers, we apply a displacement operation $D(\beta)$, $\beta > 0$, to the incoming signal, mapping the states into

$$|\alpha_j\rangle \to |\alpha_j + \beta\rangle \,. \tag{A.1.1}$$

If we fix $\beta = \alpha$ we retrieve the usual "nulling" technique, whereas when β is considered as a free parameter to be optimized we obtain the improved receiver proposed by Takeoka and Sasaki [89].

Thereafter, we perform a PNR measurement on the displaced state and obtain the outcome n. Without loss of generality, we consider ideal photo-detection, namely with infinite resolution. The MAP criterion states that, for each n, we infer the state α_j, $j = 0, 1$, with the largest *a posteriori* probability:

$$p(\alpha_j|n) = \frac{p(n|\alpha_j)\, q_j}{p(n)} \,, \tag{A.1.2}$$

where

$$p(n|\alpha_j) = e^{-|\alpha_j+\beta|^2} \frac{|\alpha_j + \beta|^{2n}}{n!} \tag{A.1.3}$$

is the probability of getting n photons given α_j and

$$p(n) = \sum_{j=0,1} q_j p(n|\alpha_j) = \frac{p(n|\alpha_0) + p(n|\alpha_1)}{2} \tag{A.1.4}$$

is the overall probability of detecting n photons. For example, we infer state α_0 if $p(\alpha_0|n) > p(\alpha_1|n)$, which is equivalent to condition $p(n|\alpha_0) > p(n|\alpha_1)$ since we have $q_j = 1/2$.

The correct decision probability is then equal to

$$\mathcal{P}_{\rm c} = q_0 \sum_{n=0}^{\infty} p(n|\alpha_0)\chi_0 + q_1 \sum_{n=0}^{\infty} p(n|\alpha_1)\chi_1 \tag{A.1.5}$$

$$= \frac{1}{2} \sum_{n=0}^{\infty} \max\left[p(n|\alpha_0), p(n|\alpha_1)\right] , \tag{A.1.6}$$

where $\chi_0 = 1$ if $p(n|\alpha_0) > p(n|\alpha_1)$ and 0 otherwise and $\chi_1 = 1$ if $p(n|\alpha_1) > p(n|\alpha_0)$ and 0 otherwise. The error probability is obtained immediately as $P_{\rm err} = 1 - \mathcal{P}_{\rm c}$.

The decision rule $p(n|\alpha_0) \lesseqgtr p(n|\alpha_1)$ is equivalent to the definition of a threshold outcome $n_{\rm th}$ such that all measurement outcomes $n \geq n_{\rm th}$ are assigned to state α_1 and all $n < n_{\rm th}$ are assigned to state α_0. The threshold number is obtained by equating $p(\bar{n}|\alpha_0) = p(\bar{n}|\alpha_1)$, $\bar{n} \in \mathbb{R}$, and considering the lowest integer greater than the obtained root $\bar{n}$, namely $n_{\rm th} = \lceil \bar{n} \rceil$, where $\lceil x \rceil$ is the ceiling function, returning the smallest integer greater than x. We have:

$$n_{\rm th} = \left\lceil \frac{|\alpha+\beta|^2 - |\alpha-\beta|^2}{\ln\left(|\alpha+\beta|^2\right) - \ln\left(|\alpha-\beta|^2\right)} \right\rceil . \tag{A.1.7}$$

Thus, $\mathcal{P}_{\rm c}$ may be equivalently written as:

$$\mathcal{P}_{\rm c} = \frac{1}{2}\left[\sum_{n=0}^{n_{\rm th}-1} p(n|0) + \sum_{n=n_{\rm th}}^{\infty} p(n|1) \right] . \tag{A.1.8}$$

Finally, we note that for the standard Kennedy receiver, where the displacement amplitude is $\beta = \alpha$, we have $p(n|\alpha_0) = \delta_{n,0}$, therefore the correct probability of Eq. (A.1.5) reduces to the well known expression $\mathcal{P}_{\rm c} = 1 - \exp(-4\alpha^2)/2$.

A.2 A model for the visibility reduction at a beam splitter

In the framework of quantum optics, phase-sensitive operations, e.g. displacement operations and homodyne detection, are implemented via interference at a beam splitter between the signal beam and a suitable local oscillator (LO) [31, 33, 39, 84]. To obtain perfect interference in realistic implementations, it is required that the two optical modes impinging at the beam splitter are perfectly matched in both the frequency and spatial domain. This represents a nontrivial task from a practical point of view. In fact, realistic optical beams are associated with a finite spatial linewidth, and perfect interference can be only achieved when the spatial profiles of both the signal and the LO are fully superimposed. On the contrary, the presence of any mode mismatch due to misalignment of the two wave-fronts, leads to reduced visibility $\xi \leq 1$ of the optical interference, determined by how the intensity distributions of the signal beam and the LO overlap with each other. Perfect mode matching corresponds to unit visibility, $\xi = 1$, whilst in the case $\xi < 1$ the LO partially overlaps with the spatial modes orthogonal to the signal mode, with detrimental effects for any quantum measurement performed thereafter [114]. Here we present a model to describe the present effect, being relevant for many applications in quantum communications.

To begin with, we deal with a particular case and consider both the signal and the LO to be excited in coherent states $|\alpha\rangle$ and $|\beta\rangle$, $\alpha, \beta \in \mathbb{C}$, respectively, as schematized

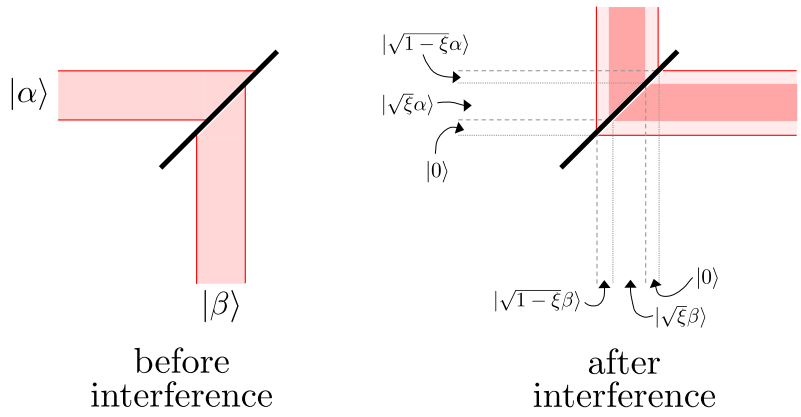


Figure A.2.1: Scheme of imperfect interference of coherent states due to mode mismatch at the beam splitter, associated with visibility $\xi \leq 1$. The two input beams before interference are misaligned, therefore only a fraction ξ of each beam is effectively overlapped, leading to quantum interference, whilst the remaining portions of both the signal and the LO interferes with spatial vacuum modes.

in Fig. A.2.1. In the presence of visibility reduction, the two input coherent beams are mismatched, and interference holds only for the beam portions that effectively overlap with each other. On the contrary, the remaining parts of both the signal and the LO overlap with spatial vacuum modes, being split into a transmitted and a reflected beam.

In turn, the presence of reduced visibility $\xi \leq 1$, quantifying the spatial overlap between the input optical beams, is equivalent to the splitting of the input coherent states into three channels, as described in Fig. A.2.1, namely:

$$|\alpha\rangle \rightarrow |\sqrt{\xi}\alpha\rangle \otimes |\sqrt{1-\xi}\alpha\rangle \otimes |0\rangle\,, \tag{A.2.1a}$$

$$|\beta\rangle \rightarrow |\sqrt{\xi}\beta\rangle \otimes |0\rangle \otimes |\sqrt{1-\xi}\beta\rangle\,, \tag{A.2.1b}$$

where only the reduced pulses $|\sqrt{\xi}\alpha\rangle$ and $|\sqrt{\xi}\beta\rangle$ are mode-matched, while the other ones impinge with further modes prepared in the vacuum. Thereafter, states (A.2.1) interfere at the beam splitter of transmissivity $\tau \leq 1$, leading to the output states on the transmitted and reflected side:

$$\begin{aligned}|\psi^{(t)}\rangle = |\sqrt{\xi}\left(\sqrt{\tau}\alpha + \sqrt{1-\tau}\beta\right)\rangle \\ \otimes |\sqrt{\tau(1-\xi)}\alpha\rangle \otimes |\sqrt{(1-\tau)(1-\xi)}\beta\rangle\,,\end{aligned} \tag{A.2.2a}$$

$$\begin{aligned}|\psi^{(r)}\rangle = |\sqrt{\xi}\left(\sqrt{\tau}\beta - \sqrt{1-\tau}\alpha\right)\rangle \\ \otimes |-\sqrt{(1-\tau)(1-\xi)}\alpha\rangle \otimes |-\sqrt{\tau(1-\xi)}\beta\rangle\,,\end{aligned} \tag{A.2.2b}$$

where the beam splitter operation acts independently on each channel. The mean number of photons $\bar{n}$ on both branches is then equal to:

$$\bar{n}^{(t)} = \tau|\alpha|^2 + (1-\tau)|\beta|^2 + 2\xi\sqrt{\tau(1-\tau)}\,\mathrm{Re}(\alpha\beta^*)\,, \tag{A.2.3a}$$

$$\bar{n}^{(r)} = \tau|\beta|^2 + (1-\tau)|\alpha|^2 - 2\xi\sqrt{\tau(1-\tau)}\,\mathrm{Re}(\alpha\beta^*)\,. \tag{A.2.3b}$$

We note that the overall effect of the mode mismatch is the reduction of the interference terms in (A.2.3), namely the terms proportional to $\mathrm{Re}(\alpha\beta^*)$.

In particular, from Eq. (A.2.3) we verify that the parameter ξ coincides with the inteference visibility $\mathcal{V}$ that can be experimentally measured. In fact, fringes visibility is measured by considering a balanced beam splitter, $\tau = 1/2$, when the LO and the signal are equal in power, namely $|\alpha|^2 = |\beta|^2$. We consider a single output port, e.g. the transmitted one, and evaluate the maximum and minimum output power as we change the phase difference between the two input beams, retrieving:

$$\mathcal{V} = \frac{\bar{n}^{(t)}_{\max} - \bar{n}^{(t)}_{\min}}{\bar{n}^{(t)}_{\max} + \bar{n}^{(t)}_{\min}} = \frac{2|\alpha|^2\xi}{2|\alpha|^2} = \xi\,. \tag{A.2.4}$$

Given the previous results, we now implement a quantum operation on the output beams, discussing the two relevant cases of displacement operation and homodyne detection. In the former one, to implement the displacement $D(\zeta)$, $\zeta \in \mathbb{C}$, we should choose $\beta = \zeta/\sqrt{1-\tau}$ in Eq. (A.2.2), take the limit $\tau \to 1$, and trace out the signal on the reflected branch [84]. Then, the mean number of photons on the transmitted beam becomes:

$$\bar{n}^{(t)}_{\mathrm{D}} = |\alpha|^2 + |\zeta|^2 + 2\xi\,\mathrm{Re}(\alpha\zeta^*) \neq |\alpha+\zeta|^2\,. \tag{A.2.5}$$

In particular, for the "nulling" displacement amplitude $\zeta = -\alpha$, we have $\bar{n}^{(t)}_{\mathrm{D}} = 2|\alpha|^2(1-\xi) \neq 0$, thus reduced visibility prevents the displacement of state $|\alpha\rangle$ into the vacuum. Instead, in the case of homodyne detection, we adopt a balanced beam splitter, $\tau = 1/2$, and the LO amplitude $\beta = ze^{i\phi}$, with $z \geq 0$ and $0 \leq \phi < \pi$. In this case, the mean number of photons on the two branches reads:

$$\bar{n}^{(t)}_{\mathrm{HD}} = \frac{|\alpha|^2 + z^2 + \xi|\alpha| z\cos\phi}{2} \quad \text{and} \quad \bar{n}^{(r)}_{\mathrm{HD}} = \frac{|\alpha|^2 + z^2 - \xi|\alpha| z\cos\phi}{2}\,. \tag{A.2.6}$$

We, then, evaluate the difference photocurrent Δ, that follows a Skellam distribution with mean value $\langle\Delta\rangle = \bar{n}^{(t)}_{\mathrm{HD}} - \bar{n}^{(r)}_{\mathrm{HD}} = \xi|\alpha| z\cos\phi$, and variance $\mathrm{Var}[\Delta] = \bar{n}^{(t)}_{\mathrm{HD}} + \bar{n}^{(r)}_{\mathrm{HD}} = |\alpha|^2 + z^2$. We conclude that reduced visibility in homodyne detection acts as a loss, playing the role of an "effective" quantum efficiency, that only reduces the average $\langle\Delta\rangle$, without affecting the variance of the homodyne distribution.

The former analysis suggests that visibility reduction may be described in terms of a loss dynamics. Therefore, we now proceed beyond coherent-states interference and provide a more general description, deriving the Heisenberg evolution of the modes impinging at a beam splitter with $\xi \leq 1$. The scheme is reported in Fig. A.2.2, where modes a_{in} and b_{in} are the signal and LO modes impinging at a (physical) beam splitter of transmissivity τ. Following the previous considerations, we model the effect of visibility on both the signal and the LO as a beam splitter with transmissivity $\xi \leq 1$, in which, before interference, modes a_{in} and b_{in} are mixed with two ancillary modes a'_{in} and b'_{in}, respectively, prepared in the vacuum state. Then, the output transmitted modes impinge at the physical beam splitter, while the reflected ones are coupled with a further pair of vacuum modes a''_{in} and b''_{in}. We describe the whole evolution via the input-output formalism. The input modes are $\mathbf{a}_{\mathrm{in}} = (a_{\mathrm{in}}, a'_{\mathrm{in}}, a''_{\mathrm{in}}, b_{\mathrm{in}}, b'_{\mathrm{in}}, b''_{\mathrm{in}})$. The evolution after the

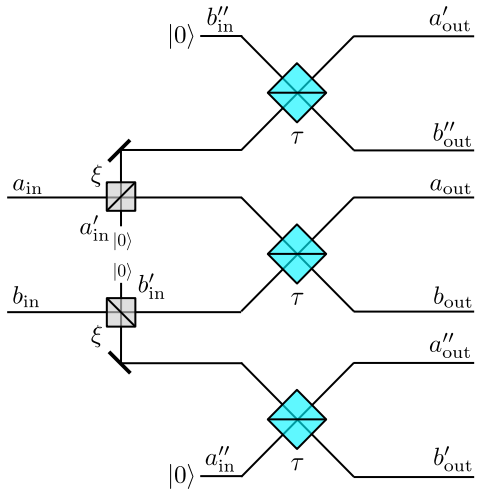


Figure A.2.2: Modes evolution in the presence of reduced visibility $\xi \leq 1$. We model the overall effect of visibility as a beam splitter of transmissivity ξ, acting on the input modes before the interference at the (physical) beam splitter of transmissivity τ.

two beam splitters modeling the visibility effect is described by the unitary matrix:

$$U_1 = \begin{pmatrix} \sqrt{\xi} & \sqrt{1-\xi} & 0 & 0 & 0 & 0 \\ -\sqrt{1-\xi} & \sqrt{\xi} & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & \sqrt{\xi} & \sqrt{1-\xi} & 0 \\ 0 & 0 & 0 & -\sqrt{1-\xi} & \sqrt{\xi} & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 \end{pmatrix} , \tag{A.2.7}$$

while the interference at the physical beam splitter of the three output channels is associated with the unitary:

$$U_2 = \begin{pmatrix} \sqrt{\tau} & 0 & 0 & \sqrt{1-\tau} & 0 & 0 \\ 0 & \sqrt{\tau} & 0 & 0 & 0 & \sqrt{1-\tau} \\ 0 & 0 & \sqrt{\tau} & 0 & \sqrt{1-\tau} & 0 \\ -\sqrt{1-\tau} & 0 & 0 & \sqrt{\tau} & 0 & 0 \\ 0 & 0 & -\sqrt{1-\tau} & 0 & \sqrt{\tau} & 0 \\ 0 & -\sqrt{1-\tau} & 0 & 0 & 0 & \sqrt{\tau} \end{pmatrix} . \tag{A.2.8}$$

