Continuous-variable quantum cryptographic protocols

Shouvik Ghorai

Continuous-Variable Quantum Cryptographic Protocols

Shouvik Ghorai

Laboratoire d'Informatique de Paris 6
SORBONNE UNIVERSITÉ

A dissertation submitted to Sorbonne Université
in accordance with the requirements of the degree of
DOCTOR OF PHILOSOPHY,
under the supervision of
Eleni Diamanti and Anthony Leverrier.

M. Antonio ACÍN, Professeur, ICFO, The Institute of Photonic Sciences	Rapporteur
M. Raúl GARCÍA-PATRÓN, Maître de Conférences, University of Edinburgh	Rapporteur
Mme. Agnes FERENCZI, Chercheur, German Aerospace Cente	Examinatrice
M. Antoine JOUX, Professeur, IMJ-PRG, Sorbonne Université	Examinateur
Mme. Eleni DIAMANTI, Directeur de Recherche, CNRS	Directrice de thèse
M. Anthony LEVERRIER, Chercheur INRIA	Co-directeur de thèse

February 2021

Acknowledgement

Writing a thesis is not an individual experience, rather it involves several people without whom this thesis would not have been possible. I am truly lucky and grateful to have met these wonderful people. They have been a cherished part of my Ph.D. journey.

First and foremost, my heartfelt thanks to my supervisors, Eleni and Anthony, for their constant support and availability, stimulating discussions, and immeasurable patience. It has been a true privilege to work with them. I am truly appreciative for the time we shared, for every opportunity provided for personal and professional growth. I will take the best of them with me and lead by their example everywhere I go.

I have been blessed with amazing friends and colleagues at LIP6, Matthieu, Federico, Victor, Luis, Simon, Matteo, Verena, Leo, Luka, Nathan, Dominik, Francesco, Rawad, Niraj, Anu, Adrien, Luka, Robert, Pierre, Raja, Shane, Andrea, Clément, Rhea, Gözde, Natansh, and Shraddha, who have provided me the best work environment one can think of and I thank them for being a source of motivation and innovation in my journey. Many thanks to the other great leaders of the QI team, who contribute to this amazing atmosphere: Damian, Elham, and Fred. I would also like to thank my colleagues at QCALL. Although we met only a few times over 3 years, discussions have been stimulating and interactions warm.

To my IISER-K friends in Paris, Chitram, Debmalya, Trinish, Abhyuday, Debanuj, Subha, and Soumitrada, thank you for being an unparalleled source of comfort and entertainment throughout this journey. Thanks to my college friends, especially Tanmoy and Subhajit for the endless friendship and support.

I must also thank, Mylene, Kaushik, Anambar, Mouli, Nilesh, and Wamsi, for making my time in Paris a memory to cherish forever. Special thanks to Gözde and Verena for innumerable restaurant invitations. And to Riya for listening to my monologues over the years.

Finally, I would like to thank my whole family for their endless sacrifices and support. This thesis is entirely dedicated to their love and care.

Abstract

This thesis is concerned with the study and analysis of two quantum cryptographic protocols: quantum key distribution (QKD) and unforgeable quantum money in the continuous-variable (CV) framework. The main advantage of continuous-variable protocols is that their implementation only requires standard telecommunication components.

QKD allows two distant parties, Alice and Bob, to establish a secure key, even in the presence of an eavesdropper, Eve. The remarkable property of QKD is that its security can be established in the information-theoretic setting, without appealing to any computational assumptions. Proving the security of CV-QKD protocols is challenging since the protocols are described in an infinite-dimensional Fock space.

One of the pressing questions in CV-QKD was establishing security for two-way QKD protocols against general attacks. We exploit the invariance of Unitary group $U(n)$ of the protocol to establish the composable security against general attacks. We also show that active symmetrization is not required to prove security. We answer another open question in the field of CV-QKD with a discrete modulation by establishing the asymptotic security of such protocols against collective attacks. We provide a general technique to derive a lower bound on the secret key rate by formulating the problem as a semidefinite program.

Quantum money exploits the no-cloning property of quantum mechanics to generate unforgeable tokens, banknotes, and credit cards. We propose a continuous-variable private-key quantum money scheme with classical verification. The motivation behind this protocol is to facilitate the process of practical implementation. Previous classical verification money schemes use single-photon detectors for verification, while our protocols require coherent detection.

CONTENTS

INTRODUCTION

The advent of Quantum Mechanics

By the end of the 19th century, classical physics, characterized by Newtonian mechanics, Boltzmann's theory on statistical mechanics, and Maxwell's theory of electromagnetism, could efficiently interpret most of the relevant physical phenomena. However, two physical phenomena were still left unexplained by classical physics: the frequency dependence of the energy emitted by a black body and the notion of Earth moving through the ether.

The beginning of the 20th century heralded an unprecedented era of turnover and re-evaluation of the classical theory that governed Physics since pre-Newtonian times. Two theories revolutionized the concept of physics: Einstein's Theory of Relativity, which shattered the notion of classical Newtonian concepts of space and time as two independent entities in the description of the physical world, and Planck's hypothesis that the radiating energy must be in discretized units, which he termed "quanta."

Planck's quantization theory was widely accepted when Einstein explained the photoelectric effect using the same theory of discrete packets of energy (quanta). Over the next three decades, thanks to the works of Bohr, de Broglie, Schrodinger, Heisenberg, Pauli, Dirac, and others, a major development took place into formulating Quantum Mechanics from the initial quantum theory.

Information is Physical

The '40s, more specifically the Second World War triggered an increase in the research and development of new theories. Although most of the developments were in the field of engineering (nuclear weapon, rocket and jet propulsion), two new theories in applied mathematics were born at that time: Information Theory and Computer Science. Claude Shannon's seminal work, "A Mathematical Theory of Communication" published in 1948 established the groundwork for the world of information we live in today. During the early years of development, information was viewed as an abstract concept. The view quickly shifted to a more physical description of information, where one can see the storage of media (e.g. hard drives) as a collection of information units.

The physical support of information was assumed to be classical, although Quantum Mechanics was well established by that time. In the early '70s, Stephen Wiesner brought a new perspective by linking Information Theory and Quantum Mechanics. He proposed

the notion of making money unforgeable using the properties of Quantum Mechanics. At the time, the idea was not widely accepted. A few years later, the idea was extended by Charles Bennett and Gilles Brassard to propose quantum protocols for two cryptographic primitives: key distribution and bit commitment. This paper became the trigger that pioneered the novel field of *Quantum Cryptography*.

This prompted physicists to study the effects of encoding information on quantum states, giving birth to *Quantum Information Theory*. This field of research deals with many topics: fundamental limits of information storage, rate of communication through channels, limits on computational capabilities to name a few. Another major contribution of this field is the insight it provides on the foundations of Quantum Mechanics, which can be experimentally tested thanks to new technological developments. The field is rapidly growing and also influencing other fields of Physics.

Security in Quantum Cryptography

Quantum Cryptography is one of the first practical applications of Quantum Information Theory. The reason that the field gathers immense attention is that quantum cryptographic protocols hold the promise of much stronger security than their classical counterparts, for instance, secure keys generated from quantum key distribution protocol can encrypt data for a longer period compared to classical key distribution protocols. Cryptographic protocols meant for secure encryption are one of the primary applications of Quantum Cryptography. Depending on the level of security, one can determine whether an adversary is able to break a *cryptosystem*[1] purposed for encryption. There are two levels of security for such cryptosystems:

- Information-theoretic security: If the adversary cannot break the cryptosystem even if (s)he has access to unlimited computational power, the system is said to be information-theoretic secure. An example is the one-time pad symmetric scheme, which requires a secret key of the same length as the message which can only be used once. Such a system is not vulnerable to future developments in computational power.

- Computational security: The system is secure against a computationally bounded adversary. The adversary can only break the system if they have unlimited computational power. The security relies on the hardness of a computational problem that cannot be solved in polynomial time with limited resources. Some of these protocols will no longer be secure with the advent of new quantum technologies, e.g., the RSA cryptosystem can be broken using Shor's quantum algorithm.

Continuous Variables

Similar to classical information, quantum information can also be divided into two families: discrete variables and continuous variables. From an implementation point of

[1] a suite of cryptographic protocols for implementing a particular security service

view, continuous-variable quantum information has many advantages over its discrete counterpart. Encoding information on the quadratures of the electromagnetic field, processing with linear optical tools, and coherent detection are enough to implement many continuous-variable quantum cryptographic protocols. Coherent detection is the current industry standard in classical optical telecommunications and offers a higher optical data rate than single-photon counters.

The large majority of quantum states that are accessible in an experimental quantum optics laboratory are Gaussian states. Gaussian operators that preserve the Gaussian property of the states comprise a major part of optical tools are easily implementable with current technology. The study of Gaussian states and Gaussian operators is crucial for the field of continuous-variable quantum information.

Outline of the thesis

The thesis focuses on the security analysis of two continuous-variable quantum cryptographic protocols, quantum key distribution (QKD) and unforgeable quantum money. Although the thesis is theoretical, the protocols focus on the ease of implementation, thus, use coherent states and linear optical tools, which are easy to realize in an experimental setting.

Chapter 1 presents the main tools of Quantum Mechanics that will be useful for the study of the cryptographic protocols in later chapters. We start with a basic description of the postulates of Quantum Mechanics followed by its inherent properties that make it such a remarkable theory.

Chapter 2 starts with the main tools of Information Theory, in both classical and quantum regimes, with a focus on the properties of relevant quantities. We then provide the necessary background on Continuous-Variable systems along with the phase space representation. We detail Gaussian states and Gaussian operators, which are crucial for the implementation of both protocols considered here. Finally, we introduce the basic concepts of semidefinite programming, which allows us to derive numerical bounds needed for the security analysis. The tools presented in this chapter have been used rather extensively throughout the thesis.

Chapter 3 introduces the two cryptographic protocols: QKD and unforgeable quantum money. First, we describe the steps of a QKD protocol, followed by its security and how is it achieved. Then we provide a detailed description of a continuous-variable QKD protocol, its security, the method to prove the security for different attacks, and the techniques or symmetries we exploit to derive the security proof. The second section introduces the unforgeable quantum money. We start with the characterization of money schemes based on the choice of verification and key, followed by the correctness and security parameters. Finally, we give a detailed description of the private-key money schemes with both quantum and classical verification.

Chapters 4, 5, and 6 present the original results of the thesis. Chapter 4 presents a general framework encompassing a number of continuous-variable quantum key distribution protocols, including standard one-way protocols, measurement-device-independent protocols as well as some two-way protocols, or any other continuous-variable protocol

involving only a Gaussian modulation of coherent states and heterodyne detection. The main interest of this framework is that the corresponding protocols are all covariant with respect to the action of the unitary group $U(n)$, implying that their security can be established thanks to the Gaussian de Finetti reduction theorem. In particular, we give a composable security proof of two-way continuous-variable quantum key distribution against general attacks. We also prove that no active symmetrization procedure is required for these protocols, which would otherwise make them prohibitively costly to implement.

Chapter 5 establishes a lower bound on the asymptotic secret key rate of continuous-variable quantum key distribution with a discrete modulation of coherent states. The bound is valid against collective attacks and is obtained by formulating the problem as a semidefinite program. We illustrate our general approach with the quadrature phase-shift keying (QPSK) modulation scheme and show that distances over 100 km are achievable for realistic values of noise. We also discuss the application to more complex quadrature amplitude modulation (QAM) schemes. This result opens the way to establishing the full security of continuous-variable protocols with a discrete modulation, and thereby to the large-scale deployment of these protocols for quantum key distribution.

Chapter 6 introduces a continuous-variable private-key quantum money scheme with classical verification. We start our analysis with a 4-state ensemble money scheme, which is insecure but allows us to present the main ideas of the scheme. Following that, we consider a money scheme with a slightly larger ensemble of 8 states and analyze the security of the scheme in a perfect memory setting as well as in a pure-loss memory setting. The scheme tolerates losses up to 2%. Finally, we generalize the money scheme for a $4N$-state ensemble and find the loss tolerance for the money scheme with various ensemble sizes. We find money schemes with a loss tolerance of 13%. We note that increasing ensemble sizes increases the loss tolerance of the money scheme.

CHAPTER 1

QUANTUM MECHANICS

This chapter aims to present the main tools of Quantum Mechanics that will be useful for the study of the cryptographic protocols. Note that most of this chapter's content can be found in Nielsen and Chuang's textbook [1].

1.1. The postulates of Quantum Mechanics

This section provides a basic description of the postulates of quantum mechanics, which is enough to appreciate the quantum information theory and its application to quantum cryptographic protocols. The postulates of quantum mechanics define a mathematical framework for the development of physical theories. However, by itself, quantum mechanics is unable to provide a complete description of nature; it requires many additional effective physical theories (such as Quantum Electrodynamics, Quantum Field Theory) to understand any physical phenomenon completely.

The first postulate of quantum mechanics introduces the framework for describing a physical system.

Postulate 1. Associated to any isolated physical system is a Hilbert space[1] known as the *state space* of the system. The system is completely described by its *state vector*, a unit vector in the system state's space.

The state vectors are symbolized by Dirac bra-ket notation: ket $|\psi\rangle$ refers to the state vector and its Hermitian conjugate is denoted by bra $\langle\psi|$. The inner product between the states $|\psi\rangle$ and $|\phi\rangle$ is denoted by $\langle\psi|\phi\rangle$ and the state vectors fulfill the *normalization condition* $\langle\psi|\psi\rangle = 1$. A general state vector can be written as a *superposition* of the *orthonormal basis* vectors $\{|\psi_k\rangle\}$ of the N-dimensional Hilbert space $\mathscr{H}$

$$|\psi\rangle = \sum_{k=1}^{N} C_k \, |\psi_k\rangle \tag{1.1}$$

[1] a complex vector space with an inner product structure

where $C_k \in \mathbb{C}$ and satisfy $\sum_{k=1}^{N} |C_k|^2 = 1$. One can only write the states in this form if all the information about the system is known. These states are known as pure states.

The second postulate aims at describing a composite system framework consisting of many quantum subsystems with variable degrees of freedom.

Postulate 2. The state space of a composite physical system is the tensor product of the state spaces of the component physical systems. Moreover, if we have systems numbered 1 through n, and system number i is prepared in the state $|\psi_i\rangle$, then the joint state of the total system is $|\psi_1\rangle \otimes |\psi_2\rangle \otimes ... \otimes |\psi_n\rangle$.

Let us consider a bipartite case, where the individual systems be described by the Hilbert spaces $\mathscr{H}_1$ and $\mathscr{H}_2$, then the Hilbert space of the composite system $\mathscr{H}_{12}$ is the *tensor product* of $\mathscr{H}_1$ and $\mathscr{H}_2$:

$$\mathscr{H}_{12} = \mathscr{H}_1 \otimes \mathscr{H}_2. \tag{1.2}$$

The dimension of the composite Hilbert space $\mathscr{H}_{12}$ is the product of dimensions of the individual Hilbert spaces, $d_{12} = d_1 d_2$, where d_i is the dimension of $\mathscr{H}_i$.

Let us now consider the scenario where the state vectors $|\psi\rangle_1 \in \mathscr{H}_1$ and $|\phi\rangle_2 \in \mathscr{H}_2$ can always describe the subsystems; then, the global system can also be always described by the elements of the set $S_{12} = \{|\psi\rangle_1 \otimes |\phi\rangle_2 : |\psi\rangle_1 \in \mathscr{H}_1, |\phi\rangle_2 \in \mathscr{H}_2\}$, whose dimension is only $d_1 + d_2 \leq d_{12}$ (for $d_1, d_2 \geq 2$). Therefore, there exist states in the composite system, whose subsystems can not be considered separately. These are termed as *entangled* states. S_{12} corresponds to the set of *product states*.

For any given bipartite state $|\psi\rangle_{12} \in \mathscr{H}_{12}$, the description of a subsystem is given by the *partial trace* of $|\psi\rangle_{12}$ over the Hilbert space of the other subsystem, i.e.,

$$\rho_1 = \mathrm{tr}_2(|\psi\rangle\langle\psi|_{12}) \quad \text{and} \quad \rho_2 = \mathrm{tr}_1(|\psi\rangle\langle\psi|_{12}). \tag{1.3}$$

The subsystem is represented by the density operator ρ, a positive semi-definite[2], hermitian operator with $\mathrm{tr}(\rho)$=1, also known as trace-one nonnegative operator.

The pure state $|\psi\rangle_{12}$ can be written as $|\psi_{12}\rangle = \sum_{i,j} c_{ij} |u_i\rangle_1 \otimes |v_j\rangle_2$, then the partial state ρ_1 reads

$$\begin{aligned}
\rho_1 &= \mathrm{tr}_2(|\psi_{12}\rangle\langle\psi_{12}|) && (1.4)\\
&= \mathrm{tr}_2 \sum_{i,j,i',j'} c_{ij} c^*_{i'j'} |u_i\rangle\langle u_{i'}|_1 \otimes |v_j\rangle\langle v_{j'}|_2 && (1.5)\\
&= \sum_{i,j,i',j'} c_{ij} c^*_{i'j'} |u_i\rangle\langle u_{i'}|_1 \otimes \langle v_{j'}|v_j\rangle_2 && (1.6)\\
&= \sum_{i,j,i'} c_{ij} c^*_{i'j} |u_i\rangle\langle u_{i'}|_1 . && (1.7)
\end{aligned}$$

Such an operator ρ is referred to as a *mixed state* as opposed to the rank-one pure state $|\psi_{12}\rangle\langle\psi_{12}|$. We note $\mathscr{P}(\mathscr{H})$ the set of trace-one nonnegative operators on the

[2]non-negative eigenvalues

Hilbert space $\mathscr{H}$. The density operator is very convenient for describing a system whose state is not completely known. The density operator for such a system is written as a convex combination of possible pure states the system might be in,

$$\rho = \sum_{k=1}^{N} p_k \left|\psi_k\right\rangle \left\langle\psi_k\right| \tag{1.8}$$

where p_k is the probability that the system lies in the pure state ψ_k. Given a density operator ρ, one can comment on its purity by calculating $\mathrm{tr}(\rho^2)$; if the value is 1, the state is pure and for values less than 1, the state is mixed.