The output modes $\mathbf{a}_{\rm out} = (a_{\rm out}, a'_{\rm out}, a''_{\rm out}, b_{\rm out}, b'_{\rm out}, b''_{\rm out})$ are then obtained as:

$$\mathbf{a}_{\rm out} = U_2 U_1 \mathbf{a}_{\rm in} \, , \tag{A.2.9}$$

where

$$a_{\rm out} = \sqrt{(1-\xi)(1-\tau)} b'_{\rm in} + \sqrt{\xi(1-\tau)} b_{\rm in} + \sqrt{\tau}\left(\sqrt{1-\xi} a'_{\rm in} + \sqrt{\xi} a_{\rm in}\right) , \tag{A.2.10a}$$

$$a'_{\rm out} = \sqrt{1-\tau} b''_{\rm in} + \sqrt{\tau}\left(\sqrt{\xi} a'_{\rm in} - \sqrt{1-\xi} a_{\rm in}\right) , \tag{A.2.10b}$$

$$a''_{\rm out} = -\sqrt{(1-\xi)(1-\tau)} b_{\rm in} + \sqrt{\xi(1-\tau)} b'_{\rm in} + \sqrt{\tau} a''_{\rm in} \, , \tag{A.2.10c}$$

$$b_{\rm out} = -\sqrt{(1-\xi)(1-\tau)}a'_{\rm in} - \sqrt{\xi(1-\tau)}a_{\rm in} + \sqrt{\tau}\left(\sqrt{1-\xi}b'_{\rm in} + \sqrt{\xi}b_{\rm in}\right), \quad \text{(A.2.10d)}$$

$$b'_{\rm out} = -\sqrt{1-\tau}a''_{\rm in} + \sqrt{\tau}\left(\sqrt{\xi}b'_{\rm in} - \sqrt{1-\xi}b_{\rm in}\right), \quad \text{(A.2.10e)}$$

$$b''_{\rm out} = \sqrt{(1-\xi)(1-\tau)}a_{\rm in} - \sqrt{\xi(1-\tau)}a'_{\rm in} + \sqrt{\tau}b''_{\rm in}. \quad \text{(A.2.10f)}$$

Moreover, the photon-number operators on the transmitted and reflected branches are equal to:

$$N^{(t)} = a^\dagger_{\rm out}a_{\rm out} + (a'_{\rm out})^\dagger a'_{\rm out} + (a''_{\rm out})^\dagger a''_{\rm out}, \quad \text{(A.2.11a)}$$

$$N^{(r)} = b^\dagger_{\rm out}b_{\rm out} + (b'_{\rm out})^\dagger b'_{\rm out} + (b''_{\rm out})^\dagger b''_{\rm out}, \quad \text{(A.2.11b)}$$

respectively. As an example, we consider homodyne detection, where we evaluate the difference photocurrent $\hat{\Delta} = N^{(t)} - N^{(r)}$ and rescale its value by the LO amplitude. In this scenario, all the ancillary modes are in the vacuum, while mode $b_{\rm in}$ is excited in the coherent state $|ze^{i\phi}\rangle$. Accordingly, in the limit $z \to \infty$ we obtain:

$$\frac{\langle ze^{i\phi}, \mathbf{0}|\,\hat{\Delta}\,|ze^{i\phi}, \mathbf{0}\rangle}{z} = \xi\,(a_{\rm in}e^{-i\phi} + a^\dagger_{\rm in}e^{i\phi}) = \xi\,x_\phi, \quad \text{(A.2.12)}$$

$$\frac{\langle ze^{i\phi}, \mathbf{0}|\,\hat{\Delta}^2\,|ze^{i\phi}, \mathbf{0}\rangle}{z^2} = \xi^2\,x_\phi^2 + (1-\xi^2), \quad \text{(A.2.13)}$$

where quadrature operators are expressed in shot-noise units and

$$|ze^{i\phi}, \mathbf{0}\rangle = |ze^{i\phi}\rangle_{b_{\rm in}}|0\rangle_{a'_{\rm in}}|0\rangle_{b'_{\rm in}}|0\rangle_{a''_{\rm in}}|0\rangle_{b''_{\rm in}}. \quad \text{(A.2.14)}$$

Thus, homodyne detection still provides measurement of quadrature x_ϕ, albeit with an "effective" quantum efficiency $\eta = \xi^2$, proving that the impact of visibility can be modeled in terms of inefficient detection, consistently with the previous discussions [114].

A.3 Effective channel parameters in ideal NLA-assisted CVQKD

In this appendix, we perform explicit derivation of the effective channel parameters in Eq. (8.79), describing the performance of the GG02 protocol assisted by an ideal NLA, associated with the unbounded operator $\mathcal{T} = g^{\hat{n}}$, where $g > 1$ is the amplifier gain and $\hat{n}$ is the photon-number operator of the incoming optical mode. As discussed in Sec. 8.2.2, the ideal NLA operation can be formally described in terms of the quantum CP map $\mathcal{E}_{\rm id}$, such that:

$$\mathcal{E}_{\rm id}(\rho) = P_{\rm id}\,\frac{\mathcal{T}\,\rho\,\mathcal{T}^\dagger}{{\rm Tr}[\mathcal{T}\,\rho\,\mathcal{T}^\dagger]} + (1-P_{\rm id})|0\rangle\langle 0|, \quad \text{(A.3.1)}$$

$P_{\rm id} \leq 1$ being the success probability of the transformation, that does not coincide with the trace of the post-selected state $\mathcal{T}\,\rho\,\mathcal{T}^\dagger$, since $\mathcal{T}$ is an unbounded operator. Furthermore, the operator $\mathcal{T}$ can be formally written as the exponential as $\mathcal{T} = \exp(H)$, $H = (\ln g)\,\hat{n}$ being a bilinear function of the creation and annihilation operators, therefore it preserves Gaussianity. That is, if ρ is Gaussian, $\mathcal{T}\,\rho\,\mathcal{T}^\dagger$ is Gaussian too. Nevertheless, due to its non-unitarity, it cannot be associated to any symplectic transformation,

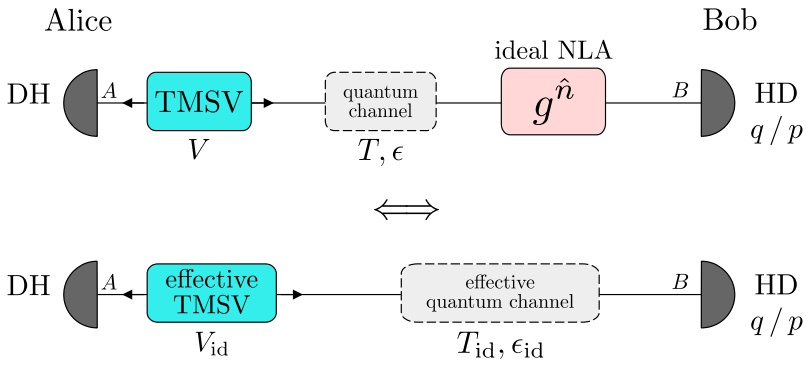


Figure A.3.1: Construction of the effective GG02 protocol associated with the ideal NLA-assisted protocol discussed in Sec. 8.4.1.

and the standard tools of Gaussian formalism cannot be straightforwardly applied to perform the security analysis of the CVQKD protocol.

Given these considerations, we conclude that the ideal NLA-assisted protocol depicted in the top panel of Fig. A.3.1, in which Alice generates a TMSV state of variance $V > 1$, namely:

$$|\text{TMSV}\rangle\rangle = \sqrt{1-\lambda^2}\sum_{n=0}^{\infty}\lambda^n|n\rangle|n\rangle\,, \tag{A.3.2}$$

where $\lambda = \sqrt{(V-1)/(V+1)}$, whose second brach, thereafter, is injected into a thermal loss channel (T,ϵ), followed by the ideal NLA $\mathcal{T}$, is equivalent to the effective GG02 scheme depicted in the bottom panel of Fig. A.3.1, where Alice generates a TMSV state with effective variance $V_{\text{id}} = (1+\lambda_{\text{id}}^2)/(1-\lambda_{\text{id}}^2)$, with $0 \leq \lambda_{\text{id}} < 1$, which then propagates throughout thermal-loss channel with effective transmissivity $T_{\text{id}} < 1$ and excess noise $\epsilon_{\text{id}} > 0$ [287]. Both the schemes are performed only for those runs when noiseless amplification is successful, occurring with probability P_{id}, otherwise the protocol is aborted. To construct this equivalent protocol, we remind that the conditional state probed by Bob after Alice's DH measurement is a displaced thermal state, while the overall state is a thermal state. Therefore, we first compute the general action of the NLA operation $\mathcal{T}$ on these states and, then, specify the results to the CVQKD scheme under investigation.

Amplified displaced thermal states. As discussed in Sec. 8.2.2, when a coherent state $|\alpha\rangle$, $\alpha \in \mathbb{C}$, undergoes ideal noiseless linear amplification, we have:

$$\mathcal{T}|\alpha\rangle = e^{-|\alpha|^2/2}\sum_{n=0}^{\infty}\frac{\alpha^n}{\sqrt{n!}}\,g^n|n\rangle = e^{(g^2-1)|\alpha|^2/2}\,|g\alpha\rangle\,, \tag{A.3.3}$$

in which we note that the output state is not normalized.

Now, we compute the output state of the ideal NLA when a displaced thermal state is considered as input, namely:

$$\rho_{\text{DT}} = D(\beta)\nu^{\text{th}}(\bar{n})D^{\dagger}(\beta)\,, \tag{A.3.4}$$

where $\beta \in \mathbb{C}$ is the displacement amplitude and $\bar{n}$ is the mean number of thermal photons. As will become clearer in the following, it is useful to define $\bar{n}$ in terms of a parameter $0 \leq \kappa < 1$ as $\bar{n} = \kappa^2/(1-\kappa^2)$, such that $\kappa^2 = \bar{n}/(\bar{n}+1)$. Eq. (A.3.4) can be also expressed in the Glauber-Sudarshan representation as $\rho_{\mathrm{DT}} = \int d^2\alpha P_{\mathrm{DT}}(\alpha)|\alpha\rangle\langle\alpha|$, where:

$$P_{\mathrm{DT}}(\alpha) = \frac{1-\kappa^2}{\pi\kappa^2} \exp\left(-\frac{1-\kappa^2}{\kappa^2}|\alpha-\beta|^2\right) \tag{A.3.5}$$

is the P-function associated with ρ_{DT} [287]. Thanks to (A.3.3), the output state ρ_g obtained after application of the NLA reads:

$$\begin{aligned}\rho_g &= \frac{1}{\mathcal{N}} \mathcal{T}\, \rho_{\mathrm{DT}}\, \mathcal{T}^\dagger \\ &= \frac{1}{\mathcal{N}} \int_{\mathbb{C}} d^2\alpha P_{\mathrm{DT}}(\alpha) e^{(g^2-1)|\alpha|^2} |g\alpha\rangle\langle g\alpha|\,,\end{aligned} \tag{A.3.6}$$

$\mathcal{N} = \mathrm{Tr}[\mathcal{T}\,\rho_{\mathrm{DT}}\,\mathcal{T}^\dagger]$ being the normalization factor. We perform the change of variable $u = g\alpha$ and re-express the former equation as $\rho_g = \int d^2u P_g(u)|u\rangle\langle u|$, where:

$$P_g(u) = \frac{1}{g^2\mathcal{N}} e^{\frac{g^2-1}{g^2}|u|^2} P_{\mathrm{DT}}\left(\frac{u}{g}\right) \tag{A.3.7}$$

is the P-function associated with ρ_g. Straightforward calculation leads to:

$$\begin{aligned}P_g(u) &= \frac{1}{g^2\mathcal{N}} \frac{1-\kappa^2}{\pi\kappa^2} \exp\left\{-\frac{g^2-1}{g^2}|u|^2 - \frac{1-\kappa^2}{g^2\kappa^2}|u-g\beta|^2\right\} \\ &= \frac{1}{g^2\mathcal{N}} \frac{1-\kappa^2}{\pi\kappa^2} \exp\left\{ -\frac{1-g^2\kappa^2}{g^2\kappa^2}|u|^2 \right. \\ &\qquad \left. -\frac{1-\kappa^2}{\kappa^2}|\beta|^2 + 2\frac{1-\kappa^2}{g^2\kappa^2}\mathrm{Re}(u^*\beta)\right\} \\ &= \frac{1}{g^2\mathcal{N}} \frac{1-\kappa^2}{\pi\kappa^2} e^{\frac{(g^2-1)(1-\kappa^2)}{1-g^2\kappa^2}|\beta|^2} \times \\ &\qquad \exp\left\{-\frac{1-g^2\kappa^2}{g^2\kappa^2}\left|u - g\frac{1-\kappa^2}{1-g^2\kappa^2}\beta\right|^2\right\}.\end{aligned} \tag{A.3.8}$$

Eq. (A.3.8) represents a Gaussian complex function up to an irrelevant normalization factor independent of u, thus state ρ_g is still a displaced thermal state in the form:

$$\rho_g = D(\beta_g)\nu^{\mathrm{th}}(\bar{n}_g)D^\dagger(\beta_g)\,, \tag{A.3.9}$$

with amplified displacement amplitude and thermal energy equal to:

$$\beta_g = g\frac{1-\kappa^2}{1-g^2\kappa^2}\beta \qquad \text{and} \qquad \bar{n}_g = \frac{\kappa_g^2}{1-\kappa_g^2} = \frac{g^2\kappa^2}{1-g^2\kappa^2}\,, \tag{A.3.10}$$

with $\kappa_g = g\kappa$, provided that condition $g\kappa < 1$ holds, which fixes a limit on the gain amplitude of the amplifier [287].

We conclude that an ideal NLA maps a displaced thermal state into another displaced thermal state with larger displacement amplitude and mean number of thermal photons. In particular, a thermal state (retrieved by fixing $\beta = 0$) is transformed into another thermal state with higher energy.

Derivation of the effective channel parameter for ideal-NLA assisted CVQKD. Given the former results, we are now ready to provide derivation of the equivalent channel displayed in Fig. A.3.1. In particular, we derive a set of 3 equations relating the original parameters (λ, T, ϵ) to the effective ones $(\lambda_{\rm id}, T_{\rm id}, \epsilon_{\rm id})$ [287]. To this aim, we proceed as follows.

To begin with, we consider the conditional state at Bob's side. That is, when Alice performs DH detection on the first mode of the TMSV, obtaining outcomes (x_A, y_A), the second branch is projected onto the coherent state $|\lambda\alpha_A\rangle$, with $\alpha_A = x_A + iy_A$. After propagation throughout the channel, the coherent pulse is transformed into a displaced thermal state $\rho_{\rm DT}(\alpha_A)$ with amplitude $\beta = \sqrt{T}\lambda\alpha_A$ and variance $1 + T\epsilon$, such that the mean number of thermal photons reads $\bar{n} = T\epsilon/2$, being associated with parameter $\kappa^2 = \bar{n}/(\bar{n}+1) = T\epsilon/(2+T\epsilon)$. Thereafter, Bob performs noiseless linear amplification on $\rho_{\rm DT}(\alpha_A)$, obtaining a displaced thermal state with $\kappa_g = g\kappa$ and the amplitude β_g reported in Eq. (A.3.10). This provides us with the first two relations [287]:

$$\sqrt{T_{\rm id}}\lambda_{\rm id}\alpha_A = g\frac{1-\kappa^2}{1-g^2\kappa^2}\sqrt{T}\lambda\alpha_A\,, \tag{A.3.11}$$

$$\frac{T_{\rm id}\epsilon_{\rm id}}{2+T_{\rm id}\epsilon_{\rm id}} = g^2\frac{T\epsilon}{2+T\epsilon}\,. \tag{A.3.12}$$

On the contrary, when Bob does not have access to the result of Alice's DH measurement, the overall state after propagation through the channel is a thermal state $\nu^{\rm th}(\bar{n}')$ with variance $T(V+\chi) = 1 + T(V-1+\epsilon)$, and mean number of photons:

$$\bar{n}' = T\left(\frac{\lambda^2}{1-\lambda^2} + \frac{\epsilon}{2}\right)\,, \tag{A.3.13}$$

associated with:

$$(\kappa')^2 = \frac{\bar{n}'}{\bar{n}'+1} = \frac{T[\lambda^2(2-\epsilon)+\epsilon]}{2+T\epsilon-\lambda^2[2-T(2-\epsilon)]}\,. \tag{A.3.14}$$

After the NLA, the state is converted into a thermal state with $\kappa_g' = g\kappa'$, leading to:

$$\frac{T_{\rm id}[\lambda_{\rm id}^2(2-\epsilon_{\rm id})+\epsilon_{\rm id}]}{2+T_{\rm id}\epsilon_{\rm id}-\lambda_{\rm id}^2[2-T_{\rm id}(2-\epsilon_{\rm id})]} = g^2\frac{T[\lambda^2(2-\epsilon)+\epsilon]}{2+T\epsilon-\lambda^2[2-T(2-\epsilon)]}\,. \tag{A.3.15}$$

Eq.s (A.3.11), (A.3.12) and (A.3.15) provide a system of equations for the variables $(\lambda_{\rm id}, T_{\rm id}, \epsilon_{\rm id})$, with corresponding solutions:

$$\lambda_{\rm id} = \lambda\sqrt{\frac{2+T(g^2-1)(2-\epsilon)}{2-T\epsilon(g^2-1)}}\,, \tag{A.3.16}$$

$$T_{\rm id} = \frac{g^2T}{1+T(g^2-1)[1+T\epsilon(g^2-1)(2-\epsilon)/4-\epsilon]}\,, \tag{A.3.17}$$

$$\epsilon_{\rm id} = \epsilon + (g^2-1)\frac{T\epsilon(2-\epsilon)}{2}\,, \tag{A.3.18}$$

retrieving the results of Eq. (8.79). Moreover, we obtain the expression of the effective TMSV variance as:

$$V_{\rm id} = \frac{1+\lambda_{\rm id}^2}{1-\lambda_{\rm id}^2} = V + \frac{T(g^2-1)Z^2}{2-T(g^2-1)(V-1+\epsilon)}\,, \tag{A.3.19}$$

with $Z = \sqrt{V^2-1}$. These parameters can be interpreted as physical parameters of an effective channel only if they keep a physical meaning, that is if they satisfy the constraints $0 \leq \lambda_{\rm id} < 1$ (equivalent to $V_{\rm id} \geq V$), $0 \leq T_{\rm id} \leq 1$ and $\epsilon_{\rm id} \geq 0$. The first request determines a tradeoff between the amplifier gain g, the channel transmissivity T, and the modulation variance V, that is:

$$T(g^2-1)(V-1+\epsilon) \leq 2\,, \tag{A.3.20}$$

which ultimately leads to Eq. (8.80). On the contrary, the second and third constraints impose conditions on the amplifier gain g and the excess noise ϵ, namely:

$$g \leq \sqrt{\frac{\epsilon\,(T\,(\epsilon-4)+2)+4\sqrt{\frac{T(\epsilon-2)+2}{\epsilon}}-2\sqrt{\epsilon\,(T\,(\epsilon-2)+2)}+4T-4}{T\,(\epsilon-2)^{\,2}}}\,, \tag{A.3.21}$$

and $\epsilon \leq 2$, respectively, the latter being equivalent to the constraint on the maximum tolerable excess noise associated with the PLOB bound [310].

Success probability of the ideal NLA. Finally, to complete the construction of the equivalent protocol, we should determine the value of the success probability $P_{\rm id}$ associated with the NLA, when one arm of the TSMV is considered as input. However, the exact computation cannot be handled, as $\mathcal{T}$ is unbounded, therefore the trace of the amplified states does not provide the corresponding success probability. Nevertheless, we establish an upper bound to $P_{\rm id}$, which can be considered as a best-case scenario for the security analysis [287].

First of all, from Eq. (A.3.1), we note that $\mathcal{E}_{\rm id}(|0\rangle\langle 0|) = |0\rangle\langle 0|$, proving the vacuum state to be a fixed point of $\mathcal{E}_{\rm id}$. Then, we invoke the contractivity of quantum maps: that is, any trace preserving quantum CP map cannot decrease the fidelity $\mathcal{F}$ between two quantum states [27, 287], thus for all states ρ we have:

$$\mathcal{F}\left(\rho, |0\rangle\langle 0|\right) \leq \mathcal{F}\left(\mathcal{E}_{\rm id}(\rho), |0\rangle\langle 0|\right)\,. \tag{A.3.22}$$

In particular, in the CVQKD protocol under investigation, the overall state transmitted into the channel is a thermal state $\nu^{\rm th}(\bar{n}') = [1-(\kappa')^2]\sum_n (\kappa')^{2n}|n\rangle\langle n|$, with $(\kappa')^2 = \bar{n}'/(\bar{n}'+1)$, see Eq. (A.3.13), while $\mathcal{E}[\nu^{\rm th}(\bar{n}')] = \nu^{\rm th}(\bar{n}'_g)$, having mean energy $\bar{n}'_g = \kappa_g^2/(1-\kappa_g^2)$, with $\kappa'_g = g\kappa'$. Then, Eq. (A.3.22) becomes:

$$\langle 0|\nu^{\rm th}(\bar{n}')|0\rangle \leq P_{\rm id}\,\langle 0|\nu^{\rm th}(\bar{n}'_g)|0\rangle + (1-P_{\rm id})\,, \tag{A.3.23}$$

being satisfied iff:

$$P_{\rm id} \leq \frac{1}{g^2}\,, \tag{A.3.24}$$

providing an upper bound to the NLA success probability [287].

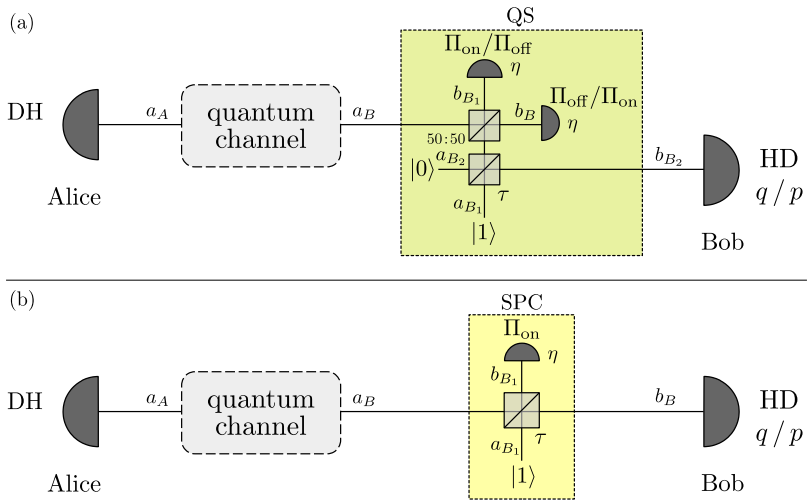


Figure A.4.1: Schematic representation of the two physical NLA-assisted protocol discussed in Sec. 8.4. (a) Strategy based on quantum scissors (QS); (b) strategy based on single-photon catalysis (SPC).

A.4 Unconditional security in physical NLA-assisted CVQKD

In the present appendix, we perform explicit derivation of the CM (8.90), being necessary for the unconditional security proof of the physical NLA-assisted CVQKD discussed in Sec. 8.4. As pointed out in the main text, we perform the security analysis by exploiting the optimality of Gaussian attacks. If Alice and Bob share a non-Gaussian state ρ, a lower bound of the exact KGR is obtained by considering a Gaussian protocol in which they share the Gaussian state $\rho_{\rm G}$ with the same CM of ρ. In particular, here we derive the CM for both the the quantum scissors (QS) and the single-photon catalysis (SPC). To do so, we exploit the input-output formalism and the phase-space representation of quantum states.

Quantum scissors (QS). By following the notation introduced in Fig. A.4.1(a), the protocol employing QS works as follows [35]. Alice prepares the TMSV and injects one mode into the thermal-loss channel, thereafter Bob performs the QS protocol on the received beam. The input modes are $\mathbf{a} = (a_A, a_B, a_{B_1}, a_{B_2})^{\mathsf{T}}$, where a_A, a_B are the modes shared by Alice and Bob after the channel whereas a_{B_1}, a_{B_2} are the modes exploited locally by Bob for the QS. The global input state, according to Glauber's formula, reads:

$$\rho_{\mathbf{a}} = \int \frac{d^2\boldsymbol{\alpha}}{\pi^4} \chi_{\mathbf{a}}(\boldsymbol{\alpha}) D_{\mathbf{a}}(\boldsymbol{\alpha})^{\dagger} , \tag{A.4.1}$$

where $\boldsymbol{\alpha} = (\alpha_A, \alpha_B, \alpha_{B_1}, \alpha_{B_2})^{\mathsf{T}}$ and

$$D_{\mathbf{a}}(\boldsymbol{\alpha}) = \bigotimes_k D_{a_k}(\alpha_k) , \tag{A.4.2}$$

where $D_{a_k}(\alpha_k)$ is the displacement operator acting on mode a_k, namely,

$$D_{a_k}(\alpha_k) = \exp(\alpha_k a_k^{\dagger} - \alpha_k^* a_k) . \tag{A.4.3}$$

Furthermore, in the previous expression we introduced the characteristic function:

$$\chi_{\mathbf{a}}(\boldsymbol{\alpha}) = \chi_{\mathrm{G}}(\alpha_A, \alpha_B) \times \left(1 - |\alpha_{B_1}|^2\right) e^{-(|\alpha_{B_1}|^2 + |\alpha_{B_2}|^2)/2}, \tag{A.4.4}$$

$\chi_{\mathrm{G}}(\alpha_A, \alpha_B)$ being the Gaussian characteristic function:

$$\chi_{\mathrm{G}}(\alpha_A, \alpha_B) = \exp\left[-\frac{1}{2}\tilde{\boldsymbol{\alpha}}_{AB}^{\mathsf{T}}\, \Gamma_{AB}\, \tilde{\boldsymbol{\alpha}}_{AB}\right], \tag{A.4.5}$$

with null prime moments and the CM Γ_{AB} introduced in Eq. (6.31), and where $\tilde{\boldsymbol{\alpha}}_{AB} = [\mathrm{Re}(\alpha_A), \mathrm{Im}(\alpha_A), \mathrm{Re}(\alpha_B), \mathrm{Im}(\alpha_B)]^{\mathsf{T}}$.

The output modes after the mode mixing operations performed by Bob are $\mathbf{b} = (b_A, b_B, b_{B_1}, b_{B_2})^{\mathsf{T}} = \mathcal{M}_{\mathrm{QS}}\mathbf{a}$, where

$$\mathcal{M}_{\mathrm{QS}} = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & \frac{1}{\sqrt{2}} & \sqrt{\tau/2} & -\sqrt{(1-\tau)/2} \\ 0 & -\frac{1}{\sqrt{2}} & \sqrt{\tau/2} & -\sqrt{(1-\tau)/2} \\ 0 & 0 & \sqrt{1-\tau} & \sqrt{\tau} \end{pmatrix}, \tag{A.4.6}$$

with $\tau = \tau_{\mathrm{QS}}(g) = (1+g^2)^{-1}$. The output state then writes:

$$\rho_{\mathbf{b}} = \int \frac{d^2\boldsymbol{\beta}}{\pi^4} \chi_{\mathbf{b}}(\boldsymbol{\beta}) D_{\mathbf{b}}(\boldsymbol{\beta})^\dagger, \tag{A.4.7}$$

where, exploiting the properties in Eq. (2.18), $\chi_{\mathbf{b}}(\boldsymbol{\beta}) = \chi_{\mathbf{a}}(\mathcal{M}_{\mathrm{QS}}^{\mathsf{T}}\boldsymbol{\alpha})$.

Finally, Bob performs on-off detection on modes b_B, b_{B_1}, corresponding to the positive-operator-valued measurement (POVM) $\{\Pi_{\mathrm{off}}, \Pi_{\mathrm{on}} = \mathbb{1} - \Pi_{\mathrm{off}}\}$, with associated characteristic functions [33, 339]:

$$\chi_{\mathrm{off}}(\alpha) = \frac{1}{\eta} \exp\left(-\frac{2-\eta}{2\eta}|\alpha|^2\right) \quad \text{and} \quad \chi_{\mathrm{on}}(\alpha) = \pi\delta^{(2)}(\alpha) - \chi_{\mathrm{off}}(\alpha). \tag{A.4.8}$$

The amplification is successful if one of the two detectors gives the outcome "on" [35, 285]. In the following we assume to retrieve the couple (on,off), respectively for modes b_B, b_{B_1}. The post-selected state then equals to:

$$\varrho_{\mathrm{QS}} = \frac{1}{\widetilde{P}_{\mathrm{QS}}} \int \frac{d^2\beta_A}{\pi} \frac{d^2\beta_{B_2}}{\pi} \chi_{\mathrm{QS}}(\beta_A, \beta_{B_2}) D_{b_A}(\beta_A)^\dagger D_{b_{B_2}}(\beta_{B_2})^\dagger, \tag{A.4.9}$$

where:

$$\chi_{\mathrm{QS}}(\beta_A, \beta_{B_2}) = \int \frac{d^2\beta_B}{\pi} \frac{d^2\beta_{B_1}}{\pi} \chi_{\mathbf{b}}(\boldsymbol{\beta}) \chi_{\mathrm{on}}(-\beta_B) \chi_{\mathrm{off}}(-\beta_{B_1}), \tag{A.4.10}$$

and

$$\begin{aligned} \widetilde{P}_{\mathrm{QS}} &= \mathrm{Tr}\left[\int \frac{d^2\beta_A}{\pi} \frac{d^2\beta_{B_2}}{\pi} \chi_{\mathrm{QS}}(\beta_A, \beta_{B_2}) D_{b_A}(\beta_A)^\dagger D_{b_{B_2}}(\beta_{B_2})^\dagger\right] \\ &= \chi_{\mathrm{QS}}(0,0) = 2\left[\frac{8\eta\tau + (w-1)(3+w)(1+\eta\tau)}{(1+w)^2(3+w)^2}\right] \end{aligned} \tag{A.4.11}$$

is the success probability of this conditional operation, with $w = 1 + \eta T(V + \epsilon - 1)$. The same results hold if Bob gets the pair (off,on), thus the global success probability of the QS-based NLA is:

$$P_{\rm QS} = 2\widetilde{P}_{\rm QS} = 4\left[\frac{8\eta\tau + (w-1)(3+w)(1+\eta\tau)}{(1+w)^2(3+w)^2}\right]. \tag{A.4.12}$$

Finally, we compute the CM associated with the state $\varrho_{\rm QS}$, for which we should compute terms proportional to $\mathrm{Tr}[D_{b_k}(\beta_k)q_{b_k}^2]$. To handle this calculation, we exploit the following property of displacement operations, derived in [35]:

$$\mathrm{Tr}\left[D(\alpha)q^2\right] = e^{-(x^2+y^2)/2}\left[\pi\delta^{(2)}(\alpha) + 2\pi y\delta(x)\frac{d}{dy}\delta(y) - \pi\delta(x)\frac{d^2}{dy^2}\delta(y)\right], \tag{A.4.13}$$

where we consider a single single radiation mode a with its corresponding quadrature $q = a + a^\dagger$, expressed in shot-noise units, with $\alpha = x + iy$ and $\delta(x)$ being the Dirac delta distribution.