From Eqs. (1.4-1.7), note that for a given mixed state $\rho_A \in \mathscr{P}(\mathscr{H}_A)$, one can define an auxiliary system E, such that there exists a pure state $|\psi_{AE}\rangle \in \mathscr{H}_A \otimes \mathscr{H}_E$[3] satisfying $\rho_A = \mathrm{tr}_E \left|\psi\right\rangle \left\langle\psi\right|_{AE}$. The state $|\psi_{AE}\rangle$ is known as the *purification* of ρ_A.

The third postulate deals with the evolution of the quantum system with respect to time.

Postulate 3. The evolution of a closed quantum system is described by a unitary transformation, that is, the state $|\psi\rangle$ of the system at time t_1 is related to the state $|\psi'\rangle$ of the system at time t_2 by a unitary operator U which depends only on the times t_1 and t_2,

$$\left|\psi'\right\rangle = U \left|\psi\right\rangle . \tag{1.9}$$

An equivalent evolution dynamics is given by the Schrodinger's equation

$$i\hbar \frac{d\left|\psi\right\rangle}{dt} = \mathcal{H} \left|\psi\right\rangle , \tag{1.10}$$

where $\mathcal{H}$ is the Hamiltonian of the system. And the relation between U and $\mathcal{H}$ reads

$$U = e^{-i\mathcal{H}(t_2 - t_1)}, \tag{1.11}$$

if the Hamiltonian is invariant with respect to time.

Any observation of a system is associated with a measurement on the system. The fourth postulate describes the measurement process in quantum mechanics.

Postulate 4. Quantum measurements are defined by a collection $\{M_m\}$ of *measurement operators*. These are operators acting on the state space of the system being measured. The index m refers to the measurement outcomes that may occur in the experiment. The measurement operators satisfy the *completeness equation*

$$\sum_m M_m^\dagger M_m = \mathbb{I}. \tag{1.12}$$

[3] $\mathscr{H}_E$ is isomorphic to $\mathscr{H}_A$

If the state of the quantum system is $|\psi\rangle$ immediately before the measurement, then the probability $p(m)$ that the result m occurs is given by

$$p(m) = \langle\psi|M_m^\dagger M_m|\psi\rangle, \tag{1.13}$$

and the state of the system after the measurement is

$$\frac{M_m\,|\psi\rangle}{\sqrt{p(m)}}. \tag{1.14}$$

Contrary to the deterministic and reversible evolution process, quantum measurements are probabilistic and irreversible. The probabilistic property is intrinsic to quantum mechanics, as it only predicts probabilities with which an outcome will be observed, not the actual outcome. After a measurement, the state collapses to one of the pure states corresponding to the measurement outcome. For instance, let us consider the general state vector from Eq. (1.1), upon measuring in the said basis; the state collapses to one of the basis vectors. That is why measurements are irreversible since the knowledge of what the state was before the measurement is lost.

Quantum observables are Hermitian measurement operators, where the eigenvalues are the possible outcomes and the corresponding eignevectors are collapsed state vectors. Here we have considered the general form of measurements, also known as *Positive Operator Valued Measure* (POVM). However, there exists a special class of measurement operators known as projective measurements, with a couple extra properties,

$$M_m M_n = \delta_{m,n} M_m \tag{1.15}$$

and the number of projective operators in the measurement collection equates to the dimension of the Hilbert space since the number of projective operators must equate to the cardinality of the bases. Another major difference between the two sets of measurements is that the results of projective measurements are repeatable, while for POVM's they are not. This is a direct consequence of the first property of projective measurements.

Quantum channels are linear maps that take an initial state $\rho \in \mathscr{P}(\mathscr{H})$ to a final state $\rho' \in \mathscr{P}(\mathscr{H}')$. Therefore, the maps must preserve the intrinsic properties of the density matrix and hence the map obeys two properties:

- Complete Positivity: meaning the positive-semidefinite nature of the density matrix must be preserved even if the map is only acts on a subsystem of the density matrix.
- Trace preservation: since it's a map with density matrices as outputs, the trace of the density matrix must remain 1.

Therefore, any physical quantum channel can be defined by a Completely Postive Trace Preserving (CPTP) map[4], whose characterization is given by Kraus decomposition

[4]the general quantum operation is defined by a Completely Postive Trace Non-increasing map

[2], which states that for a CPTP map Λ, there exist $k \leq (\dim \mathscr{H})^2$ Kraus operators $\{K_i \in \mathscr{H}\}$ satisfying $\sum_{i=1}^{k} K_i^\dagger K_i = \mathbb{I}$ such that

$$\Lambda(\rho) = \sum_{i=1}^{k} K_i \rho K_i^\dagger, \tag{1.16}$$

where $\rho \in \mathscr{P}(\mathscr{H})$.

A unitary evolution is a special case which preserves the inner product of the Hilbert space, meaning there exists only one Kraus operator U which satisfies $UU^\dagger = U^\dagger U = \mathbb{I}$.

There exists an interesting way of looking at the complete-positivity of a CPTP map, which is similar to the density-matrix form. Let us consider, a composite system of two d-dimensional Hilbert spaces $\mathscr{H}_1 \otimes \mathscr{H}_2$. One can then write the maximally entangled state as

$$|\Phi^+\rangle \langle\Phi^+| = \frac{1}{d} \sum_{1 \leq i,j, \leq d} |i\rangle \langle j| \otimes |i\rangle \langle j| . \tag{1.17}$$

One can now define the Choi-Jamiołkowski operator, $J(\Lambda) : \mathscr{H}_1 \otimes \mathscr{H}_2 \to \mathscr{H}_3 \otimes \mathscr{H}_2$ as an operator which applies the CPTP map $\Lambda : \mathscr{H}_1 \to \mathscr{H}_3$ on the first half of the entangled state:

$$J(\Lambda) = \frac{1}{d} \sum_{1 \leq i,j, \leq d} \Lambda(|i\rangle \langle j|) \otimes |i\rangle \langle j| . \tag{1.18}$$

Choi's theorem [4] then states that the map Λ is considered to be completely positive iff $J(\Lambda)$ is positive semidefinite, since Λ acts on the subsystem, and the output system is a density matrix, and Λ is trace-preserving iff or $tr_1[J(\Lambda)] = \mathbb{I}/d$, a maximally mixed state, as expected when tracing out a subsystem from a maximally entangled system.

There also exists another alternative definition to the CPTP map, given by Stinespring's dilation theorem that states, any quantum operator can be described as a unitary evolution in a larger Hilbert space: by tensoring a second system[5], followed by the unitary evolution on the joint system and finally tracing out the second system provides us with the action of the CPTP map on a density operator. Thus, for a given CPTP map on a finite-dimensional Hilbert space $\Lambda : \mathscr{H} \to \mathscr{H}'$, there exists a Hilbert space $\tilde{\mathscr{H}}$ and a unitary operator U on $\mathscr{H} \otimes \tilde{\mathscr{H}}$ such that:

$$\Lambda(\rho) = \mathrm{tr}_{\tilde{\mathscr{H}}}[U(\rho \otimes |0\rangle \langle 0|)U^\dagger], \quad \forall\, \rho \in \mathscr{P}(\mathscr{H}). \tag{1.19}$$

The ancilla space can have a maximum dimension of $(\dim \mathscr{H})^2$. This representation is unique up to unitary equivalence.

1.2. Properties of quantum mechanics

We first define a simple quantum state of utmost importance, the two-dimensional unit vector, known as the qubit. The Hilbert space $\mathbb{C}^2$ is completely spanned by the basis set $\{|0\rangle, |1\rangle\}$. Thus, a general qubit state can be written as

$$|\psi\rangle = \alpha |0\rangle + \beta |1\rangle , \tag{1.20}$$

[5] traditionally known as the *ancilla*

where $\alpha, \beta \in \mathbb{C}$ and satisfy $|\alpha|^2 + |\beta|^2 = 1$. Then the density matrix reads,

$$\rho = \begin{pmatrix} |\alpha|^2 & \alpha^*\beta \\ \alpha\beta^* & |\beta|^2 \end{pmatrix}. \tag{1.21}$$

The diagonal terms $|\alpha|^2$ and $|\beta|^2$ are the probability of measuring $|\psi\rangle$ in $|0\rangle\langle 0|$ and $|1\rangle\langle 1|$ respectively whereas the off-diagonals terms describe the *quantum coherence* of the state. A pure state exhibit coherence, whereas a mixed state which represents a statistical mixture does not display coherence. When the off-diagonal terms are zero, the state behaves classically. The density matrix in such a case reads,

$$\rho = \begin{pmatrix} |\alpha|^2 & 0 \\ 0 & |\beta|^2 \end{pmatrix}. \tag{1.22}$$

Such a density matrix is the result of preparing states $|0\rangle$ and $|1\rangle$ from a source with probability $|\alpha|^2$ and $|\beta|^2$ respectively.

Quantum coherence is an inherent property of quantum mechanics and plays a crucial role as a resource in quantum computing and cryptography. However, when the system interacts with the environment, over time, the system loses coherence. This phenomenon is known as quantum decoherence. For a completely isolated system, however, the coherence is maintained indefinitely[6]. Nevertheless, observations on such systems are impossible to examine.

Another essential feature of quantum mechanics is its inability to copy an unknown quantum state successfully. Contrary to classical physics, quantum physics does not allow for duplication; this is the *no-cloning theorem*. The theorem states that, given an arbitrary state, it is impossible to copy the state with a unit probability. The proof can be shown by contradiction.

Let us consider a composite system with the Hilbert space $\mathscr{H}_A \otimes \mathscr{H}_B$, where the state to be copied exists in system A and state is copied to system B. Let us assume, that the state we want to copy is some pure state $|\psi\rangle$ and the state in which we want to copy is also a pure state $|p\rangle$. The only possible operations are CPTP maps, which according to Stinespring's dilation theorem is a unitary evolution in a larger Hilbert space. Therefore, we perform a unitary operation such that

$$U|\psi\rangle \otimes |p\rangle = |\psi\rangle \otimes |\psi\rangle. \tag{1.23}$$

Now, the question is does the unitary operation capable of copying all pure states in $\mathscr{H}_A$. Let us assume the unitary works on another state $|\phi\rangle$ as well,

$$U|\phi\rangle \otimes |p\rangle = |\phi\rangle \otimes |\phi\rangle. \tag{1.24}$$

Taking the inner product of two equations, we get

$$\langle\phi|\psi\rangle = (\langle\phi|\psi\rangle)^2, \tag{1.25}$$

[6]Coherence if defined with respect to a basis, can change even if your system is isolated.

which implies

$$\text{either } \langle\phi|\psi\rangle = 0 \text{ or } \langle\phi|\psi\rangle = 1. \tag{1.26}$$

Therefore, a cloning operation can only clone states which are orthogonal to each other, and thus an universal quantum cloner for a general state is impossible.

One of the corollaries of the no-cloning theorem is that non-orthogonal quantum states cannot be reliably distinguished. The distinguishability of quantum states is a significant field of study, mainly because for any operational task such as key distribution we are always interested in comparing the performance of the actual task to an ideal version of the same task. Therefore, there is a need to quantify how 'close' are two quantum states and how effectively they can be distinguished. Here, we provide two quantities to calculate 'closeness': *trace distance* and *fidelity*.

The **trace distance** between two quantum states ρ and σ is given by

$$D(\rho,\sigma) := \frac{1}{2} \parallel \rho - \sigma \parallel_1 = \frac{1}{2}\text{tr}|\rho - \sigma|, \tag{1.27}$$

where $|A| = \sqrt{A^\dagger A}$. It is genuine distance measure, since it follows the triangle inequality:

$$D(\rho,\sigma) + D(\sigma,\tau) \geq D(\rho,\tau), \tag{1.28}$$

for any ρ, σ and τ. If the states are orthogonal, then $D(\rho,\sigma) = 1$.

For pure states, the trace distance reads,

$$D(\rho,\sigma) = \sqrt{1 - |\langle\psi|\phi\rangle|^2}, \tag{1.29}$$

where $\rho = |\psi\rangle\langle\psi|$ and $\sigma = |\phi\rangle\langle\phi|$. The trace distance $D(\rho,\sigma)$ is invariant under unitary operations, since it only depends on the spectrum of $|\rho - \sigma|$,

$$D(U\rho U^\dagger, U\sigma U^\dagger) = D(\rho,\sigma). \tag{1.30}$$

The **fidelity** between two quantum states ρ and σ is defined as

$$F(\rho,\sigma) = \text{tr}\sqrt{\rho^{1/2}\sigma\rho^{1/2}}. \tag{1.31}$$

When one of the state is pure, then the fidelity between $|\psi\rangle$ and σ reads,

$$F(|\psi\rangle, \sigma) = \sqrt{\langle\psi|\sigma|\psi\rangle}, \tag{1.32}$$

and if both the states are pure, then the fidelity is simply the inner product of the two states. Similar to trace distance, fidelity is also invariant under unitary operations.

The fidelity of any two mixed states can be written in terms of the fidelity of their purifications, as the maximal overlap between the two purifications. For any states ρ and σ, and a purification $|\psi\rangle$ of ρ, there exists a purification $|\phi\rangle$ of σ such that

$$F(\rho,\sigma) = |\langle\psi|\phi\rangle| = F(|\psi\rangle, |\phi\rangle). \tag{1.33}$$

This is known as the *Uhlmann's theorem*. Thus, the fidelity is a practical measure of closeness for two quantum states since the fidelity between any two states can always be equated to the inner product of two pure states.

Now that we have defined measures of closeness, we consider the probability of distinguishing two arbitrary states. Let us consider two quantum states ρ_0 and ρ_1, the maximum probability of correctly distinguishing the state is

$$p = \frac{1}{2}\left[1 + \|\rho_0 - \rho_1\|_1\right], \tag{1.34}$$

where $\|A\|_1 = \mathrm{tr}|A|$. This bound is known as the *Helström bound*, achievable for POVMs $\{M_0, \mathbb{I} - M_0\}$ where M_0 is the projector on the positive eigenspace of $\rho_0 - \rho_1$.

Trace distance gives the minimal error probability when distinguishing two quantum states prepared with the same probability, given the best possible measurement. This is why the trace distance is often chosen as an operational measure of the distance between quantum states. For any operational task (such as key distribution), we compare the performance of the actual task producing an output ρ against an ideal actualization of the task ρ_{ideal}[7]. Whenever, $D(\rho, \rho_{ideal}) \leq \epsilon$ for some small value of ϵ, then the output states ρ and ρ_{ideal} are indistinguishable except with a small probability ϵ.

Similarly to the case of distinguishing two quantum states, one might also need to distinguish between two maps, e.g., between a map representing an ideal version of the operational task and a real map of the actual implementation of the task. Thus, we need to define a distance measure. Generally, we use the *diamond norm* $\|.\|_\diamond$ for such transformations. Then, the **diamond distance** [3] between two maps is defined as

$$D_\diamond(\mathcal{E}, \mathcal{F}) = \|\mathcal{E} - \mathcal{F}\|_\diamond, \tag{1.35}$$

where $\|T\|_\diamond$ is defined as,

$$\|\mathcal{T}\|_\diamond = \sup_{k \in \mathbb{N}} \|\mathcal{T} \otimes \mathbb{I}_k\|_1 \tag{1.36}$$

where

$$\|\mathcal{S}\|_1 = \sup_{\|\sigma\|_1 \leq 1} \|\mathcal{S}(\sigma)\|_1, \tag{1.37}$$

and $\mathbb{I}_k$ is the identity map on a k-dimensional Hilbert space. The suprema are reached when k equates to the dimension of the input of $\mathcal{T}$ and σ is positive.

For any two physical processes described by the CPTP maps $\mathcal{E}$ and $\mathcal{F}$, the maximal probability of correctly distinguishing given the observer is allowed one run with a state of his choice for both maps is

$$p = \frac{1}{2}(1 + D_\diamond(\mathcal{E}, \mathcal{F})). \tag{1.38}$$

Another important property of quantum mechanics which has no classical analogue is the *uncertainty principle*. It states that for two conjugate physical observables A and B,

[7] for instance, in the case of quantum key distribution task where ideal protocol outputs the state $\rho_{ideal} = \rho_K \otimes \rho_E$, where ρ_K is the mixed uniform state corresponding to the secret keys and ρ_E is the state of the eavesdropper, completely uncorrelated to the key state

decreasing the uncertainty of one observable increases the uncertainty of the other one. This is observed when the variables are non-commuting, i.e., $[A, B] := AB - BA \neq 0$. A measurement to learn information about one variable completely destroys information about the other variable. Mathematically,

$$\Delta A \Delta B \geq \frac{\langle [A, B] \rangle}{2}, \tag{1.39}$$

where $\Delta A = \sqrt{\langle A^2 \rangle - \langle A \rangle^2}$. This law is true for any two non-commuting observables such as position and momentum, σ_x and σ_z etc.

CHAPTER 2

PRELIMINARIES

In this chapter, we present the main tools of "Information theory" and "Continuous-variable systems" that we will be using in this thesis for the study of quantum cryptographic protocols. The chapter also includes a section on semidefinite programming, which we have used rather extensively in this thesis.

2.1. Information theory

In the late 40's, Shannon introduced the information theory to study compression and transmission of data through communication channels. Here we only give a short overview of information theory. This section aims to discuss and understand the main concepts in classical information theory before delving into the analogous quantum information-theoretic ideas. For a more detailed study, refer to the textbooks "Elements of information theory" by Cover and Thomas [5] and "Information theory, inference and learning algorithms" by MacKay [6].

2.1.1 Classical information theory

We start by defining a classical source. It is described by a sequence of random variables $X_1, X_2, ..., X_n$ whose values represent the source's outputs and the values are taken from the source alphabet (or support) $\mathcal{X}$.

An independent and identically distributed (i.i.d.) source is a source where the random variables are independent, $p(x_1, x_2, \ldots, x_n) = p(x_1)p(x_2)...p(x_n)$ and identically distributed $X_i = X \; \forall \; i$.