By exploiting Eq. (A.4.13), we have:

$$V_{\rm QS} = \mathrm{Tr}\left[\varrho_{\rm QS}q_{b_A}^2\right] = -1 - \frac{\mathcal{V}_{\rm QS}}{\widetilde{P}_{\rm QS}}, \tag{A.4.14a}$$

$$W_{\rm QS} = \mathrm{Tr}\left[\varrho_{\rm QS}q_{b_{B_2}}^2\right] = -1 - \frac{\mathcal{W}_{\rm QS}}{\widetilde{P}_{\rm QS}}, \tag{A.4.14b}$$

$$Z_{\rm QS} = \mathrm{Tr}\left[\varrho_{\rm QS}q_{b_A}q_{b_{B_2}}\right] = -\frac{\mathcal{Z}_{\rm QS}}{\widetilde{P}_{\rm QS}}, \tag{A.4.14c}$$

where

$$\begin{aligned}\mathcal{V}_{\rm QS} &= \left[\frac{d^2}{dy^2}\left(e^{-y^2/2}\chi_{\rm QS}(iy,0)\right)\right]_{y=0} \\ &= 2(V+1)\left[\frac{(2+\eta T\epsilon)(1-\eta\tau)}{(1+w)^2}\right. \\ &\qquad \left. - \frac{8(3+w) + 2\eta T\epsilon(3+w-4\eta\tau) + 4\eta\tau(w-5)}{(3+w)^3}\right],\end{aligned} \tag{A.4.15a}$$

$$\begin{aligned}\mathcal{W}_{\rm QS} &= \left[\frac{d^2}{dv^2}\left(e^{-v^2/2}\chi_{\rm QS}(0,iv)\right)\right]_{y=0} \\ &= -4\,\frac{8\eta\tau + (w-1)(3+w)[2-(1-\eta)\tau]}{(1+w)(3+w)^2},\end{aligned} \tag{A.4.15b}$$

$$\begin{aligned}\mathcal{Z}_{\rm QS} &= \left[\frac{d^2}{dydv}\left(e^{-(y^2-v^2)/2}\chi_{\rm QS}(iy,iv)\right)\right]_{y=0,v=0} \\ &= \sqrt{T}Z\,\frac{8\eta\sqrt{\tau(1-\tau)}}{(3+w)^2}.\end{aligned} \tag{A.4.15c}$$

Accordingly, the CM writes:

$$\Gamma_{AB}^{(\mathrm{QS})} = \begin{pmatrix} V_{\mathrm{QS}}\,\mathbb{1}_2 & Z_{\mathrm{QS}}\,\boldsymbol{\sigma}_z \\ Z_{\mathrm{QS}}\,\boldsymbol{\sigma}_z & W_{\mathrm{QS}}\,\mathbb{1}_2 \end{pmatrix}. \tag{A.4.16}$$

Single-photon catalysis (SPC). For SPC we follow the analogous procedure of the previous subsection. The input modes depicted in Fig. A.4.1(b) are $\mathbf{a} = (a_A, a_B, a_{B_1})^{\mathsf{T}}$, where a_A, a_B are the modes shared by Alice and Bob after the channel and a_{B_1} is Bob's ancillary mode. The global input state reads:

$$\rho_{\mathbf{a}} = \int \frac{d^2\boldsymbol{\alpha}}{\pi^3} \chi_{\mathbf{a}}(\boldsymbol{\alpha}) D_{\mathbf{a}}(\boldsymbol{\alpha})^\dagger\,, \tag{A.4.17}$$

where $\boldsymbol{\alpha} = (\alpha_A, \alpha_B, \alpha_{B_1})^{\mathsf{T}}$ and

$$\chi_{\mathbf{a}}(\boldsymbol{\alpha}) = \chi_{\mathrm{G}}(\alpha_A, \alpha_B) \times e^{-|\alpha_{B_1}|^2/2}\left(1 - |\alpha_{B_1}|^2\right), \tag{A.4.18}$$

$\chi_{\mathrm{G}}(\alpha_A, \alpha_B)$ being the Gaussian characteristic function in Eq. (A.4.5) with null prime moments and the CM (6.31).

The output modes after the mode mixing operation performed by Bob are $\mathbf{b} = (b_A, b_B, b_{B_1})^{\mathsf{T}} = \mathcal{M}_{\mathrm{SPC}}\mathbf{a}$, where

$$\mathcal{M}_{\mathrm{SPC}} = \begin{pmatrix} 1 & 0 & 0 \\ 0 & \sqrt{\tau} & \sqrt{1-\tau} \\ 0 & -\sqrt{1-\tau} & \sqrt{\tau} \end{pmatrix}, \tag{A.4.19}$$

with $\tau = \tau_{\mathrm{SPC}}(g) = \left(4 + g^2 - g\sqrt{8+g^2}\right)/8$. The output state then writes:

$$\rho_{\mathbf{b}} = \int \frac{d^2\boldsymbol{\beta}}{\pi^3} \chi_{\mathbf{b}}(\boldsymbol{\beta}) D_{\mathbf{b}}(\boldsymbol{\beta})^\dagger\,, \tag{A.4.20}$$

where

$$\chi_{\mathbf{b}}(\boldsymbol{\beta}) = \chi_{\mathbf{a}}(\mathcal{M}_{\mathrm{SPC}}^{\mathsf{T}}\boldsymbol{\alpha})\,. \tag{A.4.21}$$

After the conditional on-off detection on mode b_{B_1}, the post-selected state reads:

$$\varrho_{\mathrm{SPC}} = \frac{1}{P_{\mathrm{SPC}}} \int \frac{d^2\beta_A}{\pi}\frac{d^2\beta_B}{\pi} \chi_{\mathrm{SPC}}(\beta_A, \beta_B) D_{b_A}(\beta_A)^\dagger D_{b_B}(\beta_B)^\dagger\,, \tag{A.4.22}$$

where:

$$\chi_{\mathrm{SPC}}(\beta_A, \beta_B) = \int \frac{d^2\beta_{B_1}}{\pi} \chi_{\mathbf{b}}(\boldsymbol{\beta}) \chi_{\mathrm{on}}(-\beta_{B_1})\,, \tag{A.4.23}$$

and

$$\begin{aligned} P_{\mathrm{SPC}} &= \mathrm{Tr}\left[\int \frac{d^2\beta_A}{\pi}\frac{d^2\beta_B}{\pi} \chi_{\mathrm{SPC}}(\beta_A, \beta_B) D_{b_A}(\beta_A)^\dagger D_{b_B}(\beta_B)^\dagger\right] \\ &= \chi_{\mathrm{SPC}}(0,0) = 1 - \frac{4(1-\eta\tau) + 2(w-1)(1-\tau)}{[2 + (w-1)(1-\tau)]^2} \end{aligned} \tag{A.4.24}$$

is the success probability of the SPC, and we introduced the quantity $w = 1 + \eta T(V + \epsilon - 1)$.

The CM associated with the state ϱ_{SPC} reads:

$$\Gamma_{AB}^{(\mathrm{SPC})} = \begin{pmatrix} V_{\mathrm{SPC}}\, \mathbb{1}_2 & Z_{\mathrm{SPC}}\, \boldsymbol{\sigma}_z \\ Z_{\mathrm{SPC}}\, \boldsymbol{\sigma}_z & W_{\mathrm{SPC}}\, \mathbb{1}_2 \end{pmatrix} . \tag{A.4.25}$$

As for QS, we have:

$$V_{\mathrm{SPC}} = \mathrm{Tr}\left[\varrho_{\mathrm{QS}} q_{b_A}^2\right] = -1 - \frac{\mathcal{V}_{\mathrm{SPC}}}{P_{\mathrm{SPC}}} , \tag{A.4.26}$$

$$W_{\mathrm{SPC}} = \mathrm{Tr}\left[\varrho_{\mathrm{QS}} q_{b_B}^2\right] = -1 - \frac{\mathcal{W}_{\mathrm{SPC}}}{P_{\mathrm{SPC}}} , \tag{A.4.27}$$

$$Z_{\mathrm{SPC}} = \mathrm{Tr}\left[\varrho_{\mathrm{QS}} q_{b_A} q_{b_B}\right] = -\frac{\mathcal{Z}_{\mathrm{SPC}}}{P_{\mathrm{SPC}}} , \tag{A.4.28}$$

and

$$\begin{aligned} \mathcal{V}_{\mathrm{SPC}} &= \left[\frac{d^2}{dy^2}\left(e^{-y^2/2}\chi_{\mathrm{SPC}}(iy,0)\right)\right]_{y=0} \\ &= -2(V+1)\left[\frac{1}{2} - \frac{4 + \eta T\epsilon(1-\tau)(1+q-4\eta\tau)}{(1+q)^3} \right. \\ &\qquad \left. + \frac{2(1+\eta\tau)(q-1) - 4\eta\tau}{(1+q)^3}\right] , \end{aligned} \tag{A.4.29a}$$

$$\begin{aligned} \mathcal{W}_{\mathrm{SPC}} &= \left[\frac{d^2}{dv^2}\left(e^{-v^2/2}\chi_{\mathrm{SPC}}(0,iv)\right)\right]_{y=0} \\ &= -4 - \tau(r-3) + 4\,\frac{(q-1)^2 + (r-1)(q-1)(\eta+\tau) + 2\tau(r-1) - 2\eta\tau(q-1)}{(1+q)^3} \\ &\qquad + 4\,\frac{2(w-1)(4-4\tau-\tau^2) + 4(2-\tau(1+\eta))}{(1+q)^3} , \end{aligned} \tag{A.4.29b}$$

$$\begin{aligned} \mathcal{Z}_{\mathrm{SPC}} &= \left[\frac{d^2}{dydv}\left(e^{-(y^2-v^2)/2}\chi_{\mathrm{SPC}}(iy,iv)\right)\right]_{y=0,v=0} \\ &= \sqrt{\tau T}Z\left[1 - 4\,\frac{2 + (1+\eta)(q-1) + 2\eta(1-2\tau)}{(1+q)^3}\right] , \end{aligned} \tag{A.4.29c}$$

with $q = 1 + \eta T(1-\tau)(V + \epsilon - 1)$ and $r = 1 + T(V + \epsilon - 1)$.

Bibliography

[1] A. Zeilinger, "Fundamentals of quantum information", Phys. World **11**, 35 (1998).

[2] R. Landauer, "Information is Physical", Phys. Today **44**, 23–29 (1991).

[3] R. Landauer, "The physical nature of information", Phys. Lett. A **217**, 188–193 (1996).

[4] R. Landauer, "Information is a physical entity", Phys. A: Stat. Mech. Appl. **263**, 63–67 (1999).

[5] J. P. Gordon, "Quantum effects in communications systems", Proc. IRE **50**, 1898–1908 (1962).

[6] R. L. Stratonovich, "Information capacity of a quantum communications channel. I.", Soviet Radiophysics **8**, 82–91 (1965).

[7] R. L. Stratonovich, "Information capacity of a quantum communication channel. II.", Soviet Radiophysics **8**, 92–101 (1965).

[8] C. W. Helstrom, "Quantum detection and estimation theory", J. Stat. Phys. **1**, 231–252 (1969).

[9] C. W. Helstrom, *Quantum detection and estimation theory* (Academic Press, New York, 1976).

[10] C. W. Helstrom, "Minimum mean-squared error of estimates in quantum statistics", Phys. Lett. A **25**, 101–102 (1967).

[11] A. S. Holevo, "On the capacity of quantum communication channel", Probl. Inform. Transm. **15**, 247–253 (1979).

[12] C. M. Caves, "Quantum limits on noise in linear amplifiers", Phys. Rev. D **26**, 1817–1839 (1982).

[13] C. H. Bennett and G. Brassard, "Brief history of quantum cryptography: a personal perspective", in Proceedings of IEEE International Conference on Computers, Systems and Signal Processing, Vol. 1 (1984), pp. 175–179.

[14] F. Grosshans and P. Grangier, "Continuous variable quantum cryptography using coherent states", Phys. Rev. Lett. **88**, 057902 (2002).

[15] A. S. Holevo, *Probabilistic and statistical aspects of quantum theory*, Vol. 1 (Springer, Basel, 1979).

[16] M. N. Notarnicola, M. G. A. Paris, and S. Olivares, "Hybrid near-optimum binary receiver with realistic photon-number-resolving detectors", J. Opt. Soc. Am. B **40**, 705–714 (2023).

[17] M. N. Notarnicola and S. Olivares, "Beating the standard quantum limit for binary phase-shift-keying discrimination with a realistic hybrid feed-forward receiver", Phys. Rev. A **108**, 042619 (2023).

[18] M. N. Notarnicola and S. Olivares, "A robust hybrid receiver for binary phase-shift keying discrimination in the presence of phase noise", Int. J. Quantum Inf. **22**, 2450008 (2024).

[19] M. N. Notarnicola, M. Jarzyna, S. Olivares, and K. Banaszek, "Optimizing state-discrimination receivers for continuous-variable quantum key distribution over a wiretap channel", New J. Phys. **25**, 103014 (2023).

[20] M. N. Notarnicola, S. Olivares, E. Forestieri, E. Parente, L. Potì, and M. Secondini, "Probabilistic amplitude shaping for continuous-variable quantum key distribution with discrete modulation over a wiretap channel", IEEE Trans. Commun. **72**, 375–386 (2024).

[21] M. N. Notarnicola and S. Olivares, "Long-distance continuous-variable quantum key distribution with feasible physical noiseless linear amplifiers", Phys. Rev. A **108**, 022404 (2023).

[22] M. N. Notarnicola, F. Cieciuch, and M. Jarzyna, "Continuous-variable quantum key distribution over multispan links employing phase-insensitive and phase-sensitive amplifiers", New J. Phys. **26**, 043015 (2024).

[23] M. G. A. Paris, "The modern tools of quantum mechanics: A tutorial on quantum states, measurements, and operations", Eur. Phys. J. ST **203**, 61–86 (2012).

[24] E. Ercolessi, "A short course on quantum mechanics and methods of quantization", Int. J. Geom. Methods Mod. Phys. **12**, 1560008 (2015).

[25] S. H. Friedberg, A. J. Insel, and L. E. Spence, *Linear Algebra*, 4th ed. (Pearson Education, Inc., 2014).

[26] H.-P. Breuer and F. Petruccione, *The theory of open quantum systems* (Oxford University Press, USA, 2002).

[27] M. A. Nielsen and I. L. Chuang, *Quantum Computation and Quantum Information* (Cambridge University Press, Cambridge, 2010).

[28] K. Kraus, A. Böhm, J. D. Dollard, and W. H. Wootters, *States, Effects, and Operations Fundamental Notions of Quantum Theory: Lectures in Mathematical Physics at the University of Texas at Austin* (Springer, 1983).

[29] W. F. Stinespring, "Positive functions on C*-algebras", Proc. Amer. Math. Soc. **6**, 211–216 (1955).