Given a discrete random variable X, the *Shannon entropy* of X measures the amount of uncertainty about X before the value of X is known. It is defined as

$$H(X) := -\sum_{x \in \mathcal{X}} p_X(x) \log_2 p_X(x) \tag{2.1}$$

where $\mathcal{X}$ is the support of X and p_X is the probability distribution of X. Note that, the minimum possible value for Shannon entropy is zero, when the event X is certain and

the maximum possible value equates to $\log_2 |\mathcal{X}|$, when X is a uniform distribution on the support $\mathcal{X}$, provided $\mathcal{X}$ is finite.

The *joint entropy* for a generalized n-uples of discrete random variables $X_1, X_2...X_n$ is given by

$$H(X_1, X_2...X_n) := -\sum_{x_1 \in \mathcal{X}_1} ... \sum_{x_2 \in \mathcal{X}_n} p(x_1, ..., x_n) \log_2 p(x_1, ..., x_n), \tag{2.2}$$

where $p(x_1, ..., x_n)$ is the joint probability distribution. The function H is sub-additive, i.e.,

$$H(X_1, X_2...X_n) \leq H(X_1) + H(X_2) + ... + H(X_n), \tag{2.3}$$

with equality if and only if the random variables X_i are independent.

Shannon entropy only captures the uncertainty of X on average, therefore it is not always a desirable measure of entropy. Rényi entropy allows us to make stronger statements. The Rényi entropy of order α is defined as

$$H_\alpha(X) := \frac{1}{1-\alpha} \log_2 \sum_{x \in \mathcal{X}} p_X(x)^\alpha. \tag{2.4}$$

In the limit $\alpha \to 1$, we recover the Shannon entropy, i.e., $H_1(X) := H(X)$. Among the other values of α, the ones with particular interests are:

- $\alpha \to 0, H_0(X) = \log_2 |\mathcal{X}|$, the *max-entropy* of X,
- $\alpha = 2, H_2(X) = -\log_2 \sum_{x \in \mathcal{X}} p_X(x)^2$, the *collision entropy* which plays a role in privacy amplification protocol,
- $\alpha \to \infty, H_\infty(X) = -\log_2(\sup_{x \in \mathcal{X}} p_X(x))$, the *min-entropy* of X, which is related to the maximal probability of guessing the value of X.

Following which, we have

$$H_0(X) \geq H(X) \geq H_2(X) \geq H_\infty(X), \tag{2.5}$$

meaning for a given random variable X, the Rényi entropy $H_\alpha(X)$ is a decreasing function of α. All the Rényi entropies are additive, i.e., $H_\alpha(X, Y) = H_\alpha(X) + H_\alpha(Y)$ for independent random variables X and Y .

Next, let us consider the case where we have some privileged information about X, through an another discrete random variable Y. The marginal probability distributions can be written as

$$p_X(x) = \sum_y p_{XY}(x, y) \quad \text{and} \quad p_Y(y) = \sum_x p_{XY}(x, y) \tag{2.6}$$

where $p_{XY}(x, y)$ is the joint probability distribution.

The *conditional entropy* is defined as

$$H(X|Y) := \sum_y p_Y(y) H(X|Y=y) \tag{2.7}$$

$$= -\sum_y \sum_x p_{XY}(x,y) \log_2 p(x|y), \tag{2.8}$$

which leads us to the following chain rule

$$H(X,Y) = H(X) + H(Y|X). \tag{2.9}$$

One can find this relation by using the definition of conditional probability,

$$\log p(x,y) = \log p(y|x) + \log p(x) \tag{2.10}$$

and calculating the expectation value on the both sides of the equation.

Conditioning always decreases the entropy, $H(X|Y) \leq H(X)$, with equality iff X and Y are independent random variables, $p_{XY}(xy) = p_X(x)p_Y(y)$. This relation also holds for conditional entropies

$$H(X|Y,Z) \leq H(X|Y), \tag{2.11}$$

and is known as the *strong subadditivity property.*

The *mutual information* between two discrete random variables X and Y with the joint probability distribution $p_{XY}(x,y)$ can be defined as

$$I(X:Y) := -\sum_{x,y \in \mathcal{X} \otimes \mathcal{Y}} p_{XY}(x,y) \log_2 \frac{p_{XY}(x,y)}{p_X(x) p_Y(y)}. \tag{2.12}$$

This is interpreted as the amount of correlation present between the two random variables. The mutual information can also be written in terms of joint entropy, conditional entropy, and individual Shannon entropies

$$I(X:Y) = H(X) + H(Y) - H(X,Y) \tag{2.13}$$

$$= H(X) - H(X|Y) = H(Y) - H(Y|X). \tag{2.14}$$

The previous definitions of Shannon entropy are valid for discrete variables. To define the Shannon entropy for continuous variables, we introduce the notion of *differential entropy* $h(X)$, which reads

$$h(X) := -\int_{x \in \mathcal{X}} p(x) \log_2 p(x) dx, \tag{2.15}$$

where $\mathcal{X}$ is the support alphabet and $p(x)$ is the probability density function of the continuous random variable X.

The differential entropy shares most of the properties of Shannon entropy for discrete variables, and subsequently we can define the joint, conditional and mutual differential

entropies, which follow the same relations as defined before for discrete distributions. The differential entropy can be negative, unlike the entropy.

We now introduce the case of the normal distribution which we will use quite extensively in later chapters:

$$f_{\mathcal{N}}(x) = \frac{1}{\sqrt{2\pi\sigma^2}} e^{-\frac{(x-\mu)^2}{2\sigma^2}}, \tag{2.16}$$

where μ is the mean and σ^2 is the variance of the distribution. The differential entropy for a continuous random variable X following the normal distribution, $\mathcal{N}(0, \sigma^2)$ reads

$$h(X) = -\int_{x\in\mathcal{X}} f_{\mathcal{N}}(x) \log_2 f_{\mathcal{N}}(x) dx = -\int_{-\infty}^{\infty} f_{\mathcal{N}}(x) \left(-\frac{x^2}{2\sigma^2} - \frac{\ln 2\pi\sigma^2}{2} \right) dx \tag{2.17}$$

$$= \frac{1}{2} + \frac{\log_2 2\pi\sigma^2}{2} = \frac{1}{2} \log 2e\pi\sigma^2 = \frac{1}{2} \log_2 \sigma^2. \tag{2.18}$$

For a bipartite (X and Y) normal distribution with zero mean and covariance matrix

$$K_{XY} = \begin{pmatrix} \langle x^2 \rangle & \langle xy \rangle \\ \langle xy \rangle & \langle y^2 \rangle \end{pmatrix}, \tag{2.19}$$

the differential Shannon entropy reads,

$$h(X, Y) = \frac{1}{2} \log_2(\det K_{XY}). \tag{2.20}$$

Subsequently, the conditional entropy can be written as

$$h(X|Y) = \int h(X|Y = y) dy = \frac{1}{2} \log_2 V_{X|Y}, \tag{2.21}$$

where we have used the fact $f(x|y) = f(x, y)/f(y)$ and $V_{X|Y}$ is the variance of X when Y is known,

$$V_{X|Y} = \frac{\det K_{XY}}{V_X}. \tag{2.22}$$

The mutual information then reads,

$$I(X : Y) = h(X) + h(Y) - h(X, Y) = \frac{1}{2} \log \left(\frac{V_X V_Y}{\det K_{XY}} \right). \tag{2.23}$$

The main motivation behind quantifying information, is to analyze a *communication system*. An universal communication system (Fig. 2.1) consists of five major parts:

- Source: produces a message to be communicated,
- Encoder: encodes the message in a suitable form for transmission and transmits it,
- Channel: the medium through which the encoded message is being transmitted,

- Decoder: receives and decodes the encoded message to obtain the original,
- Destination: to whom the message is intended.

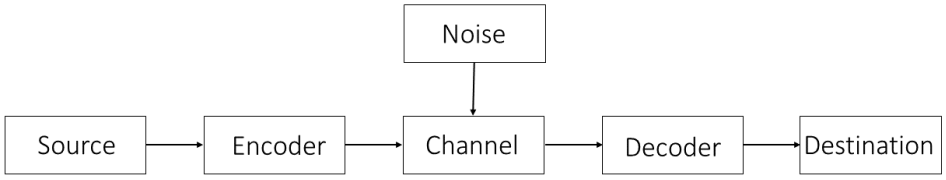


Figure 2.1: Communication system.

Information theory attempts to provide a mathematical framework for all of the components mentioned above. Here, we briefly discuss the channel components, followed by the limits of transfer of information for the said channel. A channel can be modeled as a system with an input X taking values from the alphabet $\mathcal{X}$, an output Y with values from alphabet $\mathcal{Y}$ and a probability matrix $p(y|x)$, probability of observing output x given input y. The alphabets can be discrete or continuous. *Channel capacity* is the maximum amount of information rate that can be reliably transmitted through a communication channel. The channel capacity is defined as

$$C := \max_{p(x)} I(X:Y), \tag{2.24}$$

where the maximum is taken over all possible input distributions $p(x)$.

One of the basic continuous noise channel models of immense importance is the *Additive White Gaussian Noise* (AWGN) channel. The output Y, the input X and the Gaussian noise Z are related through $Y = X + Z$, where $Z \sim \mathcal{N}(0, \sigma^2)$ and is independent of the input X. The transition probability reads,

$$p(y|x) = \frac{1}{\sqrt{2\pi\sigma^2}} e^{-\frac{(y-x)^2}{2\sigma^2}}. \tag{2.25}$$

Theoretically, the channel capacity of an AWGN channel is infinite. However, for practical reasons, an energy constraint (or power constraint) is imposed, i.e., the variance of the input is upper bounded by V_X. Then one can write the mutual information,

$$h(X:Y) = h(Y) - h(Y|X) = h(Y) - h(X+Z|X) = h(Y) - h(Z|X) \tag{2.26}$$

and since X and Z are independent, therefore, $h(X:Y) = h(Y) - h(Z)$. The variance of Y, given by

$$\langle Y^2 \rangle = \langle (X+Z)^2 \rangle = \langle X^2 + Z^2 + 2XZ \rangle \tag{2.27}$$

$$= \langle X^2 \rangle + \langle Z^2 \rangle + 2\langle X \rangle \langle Z \rangle \leq V_X + \sigma^2. \tag{2.28}$$

Therefore, the mutual information reads,

$$I(X:Y) = h(Y) - h(Z) \tag{2.29}$$

$$\leq \frac{1}{2}\log(V_X + \sigma^2) - \frac{1}{2}\log\sigma^2 = \frac{1}{2}\log\left(1 + \frac{V_X}{\sigma^2}\right). \tag{2.30}$$

The inequality saturates when the input follows a normal distribution, $X \sim \mathcal{N}(0, V_X)$. Therefore, the capacity of an AWGN channel is given by

$$C_{AWGN} = \frac{1}{2}\log\left(1 + \frac{V_X}{\sigma^2}\right) = \frac{1}{2}\log\left(1 + SNR\right), \tag{2.31}$$

where $SNR = \dfrac{V_X}{\sigma^2}$ is the signal to noise ratio.

2.1.2 Quantum regime

As discussed in section 1.2, in quantum mechanics, it is impossible to distinguish with certainty any given set of non-orthogonal states nor can one duplicate the states. Thus, cryptographic protocols using quantum states as carriers of information, provides an inherent advantage. Therefore, the question arises, equipped with such strong properties how efficiently can one transmit information via quantum states through a quantum channel.

The basic unit of information processing in quantum regime is the *qubit* (short for quantum bit). Recall that the density operator for a general qubit state is

$$\rho = \begin{pmatrix} |\alpha|^2 & \alpha^*\beta \\ \alpha\beta^* & |\beta|^2 \end{pmatrix}. \tag{2.32}$$

Measuring the state in the basis $\{|0\rangle, |1\rangle\}$, collapses it to either $\{|0\rangle$ or $|1\rangle\}$ with probability $|\alpha|^2$ and $|\beta|^2$ respectively. Therefore, one can use the density operator as a substitute for the probability distribution in Shannon entropy. Thus, the generalization of Shannon entropy for a quantum state ρ, the *von Neumman entropy* reads

$$S(\rho) := -\mathrm{tr}[\rho \log_2 \rho]. \tag{2.33}$$

In the orthogonal basis $\{|i\rangle\}$ which diagonalizes ρ

$$\rho = \sum_i \lambda_i |i\rangle\langle i|, \tag{2.34}$$

the von Neumann entropy reduces to the Shannon entropy,

$$S(\rho) = \sum_i \lambda_i \log_2 \lambda_i = H(\lambda), \tag{2.35}$$

λ denotes the distribution $\{\lambda_i\}$.

The interpretation remains the same as that of Shannon entropy. The von Neumann entropy of a pure state is zero, while it is maximal for a maximally mixed state $\rho = \mathbb{I}/d$,

$S(\rho) = \log_2 d$, where d is the dimension of the Hilbert space. Therefore, for a maximally mixed qubit state, $\rho = \mathbb{I}/2$, the von Neumann entropy is 1. In diagonalized form, $S(\rho) = H(\lambda)$, which in this case is 1.

The von Neumann entropy is invariant under unitary operations: for any unitary U, $S(U\rho\, U^\dagger) = S(\rho)$.

For a block-diagonal density matrix of the form

$$\rho = \sum_k p_k \rho_k, \tag{2.36}$$

where ρ_k have support on orthogonal subspaces, the von Neumann entropy reads,

$$S(\rho) = H(p) + \sum_k p_k S(\rho_k). \tag{2.37}$$

The entropy of a quantum system A is the entropy of the representing state ρ_A of the system, denoted by $S(A)$ or $S(\rho_A)$. For a composite system AB represented by ρ_{AB}, the *joint entropy* of the system is given by,

$$S(A,B) = S(\rho_{AB}) := -\mathrm{tr}[\rho_{AB} \log_2 \rho_{AB}]. \tag{2.38}$$

If the composite state is pure $S(A,B) = 0$, then $S(A) = S(B)$. Sub-additivity is also followed by von Neumann entropy

$$S(A,B) \leq S(A) + S(B), \tag{2.39}$$

with equality iff $\rho_{AB} = \rho_A \otimes \rho_B$.[1]

The *conditional entropy* is given by

$$S(A|B) := S(A,B) - S(B). \tag{2.40}$$

Unlike conditional Shannon entropy, conditional von Neummann entropy can be negative, happens generally in the presence of an entanglement. Conditioning reduces entropy, i.e., $S(A|B,C) \leq S(A|B) \leq S(A)$.

The mutual information is given by

$$S(A:B) := S(A) + S(B) - S(A,B) \tag{2.41}$$

$$= S(A) - S(A|B) = S(B) - S(B|A), \tag{2.42}$$

introduced to study the amount of correlation between two systems. For a product state, $\rho_{AB} = \rho_A \otimes \rho_B$, $S(A:B) = 0$, while for a maximally entangled state, $|\psi_{AB}\rangle = \sum_{i=1}^{d} \frac{1}{\sqrt{d}} |i\rangle_A \otimes |i\rangle_B$, $S(A:B) = 2\log_2 d$.

One can never increase the mutual information by discarding a system,

$$S(A:B) \leq S(A:B,C), \tag{2.43}$$

nor by applying a local quantum operation to individual systems separately, system AB mapped to system $A'B'$,

$$S(A':B') \leq S(A:B), \tag{2.44}$$

with equality iff the operation is unitary.

[1] quantum analogue for independence of classical random variables

Classical communication over quantum channel

Let us define a quantum source. A quantum source generates random quantum states, belonging to the Hilbert space $\mathscr{H}$. After n uses of quantum source, we represent the final quantum state by ρ^n. An i.i.d. quantum source generates a quantum state ρ for each run. Therefore, the state after n runs is $\rho^{\otimes n} = \rho \otimes \rho ... \otimes \rho$.

An i.i.d. *classical-quantum source* generates independent pairs of classical-quantum states, where the entire joint state of the classical register a and the quantum signal B has the density matrix $\rho_{aB} \otimes \rho_{aB} ... \otimes \rho_{aB}$. For a source generating pure states, we have,

$$\rho_{aB} = \sum_a p(a) \left|a\right\rangle \left\langle a\right| \otimes \left|\phi_a\right\rangle \left\langle \phi_a\right|, \tag{2.45}$$

where $\{\left|a\right\rangle\}_a$ is a family of mutually orthogonal vectors representing the classical values of a and $\left|\phi_a\right\rangle$ represents the quantum signal.

This type of states has many applications; they are mainly observed when one of the party has some classical information, about which another party holds some quantum information, e.g., when a party wishes to generate quantum states according to given classical information (a probability distribution).

Let us now study a task, where Alice has a classical source producing symbols $x = \{0, 1, ..., n\}$, denoted by random variable X according to a probability distribution $p(x)$. The aim for Bob is to determine the value of X. Hence, Alice prepares ρ_x chosen from a fixed set $\{\rho_0, \rho_1, ..., \rho_n\}$ according to the symbol and sends it to Bob. Then Bob performs a POVM measurement $\{E_y\}$ on the state and obtains an output Y. Depending on the value of Y, Bob makes his best guess about X.

Holevo bound. The amount of information Bob has gained about X from output Y is given by the mutual information between $I(X:Y)$. Bob can guess X with certainty if and only if $I(X:Y) = H(X)$, however, generally $I(X:Y) \leq H(X)$. Thus, Bob must choose his measurement in such a way that $I(X:Y)$ becomes really close to $H(X)$. The mutual information is upper bounded by the quantity, *Holevo bound*,

$$I(X:Y) \leq \chi_\rho(X;Y) = S(\rho) - \sum_x p_x S(\rho_x), \tag{2.46}$$

where $\rho = \sum_x p_x \rho_x$.

Note that the Holevo bound does not depend on Bob's measurements. Generally, the mutual information does not attain this bound. To attain the bound, the individual density matrices $\{\rho_x\}_{x \in \mathcal{X}}$ must have orthogonal support, which is not the usual case. However, if we consider collective measurements instead of individual (product) measurements over infinite number of symbols (states), the maximum of mutual information over all possible measurement schemes achieves the Holevo bound. This is why the Holevo bound is used to quantify the potentially accessible information to an eavesdropper performing a collective attack against a QKD protocol [41].

Operational entropic quantities

The Shannon entropy and its quantum generalization, the von Neumann entropy are relevant in the asymptotic limit where a process is repeated many times independently. However, when neither of these assumptions hold, one needs to consider more general entropic quantities.