[30] V. Paulsen, *Completely bounded maps and operator algebras*, Vol. 78 (Cambridge University Press, 2002).

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

[32] C. C. Gerry and P. L. Knight, *Introductory quantum optics* (Cambridge University Press, New York, 2005).

[33] A. Ferraro, S. Olivares, and M. G. A. Paris, *Gaussian states in continuous variable quantum information* (Bibliopolis, Napoli, 2005).

[34] S. Olivares, "Quantum optics in the phase space - A tutorial on Gaussian states", Eur. Phys. J. Special Topics **203**, 3–24 (2012).

[35] M. Ghalaii, C. Ottaviani, R. Kumar, S. Pirandola, and M. Razavi, "Long-distance continuous-variable quantum key distribution with quantum scissors", IEEE J. Sel. Top. Quantum Electron. **26**, 1–12 (2020).

[36] M. G. Genoni, M. L. Palma, T. Tufarelli, S. Olivares, M. S. Kim, and M. G. A. Paris, "Detecting quantum non-Gaussianity via the Wigner function", Phys. Rev. A **87**, 062104 (2013).

[37] N. Quesada, L. G. Helt, J. Izaac, J. M. Arrazola, R. Shahrokhshahi, C. R. Myers, and K. K. Sabapathy, "Simulating realistic non-gaussian state preparation", Phys. Rev. A **100**, 022341 (2019).

[38] K. Banaszek, L. Kunz, M. Jachura, and M. Jarzyna, "Quantum limits in optical communications", J. Light. Technol. **38**, 2741–2754 (2020).

[39] S. Olivares, "Introduction to generation, manipulation and characterization of optical quantum states", Phys. Lett. A **418**, 127720 (2021).

[40] S. Olivares, A. Allevi, and M. Bondani, "On the role of the local oscillator intensity in optical homodyne-like tomography", Phys. Lett. A **384**, 126354 (2020).

[41] S. Olivares, A. Allevi, G. Caiazzo, M. G. A. Paris, and M. Bondani, "Quantum tomography of light states by photon-number-resolving detectors", New J. Phys. **21**, 103045 (2019).

[42] G. S. Thekkadath, D. S. Phillips, J. F. F. Bulmer, W. R. Clements, A. Eckstein, B. A. Bell, J. Lugani, T. A. W. Wolterink, A. Lita, S. W. Nam, T. Gerrits, C. G. Wade, and I. A. Walmsley, "Tuning between photon-number and quadrature measurements with weak-field homodyne detection", Phys. Rev. A **101**, 031801 (2020).

[43] R. Nehra, M. Eaton, C. González-Arciniegas, M. S. Kim, T. Gerrits, A. Lita, S. W. Nam, and O. Pfister, "Generalized overlap quantum state tomography", Phys. Rev. Res. **2**, 042002 (2020).

[44] G. Chesi, L. Malinverno, A. Allevi, R. Santoro, M. Caccia, A. Martemiyanov, and M. Bondani, "Optimizing silicon photomultipliers for quantum optics", Sci. Rep. **9**, 7433 (2019).

[45] S. Cassina, A. Allevi, V. Mascagna, M. Prest, E. Vallazza, and M. Bondani, "Exploiting the wide dynamic range of silicon photomultipliers for quantum optics applications", EPJ Quantum Technol. **8**, 4 (2021).

[46] A. Sanvito, S. Cassina, M. Lamperti, M. N. Notarnicola, S. Olivares, and A. Allevi, "Assessing a binary quantum channel exploiting a silicon photomultiplier based hybrid receiver", Opt. Express **32**, 39846–39859 (2024).

[47] G. Donati, T. J. Bartley, X.-M. Jin, M.-D. Vidrighin, A. Datta, M. Barbieri, and I. A. Walmsley, "Observing optical coherence across Fock layers with weak-field homodyne detectors", Nat. Commun. **5**, 5584 (2019).

[48] A. Allevi, M. Bina, S. Olivares, and M. Bondani, "Homodyne-like detection scheme based on photon-number-resolving detectors", Int. J. Quantum Inf. **15**, 1740016 (2017).

[49] C. E. Shannon, "Communication theory of secrecy systems", Bell Syst. Tech. J. **28**, 656–715 (1949).

[50] R.-J. Essiambre, G. Kramer, P. J. Winzer, G. J. Foschini, and B. Goebel, "Capacity limits of optical fiber networks", J. Light. Technol. **28**, 662–701 (2010).

[51] G. Cariolaro, *Quantum communications*, Signals and Communication Technology (Springer, Berlin, 2015).

[52] M. N. Notarnicola and S. Olivares, "Employing weak-field homodyne detection for quantum communications", arXiv:2405.14310 [quant-ph] (2024).

[53] T. M. Cover, *Elements of information theory* (John Wiley & Sons, 1999).

[54] A. Holevo, "Statistical decision theory for quantum systems", J. Multivar. Anal. **3**, 337–394 (1973).

[55] A. Holevo, "The capacity of the quantum channel with general signal states", IEEE Trans. Inf. Theory **44**, 269–273 (1998).

[56] B. Schumacher and M. D. Westmoreland, "Sending classical information via noisy quantum channels", Phys. Rev. A **56**, 131–138 (1997).

[57] V. Giovannetti, R. García-Patrón, N. J. Cerf, and A. S. Holevo, "Ultimate classical communication rates of quantum optical channels", Nat. Photonics **8**, 796–800 (2014).

[58] V. Giovannetti, S. Guha, S. Lloyd, L. Maccone, J. H. Shapiro, and H. P. Yuen, "Classical capacity of the lossy bosonic channel: the exact solution", Phys. Rev. Lett. **92**, 027902 (2004).

[59] A. S. Holevo and R. F. Werner, "Evaluating capacities of bosonic gaussian channels", Phys. Rev. A **63**, 032312 (2001).

[60] S. Guha, "Structured optical receivers to attain superadditive capacity and the holevo limit", Phys. Rev. Lett. **106**, 240502 (2011).

[61] K. Banaszek and M. Jachura, "Structured optical receivers for efficient deep-space communication", in 2017 IEEE International Conference on Space Optical Systems and Applications (ICSOS) (2017), pp. 34–37.

[62] J. Bowen, "The effect of attenuation on the capacity of a photon channel", IEEE Trans. Inf. Theory **14**, 44–50 (1968).

[63] S. Shamai, "Capacity of a pulse amplitude modulated direct detection photon channel", Proc. Inst. Elec. Eng. **137**, 424–430 (1990).

[64] A. Martinez, "Spectral efficiency of optical direct detection", J. Opt. Soc. Am. B **24**, 739–749 (2007).

[65] M. Cheraghchi and J. Ribeiro, "Improved upper bounds and structural results on the capacity of the discrete-time poisson channel", IEEE Trans. Inf. Theory **65**, 4052–4068 (2019).

[66] K. Łukanowski and M. Jarzyna, "Capacity of a lossy photon channel with direct detection", IEEE Trans. Commun. **69**, 5059–5068 (2021).

[67] J. A. Bergou, "Discrimination of quantum states", J. Mod. Opt. **57**, 160–180 (2010).

[68] C. H. Bennett, "Quantum cryptography using any two nonorthogonal states", Phys. Rev. Lett. **68**, 3121–3124 (1992).

[69] J. A. Bergou, U. Herzog, and M. Hillery, "11 discrimination of quantum states", in *Quantum state estimation*, edited by M. G. A. Paris and J. Řeháček (Springer, Berlin, Heidelberg, 2004), pp. 417–465.

[70] S. M. Barnett and S. Croke, "Quantum state discrimination", Adv. Opt. Photon. **1**, 238–278 (2009).

[71] J. A. Bergou, "Quantum state discrimination and selected applications", J. Phys. Conf. Ser. **84**, 012001 (2007).

[72] A. Chefles, "Quantum state discrimination", Contemp. Phys. **41**, 401–424 (2000).

[73] J. Bae and L.-C. Kwek, "Quantum state discrimination and its applications", J. Phys. A Math. Theor. **48**, 083001 (2015).

[74] K. Mølmer, "Hypothesis testing with open quantum systems", Phys. Rev. Lett. **114**, 040401 (2015).

[75] W. K. Wootters and W. H. Zurek, "A single quantum cannot be cloned", Nature **299**, 802–803 (1982).

[76] D. Dieks, "Communication by EPR devices", Phys. Lett. A **92**, 271–272 (1982).

[77] V. Buzek and M. Hillery, "Quantum cloning", Phys. World **14**, 25 (2001).

[78] I. Ivanovic, "How to differentiate between non-orthogonal states", Phys. Lett. A **123**, 257–259 (1987).

[79] D. Dieks, "Overlap and distinguishability of quantum states", Phys. Lett. A **126**, 303–306 (1988).

[80] A. Peres, "How to differentiate between non-orthogonal states", Phys. Lett. A **128**, 19 (1988).

[81] S. Croke, E. Andersson, S. M. Barnett, C. R. Gilson, and J. Jeffers, "Maximum confidence quantum measurements", Phys. Rev. Lett. **96**, 070401 (2006).

[82] K. Hunter, "Measurement does not always aid state discrimination", Phys. Rev. A **68**, 012306 (2003).

[83] R. S. Kennedy, "A near-optimum receiver for the binary coherent state quantum channel", MIT Res. Lab. Electron. Quart. Prog. Rep. **108**, 219–225 (1973).

[84] M. G. A. Paris, "Displacement operator by beam splitter", Phys. Lett. A **217**, 78–80 (1996).

[85] C.-W. Lau, V. A. Vilnrotter, S. Dolinar, J. Geremia, and H. Mabuchi, "Binary quantum receiver concept demonstration", in Free-Space Laser Communication Technologies XVIII, Vol. 6105 (SPIE, 2006), pp. 144–150.

[86] C. Wittmann, M. Takeoka, K. N. Cassemiro, M. Sasaki, G. Leuchs, and U. L. Andersen, "Demonstration of near-optimal discrimination of optical coherent states", Phys. Rev. Lett. **101**, 210501 (2008).

[87] K. Tsujino, D. Fukuda, G. Fujii, M. Takeoka, M. Fujiwra, S. Inoue, and M. Sasaki, "Experimental demonstration of near-optimal quantum receiver using a superconducting transition edge sensor", in CLEO/Europe and EQEC 2009 Conference Digest (Optica Publishing Group, 2009), ED4_1.

[88] M. L. Shcherbatenko, M. S. Elezov, G. N. Goltsman, and D. V. Sych, "Sub-shot-noise-limited fiber-optic quantum receiver", Phys. Rev. A **101**, 032306 (2020).

[89] M. Takeoka and M. Sasaki, "Discrimination of the binary coherent signal: gaussian-operation limit and simple non-gaussian near-optimal receivers", Phys. Rev. A **78**, 022320 (2008).

[90] C. Wittmann, U. L. Andersen, and G. Leuchs, "Discrimination of optical coherent states using a photon number resolving detector", J. Mod. Opt. **57**, 213–217 (2010).

[91] C. Wittmann, U. L. Andersen, M. Takeoka, D. Sych, and G. Leuchs, "Demonstration of coherent-state discrimination using a displacement-controlled photon-number-resolving detector", Phys. Rev. Lett. **104**, 100505 (2010).

[92] M. T. DiMario, E. Carrasco, R. A. Jackson, and F. E. Becerra, "Implementation of a single-shot receiver for quaternary phase-shift keyed coherent states", J. Opt. Soc. Am. B **35**, 568–574 (2018).

[93] M. T. DiMario, L. Kunz, K. Banaszek, and F. E. Becerra, "Optimized communication strategies with binary coherent states over phase noise channels", npj Quantum Inf. **5**, 65 (2019).

[94] S. J. Dolinar, "An optimum receiver for the binary coherent state quantum channel", MIT Res. Lab. Electron. Quart. Prog. Rep. **11**, 115–120 (1973).

[95] A. Assalini, N. Dalla Pozza, and G. Pierobon, "Revisiting the Dolinar receiver through multiple-copy state discrimination theory", Phys. Rev. A **84**, 022342 (2011).

[96] E. Parzen, *Stochastic processes* (Holden Day, San Francisco, 1962).

[97] D. Brody and B. Meister, "Minimum decision cost for quantum ensembles", Phys. Rev. Lett. **76**, 1–5 (1996).

[98] A. Acín, E. Bagan, M. Baig, L. Masanes, and R. Muñoz-Tapia, "Multiple-copy two-state discrimination with individual measurements", Phys. Rev. A **71**, 032338 (2005).

[99] J. M. Geremia, "Distinguishing between optical coherent states with imperfect detection", Phys. Rev. A **70**, 062303 (2004).

[100] R. Cook, P. Martin, and J. M. Geremia, "Optical coherent state discrimination using a closed-loop quantum measurement", Nature **446**, 774–777 (2007).

[101] D. Sych and G. Leuchs, "Practical receiver for optimal discrimination of binary coherent signals", Phys. Rev. Lett. **117**, 200501 (2016).

[102] M. J. Fitch, B. C. Jacobs, T. B. Pittman, and J. D. Franson, "Photon-number resolution using time-multiplexed single-photon detectors", Phys. Rev. A **68**, 043814 (2003).

[103] V. Schettini, S. V. Polyakov, I. P. Degiovanni, G. Brida, S. Castelletto, and A. L. Migdall, "Implementing a multiplexed system of detectors for higher photon counting rates", IEEE J. Sel. Top. Quantum Electron. **13**, 978–983 (2007).

[104] M. Sasaki and O. Hirota, "Optimum decision scheme with a unitary control process for binary quantum-state signals", Phys. Rev. A **54**, 2728–2736 (1996).

[105] M. G. Raymer, J. Cooper, H. J. Carmichael, M. Beck, and D. T. Smithey, "Ultrafast measurement of optical-field statistics by dc-balanced homodyne detection", J. Opt. Soc. Am. B **12**, 1801–1812 (1995).

[106] H. Hansen, T. Aichele, C. Hettich, P. Lodahl, A. I. Lvovsky, J. Mlynek, and S. Schiller, "Ultrasensitive pulsed, balanced homodyne detector: application to time-domain quantum measurements", Opt. Lett. **26**, 1714–1716 (2001).

[107] A. Zavatta, M. Bellini, P. L. Ramazza, F. Marin, and F. T. Arecchi, "Time-domain analysis of quantum states of light: noise characterization and homodyne tomography", J. Opt. Soc. Am. B **19**, 1189–1194 (2002).

[108] G. Humer, M. Peev, C. Schaeff, S. Ramelow, M. Stipčević, and R. Ursin, "A simple and robust method for estimating afterpulsing in single photon detectors", J. Light. Technol. **33**, 3098–3107 (2015).

[109] S. Izumi, M. Takeoka, M. Fujiwara, N. D. Pozza, A. Assalini, K. Ema, and M. Sasaki, "Displacement receiver for phase-shift-keyed coherent states", Phys. Rev. A **86**, 042328 (2012).

[110] M. T. DiMario, E. Carrasco, R. A. Jackson, and F. E. Becerra, "Implementation of a single-shot receiver for quaternary phase-shift keyed coherent states", J. Opt. Soc. Am. B **35**, 568–574 (2018).

[111] S. Izumi, J. S. Neergaard-Nielsen, and U. L. Andersen, "Adaptive generalized measurement for unambiguous state discrimination of quaternary phase-shift-keying coherent states", PRX Quantum **2**, 020305 (2021).

[112] G. S. Thekkadath, S. Sempere-Llagostera, B. A. Bell, R. B. Patel, M. S. Kim, and I. A. Walmsley, "Single-shot discrimination of coherent states beyond the standard quantum limit", Opt. Lett. **46**, 2565–2568 (2021).