One such quantity is the *conditional min-entropy*. For a bipartite quantum state ρ_{AB}, the conditional min-entropy is defined as

$$H_{\min}(A|B)_{\rho_{AB}} := -\inf_{\sigma_B} D_\infty(\rho_{AB} \parallel \mathbb{I}_A \otimes \sigma_B). \tag{2.47}$$

where infimum is taken over all normalized density operators σ_B on subsystem B and

$$D_\infty(\rho \parallel \sigma) := \inf\{\lambda \in \mathbb{R} : \rho \leq 2^\lambda \sigma\}, \tag{2.48}$$

is the generalization of the *relative entropy*[2] of two states ρ and σ.

Operational interpretation of min-entropy. Let us consider the same task as before where Alice prepares quantum state ρ_x according to the symbol $x \in \{0, 1, ..., n\}$ produced from a classical source following a probability distribution $p(x)$. The symbols are denoted by random variable X. She sends the quantum states to Bob. The classical-quantum state ρ for the task has the same form as Eq. (2.45).

$$\rho_{XB} = \sum_x p_X(x) \left|x\right\rangle \left\langle x\right| \otimes \rho^x. \tag{2.49}$$

The aim for Bob is to determine the value of X. Bob chooses to perform a POVM measurement $\{E_x\}$ on the states and the corresponding success probability is given by

$$p_{guess}(X|B)_{\{E_x\}} = \sum_x p(x) \mathrm{tr}[E_x \rho_x]. \tag{2.50}$$

The *guessing probability* is defined as the probability obtained for optimal measurement:

$$p_{guess}(X|B) := \max_{E_x} p_{guess}(X|B)_{\{E_x\}}. \tag{2.51}$$

In [17], the authors proved that the min-entropy of X conditioned on B is linked to the guessing probability through the following relation,

$$p_{guess}(X|B) = 2^{-H_{\min}(X|B)_{\rho_{XB}}}. \tag{2.52}$$

Therefore, when a classical system is conditioned on a quantum system, the conditional min-entropy of equates to the guessing probability.

[2]The relative entropy between the states ρ and σ is given by

$$D(\rho \parallel \sigma) := \mathrm{tr}[\rho(\log_2 \rho - \log_2 \sigma)]$$

Smooth min-entropy. Here, we consider a slightly generalized version of the min-entropy called the *smooth min-entropy*. For a bipartite quantum state ρ, the smooth min-entropy of A conditioned on B is defined as

$$H_{\min}^{\epsilon}(A|B)_{\rho} := \sup_{\rho'} H_{\min}(A|B)_{\rho'}, \tag{2.53}$$

where ϵ is the smoothness parameter and the supremum ranges over all the density operators ρ' which are ϵ-close of ρ for the trace-distance, i.e., $\| \rho - \rho' \|_1 \leq \epsilon$.

The smooth min-entropy is a generalization of Von Neumann entropy, in [17] the authors show that one recovers von Neumann entropy in the limit of infinite many copies of the state

$$S(A|B)_{\rho} = \lim_{\epsilon \to 0} \lim_{n \to \infty} \frac{1}{n} H_{\min}^{\epsilon}(A^n|B^n)_{\rho^{\otimes n}}. \tag{2.54}$$

It also shares some properties with the von Neumann entropy, particularly, it is also strongly subadditive:

$$H_{\min}^{\epsilon}(A|B) \geq H_{\min}^{\epsilon}(A|BC). \tag{2.55}$$

The smooth min-entropy is used to quantify operational tasks such as *privacy amplification* (also known as *randomness extraction*). It is the art of transforming a partially secure X into a fully secure key S, where X is a classical random variable on which an adversary has some partial information B. The fully secure key S appears completely random from the point of view of an adversary having access to the system B. Let us denote $l_{\text{extr}}^{\epsilon}(X|B)$ as the length of the fully secure key S which is ϵ-close to a string perfectly uniform and independent of B. One has [25]:

$$l_{\text{extr}}^{\epsilon}(X|B) = H_{\min}^{\epsilon'}(X|B) + O(\log 1/\epsilon) \tag{2.56}$$

for some $\epsilon' \in [\frac{1}{2}\epsilon, 2\epsilon]$. This result is relevant in the study of quantum key distribution protocols as it gives the secure key rate of the protocol. Unfortunately, the value of $H_{\min}^{\epsilon'}(X|B)$ is often difficult to compute.

2.2. Continuous-Variable Systems

The aim of this section is to present the formalism specific to the study of quantum information with the continuous variables of a bosonic system. Most of the content of this chapter can be found in the textbooks “Introductory Quantum Optics" by Gerry and Knight [7] and “Essential Quantum Optics" by Leonhardt [8].

A continuous-variable (CV) system of N canonical bosonic modes is described by a Hilbert space

$$\mathscr{H} = \bigotimes_{k=1}^{N} \mathscr{H}_k \tag{2.57}$$

resulting from the tensor product structure of infinite-dimensional Hilbert spaces $\mathscr{H}_k$'s, described by observables with continuous eigenspectra. One can think for instance to the

quantized electromagnetic field, whose Hamiltonian describes a system of N harmonic oscillators,

$$\mathcal{H} = \sum_{k=1}^{N} \hbar\omega_k \Big(\hat{a}_k^\dagger \hat{a}_k + \frac{1}{2}\Big), \tag{2.58}$$

where $\hbar$ is the reduced Planck's constant.

Here, $\hat{a}_k^\dagger$ and $\hat{a}_k$ are creation and annihilation operators of a photon in mode k (with frequency ω_k), which satisfy the commutation relation

$$[\hat{a}_k, \hat{a}_{k'}^\dagger] = \delta_{k,k'}, \qquad [\hat{a}_k \hat{a}_{k'}] = [\hat{a}_k^\dagger, \hat{a}_{k'}^\dagger] = 0. \tag{2.59}$$

The corresponding quadrature operators (position and momentum) for each mode are defined as

$$\hat{x}_k = \frac{1}{\sqrt{2}}(\hat{a}_k^\dagger + \hat{a}_k), \quad \hat{p}_k = \frac{i}{\sqrt{2}}(\hat{a}_k^\dagger - \hat{a}_k). \tag{2.60}$$

We can group together the canonical operators in the vector

$$\hat{R} = (\hat{x_1}, \hat{p_1}, ...\hat{x_N}, \hat{p_N})^\top, \tag{2.61}$$

which enables us to write a compact form of the bosonic commutation relations between the quadrature operators,

$$[\hat{R}_k, \hat{R}_l] = i\Omega_{kl} \tag{2.62}$$

where Ω is the symplectic form

$$\Omega := \bigoplus_{k=1}^{N} \omega, \quad \omega := \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}. \tag{2.63}$$

The space $\mathscr{H}_k$ is spanned by the Fock basis $\{|0\rangle_k, |1\rangle_k, ..., |n\rangle_k, ...\}$, where the Fock state $|n\rangle_k$ describes the state of n (indistinguishable) photons present in mode k. The Fock states are the eigenstates of the number operator $\hat{n}_k = \hat{a}_k^\dagger \hat{a}_k$, representing the Hamiltonian of the non-interacting mode, (Eq. (2.58)),

$$\hat{n}_k |n\rangle_k = n |n\rangle_k . \tag{2.64}$$

From Eqs. (2.59) and (2.64), one can derive the following relations

$$\hat{a}_k |n\rangle_k = \sqrt{n}\, |n-1\rangle_k , \quad \hat{a}_k^\dagger |n\rangle_k = \sqrt{n+1}\, |n+1\rangle_k . \tag{2.65}$$

The Fock states form a complete basis of orthonormal states,

$$\begin{aligned} \langle n|m\rangle &= \delta_{n,m}, \\ \sum_{n}^{\infty} |n\rangle \langle n| &= \mathbb{I}. \end{aligned} \tag{2.66}$$

The state containing no photons ($|0\rangle$) is called the vacuum state, for which $\hat{a}_k |0\rangle_k = 0$. The Fock basis of the global Hilbert space $\mathscr{H}$ is the tensor product of the Fock bases of the individual Fock spaces and its generic element is given by $|n_1, n_2, ..., n_N\rangle$, where $n_k \in \mathbb{N}$ for mode k. Using Eq. (2.65), one can define the multi-mode Fock state in the following way:

$$|n_1, n_2, ..., n_N\rangle = \frac{1}{\sqrt{n_1! n_2! ... n_N!}} \hat{a}_1^{\dagger n_1} \hat{a}_2^{\dagger n_2} ... \hat{a}_N^{\dagger n_N} |0\rangle \tag{2.67}$$

where $|0\rangle \equiv |0, 0, ...0\rangle$ is the global vacuum state.

From the commutation relation Eq. (2.62), one can rewrite the commutation relation between the quadrature operators as

$$[\hat{x}_i, \hat{x}_j] = [\hat{p}_i, \hat{p}_j] = 0, \quad [\hat{x}_i, \hat{p}_j] = i\delta_{i,j}, \tag{2.68}$$

which gives us the well-known Heisenberg uncertainty principle

$$\Delta\hat{x}\Delta\hat{p} \geq \frac{1}{2}|\langle[\hat{x}, \hat{p}]\rangle| = \frac{1}{2}, \tag{2.69}$$

where $\Delta A = \sqrt{\langle A^2\rangle - \langle A\rangle^2}$.

For the upcoming parts, we shall be only dealing with single-mode systems, thus the index k denoting a particular mode is omitted.

The eigenstates of the quadratures are

$$\hat{x} |x\rangle = x |x\rangle , \tag{2.70}$$

$$\hat{p} |p\rangle = p |p\rangle , \tag{2.71}$$

where $|x\rangle$ is a position eigenstate whereas $|p\rangle$ is a momentum eigenstate[3] and $x, p \in \mathbb{R}$. They give rise to two orthonormal bases

$$\langle x|x'\rangle = \delta(x - x'), \tag{2.72}$$

$$\langle p|p'\rangle = \delta(p - p'), \tag{2.73}$$

and provide two resolutions of the identity

$$\int_{\mathbb{R}} |x\rangle \langle x| \, dx = \mathbb{I} = \int_{\mathbb{R}} |p\rangle \langle p| \, dp. \tag{2.74}$$

The bases are related via a Fourier transformation

$$|p\rangle = \frac{1}{\sqrt{2\pi}} \int_{-\infty}^{\infty} dp e^{ixp} |x\rangle , \tag{2.75}$$

$$|x\rangle = \frac{1}{\sqrt{2\pi}} \int_{-\infty}^{\infty} dx e^{-ixp} |p\rangle . \tag{2.76}$$

[3]Strictly speaking, $|x\rangle$ and $|p\rangle$ are not proper eigenstates since they are non-normalizable, thus lies outside the Hilbert space.

The quadrature eigenstates are a useful tool in quantum mechanics because the wave function $\psi(x)$ of a quantum state $|\psi\rangle$ and its Fourier transform are $\psi(p)$ related to them

$$\psi(x) = \langle x|\psi\rangle \tag{2.77}$$
$$\psi(p) = \langle p|\psi\rangle. \tag{2.78}$$

The quadrature eigenstates play a major role in CV systems. Another important set of states are the eigenstates of the annihilation operator $\hat{a}$, which constitute the important set of *coherent states*. The states result from applying the single-mode *Weyl displacement operator* $D(\alpha)$ to the vacuum $|0\rangle$, $|\alpha\rangle := D(\alpha)\,|0\rangle$ where

$$D(\alpha) := e^{\alpha\hat{a}^\dagger - \alpha^*\hat{a}}, \tag{2.79}$$

and satisfy

$$\hat{a}\,|\alpha\rangle = \alpha\,|\alpha\rangle\,, \tag{2.80}$$

where $\alpha \in \mathbb{C}$.

Since, the displacement operator is unitary[4], one obtain

$$D^\dagger(\alpha) = D^{-1}(\alpha) = D(-\alpha). \tag{2.81}$$

Using the Baker-Campbell-Hausdorff formula, one can rewrite the displacement operator as

$$D(\alpha) = e^{-\frac{|\alpha|^2}{2}} e^{\alpha\hat{a}^\dagger} e^{-\alpha^*\hat{a}} = e^{\frac{|\alpha|^2}{2}} e^{-\alpha\hat{a}^\dagger} e^{\alpha^*\hat{a}} \tag{2.82}$$

and for any given two operators A and B, such that [A,[A,B]] = 0, one can write the following

$$e^A B e^{-A} = B + [A, B]. \tag{2.83}$$

Hence, the action of the displacement operator on the annihilation and creation operators reads

$$D^\dagger(\alpha)\hat{a}D(\alpha) = \hat{a} + \alpha, \tag{2.84}$$
$$D^\dagger(\alpha)\hat{a}^\dagger D(\alpha) = \hat{a}^\dagger + \alpha^*. \tag{2.85}$$

Therefore,

$$\hat{a}D(\alpha)\,|0\rangle = D(\alpha)(\hat{a} + \alpha)\,|0\rangle = \alpha D(\alpha)\,|0\rangle\,. \tag{2.86}$$

The displacement operator acts on the quadrature operators, in the following way

$$D^\dagger(\alpha)\hat{x}D(\alpha) = \hat{x} + \sqrt{2}\mathrm{Re}(\alpha), \tag{2.87}$$
$$D^\dagger(\alpha)\hat{p}D(\alpha) = \hat{p} + \sqrt{2}\mathrm{Im}(\alpha), \tag{2.88}$$

where $\mathrm{Re}(\alpha)$ and $\mathrm{Im}(\alpha)$ are the real and imaginary part of α respectively. We notice that, a coherent state is obtained by displacing a vacuum state by the amount $(d_x, d_p) =$

[4]the quantity $i(\alpha\hat{a}^\dagger - \alpha^*\hat{a})$ is Hermitian

$(\sqrt{2}\mathrm{Re}(\alpha), \sqrt{2}\mathrm{Im}(\alpha)$ along $(\hat{x}, \hat{p})$ quadratures. Using Eq. (2.82), we can write the coherent state in terms of the Fock basis,

$$|\alpha\rangle = e^{-\frac{1}{2}|\alpha|^2} \sum_{n=1}^{\infty} \frac{\alpha^n}{n!} |n\rangle . \tag{2.89}$$

Note that, coherent states have an undefined number of photons, but the average photon number of the field is

$$\bar{n} := \langle\alpha| \hat{n} |\alpha\rangle = |\alpha|^2, \tag{2.90}$$

while the probability of detecting n photons in a coherent state is given by

$$P_n = |\langle n|\alpha\rangle|^2 = e^{-|\alpha|^2} \frac{|\alpha|^{2n}}{n!}, \tag{2.91}$$

a Poisson distribution with mean and variance of $|\alpha|^2$.

Another interesting property of coherent states is that they are non-orthogonal, which means perfectly distinguishing two coherent states is impossible

$$\langle\beta|\alpha\rangle = e^{-\frac{1}{2}(|\alpha|^2+|\beta|^2-2\beta^*\alpha)} \neq 0. \tag{2.92}$$

However, they follow a closure relation,

$$\frac{1}{\pi} \int_{\mathbb{C}} |\alpha\rangle \langle\alpha| \, \mathrm{d}^2\alpha = \mathbb{I}, \tag{2.93}$$

implying that any state can be decomposed on the set of coherent states, hence forming an overcomplete basis.

2.2.1 Phase space representation

In classical Hamiltonian mechanics, the state of a particle is specified by its *canonical variables*: position x and momentum p. For N particles, the state is described by the $(x_1, \ldots, x_N)$ and $(p_1, \ldots, p_N)$, where the canonical variables satisfy the Poisson bracket relations :

$$\{x_i, x_j\} = \{p_i, p_j\} = 0, \quad \{x_i, p_j\} = \delta_{i,j}. \tag{2.94}$$

The only allowed transformations in Hamiltonian mechanics are the ones that leave these Poisson bracket invariant.

One can generalize these framework into quantum mechanics by the process of *canonical quantization*. The canonical variables are replaced by the quadrature operators $\hat{x}_i$ and $\hat{p}_i$. The Poisson bracket is replaced by the commutator and the relation between the quadratures is given by Eq. (2.68). Similar to the classical Hamiltonian mechanics, the only transformations allowed are the ones which keeps the symplectic form invariant.

Phase space is an abstract space used for representing states of a system in terms ordered pairs of positions and momenta. Due to the equivalence between quadrature operators, and position and momentum operators, it is convenient to employ phase space

representation for studying the behaviours of continuous-variable systems. Classically, a state can be represented as a point in phase space because both position and momentum of the state are allowed to have a precise value. However, this is not permitted in quantum mechanics because of the uncertainty principle. Phase space regions (whose area depends on the product of the uncertainties of the canonical operators) are thus typically adopted to represent pictorially a particular state.

The states of a CV system are the set of positive trace-class operators $\{\rho\}$ on the Hilbert space $\mathscr{H}$. However, the complete description of any quantum state ρ of such an infinite-dimensional system can be provided by one of its *s-ordered characteristic functions*

$$\chi_s(\xi) := Tr[\rho \hat{D}_\xi] e^{s\|\xi\|^2/2}, \tag{2.95}$$

where $\hat{D}_\xi$ is the Weyl operator, the generalized displacement operator for N modes and defined as

$$\hat{D}_\xi := e^{-i\xi^\top \Omega \hat{R}} \tag{2.96}$$

with $\xi \in \mathbb{R}^{2N}$ and $\|.\|$ is the norm. The real $2N$-dimensional space equipped with the symplectic form Ω: $\Xi = (\mathbb{R}^{2N}, \Omega)$, is called quantum *phase space*, in analogy with the Liouville phase space of classical Hamiltonian mechanics. One can see from the definition of the characteristic functions that in the phase space picture, the tensor product structure is replaced by a direct sum structure, so that the N-mode phase space is $\Xi = \oplus_k \Xi_k$ where $\Xi_k = (\mathbb{R}^2, \omega)$ is the local phase space associated with mode k.

The family of *characteristic functions* is in turn related, via complex Fourier transform, to the quasi-probability distributions W^s, which constitute another set of complete descriptions of the quantum states. Here, $s = 0$ corresponds to the so-called 'Wigner function', while $s = 1$ gives us Glauber-Sudarshan 'P-representation'. These distributions are referred as 'quasi'-probability because they sum up to unity, yet do not behave entirely as one would expect from probability distributions, for instance, there are (infinitely many) quantum states for which the Wigner function assumes negative values.

The Wigner function for a given state ρ is defined as

$$W_\rho(\xi) := \frac{1}{(2\pi)^N} \int d^{2N}\zeta e^{i\xi^T \Omega \zeta} \chi_0(\zeta). \tag{2.97}$$

For an N-mode bosonic quantum system, the Wigner function can be written as follows in terms of the position eigenvectors $|x\rangle$ of the quadrature operators $\{\hat{x}_j\}$

$$W_\rho(x_1, p_1, ..., x_N, p_N) = \frac{1}{\pi^N} \int_{\mathbb{R}^N} \langle x - x' | \rho | x + x' \rangle e^{2ix'p} \, d^N x', \tag{2.98}$$

$$= \frac{1}{\pi^N} \int_{\mathbb{R}^N} \psi^*(x + x') \psi(x - x') e^{2ix'p} \, d^N x'. \tag{2.99}$$

For a comprehensive discussion about the Wigner function and its properties, refer to [9].

Note that, the Wigner function depends on a finite number of variables, thus easier to manage compared to the density matrix, which due to the infinite-dimensionality of

the Hilbert space has infinite variables. Since the Wigner function provides the same information as ρ, one can simply use the Wigner functions as an alternative for ρ.

As witnessed, there exist two different space representations for CV systems: phase space and Fock space. Therefore, there are two main types of measurements one can perform on CV states. One can measure the photon number of the state, or one can measure a quadrature of the state in phase space, known as homodyne measurement.

In a homodyne measurement, the measurement operators are projectors over the quadrature basis $|x\rangle\langle x|$ (or $|p\rangle\langle p|$). The outcome probability of the results is obtained by integrating the Wigner function over the quadratures that have not been measured. For a single mode state, one finds:

$$\int_{-\infty}^{\infty} dp\, W_\rho(x,p) = \mathrm{tr}[\rho\,|x\rangle\langle x|], \tag{2.100}$$

$$\int_{-\infty}^{\infty} dx\, W_\rho(x,p) = \mathrm{tr}[\rho\,|p\rangle\langle p|], \tag{2.101}$$

which in the case of a pure state, is $|\psi(x)|^2$ and $|\psi(p)|^2$ respectively.

One can generalize the above result, for a partial homodyne measurement on a multimode N bosonic system,

$$P(x_1,p_N) = \int W(x_1,...,x_N,p_1,...,p_N)dx_2dx_3...dx_Ndp_1dp_2...dp_{N-1}. \tag{2.102}$$

We will discuss in detail about these measurements at the end of the section.

To recover the trace of the state, one has to integrate the Wigner function over the whole phase space

$$\int d\xi\, W_\rho(\xi) = \mathrm{tr}[\rho] = 1. \tag{2.103}$$

For a mixed state, $\rho = \sum_i p_i\rho_i$, the Wigner function reads

$$W_\rho(\xi) = \sum_i p_i\, W_{\rho_i}(\xi). \tag{2.104}$$

2.2.2 Gaussian states

Gaussian states are particularly relevant to the study of continuous-variable quantum systems, both, experimentally and theoretically. These states are called as Gaussian because the characteristic function (and subsequently, the Wigner function) is a Gaussian function in phase-space.

The state can therefore be completely characterized by the first two moments: mean and variance (uncertainties). Given a density operator ρ, we define the displacement vector (the mean value), $d \in \mathbb{R}^{2N}$

$$d := \langle\hat{R}\rangle = \mathrm{tr}[\rho\hat{R}] \tag{2.105}$$

and the $2N \times 2N$ covariance matrix γ:

$$\gamma_{\alpha\beta} := \langle\{\Delta\hat{R}_\alpha, \Delta\hat{R}_\beta\}\rangle, \tag{2.106}$$

where $\Delta\hat{R}_\alpha := \hat{R}_\alpha - \langle\hat{R}_\alpha\rangle$ and $\langle\hat{R}_\alpha\rangle = tr(\hat{R}_\alpha\rho)$. The diagonal element provides the variance of the quadrature operators. Then, the Gaussian states are described by the following Gaussian characteristic function

$$\chi_\rho(\xi) = e^{(-\frac{1}{4}\xi^\top\Gamma\xi + iD^T\xi)}, \tag{2.107}$$

where $\Gamma = -\Omega\gamma\Omega^\top$ and $D = \Gamma d$ and the Wigner form of Gaussian state reads

$$W(R) = \frac{1}{\pi^{2N}\det(\gamma)} e^{-(R-d)^\top\gamma^{-1}(R-d)}. \tag{2.108}$$

As we can see from the definitions, despite the infinite dimensionality of the Hilbert space, a complete description of a Gaussian state of N modes, requires only a finite number of parameters, which is quadratic in N.

Note that, although the covariance matrix is $2N \times 2N$ positive-semidefinite symmetric matrix, all such matrices do not fulfill the criteria to be a covariance matrix. A physical system must obey the uncertainty principle, therefore a covariance matrix must also obey the uncertainty relation, which in case of continuous-variable system reads as [10]

$$\gamma + i\sigma \geq 0. \tag{2.109}$$

This can be easily shown by expanding the form of γ, using the non-negativity of ρ and assuming, without loss of generality that the first-order moment value (d) as zeros. This is a necessary and sufficient condition which has to be satisfied by the covariance matrix of a physical Gaussian state; in fact, this is also a necessary condition for non-Gaussian states.

Using Williamson's theorem [11] we can diagonalize the covariance matrix. It states that, for every positive and symmetric matrix, there exists a symplectic operator S such that

$$S\gamma S^\top = v = \bigoplus_{k=1}^{N} \begin{pmatrix} v_k & 0 \\ 0 & v_k \end{pmatrix} \tag{2.110}$$

where v_k are the symplectic eigenvalues and form the symplectic spectrum of γ.

An operator is called symplectic if the symplectic form (Eq. (2.63)) remains invariant under its action

$$S\Omega S^\top = \Omega. \tag{2.111}$$

Given a symplectic matrix S, the matrices $S^{-1}, S^\top$ and $-S$ are also symplectic. Using Eq. (2.111) and $\Omega^\top\Omega = \mathbb{I}$, we get, $S^{-1} = -\Omega S^\top\Omega$. The set of symplectic operators forms a group denoted $\mathrm{Sp}(2N, \mathbb{R})$.

The symplectic eigenvalues are the eigenvalues of the operator $|i\Omega\gamma|$, where $|A| = \sqrt{A^\dagger A}$. Thus, one can rewrite the uncertainty principle in terms of symplectic eigenvalues as

$$v_k \geq 1, \quad \text{for } k = 1, ..., N. \tag{2.112}$$

Another way of finding the symplectic eigenvalues is to use the symplectic invariants, quantities which remain invariant under the action of $Sp(2N, \mathbb{R})$. One such quantity is the determinant of the covariance matrix,

$$\det(\gamma) = \det(v) = \prod_{k}^{N} v_k^2 \tag{2.113}$$

since, $\det(S) = 1$.[5].

One-mode Gaussian states

Here, we review the single-mode states with their corresponding displacement vector d and covariance matrix γ. The vacuum state is charaterized by d=(0,0) and $\gamma = \mathbb{I}$, the position and momentum variances equate to 1. This is the minimum value that the quadratures can reach symmetrically known as the quantum shot noise.

Coherent states being displaced vacuum states has the same covariance matrix as that vacuum states $\gamma = \mathbb{I}$ with non-zero displacement vectors in phase-space, $d = (d_x, d_p)$. A generalization of the coherent states is given by the squeezed coherent states which have a covariance matrix of the form

$$\gamma = \begin{pmatrix} e^{-2s} & 0 \\ 0 & e^{2s} \end{pmatrix}, \tag{2.114}$$

where s is the squeezing parameter. Depending on the parameter s, we call the coherent state $\hat{x}$-squeezed ($s >0$) or $\hat{p}-$squeezed ($s < 0$) and for $s = 0$, we recover the coherent state. The squeezed vacuum states also have the same covariance matrix but with d=(0,0).

Another useful one-mode Gaussian states are thermal states characterized by null displacement vector and covariance matrix

$$\gamma = \begin{pmatrix} V & 0 \\ 0 & V \end{pmatrix} \tag{2.115}$$

with $V = 2\bar{n} + 1, \bar{n}$ is the mean photon number of the state. For $\bar{n} = 0$, we recover the vacuum state.

The symplectic eigenvalue for a single-mode state is given by

$$v_1 = \sqrt{\det(\gamma)}. \tag{2.116}$$

Two-mode Gaussian states

A general two-mode Gaussian state can be characterized by the displacement vector $d = (d_{x_1}, d_{p_1}, d_{x_2}, d_{p_2})$ and the covariance matrix γ_{12}

$$\gamma = \begin{pmatrix} \gamma_1 & C \\ C^\top & \gamma_2 \end{pmatrix} \tag{2.117}$$

[5]all matrices in $\mathrm{Sp}(2N, \mathbb{R})$ have determinant 1

where $\gamma_{1,2}$ is the variance of the corresponding mode and C is a 2×2 real matrix that gives the correlation between the two modes. The case $C = 0$ corresponds to a tensor product of two one-mode Gaussian states

$$\rho_{12} = \rho_1 \otimes \rho_2. \tag{2.118}$$

To find the symplectic eigenvalues of two-mode Gaussian states, we define another symplectic invariant [12]

$$\Delta = v_1^2 + v_2^2 = \det(\gamma_1) + \det(\gamma_2) + 2\det(C) \tag{2.119}$$

and we already have

$$\det(\gamma_{12}) = v_1^2 v_2^2. \tag{2.120}$$

It is easy to see that the square of the symplectic eigenvalues are the roots of the following quadratic equation

$$y^2 - \Delta y + \det(\gamma_{12}) = 0, \tag{2.121}$$

which gives us

$$v_{1,2}^2 = \frac{1}{2}\left[\Delta \pm \sqrt{\Delta^2 - 4\det(\gamma_{12})}\right]. \tag{2.122}$$

Two-mode squeezed states play a vital role for practical implementation of many CV protocols. The state is characterized by a null displacement vector and the covariance state

$$\gamma_{TMSS} = \begin{pmatrix} \cosh 2s\ \mathbb{I}_2 & \sinh 2s\ \sigma_z \\ \sinh 2s\ \sigma_z & \cosh 2s\ \mathbb{I}_2 \end{pmatrix}, \quad \text{where } \sigma_z = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}. \tag{2.123}$$

Multi-mode Gaussian states

One can generalize the previous definitions to a system of N modes [13]. The symplectic invariants $\Delta_i^N (i = 1...N)$ for a multi-mode Gaussian state can be obtained by calculating the principal minor of order $2k$ for the matrix $\Omega\gamma$,

$$\Delta_i^N = M_{2k}(\Omega\gamma). \tag{2.124}$$

Therefore, the relation between symplectic eigenvalues and the symplectic invariants reads

$$\Delta_i^N(v_1, ..., v_N) = \sum_{\mathscr{S}_i^N} \prod_{j \in \mathscr{S}_i^N} v_j^2. \tag{2.125}$$

The sum is taken over all possible i-subsets $\mathscr{S}_i^N$ of the first N natural integers (over all possible combination of i integers). Then we can solve a polynomial equation of degree N whose roots are the symplectic eigenvalues.

Though there is a possibility of N modes being distributed over N different parties, most often, we encounter cases where the N modes are distributed over two parties, such as in the case of key distribution protocols.

For a bipartite multi-mode $(N_A + N_B)$ Gaussian state, the covariance matrix reads

$$\gamma = \begin{pmatrix} \gamma_A & C \\ C^\top & \gamma_B, \end{pmatrix} \tag{2.126}$$

with $\gamma_{A(B)}$ are the local covariance matrices of $N_{A,(B)}$ modes and C is the correlation matrix between the two parties A and B.

2.2.3 Gaussian operations

Quantum operations that map any Gaussian state to a Gaussian state are called Gaussian operations. Since Gaussian states are easy to characterize, it turns out that a large class of transformations acting on these states are easy to characterize too. These include operations that can be performed by linear optical tools such as phase shifts, beamsplitters, squeezers along with homodyne measurements. The study of these operators is particularly relevant because these can be implemented experimentally with present technology.

Symplectic Operations

An operation is Gaussian if it transforms Gaussian states to Gaussian states. These are generated from Hamiltonians $\mathcal{H}$ which are second order polynomials in field operators, via $U = \exp(-i\mathcal{H}/2)$. As a consequence of the Stone-von Neumann theorem, any such unitary transformation corresponds to a displacement operation $\hat{D}_\xi$ in phase space and a symplectic operation (matrix) $S \in Sp(2N, \mathbb{R})$ which acts on the quadrature operator as follows:

$$\hat{R} \to S\hat{R} + \xi. \tag{2.127}$$

In terms of moments, under a Gaussian operation, a Gaussian state with mean value d and covariance matrix γ transforms into a Gaussian state with displacement vector d' and covariance matrix γ'

$$d' = Sd + \xi, \tag{2.128}$$

$$\gamma' = S\gamma S^\top. \tag{2.129}$$

An important subset of symplectic transformations which are also orthogonal forms a special group of transformations, $K(N) := Sp(2N, \mathbb{R}) \cap O(2N)$, which preserves the total photon number of a state. Such transformations include phase rotations and beamsplitter interactions.

Phase Rotation is a single-mode operation equivalent to rotation of the phase-space, characterized by the parameter θ. The symplectic transformation $S_{PR}(\theta) \in \mathrm{Sp}(2, \mathbb{R})$ reads

$$S_{PR}(\theta) := \begin{bmatrix} \cos\theta & \sin\theta \\ -\sin\theta & \cos\theta \end{bmatrix} \tag{2.130}$$

and the corresponding unitary transformation is $U_{PR}(\theta) := \exp(-i\theta\hat{a}^\dagger\hat{a})$.

A **beamsplitter** transformation of transmittance T makes a coherent combination of two modes and is described by the symplectic operator $S_{BS}(T) \in \mathrm{Sp}(4,\mathbb{R})$

$$S_{BS}(T) = \begin{bmatrix} \sqrt{T}\mathbb{I}_2 & \sqrt{1-T}\mathbb{I}_2 \\ -\sqrt{1-T}\mathbb{I}_2 & \sqrt{T}\mathbb{I}_2 \end{bmatrix} \tag{2.131}$$

the corresponding unitary transformation is $U_{BS}(\theta) = \exp[\theta(\hat{a}^\dagger\hat{b} - \hat{a}\hat{b}^\dagger)]$, where $\hat{a}$ and $\hat{b}$ are the annihilation operators of the two modes and $T = \cos^2\theta \in [0,1]$.

There exists another subset of symplectic operators which does not preserve the photon number of the state rather inject photons in the system, e.g., squeezing operations. A **single-mode squeezing** Gaussian unitary reads

$$U_{sq}(s) := \exp[s(\hat{a}^2 - \hat{a}^{\dagger 2})] \tag{2.132}$$

and the corresponding symplectic operator is

$$S_{sq}(s) := \begin{bmatrix} e^{-s} & 0 \\ 0 & e^{s} \end{bmatrix}, \tag{2.133}$$

where s is the squeezing parameter. The one-mode squeezed vacuum state is obtained by applying the squeezing operator to a vacuum state, which in the Fock basis reads

$$U_{sq}(s)\,|0\rangle := \frac{1}{\sqrt{\cosh s}} \sum_{n=0}^{\infty} \frac{\sqrt{(2n)!}}{2^n n!} \tanh^n s\,|2n\rangle\,. \tag{2.134}$$

The mean photon number is $\bar{n} = \sinh^2 s$, positive for non-zero s.

The Gaussian unitary for the **two-mode squeezing** operator is given by

$$U_{sq2}(s) := \exp[s(\hat{a}\hat{b} - \hat{a}^\dagger\hat{b}^\dagger)] \tag{2.135}$$

and the corresponding symplectic operator is given by

$$S_{sq2}(s) := \begin{bmatrix} \cosh s\mathbb{I}_2 & \sinh s\sigma_z \\ \sinh s\sigma_z & \cosh s\mathbb{I}_2 \end{bmatrix}. \tag{2.136}$$

By applying $S_{sq2}(s)$ to a couple of vacuum states, one obtains a two-mode squeezed vacuum state (TMSS), also known as the EPR state

$$|\mathrm{TMSS}\rangle = U_{sq2}(s)\,|0,0\rangle = \sqrt{1-\lambda^2} \sum_{n=0}^{\infty} (-\lambda)^n\,|n,n\rangle\,, \tag{2.137}$$

where $\lambda = \tanh s$. TMSS play a central role in many CV protocols. It has the same significance as the Bell state $|\Phi^+\rangle = (|00\rangle + |11\rangle)/\sqrt{2}$.

On tracing out one of the two modes of a two-mode squeezed state, we obtain the following mixed state

$$\rho = \frac{1}{\cosh s} \sum_{n=0}^{\infty} \tanh^{2n} s\,|n\rangle\langle n|\,. \tag{2.138}$$

The average photon number turns out to be $\bar{n} = \cosh s - 1$, the one can rewrite the mixed state as

$$\rho = \sum_{n=0}^{\infty} \frac{\bar{n}^n}{(\bar{n}+1)^{n+1}} |n\rangle \langle n| , \tag{2.139}$$

which is exactly the equation of a thermal state with a Bose-Einstein distribution.

Any N-mode symplectic operation can be decomposed as

$$S = P_1 \left(\bigoplus_{i=1}^{N} \begin{bmatrix} e^{-s_i} & 0 \\ 0 & e^{s_i} \end{bmatrix} \right) P_2 \tag{2.140}$$

where $P_1, P_2 \in K(N)$ and $s_i \in \mathbb{R}^N \; \forall \; i$. It means any Gaussian unitary can be applied by a passive linear interferometer, followed by a parallel set of single-mode squeezers over N modes and a second passive transformation.

Completely Positive Maps

The set of unitary operations does not contain all the transformations that can be applied to a quantum state. The most general transformation (even measurement) is defined by a map $\mathcal{E} : \rho \to \mathcal{E}(\rho)$, which is completely positive (CP) and trace-decreasing map. A quantum operation is then called a channel when it preserves the trace of the state, i.e., $\mathrm{tr}[\mathcal{E}(\rho)]$ =1. The maps which are reversible form the set of unitary operations.