[113] J. S. Sidhu, S. Izumi, J. S. Neergaard-Nielsen, C. Lupo, and U. L. Andersen, "Quantum receiver for phase-shift keying at the single-photon level", PRX Quantum **2**, 010332 (2021).

[114] P. Gupta, R. W. Speirs, K. M. Jones, and P. D. Lett, "Effect of imperfect homodyne visibility on multi-spatial-mode two-mode squeezing measurements", Opt. Express **28**, 652–664 (2020).

[115] S. Banerjee and R. Srikanth, "Phase diffusion in quantum dissipative systems", Phys. Rev. A **76**, 062109 (2007).

[116] H. Ishii, K. Kasaya, and H. Oohashi, "Wavelength-tunable lasers for next-generation optical networks", NTT Technical Review **9**, 1 (2011).

[117] Z. Amiri, B. A. Bash, and J. Nötzel, "Performance of quantum preprocessing under phase noise", in IEEE Globecom Workshops (2022), pp. 298–303.

[118] G. Bertaina, C. Clivati, S. Donadello, C. Liorni, A. Meda, S. Virzì, M. Gramegna, M. Genovese, F. Levi, D. Calonico, M. Dispenza, and I. P. Degiovanni, "Phase noise in real-world twin-field quantum key distribution", arXiv: 2310.08621 [quant-ph] (2024).

[119] M. G. Genoni, S. Olivares, and M. G. A. Paris, "Optical phase estimation in the presence of phase diffusion", Phys. Rev. Lett. **106**, 153603 (2011).

[120] S. Cialdi, E. Suerra, S. Olivares, S. Capra, and M. G. A. Paris, "Squeezing phase diffusion", Phys. Rev. Lett. **124**, 163601 (2020).

[121] S. Olivares, S. Cialdi, F. Castelli, and M. G. A. Paris, "Homodyne detection as a near-optimum receiver for phase-shift-keyed binary communication in the presence of phase diffusion", Phys. Rev. A **87**, 050303 (2013).

[122] H.-M. Chin, J. N., D. Zibar, U. L. Andersen, and T. Gehring, "Machine learning aided carrier recovery in continuous-variable quantum key distribution", npj Quantum Inf. **7**, 20 (2021).

[123] H. P. Yuen, "Communication theory of quantum systems", Res. Lab. Electron., M.I.T. Cambridge, Mass., Tech. Rep. **482**, 116–129 (1970), (Ph.D. dissertation submitted to the Dep. Elec. Eng., M.I.T., June 1970).

[124] H. Yuen, R. Kennedy, and M. Lax, "On optimal quantum receivers for digital signal detection", Proc. IEEE **58**, 1770–1773 (1970).

[125] H. P. Yuen, R. Kennedy, and M. Lax, "Optimum testing of multiple hypotheses in quantum detection theory", IEEE Trans. Inf. Theory **21**, 125–134 (1975).

[126] M. Ban, K. Kurokawa, R. Momose, and O. Hirota, "Optimum measurements for discrimination among symmetric quantum states and parameter estimation", Int. J. Theor. Phys. **36**, 1269–1288 (1997).

[127] P. Hausladen and W. K. Wootters, "A 'pretty good' measurement for distinguishing quantum states", J. Mod. Opt. **41**, 2385–2390 (1994).

[128] P. Hausladen, R. Jozsa, B. Schumacher, M. Westmoreland, and W. K. Wootters, "Classical information capacity of a quantum channel", Phys. Rev. A **54**, 1869–1876 (1996).

[129] M. Sasaki, K. Kato, M. Izutsu, and O. Hirota, "Quantum channels showing superadditivity in classical capacity", Phys. Rev. A **58**, 146–158 (1998).

[130] M. Sasaki, T. Sasaki-Usuda, M. Izutsu, and O. Hirota, "Realization of a collective decoding of code-word states", Phys. Rev. A **58**, 159–164 (1998).

[131] K. Kato, M. Osaki, M. Sasaki, and O. Hirota, "Quantum detection and mutual information for qam and psk signals", IEEE Trans. Commun. **47**, 248–254 (1999).

[132] Y. C. Eldar and G. D. Forney, "On quantum detection and the square-root measurement", IEEE Trans. Inf. Theory **47**, 858–872 (2001).

[133] Y. Eldar and G. Forney, "Optimal tight frames and quantum measurement", IEEE Trans. Inf. Theory **48**, 599–610 (2002).

[134] Y. Eldar, A. Megretski, and G. Verghese, "Optimal detection of symmetric mixed quantum states", IEEE Trans. Inf. Theory **50**, 1198–1207 (2004).

[135] L. Vandenberghe and S. Boyd, "Semidefinite programming", SIAM Rev. **38**, 49–95 (1996).

[136] I. Csiszár and J. Körner, *Information Theory: Coding Theorems for Discrete Memoryless Systems* (Cambridge University Press, 2011).

[137] D. G. Luenberger, *Optimization by vector space methods* (John Wiley & Sons, 1997).

[138] C. W. Helstrom, "Detection theory and quantum mechanics", Inform. Contr. **10**, 254–291 (1967).

[139] J. Liu, "Reliability of quantum-mechanical communication systems", IEEE Trans. Inf. Theory **16**, 319–329 (1970).

[140] Y. Eldar, A. Megretski, and G. Verghese, "Designing optimal quantum detectors via semidefinite programming", IEEE Trans. Inf. Theory **49**, 1007–1012 (2003).

[141] G. Cariolaro, R. Corvaja, and G. Pierobon, "Compression of pure and mixed states in quantum detection", in 2011 IEEE Global Telecommunications Conference - GLOBECOM 2011 (2011), pp. 1–5.

[142] R. S. Kennedy, "On the optimum receiver for the M-ary linearly independent pure state problem", MIT Res. Lab. Electron. Quart. Prog. Rep. **110** (1973).

[143] G. Forney, "Geometrically uniform codes", IEEE Trans. Inf. Theory **37**, 1241–1260 (1991).

[144] A. Assalini, G. Cariolaro, and G. Pierobon, "Efficient optimal minimum error discrimination of symmetric quantum states", Phys. Rev. A **81**, 012315 (2010).

[145] P. J. Davis, *Circulant Matrices* (Wiley, New York, 1970).

[146] A. S. Holevo, "On asymptotically optimal hypothesis testing in quantum statistics", Theory Probab. Its Appl. **23**, 411–415 (1979).

[147] G. Cariolaro and G. Pierobon, "Performance of quantum data transmission systems in the presence of thermal noise", IEEE Trans. Commun. **58**, 623–630 (2010).

[148] G. Cariolaro and G. Pierobon, "Theory of quantum pulse position modulation and related numerical problems", IEEE Trans. Commun. **58**, 1213–1222 (2010).

[149] S. Izumi, J. S. Neergaard-Nielsen, S. Miki, H. Terai, and U. L. Andersen, "Experimental demonstration of a quantum receiver beating the standard quantum limit at telecom wavelength", Phys. Rev. Appl. **13**, 054015 (2020).

[150] R. S. Bondurant, "Near-quantum optimum receivers for the phase-quadrature coherent-state channel", Opt. Lett. **18**, 1896–1898 (1993).

[151] F. E. Becerra, J. Fan, G. Baumgartner, S. V. Polyakov, J. Goldhar, J. T. Kosloski, and A. Migdall, "M-ary-state phase-shift-keying discrimination below the homodyne limit", Phys. Rev. A **84**, 062324 (2011).

[152] C. R. Müller, M. A. Usuga, C. Wittmann, M. Takeoka, C. Marquardt, U. L. Andersen, and G. Leuchs, "Quadrature phase shift keying coherent state discrimination via a hybrid receiver", New J. Phys. **14**, 083009 (2012).

[153] S. Izumi, M. Takeoka, K. Ema, and M. Sasaki, "Quantum receivers with squeezing and photon-number-resolving detectors for M-ary coherent state discrimination", Phys. Rev. A **87**, 042328 (2013).

[154] F. E. Becerra, J. Fan, G. Baumgartner, J. T. K. J. Goldhar, J. T. Kosloski, and A. Migdall, "Experimental demonstration of a receiver beating the standard quantum limit for multiple nonorthogonal state discrimination", Nat. Photonics **7**, 147–152 (2013).

[155] C. R. Müller and C. Marquardt, "A robust quantum receiver for phase shift keyed signals", New Journal of Physics **17**, 032003 (2015).

[156] R. E. Blahut, *Principles and Practice of Information Theory* (Addison Wesley, 1988).

[157] R. Griffin and A. Carter, "Optical differential quadrature phase-shift key (odqpsk) for high capacity optical transmission", in Optical Fiber Communications Conference (2002), WX6.

[158] G. Kramer, A. Ashikhmin, A. J. van Wijngaarden, and X. Wei, "Spectral efficiency of coded phase-shift keying for fiber-optic communication", J. Light. Technol. **21**, 2438 (2003).

[159] D.-S. Ly-Gagnon, S. Tsukamoto, K. Katoh, and K. Kikuchi, "Coherent detection of optical quadrature phase-shift keying signals with carrier phase estimation", J. Light. Technol. **24**, 12 (2006).

[160] M. C. Gursoy, "On the Low-SNR Capacity of Phase-Shift Keying with Hard-Decision Detection", in 2007 IEEE International Symposium on Information Theory (2007), pp. 166–170.

[161] R. Bhadani and I. B. Djordjevic, "Constellation optimization for phase-shift keying coherent states with displacement receiver to maximize mutual information", IEEE Access **8**, 224409–224419 (2020).

[162] A. Leverrier and P. Grangier, "Unconditional security proof of long-distance continuous-variable quantum key distribution with discrete modulation", Phys. Rev. Lett. **102**, 180504 (2009).

[163] Q. Liao, Y. Guo, D. Huang, P. Huang, and G. Zeng, "Long-distance continuous-variable quantum key distribution using non-gaussian state-discrimination detection", New J. Phys. **20**, 023015 (2018).

[164] S. Ghorai, P. Grangier, E. Diamanti, and A. Leverrier, "Asymptotic security of continuous-variable quantum key distribution with a discrete modulation", Phys. Rev. X **9**, 021059 (2019).

[165] J. Lin, T. Upadhyaya, and N. Lütkenhaus, "Asymptotic security analysis of discrete-modulated continuous-variable quantum key distribution", Phys. Rev. X **9**, 041064 (2019).

[166] J. Lin and N. Lütkenhaus, "Trusted detector noise analysis for discrete modulation schemes of continuous-variable quantum key distribution", Phys. Rev. Appl. **14**, 064030 (2020).

[167] P. Papanastasiou and S. Pirandola, "Continuous-variable quantum cryptography with discrete alphabets: composable security under collective gaussian attacks", Phys. Rev. Res. **3**, 013047 (2021).

[168] C. Lupo and Y. Ouyang, "Quantum key distribution with nonideal heterodyne detection: composable security of discrete-modulation continuous-variable protocols", PRX Quantum **3**, 010341 (2022).

[169] M. Zhao, R. Yuan, C. Feng, S. Han, and J. Cheng, "Security of coherent-state quantum key distribution using displacement receiver", IEEE J. Sel. Areas Commun., 1–1 (2024).

[170] M. V. Jabir, I. A. Burenkov, N. F. R. Annafianto, A. Battou, and S. V. Polyakov, "Experimental demonstration of the near-quantum optimal receiver", OSA Contin. **3**, 3324–3331 (2020).

[171] N. Gisin, G. Ribordy, W. Tittel, and H. Zbinden, "Quantum cryptography", Rev. Mod. Phys. **74**, 145–195 (2002).

[172] V. Scarani, H. Bechmann-Pasquinucci, N. J. Cerf, M. Dušek, N. Lütkenhaus, and M. Peev, "The security of practical quantum key distribution", Rev. Mod. Phys. **81**, 1301–1350 (2009).

[173] E. Diamanti, H.-K. Lo, B. Qi, and Z. Yuan, "Practical challenges in quantum key distribution", npj Quantum Inf. **2**, 16025 (2016).

[174] S. Pirandola, U. L. Andersen, L. Banchi, M. Berta, D. Bunandar, R. Colbeck, D. Englund, T. Gehring, C. Lupo, C. Ottaviani, J. L. Pereira, M. Razavi, J. S. Shaari, M. Tomamichel, V. C. Usenko, G. Vallone, P. Villoresi, and P. Wallden, "Advances in quantum cryptography", Adv. Opt. Photon. **12**, 1012–1236 (2020).

[175] F. Grosshans, G. Van Assche, J. Wenger, R. Brouri, N. J. Cerf, and P. Grangier, "Quantum key distribution using Gaussian-modulated coherent states", Nature **421**, 238–241 (2003).

[176] F. Grosshans, N. J. Cerf, J. Wenger, R. Tualle-Brouri, and P. Grangier, "Virtual entanglement and reconciliation protocols for quantum cryptography with continuous variables", Quantum Inf. Comput. **3**, 535–552 (2003).

[177] F. Grosshans, "Collective attacks and unconditional security in continuous variable quantum keydistribution", Phys. Rev. Lett. **94**, 020504 (2005).

[178] M. Navascués, F. Grosshans, and A. Acín, "Optimality of Gaussian Attacks in Continuous-Variable Quantum Cryptography", Phys. Rev. Lett. **97**, 190502 (2006).

[179] R. García-Patrón and N. J. Cerf, "Unconditional Optimality of Gaussian Attacks against Continuous-Variable Quantum Key Distribution", Phys. Rev. Lett. **97**, 190503 (2006).

[180] A. Leverrier, "Theoretical study of continuous-variable quantum key distribution", Phd Thesis (Télécom ParisTech, 2009).

[181] R. L. Rivest, A. Shamir, and L. Adleman, "A method for obtaining digital signatures and public-key cryptosystems", Commun. ACM **21**, 120–126 (1978).

[182] G. S. Vernam, "Cipher printing telegraph systems for secret wire and radio telegraphic communications", Trans. Am. Inst. Electr. Eng. **XLV**, 295–301 (1926).

[183] P. W. Shor, "Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer", SIAM J. Comput. **26**, 1484–1509 (1997).

[184] M. Agrawal, N. Kayal, and N. Saxena, "Primes is in p", Ann. Math. **160**, 781–793 (2004).

[185] S. Wiesner, "Conjugate coding", SIGACT News **15**, 78–88 (1983), *written around 1970 and belatedly published*.

[186] G. Brassard, "Brief history of quantum cryptography: a personal perspective", in IEEE Information Theory Workshop on Theory and Practice in Information-Theoretic Security 2005 (2005), pp. 19–23.

[187] A. K. Ekert, "Quantum cryptography based on bell's theorem", Phys. Rev. Lett. **67**, 661–663 (1991).

[188] X.-B. Wang, "Beating the photon-number-splitting attack in practical quantum cryptography", Phys. Rev. Lett. **94**, 230503 (2005).

[189] H.-K. Lo, X. Ma, and K. Chen, "Decoy state quantum key distribution", Phys. Rev. Lett. **94**, 230504 (2005).

[190] X.-B. Wang, "Decoy-state protocol for quantum cryptography with four different intensities of coherent light", Phys. Rev. A **72**, 012322 (2005).

[191] J. Lodewyck, T. Debuisschert, R. Tualle-Brouri, and P. Grangier, "Controlling excess noise in fiber-optics continuous-variable quantum key distribution", Phys. Rev. A **72**, 050303 (2005).

[192] J. Lodewyck, M. Bloch, R. García-Patrón, S. Fossier, E. Karpov, E. Diamanti, T. Debuisschert, N. J. Cerf, R. Tualle-Brouri, S. W. McLaughlin, and P. Grangier, "Quantum key distribution over 25 km with an all-fiber continuous-variable system", Phys. Rev. A **76**, 042305 (2007).

[193] S. Fossier, E. Diamanti, T. Debuisschert, A. Villing, R. Tualle-Brouri, and P. Grangier, "Field test of a continuous-variable quantum key distribution prototype", New J. Phys. **11**, 045023 (2009).

[194] T. C. Ralph, "Continuous variable quantum cryptography", Phys. Rev. A **61**, 010303 (1999).

[195] T. C. Ralph, "Security of continuous-variable quantum cryptography", Phys. Rev. A **62**, 062306 (2000).

[196] M. Hillery, "Quantum cryptography with squeezed states", Phys. Rev. A **61**, 022309 (2000).

[197] M. D. Reid, "Quantum cryptography with a predetermined key, using continuous-variable einstein-podolsky-rosen correlations", Phys. Rev. A **62**, 062308 (2000).

[198] N. J. Cerf, M. Lévy, and G. V. Assche, "Quantum distribution of gaussian keys using squeezed states", Phys. Rev. A **63**, 052311 (2001).

[199] D. Gottesman and J. Preskill, "Secure quantum key distribution using squeezed states", Phys. Rev. A **63**, 022309 (2001).

[200] C. Weedbrook, A. M. Lance, W. P. Bowen, T. Symul, T. C. Ralph, and P. K. Lam, "Quantum cryptography without switching", Phys. Rev. Lett. **93**, 170504 (2004).

[201] V. C. Usenko and R. Filip, "Squeezed-state quantum key distribution upon imperfect reconciliation", New J. Phys. **13**, 113007 (2011).

[202] V. C. Usenko and F. Grosshans, "Unidimensional continuous-variable quantum key distribution", Phys. Rev. A **92**, 062337 (2015).

[203] V. C. Usenko, "Unidimensional continuous-variable quantum key distribution using squeezed states", Phys. Rev. A **98**, 032321 (2018).

[204] V. C. Usenko and A. n. Oruganti, "Role of anti-squeezing noise in continuous-variable quantum cryptography", in 2020 43rd International Conference on Telecommunications and Signal Processing (TSP) (2020), pp. 421–425.

[205] I. Derkach, V. C. Usenko, and R. Filip, "Squeezing-enhanced quantum key distribution over atmospheric channels", New J. Phys. **22**, 053006 (2020).

[206] S. Pirandola, "Limits and security of free-space quantum communications", Phys. Rev. Res. **3**, 013279 (2021).

[207] P. Papanastasiou, C. Weedbrook, and S. Pirandola, "Continuous-variable quantum key distribution in uniform fast-fading channels", Phys. Rev. A **97**, 032311 (2018).

[208] X. Tang, Z. Chen, Z. Zhao, R. Kumar, and Y. Dong, "Experimental study on underwater continuous-variable quantum key distribution with discrete modulation", Opt. Express **30**, 32428–32437 (2022).

[209] C. Bennett, G. Brassard, C. Crepeau, and U. Maurer, "Generalized privacy amplification", IEEE Trans. Inf. Theory **41**, 1915–1923 (1995).

[210] M. Bloch, A. Thangaraj, S. McLaughlin, and J.-M. Merolla, "LDPC-based Gaussian key reconciliation", in 2006 IEEE Information Theory Workshop - ITW '06 Punta del Este (2006), pp. 116–120.

[211] M. G. A. Paris, "Quantum estimation for quantum technology", Int. J. Quantum Inf. **07**, 125–137 (2009).

[212] R. Renner, "Symmetry of large physical systems implies independence of subsystems", Nat. Phys. **3**, 645–649 (2007).

[213] R. Renner, "Security of quantum key distribution", Int. J. Quantum Inf. **06**, 1–127 (2008).

[214] R. Renner and J. I. Cirac, "De finetti representation theorem for infinite-dimensional quantum systems and applications to quantum cryptography", Phys. Rev. Lett. **102**, 110504 (2009).

[215] V. Scarani and R. Renner, "Quantum cryptography with finite resources: unconditional security bound for discrete-variable protocols with one-way postprocessing", Phys. Rev. Lett. **100**, 200501 (2008).

[216] L. Sheridan, T. P. Le, and V. Scarani, "Finite-key security against coherent attacks in quantum key distribution", New J. Phys. **12**, 123019 (2010).

[217] M. Tomamichel, C. C. W. Lim, N. Gisin, and R. Renner, "Tight finite-key analysis for quantum cryptography", Nat. Commun. **3**, 634 (2012).

[218] F. Furrer, T. Franz, M. Berta, A. Leverrier, V. B. Scholz, M. Tomamichel, and R. F. Werner, "Continuous variable quantum key distribution: finite-key analysis of composable security against coherent attacks", Phys. Rev. Lett. **109**, 100502 (2012).

[219] A. Leverrier, "Security of continuous-variable quantum key distribution via a gaussian de finetti reduction", Phys. Rev. Lett. **118**, 200501 (2017).

[220] S. Pirandola, "Composable security for continuous variable quantum key distribution: trust levels and practical key rates in wired and wireless networks", Phys. Rev. Res. **3**, 043014 (2021).

[221] C. Lupo, C. Ottaviani, P. Papanastasiou, and S. Pirandola, "Continuous-variable measurement-device-independent quantum key distribution: composable security against coherent attacks", Phys. Rev. A **97**, 052327 (2018).

[222] F. Laudenbach, C. Pacher, C.-H. F. Fung, A. Poppe, M. Peev, B. Schrenk, M. Hentschel, P. Walther, and H. Hübel, "Continuous-variable quantum key distribution with gaussian modulation—the theory of practical implementations", Adv. Quantum Technol. **1**, 1800011 (2018).

[223] A. Denys, P. Brown, and A. Leverrier, "Explicit asymptotic secret key rate of continuous-variable quantum key distribution with an arbitrary modulation", Quantum **5**, 540 (2021).

[224] F. Kanitschar and C. Pacher, "Optimizing continuous-variable quantum key distribution with phase-shift keying modulation and postselection", Phys. Rev. Appl. **18**, 034073 (2022).

[225] F. Roumestan, A. Ghazisaeidi, J. Renaudier, L. T. Vidarte, E. Diamanti, and P. Grangier, "High-rate continuous variable quantum key distribution based on probabilistically shaped 64 and 256-qam", in 2021 European Conference on Optical Communication (ECOC) (2021), pp. 1–4.

[226] F. Roumestan, A. Ghazisaeidi, J. Renaudier, L. T. Vidarte, A. Leverrier, E. Diamanti, and P. Grangier, "Experimental demonstration of discrete modulation formats for continuous variable quantum key distribution", arXiv:2207.11702 [quant-ph] (2022).

[227] I. B. Djordjevic, "Optimized-eight-state cv-qkd protocol outperforming gaussian modulation based protocols", IEEE Photonics J. **11**, 1–10 (2019).

[228] M. Almeida, D. Pereira, N. J. Muga, M. Facão, A. N. Pinto, and N. A. Silva, "Secret key rate of multi-ring m-apsk continuous variable quantum key distribution", Opt. Express **29**, 38669–38682 (2021).

[229] D. Pereira, M. Almeida, M. Facão, A. N. Pinto, and N. A. Silva, "Probabilistic shaped 128-apsk cv-qkd transmission system over optical fibres", Opt. Lett. **47**, 3948–3951 (2022).

[230] A. Leverrier and P. Grangier, "Continuous-variable quantum key distribution protocols with a discrete modulation", arXiv:1002.4083 [quant-ph] (2010).

[231] A. Leverrier and P. Grangier, "Continuous-variable quantum-key-distribution protocols with a non-Gaussian modulation", Phys. Rev. A **83**, 042312 (2011).

[232] A. Becir, F. A. A. El-Orany, and M. R. B. Wahiddin, "Continuous-variable quantum key distribution protocols with eight-state discrete modulation", Int. J. Quantum Inf. **10**, 1250004 (2012).

[233] T. Hirano, T. Ichikawa, T. Matsubara, M. Ono, Y. Oguri, R. Namiki, K. Kasai, R. Matsumoto, and T. Tsurumaru, "Implementation of continuous-variable quantum key distribution with discrete modulation", Quantum Sci. Technol. **2**, 024010 (2017).

[234] Z. Qu and I. B. Djordjevic, "Four-dimensionally multiplexed eight-state continuous-variable quantum key distribution over turbulent channels", IEEE Photonics J. **9**, 1–8 (2017).

[235] Q. Liao, G. Xiao, C.-G. Xu, Y. Xu, and Y. Guo, "Discretely modulated continuous-variable quantum key distribution with an untrusted entanglement source", Phys. Rev. A **102**, 032604 (2020).

[236] G. P. Agrawal, *Fiber-optic communication systems* (Wiley, 2012).

[237] P. Jouguet, S. Kunz-Jacques, A. Leverrier, P. Grangier, and E. Diamanti, "Experimental demonstration of long-distance continuous-variable quantum key distribution", Nat. Photonics **7**, 378–381 (2013).

[238] Z. Pan, K. P. Seshadreesan, W. Clark, M. R. Adcock, I. B. Djordjevic, J. H. Shapiro, and S. Guha, "Secret key distillation over a pure loss quantum wiretap channel under restricted eavesdropping", in 2019 IEEE International Symposium on Information Theory (ISIT) (2019), pp. 3032–3036.

[239] Z. Pan, K. P. Seshadreesan, W. Clark, M. R. Adcock, I. B. Djordjevic, J. H. Shapiro, and S. Guha, "Secret-key distillation across a quantum wiretap channel under restricted eavesdropping", Phys. Rev. Appl. **14**, 024044 (2020).

[240] I. Devetak and A. Winter, "Distillation of secret key and entanglement from quantum states", Proc. R. Soc. A **461**, 207–235 (2005).

[241] C. Weedbrook, S. Pirandola, and T. C. Ralph, "Continuous-variable quantum key distribution using thermal states", Phys. Rev. A **86**, 022318 (2012).

[242] E. T. Jaynes, "Information theory and statistical mechanics", Phys. Rev. **106**, 620–630 (1957).

[243] G. Lindblad, "Expectations and entropy inequalities for finite quantum systems", Commun. Math. Phys. **39**, 111–119 (1974).

[244] P. Jouguet, S. Kunz-Jacques, E. Diamanti, and A. Leverrier, "Analysis of imperfections in practical continuous-variable quantum key distribution", Phys. Rev. A **86**, 032309 (2012).

[245] C. Weedbrook, S. Pirandola, R. García-Patrón, N. J. Cerf, T. C. Ralph, J. H. Shapiro, and S. Lloyd, "Gaussian quantum information", Rev. Mod. Phys. **84**, 621–669 (2012).

[246] I. B. Djordjevic, "On the discretized gaussian modulation (dgm)- based continuous variable-qkd", IEEE Access **7**, 65342–65346 (2019).

[247] A. J. K. Bencheikh Th. Symul and J. A. Levenson, "Quantum key distribution with continuous variables", J. Mod. Opt. **48**, 1903–1920 (2001).

[248] G. Van Assche, J. Cardinal, and N. Cerf, "Reconciliation of a quantum-distributed gaussian key", IEEE Trans. Inf. Theory **50**, 394–400 (2004).

[249] T. Richardson and R. Urbanke, "Multi-edge type ldpc codes", in Workshop honoring Prof. Bob McEliece on his 60th birthday, California Institute of Technology, Pasadena, California (Citeseer, 2002), pp. 24–25.

[250] M. Ghalaii, C. Ottaviani, R. Kumar, S. Pirandola, and M. Razavi, "Discrete-modulation continuous-variable quantum key distribution enhanced by quantum scissors", IEEE J. Sel. Areas Commun. **38**, 506–516 (2020).

[251] F. Kanitschar and C. Pacher, "Optimizing continuous-variable quantum key distribution with phase-shift keying modulation and postselection", Phys. Rev. Appl. **18**, 034073 (2022).

[252] A. Leverrier, F. Grosshans, and P. Grangier, "Finite-size analysis of a continuous-variable quantum key distribution", Phys. Rev. A **81**, 062343 (2010).

[253] R. E. Blahut, *Principles and practice of information theory* (Addison-Wesley Longman Publishing Co., Inc., 1987).

[254] L. Kunz, M. G. A. Paris, and K. Banaszek, "Noisy propagation of coherent states in a lossy kerr medium", J. Opt. Soc. Am. B **35**, 214–222 (2018).

[255] A. Allevi, S. Olivares, and M. Bondani, "Manipulating the non-gaussianity of phase-randomized coherent states", Opt. Express **20**, 24850–24855 (2012).

[256] G. Böcherer, F. Steiner, and P. Schulte, "Bandwidth efficient and rate-matched low-density parity-check coded modulation", IEEE Trans. Commun. **63**, 4651–4665 (2015).

[257] F. Buchali, F. Steiner, G. Böcherer, L. Schmalen, P. Schulte, and W. Idler, "Rate adaptation and reach increase by probabilistically shaped 64-qam: an experimental demonstration", J. Light. Technol. **34**, 1599–1609 (2016).

[258] T. Fehenberger, A. Alvarado, G. Böcherer, and N. Hanik, "On probabilistic shaping of quadrature amplitude modulation for the nonlinear fiber channel", J. Light. Technol. **34**, 5063–5073 (2016).

[259] P. Schulte and G. Böcherer, "Constant composition distribution matching", IEEE Trans. Inf. Theory **62**, 430–434 (2016).

[260] S. Civelli and M. Secondini, "Hierarchical distribution matching for probabilistic amplitude shaping", Entropy **22**, 958 (2020).

[261] Y. C. Gültekin, T. Fehenberger, A. Alvarado, and F. M. J. Willems, "Probabilistic shaping for finite blocklengths: distribution matching and sphere shaping", Entropy **22**, 581 (2020).

[262] F. Kschischang and S. Pasupathy, "Optimal nonuniform signaling for gaussian channels", IEEE Trans. Inf. Theory **39**, 913–929 (1993).

[263] J. G. Proakis and M. Salehi, *Digital communications* (McGraw Hill, 2001).

[264] F. Laudenbach and C. Pacher, "Analysis of the trusted-device scenario in continuous-variable quantum key distribution", Adv. Quantum Technol. **2**, 1900055.

[265] M. Jarzyna, R. García-Patrón, and K. Banaszek, "Ultimate capacity limit of a multi-span link with phase-insensitive amplification", in 45th European Conference on Optical Communication (ECOC 2019) (2019), pp. 1–4.

[266] K. Łukanowski, K. Banaszek, and M. Jarzyna, "Quantum limits on the capacity of multispan links with phase-sensitive amplification", J. Light. Technol. **41**, 5017–5025 (2023).

[267] V. C. Usenko, B. Heim, C. Peuntinger, C. Wittmann, C. Marquardt, G. Leuchs, and R. Filip, "Entanglement of gaussian states and the applicability to quantum key distribution over fading channels", New J. Phys. **14**, 093048 (2012).

[268] L. Ruppert, C. Peuntinger, B. Heim, K. Günthner, V. C. Usenko, D. Elser, G. Leuchs, R. Filip, and C. Marquardt, "Fading channel estimation for free-space continuous-variable secure quantum communication", New J. Phys. **21**, 123036 (2019).

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

[270] R. Renner, N. Gisin, and B. Kraus, "Information-theoretic security proof for quantum-key-distribution protocols", Phys. Rev. A **72**, 012332 (2005).

[271] R. García-Patrón, "Quantum Information with Optical Continuous Variables: from Bell Tests to Key Distribution", Phd Thesis (Université Libre de Bruxelles, 2008).