The Gaussian CP maps are characterized by two $2N \times 2N$ matrices X and Y, which transforms a Gaussian state (d, γ) to a Gaussian state (d', γ') as

$$d' = Xd \tag{2.141}$$

and

$$\gamma' = X\gamma X^\top + Y. \tag{2.142}$$

Y is a symmetric matrix and the positivity of the map is satisfied if the following relation holds

$$Y + i\Omega - iX\Omega X^\top \geq 0. \tag{2.143}$$

A Gaussian channel also preserves the Gaussian characteristics of the states. Now, we describe some of the important Gaussian channels:

- A *pure loss channel* of transmittance T is characterized by $X = \sqrt{T}\mathbb{I}$ and $Y = (1-T)\mathbb{I}$. It is modeled by combining the signal with a vacuum on a beamsplitter of transmittance T and the tracing out the second output mode.

- An *amplification channel* with amplification factor $\eta \geq 1$ is characterized by $X = \sqrt{\eta}\mathbb{I}$ and $Y = (1-\eta)\mathbb{I}$. It can be modeled by injecting the input signal into a two-mode squeezed with a squeezing factor such that $\eta = \cosh^2 s$ for which the idler mode is traced out.

  Quantum amplification channels are at the core of several physical processes. They not only model the optical process of spontaneous parametric down-conversion in

non-linear systems, but the transformation corresponding to an amplifier channel also describes the physics of the dynamical Casimir effect in superconducting circuits, the Unruh effect, and Hawking radiation.

- A realistic model for Gaussian quantum channels that typically occur in experiments is given by a *thermal noise channel* of transmittance T and excess noise ξ is characterized by $X = \sqrt{T}\mathbb{I}$ and $Y = T\chi\mathbb{I}$, where χ is the added noise referred to the input
$$\chi = \frac{1-T}{T} + \xi. \tag{2.144}$$
It can be modeled by combining a thermal state of variance $N = T\chi/(1-T)$ with the input state via a beamsplitter of transmittance T.

Measuring Gaussian states

The most general quantum measurement is described as a POVM. In CV systems, quantum measurements are mostly described by continuous outcomes $i \in \mathbb{R}$, making the probability outcomes p_i a probability density. A measurement is said to be Gaussian, if the outcome obtained after measuring Gaussian states follows Gaussian distribution. These are the measurements that are typically performed in the lab.

A **Homodyne Measurement** measures a quadrature ($\hat{x}$ or $\hat{p}$) of the state in phase-space. Its measurement operators are projectors over the quadrature basis $|x\rangle\langle x|$ (or $|p\rangle\langle p|$). The corresponding outcome probability is given by the marginal integral of Wigner distribution over the conjugate quadrature:

$$P(x) = \int dp\, W(x,p), \qquad P(p) = \int dp\, W_\rho(x,p), \tag{2.145}$$

where the probability density $P(x)$ and $P(p)$ follow Gaussian distribution.

Experimentally, a homodyne measurement is implemented by combining the target signal mode $(\hat{x}_S, \hat{p}_S)$ with a local oscillator with quadratures $(E_L\cos\theta, E_L\sin\theta)$ into a balanced beamsplitter ($T = 1/2$) to obtain the outgoing modes

$$\begin{aligned}
\hat{x}_+ &= (\hat{x}_S + E_L\cos\theta)/\sqrt{2} \\
\hat{p}_+ &= (\hat{p}_S + E_L\sin\theta)/\sqrt{2} \\
\hat{x}_- &= (\hat{x}_S - E_L\cos\theta)/\sqrt{2} \\
\hat{p}_- &= (\hat{p}_S - E_L\sin\theta)/\sqrt{2}
\end{aligned}$$

and measuring the intensity of the outgoing modes using two photodetectors

$$I_\pm = \hat{n}_\pm = \frac{1}{2}(\hat{x}_\pm^2 + \hat{p}_\pm^2 - 1). \tag{2.146}$$

where we take proportionality constant equal to 1 for simplicity. The difference between the two intensities gives us the value of the homodyne detection

$$\Delta I = I_+ - I_- = \hat{x}_S E_{LO}\cos\theta + \hat{p}_S E_{LO}\sin\theta. \tag{2.147}$$

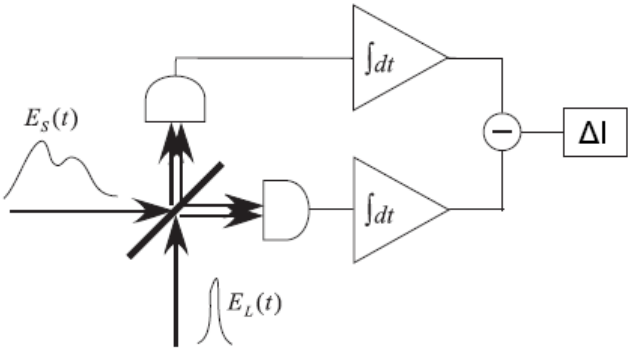


Figure 2.2: Homodyne detection setup (from Ref [14]).

The phase θ can be adjusted using a piezoelectric transducer, and depending on the choice of $\theta = 0$ or $\pi/2$, one can either measure $\hat{x}_S$ or the $\hat{p}_S$. In principle, any rotated quadrature $\hat{x}_\theta = \hat{x}_s \cos\theta + \hat{p}_s \sin\theta$ can be measured via a homodyne measurement using suitable phase between the signal and the local oscillator.

Let us assume a bipartite $(N_A + N_B)$-mode Gaussian state, with $N_A, N_B \geq 1$, which is characterized by the displacement vector $d = (d_A, d_B)$ and the covariance matrix, given by Eq. (2.126)

$$\gamma = \begin{pmatrix} \gamma_A & C \\ C^\top & \gamma_B \end{pmatrix}. \tag{2.148}$$

Suppose, one measures the B-part (all N_B modes) of the state using homodyne measurement measuring $\hat{x}$-quadrature, one obtains the result $m_B = (x_1, 0, x_2, 0, ..., x_{N_B}, 0)$. Then the A-part of the state transforms into ρ'_A which is characterized by the displacement vector

$$d' = d_A + C(X\gamma_B X)^{MP}(m_B - d_B) \tag{2.149}$$

and the covariance matrix

$$\gamma'_A = \gamma_A - C(X\gamma_B X)^{MP} C^\top \tag{2.150}$$

where $X = \text{diag}(1,0,1,0,...1,0)$, keeps tracks of which quadratures were measured and MP denotes the inverse on range. Note that, the covariance matrix of the new state ρ'_A does not depend on the measurement result m, which is one of the properties of Gaussian states.

Heterodyne measurement[15] is a generalized POVM that projects onto coherent states

$$E(\alpha) = \frac{1}{\pi} |\alpha\rangle \langle\alpha| , \tag{2.151}$$

with

$$\mathbb{I} = \frac{1}{\pi} \int_{\mathbb{C}} |\alpha\rangle \langle\alpha| \, d\alpha. \tag{2.152}$$

It can be understood as two different homodyne measurements ($\hat{x}$ and $\hat{p}$) where the states measured are a coherent combination of the signal mode and a vacuum ancillary mode via a balanced beamsplitter.

If one performs heterodyne measurements on B-part of the above-mentioned Gaussian state to obtain the result $m = (x_1, p_1, x_2, p_2, ..., x_n, p_n)$. Then the state $\rho_A \to \rho'_A$ is charaterized by the displacement vector

$$d' = d_A + \sqrt{2}C(\gamma_B + \mathbb{I}_{2N_B})^{-1}(m - d_B) \tag{2.153}$$

and the covariance matrix

$$\gamma'_A = \gamma_A - C(\gamma_B + \mathbb{I}_{2N_B})^{-1}C^\top. \tag{2.154}$$

The covariance matrix does not depend on the measurement outcome, similarly to the homodyne case.

Therefore, given a $(N_A + N_B)$-mode Gaussian state, with $N_A, N_B \geq 1$, if a Gaussian measurement is performed on N_A modes, then the classical outcome is a Gaussian distribution and the unmeasured N_B modes are still left in Gaussian state.

Counting and Detecting Photons. One can count the number of photons using the POVM corresponding to the Fock basis $\{|0\rangle\langle 0|, |1\rangle\langle 1|, ..., |n\rangle\langle n|, ...\}$. However, such measurements are extremely challenging to implement. Therefore, the detection of photons, given by the POVM $\{|0\rangle\langle 0|, \mathbb{I} - |0\rangle\langle 0|\}$ seems easier to implement, which just distinguishes between the presence or the absence of photons. The quality of a detector depends on two factors: the detection efficiency and dark counts, spontaneous clicks in the absence of a photon. The current state of the art superconducting nanowires single photon-detectors (SNSPD) has high detection efficiency of 93% and low dark count rate of less than 1 click per second at near-infrared wavelengths [16].

2.2.4 Entropy of Gaussian states

Unlike Shannon entropy, we don't need to introduce a new function to calculate entropy for continuous-variable system, since the Fock space though infinite is countable. We restrict ourselves to Gaussian states.

A Gaussian state is characterized by its two moments. However, the entropy of a Gaussian state depends only on the covariance matrix. The entropy of a Gaussian state remains invariant under the action of the displacement operator, which is an unitary operator[6],

$$S(\rho) = S(D(\alpha)^\dagger \rho D(\alpha)), \tag{2.155}$$

meaning the mean value does not account in entropy calculation. Thus, for simplification, we consider Gaussian states with zero mean value, $\rho_G(0, \gamma)$.

A Gaussian state with null mean value can be described as a product of thermal state with covariance matrix v, which is the diagonalized form of the covariance matrix

[6] trace operation is invariant under unitary transformation

γ, given by Eq. (2.110)

$$S\gamma S^\top = v = \bigoplus_{k=1}^{N} \begin{pmatrix} v_k & 0 \\ 0 & v_k \end{pmatrix}. \tag{2.156}$$

Therefore, finding the entropy of any Gaussian state equates to finding the entropy of the product of the thermal states. Recall from Eq. (2.139) that the density operator of a thermal state is

$$\rho_{th} = \sum_{n=0}^{\infty} \frac{\bar{n}^n}{(\bar{n}+1)^{n+1}} |n\rangle \langle n|, \tag{2.157}$$

where the mean number and the symplectic eigenvalue is related by $v = 2\bar{n} + 1$. The entropy thus reads

$$\begin{aligned} S(\rho_{th}) &= -\sum_{n=0}^{\infty} \frac{\bar{n}^n}{(\bar{n}+1)^{n+1}} \log_2 \frac{\bar{n}^n}{(\bar{n}+1)^{n+1}} \\ &= (\bar{n}+1)\log_2(\bar{n}+1) - \bar{n}\log_2 \bar{n}. \end{aligned} \tag{2.158}$$

Therefore, von Neumann entropy of a Gaussian state is,

$$S(\rho_G) = \sum_{k=1}^{N} S(\rho_{th}(\bar{n}_k)) = G(\bar{n}_k = (v_k - 1)/2), \tag{2.159}$$

where $G(x)$ is

$$G(x) = (x+1)\log_2(x+1) - x\log_2 x. \tag{2.160}$$

2.3. Semidefinite Programs

In this section, we briefly acquaint ourselves with the field of semidefinite programming from an information-theoretic prospect and how this helps us to solve quantum information problems, more specifically, to obtain the numerical bounds. The methodology applies to both cryptographic tasks: QKD and quantum money. For a detailed study, refer to the lecture notes by Watrous [18] for a simple introduction to the field, while the book by Vandenberghe and Boyd [19] provides a deeper understanding of general convex optimization.

In quantum cryptography, security analysis involves dealing with optimization over density operators, POVM's, CPTP maps, all of which are positive semidefinite matrices. Semidefinite programming provides a methodology to construct such optimization problems over positive semidefinite variables, constrained to some linear conditions.

The set of positive semidefinite matrices form a *convex cone* $\mathscr{C}$, defined as a subset of a vector space that is closed under linear combinations with positive coefficients. Specifically, it means that, given any operators $X, Y \in \mathscr{C}$, the operator $\alpha X + \beta Y$ also belongs in $\mathscr{C}$, for positive scalars α and β.

Let us now define an *affine slice* $\mathscr{A}$, which is a subset of a general vector space, satisfying

$$Z \in \mathscr{A} \Rightarrow \Lambda(Z) = C, \tag{2.161}$$

where operator $C \in \mathscr{V}$ and Λ is linear map. Thus, an affine slice satisfies a particular linear constraint.

Semidefinite programming is a convex optimization problem, where one optimizes a linear convex objective function over all operators which lie in the intersection of the convex cone of positive semidefinite matrices with an affine slice.

2.3.1 Primal and Dual SDP

Let us suppose we want to minimize $C(X)$ over all possible values of X given that $X \in \mathscr{V}$ and follows some linear constraints, where C is a linear operator belonging to the vector space $\mathscr{V}$. One can think of X as a matrix, or equivalently, as an array of n^2 components of the form $(x_{11}, ..., x_{nn})$. Both visualizations of X are useful. Then, one can rewrite $C(X)$ as

$$C(X) = \sum_{i,j} C_{ij} X_{ij} = \text{tr}(C^\dagger X), \tag{2.162}$$

which serves as our objective function, while X fulfills the role of the variable.

One of the constraints of X is that it is positive semidefinite, meaning it is Hermitian. Then, without loss of generality, we can also assume that C is a symmetric matrix. And let us consider the set of linear constraints is given by the symmetric matrices $A_1, A_2, ..., A_m$ and reals $b_1, b_2, ..., b_m$. Then the SDP (primal form) concerning the minimization of objective function reads,

$$\begin{aligned} &\min \text{tr}(C^\dagger X) \\ &s.t.\ \ A_i X = b_i,\ i = 1, ..., m \\ &\qquad X \geq 0. \end{aligned} \tag{2.163}$$

Any operator X satisfying the above constraints is said to be *primal feasible*, and the set containing such operators is termed as primal feasible set S_p. The *primal optimal value* s_p is defined as the infimum of over all possible values of objective function for all $X \in S_p$.

Interestingly, similar to linear programming, semidefinite programs have an elegant dual structure, which associates a dual optimization problem to each primal optimization problem.

The dual problem is obtained by forming the Lagrangian of a minimization problem by using non-negative Lagrange multipliers, to add the constraints to the objective function. Then, the new problem is to maximize the new objective function with respect to the dual variables (Lagrange multipliers) under the derived constraints on the dual variables (including at least the non-negativity constraints). Therefore, for the primal problem mentioned in Eq. (2.163), the corresponding dual problem reads,

$$\begin{aligned} &\max \sum_{i=1}^{m} b_i y_i = b^\top y \\ &s.t.\ \ C - \sum A_i y_i \geq 0. \end{aligned} \tag{2.164}$$

The dual variables are real numbers for this problem. However, there might be scenarios when b_i's are matrices, in these types of cases, the dual variables are Hermitian matrices.

Similar to primal terminology, dual variables satisfying the constraints are known as *dual feasible* and belongs to the dual feasible set S_d. The *dual optimal value* s_d is defined as the supremum of over all possible values of objective function for all $\{y_1, ..., y_m\}$, where $y_i \in \mathbb{R}$.

Weak duality vs strong duality: The Lagrange multiplier method helps us to find the local extremum for a constrained function. Therefore, the optimal value of the primal problem lower bounds the optimal value of the dual problem, while the optimal value of the dual upper bounds that of the primal. This can be simply expressed as,

$$s_p \geq s_d. \tag{2.165}$$

This is termed as *weak duality*.

Under some conditions on the sdp, one can even have *strong duality* implying that both values coincide,

$$s_p = s_d. \tag{2.166}$$

CHAPTER 3

QUANTUM CRYPTOGRAPHY

Primarily, cryptography meant studying techniques for encryption of secret texts (communication), from something meaningful to completely meaningless to anyone other than the recipients. However, over time, it encompassed everything needed for secure communication, even in the presence of third parties called adversaries or eavesdroppers, such as authentication, secret-sharing, key distribution, counterfeiting, confidentiality, to name a few. With the ever-increasing success of technologies, cryptography plays an indispensable role in this Information age. Every day billions of people are performing sensitive tasks - online banking, secret messaging, data storing, digital signatures. Therefore, a considerable amount of human resources and capital are being invested in creating and analyzing cryptographic protocols. The idea of security is paramount to any of these tasks. Therefore, for any protocol, a rigorous definition of security is fundamental.

One of the primitive cryptographic tasks is establishing a secret communication between two spatially separated parties even in the presence of a possible eavesdropper, conventionally named Eve. Let us call them Alice and Bob. To accomplish this task, they establish a *secret key*, which is done by a *key distribution* protocol. Using only classical resources, the security of the key can only be provided for a finite period, as it relies on the hardness of the encryption function. Such encryption functions are chosen which are challenging to solve and time-consuming such as the RSA encryption scheme, based on factorization problem of large numbers. Problems that are hard to solve but not impossible thus provides security over a limited timescale of interest but not everlasting. This is known as *computational security*.

However, with the help of a one-time pad symmetric encryption-decryption scheme (XOR), one can have *unconditional security*[1], although with some conditions: the key and the message must be strings of the same length and kept secret, the key should also be random, and only used once. This type of security is also known as *information-theoretic security* which means that the adversary can not learn anything about the message

[1]This type of security does not depend on adversary's computational assumptions. Also known as everlasting security, since the security has not been compromised by over the elapsed time since the communication.

except with negligible property, a stronger security condition than the computational security. Note that, there are requirements on the randomness and the security of the key. One can only achieve these requirements using quantum resources.