[272] A. D. Wyner, "The wire-tap channel", Bell Syst. Tech. J. **54**, 1355–1387 (1975).

[273] D. Huang, P. Huang, D. Lin, and G. Zeng, "Long-distance continuous-variable quantum key distribution by controlling excess noise", Sci. Rep. **6**, 19201 (2016).

[274] Y. Zhang, Z. Chen, S. Pirandola, X. Wang, C. Zhou, B. Chu, Y. Zhao, B. Xu, S. Yu, and H. Guo, "Long-distance continuous-variable quantum key distribution over 202.81 km of fiber", Phys. Rev. Lett. **125**, 010502 (2020).

[275] Y. Pi, H. Wang, Y. Pan, Y. Shao, Y. Li, J. Yang, Y. Zhang, W. Huang, and B. Xu, "Sub-Mbps key-rate continuous-variable quantum key distribution with local local oscillator over 100-km fiber", Opt. Lett. **48**, 1766–1769 (2023).

[276] Y. Bian, Y.-C. Zhang, C. Zhou, S. Yu, Z. Li, and H. Guo, "High-rate point-to-multipoint quantum key distribution using coherent states", arXiv:2302.02391 [quant-ph] (2023).

[277] A. A. E. Hajomer, I. Derkach, N. Jain, H.-M. Chin, U. L. Andersen, and T. Gehring, "Long-distance continuous-variable quantum key distribution over 100 km fiber with local local oscillator", arXiv:2305.08156 [quant-ph] (2023).

[278] X.-B. Wang, "Beating the photon-number-splitting attack in practical quantum cryptography", Phys. Rev. Lett. **94**, 230503 (2005).

[279] Y. Zhao, B. Qi, X. Ma, H.-K. Lo, and L. Qian, "Experimental quantum key distribution with decoy states", Phys. Rev. Lett. **96**, 070502 (2006).

[280] C.-Z. Peng, J. Zhang, D. Yang, W.-B. Gao, H.-X. Ma, H. Yin, H.-P. Zeng, T. Yang, X.-B. Wang, and J.-W. Pan, "Experimental long-distance decoy-state quantum key distribution based on polarization encoding", Phys. Rev. Lett. **98**, 010505 (2007).

[281] D. Rosenberg, J. W. Harrington, P. R. Rice, P. A. Hiskett, C. G. Peterson, R. J. Hughes, A. E. Lita, S. W. Nam, and J. E. Nordholt, "Long-distance decoy-state quantum key distribution in optical fiber", Phys. Rev. Lett. **98**, 010503 (2007).

[282] T. Schmitt-Manderbach, H. Weier, M. Fürst, R. Ursin, F. Tiefenbacher, T. Scheidl, J. Perdigues, Z. Sodnik, C. Kurtsiefer, J. G. Rarity, A. Zeilinger, and H. Weinfurter, "Experimental Demonstration of Free-Space Decoy-State Quantum Key Distribution over 144 km", Phys. Rev. Lett. **98**, 010504 (2007).

[283] A. Boaron, G. Boso, D. Rusca, C. Vulliez, C. Autebert, M. Caloz, M. Perrenoud, G. Gras, F. Bussières, M.-J. Li, D. Nolan, A. Martin, and H. Zbinden, "Secure Quantum Key Distribution over 421 km of Optical Fiber", Phys. Rev. Lett. **121**, 190502 (2018).

[284] H.-A. Bachor and T. C. Ralph, *A Guide to Experiments in Quantum Optics* (Wiley, 2019).

[285] T. C. Ralph and A. P. Lund, "Nondeterministic noiseless linear amplification of quantum systems", in AIP Conference Proceedings, Vol. 1110, 1 (Apr. 2009), pp. 155–160.

[286] G. Y. Xiang, T. C. Ralph, A. P. Lund, N. Walk, and G. J. Pryde, "Heralded noiseless linear amplification and distillation of entanglement", Nat. Photonics **4**, 316–319 (2010).

[287] R. Blandino, A. Leverrier, M. Barbieri, J. Etesse, P. Grangier, and R. Tualle-Brouri, "Improving the maximum transmission distance of continuous-variable quantum key distribution using a noiseless amplifier", Phys. Rev. A **86**, 012327 (2012).

[288] J. J. Guanzon, M. S. Winnel, A. P. Lund, and T. C. Ralph, "Noiseless linear amplification and loss-tolerant quantum relay using coherent-state superpositions", Phys. Rev. A **108**, 032411 (2023).

[289] J. Fiurá šek, "Engineering quantum operations on traveling light beams by multiple photon addition and subtraction", Phys. Rev. A **80**, 053822 (2009).

[290] G.-Y. Xiang, T. C. Ralph, A. P. Lund, N. Walk, and G. J. Pryde, "Heralded noiseless linear amplification and distillation of entanglement", Nat. Photonics **4**, 316–319 (2010).

[291] N. A. McMahon, A. P. Lund, and T. C. Ralph, "Optimal architecture for a nondeterministic noiseless linear amplifier", Phys. Rev. A **89**, 023846 (2014).

[292] S. Zhang and X. Zhang, "Photon catalysis acting as noiseless linear amplification and its application in coherence enhancement", Phys. Rev. A **97**, 043830 (2018).

[293] M. S. Winnel, N. Hosseinidehaj, and T. C. Ralph, "Generalized quantum scissors for noiseless linear amplification", Phys. Rev. A **102**, 063715 (2020).

[294] J. Fiurášek, "Teleportation-based noiseless quantum amplification of coherent states of light", Opt. Express **30**, 1466–1489 (2022).

[295] J. J. Guanzon, M. S. Winnel, A. P. Lund, and T. C. Ralph, "Ideal quantum teleamplification up to a selected energy cutoff using linear optics", Phys. Rev. Lett. **128**, 160501 (2022).

[296] J. Fiurášek, "Optimal linear-optical noiseless quantum amplifiers driven by auxiliary multiphoton fock states", Phys. Rev. A **105**, 062425 (2022).

[297] Ş. K. Özdemir, A. Miranowicz, M. Koashi, and N. Imoto, "Quantum-scissors device for optical state truncation: a proposal for practical realization", Phys. Rev. A **64**, 063818 (2001).

[298] F. Ferreyrol, M. Barbieri, R. Blandino, S. Fossier, R. Tualle-Brouri, and P. Grangier, "Implementation of a nondeterministic optical noiseless amplifier", Phys. Rev. Lett. **104**, 123603 (2010).

[299] F. Ferreyrol, R. Blandino, M. Barbieri, R. Tualle-Brouri, and P. Grangier, "Experimental realization of a nondeterministic optical noiseless amplifier", Phys. Rev. A **83**, 063801 (2011).

[300] A. I. Lvovsky and J. Mlynek, "Quantum-optical catalysis: generating nonclassical states of light by means of linear optics", Phys. Rev. Lett. **88**, 250401 (2002).

[301] T. J. Bartley, G. Donati, J. B. Spring, X.-M. Jin, M. Barbieri, A. Datta, B. J. Smith, and I. A. Walmsley, "Multiphoton state engineering by heralded interference between single photons and coherent states", Phys. Rev. A **86**, 043820 (2012).

[302] M. N. Notarnicola, M. G. Genoni, S. Cialdi, M. G. A. Paris, and S. Olivares, "Phase noise mitigation by a realistic optical parametric oscillator", J. Opt. Soc. Am. B **39**, 1059–1067 (2022).

[303] A. Yariv, "Signal-to-noise considerations in fiber links with periodic or distributed optical amplification", Opt. Lett. **15**, 1064–1066 (1990).

[304] C. Antonelli, A. Mecozzi, M. Shtaif, and P. J. Winzer, "Quantum limits on the energy consumption of optical transmission systems", J. Light. Technol. **32**, 1853–1860 (2014).

[305] F. Furrer and W. J. Munro, "Repeaters for continuous-variable quantum communication", Phys. Rev. A **98**, 032335 (2018).

[306] S. Pirandola, "End-to-end capacities of a quantum communication network", Commun. Phys. **2**, 1 (2019).

[307] J. Dias, M. S. Winnel, N. Hosseinidehaj, and T. C. Ralph, "Quantum repeater for continuous-variable entanglement distribution", Phys. Rev. A **102**, 052425 (2020).

[308] E. Bersin, M. Sutula, Y. Q. Huan, A. Suleymanzade, D. R. Assumpcao, Y.-C. Wei, P.-J. Stas, C. M. Knaut, E. N. Knall, C. Langrock, N. Sinclair, R. Murphy, R. Riedinger, M. Yeh, C. Xin, S. Bandyopadhyay, D. D. Sukachev, B. Machielse, D. S. Levonian, M. K. Bhaskar, S. Hamilton, H. Park, M. Lončar, M. M. Fejer, P. B. Dixon, D. R. Englund, and M. D. Lukin, "Telecom networking with a diamond quantum memory", PRX Quantum **5**, 010303 (2024).

[309] A. Wallucks, I. Marinković, B. Hensen, R. Stockill, and S. Gröblacher, "A quantum memory at telecom wavelengths", Nat. Phys. **16**, 772–777 (2020).

[310] S. Pirandola, R. Laurenza, C. Ottaviani, and L. Banchi, "Fundamental limits of repeaterless quantum communications", Nat. Commun. **8**, 1–15 (2017).

[311] J. Fiurášek and N. J. Cerf, "Gaussian postselection and virtual noiseless amplification in continuous-variable quantum key distribution", Phys. Rev. A **86**, 060302 (2012).

[312] N. Walk, T. C. Ralph, T. Symul, and P. K. Lam, "Security of continuous-variable quantum cryptography with gaussian postselection", Phys. Rev. A **87**, 020303 (2013).

[313] H. M. Chrzanowski, N. Walk, S. M. Assad, J. Janousek, S. Hosseini, T. C. Ralph, T. Symul, and P. K. Lam, "Measurement-based noiseless linear amplification for quantum communication", Nat. Photonics **8**, 333–338 (2014).

[314] J. Bernu, S. Armstrong, T. Symul, T. C. Ralph, and P. K. Lam, "Theoretical analysis of an ideal noiseless linear amplifier for einstein–podolsky–rosen entanglement distillation", J. Phys. B: At. Mol. Opt. Phys. **47**, 215503 (2014).

[315] J. Zhao, J. Y. Haw, T. Symul, P. K. Lam, and S. M. Assad, "Characterization of a measurement-based noiseless linear amplifier and its applications", Phys. Rev. A **96**, 012319 (2017).

[316] L. Hu, M. Al-amri, Z. Liao, and M. S. Zubairy, "Continuous-variable quantum key distribution with non-Gaussian operations", Phys. Rev. A **102**, 012608 (2020).

[317] L. Lami, L. Mišta, and G. Adesso, "Fundamental limitations to key distillation from gaussian states with gaussian operations", Phys. Rev. Res. **5**, 033153 (2023).

[318] W.-B. Liu, C.-L. Li, Y.-M. Xie, C.-X. Weng, J. Gu, X.-Y. Cao, Y.-S. Lu, B.-H. Li, H.-L. Yin, and Z.-B. Chen, "Homodyne detection quadrature phase shift keying continuous-variable quantum key distribution with high excess noise tolerance", PRX Quantum **2**, 040334 (2021).

[319] D. Sych and G. Leuchs, "Coherent state quantum key distribution with multi letter phase-shift keying", New J. Phys. **12**, 053019 (2010).

[320] T. Upadhyaya, T. van Himbeeck, J. Lin, and N. Lütkenhaus, "Dimension reduction in quantum key distribution for continuous- and discrete-variable protocols", PRX Quantum **2**, 020325 (2021).

[321] M. Cattaneo, M. G. A. Paris, and S. Olivares, "Hybrid quantum key distribution using coherent states and photon-number-resolving detectors", Phys. Rev. A **98**, 012333 (2018).

[322] K. Banaszek, M. Jachura, P. Kolenderski, and M. Lasota, "Optimization of intensity-modulation/direct-detection optical key distribution under passive eavesdropping", Opt. Express **29**, 43091–43103 (2021).

[323] I. Derkach and V. C. Usenko, "Applicability of squeezed- and coherent-state continuous-variable quantum key distribution over satellite links", Entropy **23**, 55 (2021).

[324] N. K. Kundu, M. R. McKay, A. Conti, R. K. Mallik, and M. Z. Win, "Mimo terahertz quantum key distribution under restricted eavesdropping", IEEE Trans. Quantum Eng. **4**, 1–15 (2023).

[325] E. T. H. Medlock, "Continuous variable quantum key distribution in presence of emulated atmospheric turbulence and with passive eavesdropping", Phd Thesis (University of York, 2021).

[326] M. Ghalaii, S. Bahrani, C. Liorni, F. Grasselli, H. Kampermann, L. Wooltorton, R. Kumar, S. Pirandola, T. P. Spiller, A. Ling, B. Huttner, and M. Razavi, "Satellite-based quantum key distribution in the presence of bypass channels", PRX Quantum **4**, 040320 (2023).

[327] M. Jarzyna, M. Jachura, and K. Banaszek, "Quantum pulse gate attack on im/dd optical key distribution exploiting symbol shape distortion", IEEE Commun. Lett. **27**, 1699–1703 (2023).

[328] W. H. Press, S. A. Teukolsky, W. T. Vetterling, and B. P. Flannery, *Numerical recipes 3rd edition: The art of scientific computing* (Cambridge University Press, 2007).

[329] R. Cheng, Y. Zhou, S. Wang, M. Shen, T. Taher, and H. X. Tang, "A 100-pixel photon-number-resolving detector unveiling photon statistics", Nat. Photonics **17**, 112–119 (2023).

[330] M. Endo, T. Sonoyama, M. Matsuyama, F. Okamoto, S. Miki, M. Yabuno, F. China, H. Terai, and A. Furusawa, "Quantum detector tomography of a superconducting nanostrip photon-number-resolving detector", Opt. Express **29**, 11728–11738 (2021).

[331] J. W. N. Los, M. Sidorova, B. Lopez-Rodriguez, P. Qualm, J. Chang, S. Steinhauer, V. Zwiller, and I. E. Zadeh, "High-performance photon number resolving detectors for 850–950 nm wavelength range", APL Photonics **9**, 066101 (2024).

[332] C. Thomas, M. Weidner, and S. Durrani, "Digital Amplitude-Phase Keying with M-Ary Alphabets", IEEE Trans. Commun. **22**, 168–180 (1974).

[333] R. De Gaudenzi, A. Guillén i Fábregas, and A. Martinez, "Turbo-coded APSK modulations design for satellite broadband communications", Int. J. Satell. Commun. Netw. **24**, 261–281 (2006).

[334] H. Méric, "Approaching the Gaussian Channel Capacity With APSK Constellations", IEEE Commun. Lett. **19**, 1125–1128 (2015).

[335] A. Öztekin and E. Erçelebi, "Quadrature-carrier amplitude phase shift keying", IET Commun. **13**, 560–568 (2019).

[336] K. Inoue and T. Honjo, "Quantum conference key agreement based on differential-phase-shift quantum key distribution", Quantum Inf. Process. **23**, 253 (2024).

[337] T. Wang and T. S. Usuda, "Security enhancement of amplitude-shift keying-type asymmetric quantum communication systems", Quantum Inf. Process. **23**, 197 (2024).

[338] J. Schafer, E. Karpov, O. V. Pilyavets, and N. J. Cerf, "Classical capacity of phase-sensitive Gaussian quantum channels", arXiv:1609.04119 [quant-ph] (2016).

[339] S. Olivares and M. G. A. Paris, "Squeezed Fock state by inconclusive photon subtraction", J. Opt. B Quantum Semiclassical Opt. **7**, S616 (2005).