Wiesner, in the early '70s, introduced the novel concept of encoding information on quantum observables [46]. More specifically, he showed that by encoding information on two non-commuting observables (conjugate variables), one can exploit the inherent properties of quantum mechanics to get unconditional security for cryptographic tasks. Recall that, for any two non-commuting observables A and B, the following relation holds:

$$\Delta A \Delta B \geq \frac{\langle [A, B] \rangle}{2}, \tag{3.1}$$

where ΔA and ΔB are the variances of the two observables. Let us consider the Pauli operators, σ_x and σ_z and their eigenvectors, $\{|0\rangle, |1\rangle\}$ and $\{|+\rangle, |-\rangle\}$. Since the observables are non-commuting, the uncertainty upon measurement (of a random state chosen from these 4 states) on either basis obeys the uncertainty principle. Thus, if one encodes the bit 0 in either the $|0\rangle$-state or $|+\rangle$-state, and the bit 1 in either $|1\rangle$-state or $|-\rangle$-state, then the value of the bit is hidden unless the adversary knows the encoding basis. Thus, a projective measurement over any of the bases destroys the information contained in the other basis, which provides us with unique security where we harness the innate property of nature and do not depend on the assumptions of computational prowess of the adversary. Quantum cryptography thus provides far stronger security than the classical counterpart; secure even against an adversary with infinite computational power and speed.

Using conjugate coding, Wiesner presented the very first quantum cryptographic protocol: unforgeable quantum money [46]. This idea of conjugate coding was also used in the famous BB84 quantum key distribution protocol [20]. In this thesis, we are interested in these two cryptographic tasks, but in the continuous-variable scenario, i.e., information is encoded on the electromagnetic field's quadratures. In the following sections, we give a brief overview of quantum key distribution and unforgeable quantum money, including their security definitions, developments over the years, and the necessary mathematical tools required for the upcoming chapters.

3.1. Quantum Key Distribution (QKD)

QKD allows two honest distant parties, traditionally named Alice and Bob, with access to an untrusted quantum channel and an authenticated classical channel, to share a secret key that remains secret to any adversary, usually referred to as Eve. The quantum channel is insecure and considered to be controlled by Eve while the classical channel is authenticated, meaning communication over this channel can be monitored by Eve but can not be altered, i.e., Eve can not pretend to be either Alice or Bob. Any QKD protocol can be divided into two steps: quantum communication and classical post-processing.

The quantum communication step consists of two parts:

- Quantum state distribution: In the *Prepare and Measure* (PM) version of a QKD protocol, the sender (Alice) encodes a random classical variable X following a probability distribution into non-orthogonal quantum states. These states are sent over the quantum channel (optical fiber, free-space link) to the receiver (Bob).

- Measurement: At the communication channel's output, Bob measures the incoming signals and obtains a random classical variable Y. After several uses (say N uses) of the channel, Alice and Bob share the raw data described by two correlated variables X^N and Y^N respectively.

Classical post-processing step transforms the raw data generated at the end of quantum communication step into a pair of secret keys shared by Alice and Bob. Alice and Bob use the authenticated classical channel for post-processing [2]. The classical post-processing steps are as follows:

- Parameter Estimation: This step ensures if a secret key can be processed from the raw data. It checks whether the correlation between the parties is high enough to amount to a secure key, i.e., Eve only has limited knowledge about the raw data. If not, the protocol is aborted. In order to do so, they use some classical variables X^m and Y^m $(m = N - n)$ to estimate the parameters of the channel, such as its transmissivity and noise.

- Error reconciliation[3]: This step allows the parties to detect and eliminate errors encountered during transmission and agree on a common bit string $Z^n = f(X^n)$ or $z = f(Y^n)$ via a key map f. This is done so that, the raw key X^n or Y^n can be processed into bit-strings.

- Privacy amplification: The parameter estimation step ensures that Eve only has limited knowledge about the raw key. Privacy amplification insures that Eve has negligible knowledge about the final keys. Using universal hash functions, Alice and Bob turn z into two secure keys S_A and S_B of length l.

QKD was first introduced with single photons acting as information carrier [20, 21]. The exchanged quantum states are encoded into the polarization, phase or time bin of the transmitted qubits, and the secret key is established upon detection of the individual photons. The measurement apparatus for such protocols is a single-photon detector, which detects a click when a photon has hit the detector or no click otherwise; thus, the outcomes are discrete. Hence the name "*discrete-variable*" (DV) QKD.

With a delay of nearly fifteen years after the first DV-QKD protocol, QKD with continuous variables was introduced as a promising alternative [22–24]. The idea was to exploit degrees of freedom in phase space, which resulted in measuring the quadratures of the electric field of the incident light using a homodyne detector, yielding continuous

[2] One needs a short secret key to authenticate the classical channel. After the post-processing, QKD returns a larger secret key. Thus, people also refer to QKD as a key-expansion protocol.

[3] there are protocols where the reconciliation step is applied before the parameter estimation step, and this order turns out to be more efficient

values as a measurement result. Thus the name "*continuous-variable*" (CV) QKD. The main advantage of CV-QKD is the simplification of implementation, as one can use only standard telecom components (such as PIN photodiodes) that are much more mature from a technological point of view than single-photon detectors whose primary use is QKD. The advantages and disadvantages of a CV-QKD protocol over a DV-QKD protocol have been discussed in [28].

There exists another way of distribution of quantum states for a QKD protocol, where Alice prepares N bipartite entangled states and sends one half to Bob, and keeps the other half. This type of protocols are known as the *Entanglement-based* protocols. The two types of QKD protocols whose distinction lies only in the state distribution, PM and EB are equivalent, i.e., they provide the same description of the protocol. The next section contains a detailed description of the two QKD protocols and their equivalence. For experimental purposes, we mostly use PM protocols while for security analysis we use the EB model. But, the crucial thing to note that is at the end of state distribution, we can assume that Alice and Bob share N bipartite quantum systems in $(\mathcal{H}_A \otimes \mathcal{H}_B)^N$.

Any QKD protocol, be it based on discrete or continuous variables, follows the above-mentioned steps. From the steps of the QKD protocol, we can define a QKD protocol as a CPTP map $\mathcal{E}$ that takes quantum states as input and outputs two classical secret keys[4], with the help of some classical communication.

$$\begin{aligned} \mathcal{E} : \mathscr{H}_A \otimes \mathscr{H}_B &\to \mathscr{S}_A \otimes \mathscr{S}_B \otimes \mathscr{C} \\ \rho_{AB}^N &\mapsto \rho_{S_A S_B C}, \end{aligned} \tag{3.2}$$

where $\mathscr{H}_A$ and $\mathscr{H}_B$ denote the Hilbert spaces for Alice and Bob respectively. The spaces $\mathscr{S}_A, \mathscr{S}_B$ and $\mathscr{C}$ correspond to classical registers, where $\mathscr{S}$ are that of the final keys (with subscripts A and B referring to Alice and Bob, respectively) and $\mathscr{C}$ is the public transcript of the protocol, corresponding to the classical information exchanged on the authenticated classical channel and therefore accessible to Eve. For instance, the register C contains the size l of the final key.

We must include a register E corresponding to the Hilbert space $\mathscr{E}$ of the adversary. To formalize it, we consider that the actual input space of the protocol is $\mathscr{H}_A \otimes \mathscr{H}_B \otimes \mathscr{H}_E$, and that the input state ρ_{ABE} is a pure state[5]. The protocol then acts as $\mathcal{E}_{AB} \otimes \mathbb{I}_E$, i.e. it acts trivially on the adversary' s space. The output space is $\mathscr{S}_A \otimes \mathscr{S}_B \otimes \mathscr{C} \otimes \mathscr{H}_E$. Then, we are interested about the security of the output state $\rho_{S_A S_B E'}$, where E' denotes the new register of the space accessible to Eve, $\mathscr{H}_{E'} = \mathscr{C} \otimes \mathscr{H}_E$.

3.1.1 Security of QKD

A QKD protocol is considered *secure*, if the protocol obeys both properties of *correctness* and *secrecy*. The correctness property ensures that the key is identical for both Alice and Bob for any strategy of the adversary, i.e., any initial state ρ_{ABE} while the secrecy of the key refers to the fact that the adversary Eve has negligible knowledge about it.

[4] an exception is device-independent QKD where the inputs are also classical but then, the violation of a Bell inequality ensures that Alice and Bob are indeed measuring an entangled quantum system.

[5] a purification of the input state

Therefore, the final keys obtained from a secure protocol has the following properties:

- identical,
- uniformly distributed,
- independent from adversary's knowledge.

A QKD protocol aims at generating keys with the above-mentioned properties. The legitimate parties, Alice and Bob tries to distill a secure key and if they are unsuccessful, they *abort* the protocol. The trivial protocol that generates no key is secure from this point of view, but not interesting. The final key obtained may be used as an input for some other cryptographic task. Therefore, we aim for composable security, which ensures that the protocols remain secure even if arbitrarily composed with other instances of the same or other protocols.

We use the same notations as before. We note l the size of a secret key, N the number of quantum signal exchanged during the protocol, and S_A and S_B are the final keys obtained from the protocol. The first property (of correctness) can be rewritten as, a QKD protocol is ϵ_{cor}-correct if

$$Pr[S_A \neq S_B] \leq \epsilon_{cor}. \tag{3.3}$$

The last two properties can be written in the same equation, which defines the secrecy property of the key. A key S is called δ-secret if

$$\frac{1}{2} \parallel \rho_{SE'} - \tau_S \otimes \rho_{E'} \parallel_1 \leq \delta, \tag{3.4}$$

where $\tau_S = \sum_{s \in \mathcal{S}} \frac{1}{|\mathcal{S}|} |s\rangle \langle s|$ describes completely mixed states of possible key of length l and tensor product state indicates the independence of Eve's system from the final key, which in together is the ideal state. We note that in the event the protocol aborts, the corresponding key is automatically secret, since the key is empty in that case, and by definition an empty key is secure. A QKD protocol is ϵ_{sec}-secret if it outputs δ-secret keys with $(1 - p_{\text{abort}})\delta \leq \epsilon_{sec}$, where p_{abort} represents the probability the protocol aborts. This probability depends on the strategy of the adversary, that is on the input state ρABE. It can be estimated for typical conditions and usually close to zero. Finally, we can write that a QKD protocol is ϵ-secure if it is ϵ_{cor}-correct and ϵ_{sec}-secret with $\epsilon_{cor} + \epsilon_{sec} \leq \epsilon$, i.e., the following relation holds

$$\frac{1}{2} \parallel \rho_{S_A S_B E'} - \tau_{SS} \otimes \rho_{E'} \parallel_1 \leq \epsilon, \tag{3.5}$$

where $\tau_{SS} = \frac{1}{2^l} \sum_{s \in \{0,1\}^l} |s, s\rangle \langle s, s|$ denotes a uniformly-chosen key of length l, identical for Alice and Bob. This means, the probability that Alice and Bob do not abort and the adversary gets information about the key is at most ϵ. This security definition was introduced in Renato Renner's PhD thesis [25].

Moreover, the protocol should also be *robust* in the sense that it should output nontrivial keys if there is no active attack on the quantum channel by Eve. It is

measured by the *robustness* parameter, ϵ_{rob}, which corresponds to the abort probability if the adversary is passive and if the characteristics of the quantum channel conform to what is expected. For instance, in CV-QKD, a quantum channel corresponding to an optical fiber will be a Gaussian channel with a fixed transmittance T and excess noise ξ.

A generic technique in proving that a QKD protocol is ϵ-secure is to show that the real protocol $\mathcal{E}$ is indistinguishable from an ideal version of the same protocol $\mathcal{F}$,

$$\frac{1}{2} \parallel \mathcal{E} - \mathcal{F} \parallel_{\diamond} \leq \epsilon. \tag{3.6}$$

The ideal version is obtained by concatenating $\mathcal{E}$ with a (virtual) protocol $\mathcal{E}_{\mathcal{V}}$ which replaces the final keys S_A and S_B by a perfect key S: $\mathcal{E}_{\mathcal{V}}(\rho_{S_A S_B E'}) = \tau_{SS} \otimes \rho_{E'}$. One defines $\mathcal{F} = \mathcal{E}_{\mathcal{V}} \circ \mathcal{E}$. The Eqs. (3.5) and (3.6) are therefore equivalent. The indistinguishability in Eq. (3.6) is between two CPTP maps and is defined by diamond distance between two maps, Eq. (1.35).

Generally, we assume that Eve has full access to the quantum channel, which she can control and manipulate however she wishes. For her eavesdropping attack, Eve is allowed to prepare arbitrary ancillary states to interact with the transmitted signal states and subsequently performs measurements on. Very importantly, we also assume that she might be in possession of a quantum memory which allows her to store her states and perform her measurement at a later time according to what she learned during the classical post-processing. Also, Eve has no limit in terms of computational power, but, has no access to Alice or Bob's devices. Without this assumption a QKD protocol remains insecure [26]. We distinguish two different types of eavesdropping attacks that are typically considered in security proofs, classified according to her powers:

- Collective Attack: Eve performs an i.i.d. attack with separable ancilla states, stores her state in a quantum memory and performs an optimal collective measurement on all quantum states at any later time (generally, after post-processing).

  For a collective attack, the bipartite state ρ_{AB}^{N} takes a simple form:

  $$\rho_{AB}^{N} = \int d\sigma_{AB} p(\sigma_{AB}) \sigma_{AB}^{\otimes N}, \tag{3.7}$$

  where $p(\sigma_{AB})$ is a probability distribution on $\mathscr{H}_A \otimes \mathscr{H}_B$.

- Coherent Attack (or General attack): The most general attack where no (i.i.d.) assumption is made. In particular, Eve may prepare an optimal global ancilla state whose (possibly mutually dependent) modes interact with the signal pulses in the channel and are then stored and collectively measured after the classical post-processing.

The actual degree of information-theoretic security of a given QKD protocol depends on the assumed technological capabilities a potential eavesdropper might have. Depending on Eve's resources and attacks, we summarize the various notions of security proofs, from the strongest to the weakest one:

- Composable security against coherent attacks, bounding the trace distance of Eq. (3.5) without any restriction on the input state ρ_{AB}^{N}, for finite N.
- Composable security against collective attacks, bounding the trace distance of Eq. (3.5) under the condition that the input state is i.i.d., $\rho_{AB}^{N} = \rho_{AB}^{\otimes N}$.
- Security against collective attack in the asymptotic limit, $N \to \infty$.

Naturally, the asymptotic limit does not directly apply to any realistic system. Nonetheless, its analysis is immensely useful since it provides an upper bound on the corresponding non-asymptotic or finite-size results and because it can typically be derived more easily.

Prepare and Measure vs Entanglement-based protocol

The first protocols to be introduced in the literature are PM protocols [20]. Alice prepares N quantum states $|\psi_1\rangle, |\psi_2\rangle, ..., |\psi_N\rangle$, where ψ_i are i.i.d. complex variables and sends them to Bob through the quantum channel. Bob proceeds by measuring these states in a chosen detection setting. One can then consider the state generating source to be a classical-quantum source, with the density matrix $\rho^{\otimes N} = \rho_{aB} \otimes \rho_{aB} ... \otimes \rho_{aB}$, where ρ_{aB} are classical-quantum states given by Eq. (2.45)

$$\rho_{aB} = \sum_{a} p(a) |a\rangle \langle a| \otimes |\phi_a\rangle \langle \phi_a| . \tag{3.8}$$

However, in an EB protocol, the situation is a little bit different. An i.i.d entanglement source of bipartite quantum states is used where Alice retains one half and sends the other half to Bob. This idea was first formulated by Ekert in [21]. Alice and Bob proceed with measuring the states they receive with their choice of detection. An i.i.d. *entanglement source* generates independent entangled states, where the entire bipartite message state reads $\rho^{\otimes N} = |\psi\rangle_{AB} \otimes |\psi\rangle_{AB} ... \otimes |\psi\rangle_{AB}$, where

$$|\psi\rangle_{AB} = \sum_{i} \sqrt{p_i} |i\rangle_A \otimes |\phi_i\rangle_B . \tag{3.9}$$

The two states are equivalent, i.e., by applying the projective measurement $\sum_i |i\rangle \langle i|$ on the entangled source's state, with i as Alice's output, enforces Bob's state to project onto $|\phi_i\rangle_B$, which is a classical-quantum state. Therefore, although the state distribution steps in PM and EB are different, theoretically they are equivalent as long as Alice's lab and preparation are trusted. To the adversary Eve, the two protocols are indistinguishable from one another. Both the scenarios provide a complete and equivalent protocol; switching from one viewpoint to the other is simply a question of convenience. An EB protocol is clearly less practical than a PM protocol since an entangled source is necessary and bipartite separable states are not sufficient to perform QKD with an EB protocol while proving security of the protocol is much easier in the EB protocol.

Secret key rate of a QKD protocol

We use the same notations as before. The secret key rate K is defined as the ratio between the size of the secret key l and the number of quantum signal exchanged during the protocol N:

$$K := \frac{l}{N}. \tag{3.10}$$

This holds true for finite N. In the limit $N \to \infty$, the asymptotic secret key rate is given by

$$K^{asympt} = \lim_{N\to\infty} K. \tag{3.11}$$

such that the protocol is ϵ-secure for any $\epsilon > 0$. The size of the final key depends on the smooth min entropy $H^{\epsilon}_{\min}(Z|E)$, where Z can be either Alice's classical variable X or Bob's classical variable Y and E corresponds to Eve's quantum system.

Let us recall from section 2.1.2, that the size of the secret key obtained on performing the privacy amplification task is given by the conditional smooth min-entropy (Eq. (2.56)),

$$l = l^{\epsilon}_{\text{extr}}(Z|E) = H^{\epsilon'}_{\min}(Z|E) + O(\log 1/\epsilon) \tag{3.12}$$

for some $\epsilon' \in [\frac{1}{2}\epsilon, 2\epsilon]$ and Z is a classical random variable on which an adversary has some partial information E. However, a QKD protocol also involves an error reconciliation step, where Alice helps Bob (or vice-versa) correct his errors and guess the value of X^n (or Y^n) which will be used for privacy amplification, and agree on a common bit string. Without loss of generality we choose Y as the raw key. Then the size of ϵ-secure secret key, l is given by [25]

$$l = H^{\epsilon'}_{\min}(Y^n|E^n) - \text{leak}_{ER} - 2\log_2 \frac{1}{2(\epsilon - \epsilon' - \epsilon_{ER})}, \tag{3.13}$$

for some $\epsilon' > 0$. The quantity leak_{ER} refers to the number of bits transmitted by Bob to Alice during the reconciliation process to correctly guess Y^n and ϵ_{ER} is the failure probability of the reconciliation, the probability that Alice makes a wrong guess about Y^n.

Therefore, if one is able to estimate the smooth min-entropy, one can find the key rate of a QKD protocol. Unfortunately, it is rather difficult to compute. However, if one restricts the adversary to only perform collective attacks, the computation is simplified. For such attacks, the input state ρ^N_{AB} takes a simple form of i.i.d. states, i.e., $\rho^N_{AB} = \rho^{\otimes N}_{AB}$.

Let us now consider the secret key rate of a QKD protocol against collective attacks in the asymptotic limit. The smooth min-entropy can be written as a conditional von Neumann entropy, given by Eq. (2.54), i.e.,

$$S(Y|E)_{\rho} = \lim_{\epsilon'\to 0} \lim_{n\to\infty} \frac{1}{n} H^{\epsilon'}_{\min}(Y^n|E^n)_{\rho^{\otimes n}}. \tag{3.14}$$

The quantity leak_{ER}/n per symbol can be made arbitrarily close from the Shannon limit $H(Y|X)$ as per the channel coding theorem. As a consequence, for this scenario where we choose Y as the raw key, one recovers the result of Devetak and Winter [41]:

$$K^{asympt}_{coll} = S(Y|E) - H(Y|X), \tag{3.15}$$

which can be also written as

$$K_{coll}^{asympt} = I(X:Y) - \chi(Y;E), \tag{3.16}$$

where $I(X:Y)$ is the mutual information between Alice and Bob and $\chi(Y;E)$ is the Holevo information between Bob's data and Eve's quantum system.

3.1.2 Continuous-Variable QKD

The idea of CV-QKD is to encode information in phase space. To do so, Alice and Bob will exchange quantum states whose Wigner functions are peaked near specific values in phase space. In a PM protocol, Alice will send N quantum states from a family of states $\{|\phi_1\rangle, \ldots, |\phi_M\rangle\}$ with M possibly equal to ∞ such that the Wigner function of $|\phi_k\rangle$ is peaked around a complex variable α_k or around a real variable x_k or p_k. One must be careful when considering the family of quantum states. The family of states must contain non-orthogonal states; otherwise, one can always find a measurement that allows one to distinguish them correctly. If there are non-orthogonal states, however, one cannot deterministically distinguish them. Another important requirement for a QKD protocol is to be practical. In particular, the quantum states $|\phi_k\rangle$ should be easy to generate. For this reason, the states usually considered are Gaussian states: coherent states and squeezed states. There are two types of QKD protocols depending on the encoding scheme: (a) encoded using a discrete probability distribution, or discrete modulated, and (b) encoded using continuous probability distribution, usually Gaussian distribution. Obviously, for practical implementations, any modulation scheme only uses a finite number of states, due to the limited precision of both the random number generators and the modulators. However, in the case of Gaussian modulation, the number of possible inputs is much larger than the one for a discrete-modulation scheme, which usually requires 4 different states.

CV-QKD protocols were firstly proposed with discrete modulation of squeezed states [22–24, 27], the concept was soon developed further to Gaussian-modulated CV-QKD with coherent states [29]. It would seem that squeezed states are well suited for protocols involving a homodyne detection whereas coherent states are more natural for protocols with a heterodyne detection.

In CV-QKD systems with Gaussian modulation, for EB protocols, we use two-mode squeezed state as our entangled state. If one of the modes is measured with homodyne detection, the other mode collapses to a squeezed state, while if the mode is measured via a heterodyne detection, we get coherent states on the other mode.

This can be easily shown by using the partial measurement results of Homodyne and heterodyne measurements, Eqs. (2.149) and (2.150), and Eqs. (2.153) and (2.154) respectively, while choosing γ to be the covariance matrix of TMSS, Eq. (2.123). For details, see Appendix A.

We now give a detailed description of a CV-QKD protocol. Here, we have considered the no-switching protocol [30].

1. Alice picks 2N random variables according to a centered normal distribution with variance V_A:
$$q_1, p_1, \dots q_N, p_N \sim \mathcal{N}(0, V_0). \tag{3.17}$$
Then she sends N coherent states $|\alpha_1\rangle, |\alpha_2\rangle, ..., |\alpha_N\rangle$ to Bob via the quantum channel, where $\alpha_j = q_j + ip_j$.

2. For each state, Bob performs a heterodyne measurement, where both quadrature values are measured. He obtains $2N$ classical variables[6].

3. For parameter estimation, Alice and Bob sacrifice some $m = N - n$ subsystems, and publicly announce the results on the authenticated public channel. They estimate the value of the transmission T and excess noise ξ, which helps then estimate the level of correlation between their subsystems. If the correlation amount is high enough, they proceed with the remaining of the protocol or else they abort the protocol if the correlation is too low to distill a secret key. This step allows then obtain an upper bound on the information accessible by Eve.

   At this point Alice and Bob share $2n$ couples of correlated classical variables. Let us denote Alice's remaining data set by $x = \{x_1, x_2, ..., x_{2n}\}$ and Bob's set by $y = \{y_1, y_2, ..., y_{2n}\}$.

4. The two parties communicate on the authenticated classical channel, to agree on a common bit-string z. One can choose either x or y as the raw key, depending on this choice, the direction of classical communication varies. There are two types of reconciliation methods: *direct reconciliation*, where Alice sends side information about the raw key x to Bob, so that he can recover x from y and *reverse reconciliation*, where Bob sends side information about the raw key y to Alice. It has been shown that reverse reconciliation performs better than direct reconciliation[29]. This reconciliation is achieved thanks to error correction techniques very similar to those that are widely used in the telecom industry.

   After reverse reconciliation, they agree on a common bit-string $z = f(y)$ via a key map $f : \mathbb{R}^{2n} \to \{0,1\}^{2n}$ of choice.

5. Alice and Bob now share a common bit-string z. However, z is not completely secret and does not constitute a secret key. The extraction of the key is done through two-universal hashing[7]: Alice and Bob choose randomly a hashing function from a so-called two-universal family of hash functions that takes z as input and outputs a secure key of size l.

---

[6] There is no need for Bob to inform Alice about the choice of his basis as he does in the case of GG02[29], where he measures the states via homodyne detection.

[7] Two-universal family of hash functions refers to the family of hashing functions F which takes an input from $\mathcal{X}$ and outputs to $\mathcal{Z}$ with P_F being a probability distribution on F, such that $Pr_f[f(x) = f(x')] \leq \frac{1}{|\mathcal{Z}|}$, for any distinct $x, x' \in \mathcal{X}$ and f chosen at random from F according to the distribution P_F. This allows us to upper bound the trace distance between the ideal (uniform and uncorrelated) key to the correlated key.

3.1.3 Security of CV-QKD

The usual methods of DV protocols - de Finetti theorems [38–40], entropic uncertainty relations [70, 99], entropy accumulation [71] – need not directly work in the CV setting due to the infinite-dimensionality of the Fock space and therefore, it is quite difficult to prove security against coherent attacks in the composable setting.

For CV protocols, we need to properly estimate the covariance matrix. Unlike the case of DV protocols such as BB84-types where the error rate lies between 0 and 1, meaning the parameters are bounded. In CV protocols, the parameters are unbounded due to the infinite-dimensionality of the Fock space. Therefore, we need to try computing a *confidence region* for the elements of the covariance matrix, which requires the protocol to show a symmetry or an invariance in phase space or some additional assumptions for instance, that the state is Gaussian or that some moments of the variables are upper bounded by some explicit value.

One usually achieves composable security using uncertainty principle relations [27, 31–33], which has been successfully applied to the protocol of Ref.[34], where Alice prepares squeezed states. At the moment, it is still unclear whether a tighter version of the entropic uncertainty principle could also work for protocols with coherent states (see Ref.[35, 37]).

Reduction from general to collective attacks

Another alternative is to appeal to a de Finetti-type theorem to reduce the problem to the case of collective attacks by exploiting the symmetries of the protocol. Thanks to the de Finetti theorem, in the asymptotic limit, if the composite states show some fundamental symmetry (e.g. invariance under permutations of its parts), then the composite states can be well approximated by identical independent subsystems. The theorem relates the symmetric states, i.e., states that are invariant under permutations of their subsystems (ρ such that $\rho = \pi\rho\pi^\dagger$ for any permutation $\pi \in \mathscr{S}_n$), and mixtures of i.i.d. states of the form $\sigma^{\otimes N}$ for some state $\sigma \in \mathscr{H}$. An i.i.d. state is obviously symmetric, however, the converse is not true in general. A symmetric state becomes increasingly close to a mixture of i.i.d. states as one traces out more of its parts. One can then simply consider collective attacks instead of general attacks. In the asymptotic limit, one can now properly estimate the covariance matrix using *optimality of Gaussian states*, which will be shown in the next subsection.

However, in the finite-size scenario, the situation is complicated. The de Finetti approach mentioned above is impractical for CV-QKD since the required number of signals exchanged is too large. The problem can be solved by symmetrizing the protocol under the action of the unitary group [88]. Upon *symmetrization*, the CV-QKD protocol (and respectively the states) now exhibits a new symmetry, invariance under the action of unitary group $U(N)$ (instead of the symmetric group as in usual de Finetti theorem). The symmetrization step does not need to be implemented by a physical unitary transformation. Instead, one can measure all the modes and implement a random rotation on their data sets in $\mathbb{R}^{2N}$ according to $V \in U(N) \cong Sp(2N) \cap O(2N)$. Therefore,

currently, the only protocols for which we are able to properly analyze the parameter estimation (of a covariance matrix), with proper error bound, are the protocols showing a symmetry or an invariance in phase space.

Gaussian de Finetti reduction theorem: The symmetrization step ensures the protocol is invariant under the action of the unitary group. Then we can consider a stronger form of de Finetti theorem, Gaussian de Finetti theorem, which states it is sufficient to prove security against collective attacks in order to prove security of the protocol against general attacks. To prove composable security against collective attacks, instead of all i.i.d states one can simply consider Gaussian i.i.d attacks. In other words, it is sufficient to show that the protocol is secure when the overall initial pure state ρ_{ABE} is a mixture of such *de Finetti states* or $SU(q,q)$ coherent states, where q is total number of modes held by Alice and Bob per round of the protocol. The states exhibit invariance under the action of the unitary group.

$SU(q,q)$ generalized coherent states are i.i.d. Gaussian states of the form $|\Lambda\rangle^{\otimes q}$, where $|\Lambda\rangle$ is a $2q$-mode Gaussian state parametrized by an $q \times q$ matrix $\Lambda = [\Lambda_{i,j}]$ with spectral norm $\| \Lambda \| < 1$ and is defined as

$$|\Lambda\rangle = \det(\mathbb{I} - \Lambda\Lambda^\dagger)^{1/2} \exp\left(\sum_{i,j=1}^{q} \Lambda_{i,j} \hat{a}_i^\dagger \hat{b}_j^\dagger\right) |vac\rangle\,. \tag{3.18}$$

where the creation operators of Alice and Bob's modes are denoted $\hat{a}_1^\dagger, \ldots, \hat{a}_q^\dagger, \hat{b}_1^\dagger, \ldots, \hat{b}_q^\dagger$. For example, $SU(1,1)$ coherent states are simply two-mode squeezed states. In the case of no-switching protocol, to prove ϵ-security against collective attacks, we can just consider ρ_{ABE} as a mixture of $SU(2,2)$ coherent states.

In particular, if a protocol is ϵ-secure against Gaussian collective attacks then the protocol is ϵ'-security against general attacks, with $\epsilon'/\epsilon = \text{poly}(n)$. Note that, the reduction theorem is only applicable for CV protocols with Gaussian modulation.

Security against collective attacks in the asymptotic limit

In the asymptotic limit, de Finetti's theorem [38, 39] guarantees that collective attacks are optimal. Proving the security of a protocol with Gaussian modulation against collective attacks in the asymptotic regime is easier than in the composable setting. One only needs to compute the corresponding asymptotic secure key-rate, given by the Devetak-Winter formula (Eq. (3.16)),

$$K_{coll}^{asympt} = I(a:b) - \chi(b;E), \tag{3.19}$$

where $I(a:b)$ is the mutual information between Alice and Bob's measurement outcomes and $\chi(b;E)$ is the Holevo information between Bob's data and Eve's quantum system, considering reverse reconciliation.

However, in a real scenario, Alice and Bob cannot extract all the information their data contains, and the quantity $I(a:b)$ is multiplied by a factor $\beta \in (0,1)$, called

the reconciliation efficiency. The quantity $\beta I(a:b)$ can be directly obtained from an experiment, while the quantity $\chi(b;E)$ requires our utmost attention. We need to calculate its value or at least an upper bound for it.

Before moving on to the *how* this can be achieved, the *why* that this can be achieved is more interesting and very much counter-intuitive. First, $\chi(b;E)$ must be obtained from the state ρ_{AB} shared by Alice and Bob in an EB version of the protocol. Indeed, in such a protocol, without loss of generality we can assume Eve holds a purifying system of ρ_{AB}, i.e., the state ρ_{ABE} shared by Alice, Bob and Eve is considered to be pure. That said, thanks to Stinespring's dilation theorem (Eq. (1.19)), Eve's quantum state, $\rho_E = \mathrm{tr}_{AB}[\rho_{ABE}]$ is defined up to a unitary operation on the system E. However, the quantity $\chi(b;E) = S(E) - S(E|b)$ remains invariant under such unitaries, a direct consequence of von Neumann entropies being invariant under unitary operations. This means that there exists a function f such that $\chi(b;E) = f(\rho_{AB})$.

Now, to evaluate $\chi(b;E)$, the first problem we encounter is that we have no idea how to compute f for a generic state, since we need to optimize for all states in the infinite-dimensional Hilbert space. However, for specific families of states we do know how to compute f. One of them is the entangled family, in which case Eve's quantum state can be factorized from Alice and Bob's state, meaning that $\chi(b;E)$ is necessarily null in this case. Unfortunately, in practice, ρ_{AB} is never a pure entangled state. Another family of states for which f can be computed are Gaussian states, but proving a given state is Gaussian is impossible in practice as it would in principle require an infinite number of copies of the state. However the restriction to collective attacks simplifies the analysis as the state ρ_{AB} describing Alice and Bob's respective N systems can be written as

$$\rho_{AB}^N = \int d\sigma_{AB} p(\sigma_{AB}) \sigma_{AB}^{\otimes N}. \tag{3.20}$$

Even under this restriction, it does not seem sensible to assume that Alice and Bob have complete knowledge about the shared state. Under these conditions, it would be favourable if we can at least upper bound the quantity $\chi(b;E)$.

The optimality of Gaussian states [35, 42] comes to the rescue: for any continuous function g which is strongly sub-additive and invariant under local *Gaussification* unitaries $g(U^{\otimes N}\rho U^{\dagger\otimes N}) = g(\rho)$, there exists a Gaussian state ρ^G with the same finite first and second moments as ρ which satisfies the condition

$$g(\rho) \leq g(\rho^G). \tag{3.21}$$

We now check if the function $f : \rho_{AB} \to f(\rho_{AB}) = \chi(b;E)$ satisfies the above-mentioned conditions of the function. Here we follow the steps presented in Raul García-Patrón's PhD thesis [36].

Continuity: If for two quantum states ρ_{AB} and σ_{AB}, $\| \rho_{AB} - \sigma_{AB} \|_1 \leq \epsilon$ holds true, then there exist respective purifications ρ_{ABE} and σ_{ABE} such that $\| \rho_{ABE} - \sigma_{ABE} \|_1 \leq 2\sqrt{\epsilon}$. Partial trace can only decreases the trace norm, we have $\| \rho_{BE} - \sigma_{BE} \|_1 \leq 2\sqrt{\epsilon}$ and $\| \rho_E - \sigma_E \|_1 \leq 2\sqrt{\epsilon}$. Moreover, a heterodyne measurement being a quantum

operation can only decreases the trace norm, meaning $\| \rho_{bE} - \sigma_{bE} \|_1 \leq 2\sqrt{\epsilon}$. Finally, one needs to use a continuity argument for the von Neumann entropy. Unfortunately, it is known that the von Neumann entropy is discontinuous almost everywhere in an infinite dimensional Hilbert space. In order to restore the continuity of this function, one can for instance bound the energy of the system in order to make the set of states compact (see for example Proposition 6.6 of [45]). Note that requiring the energy of the system to be bounded appears as a reasonable assumption. On the compact states of bounded energy, the von Neumann entropy is therefore continuous and so is the quantity $\chi(b;E) = S(E) - S(E|b)$.

Strong subadditivity: Let us consider a case where Alice and Bob share a bipartite state $\rho_{A_1B_1A_2B_2}$ and Eve holds a purifying system E such that $\rho_{A_1B_1A_2B_2E}$ is pure.

$$\begin{aligned} f(\rho_{A_1B_1A_2B_2}) = \chi(b_1,b_2;E) &= S(b_1,b_2) - S(b_1,b_2|E) \\ &= \underbrace{S(b_1,b_2)}_{\leq S(b_1)+S(b_2)} - \underbrace{S(b_1|b_2E)}_{\geq S(b_1|A_2B_2E)} - \underbrace{S(b_2|b_1E)}_{\geq S(b_2|A_1B_1E)} - \underbrace{\chi(b_1;b_2|E)}_{\geq 0} \\ &\leq S(b_1) + S(b_2) - S(b_1|A_2B_2E) - S(b_2|A_1B_1E) \end{aligned} \tag{3.22}$$

Finally, noticing that the system $E_1 \equiv A_2B_2E$ (resp. $E_2 \equiv A_1B_1E$) purifies A_1B_1 (resp. A_2B_2), one obtains

$$f(\rho_{A_1B_1A_2B_2}) \leq \chi(b_1;E_1) + \chi(b_2;E_2) = f(\rho_{A_1B_1}) + f(\rho_{A_2B_2}), \tag{3.23}$$

which is the strong subadditivity. The additivity of f is a straightforward result of the additivity of the von Neumann entropy.

Invariance under local Gaussification unitaries: A Gaussification unitary operation acts on the quadratures. But, Gaussification unitary operation does not mix the different quadratures and neither does the measurement process of the CV QKD protocol, the two processes can be interchanged. Hence it leaves the quantity $\chi(b;E)$ invariant.

This concludes the proof that the function f indeed satisfies the conditions of optimality of Gaussian states. This means that, optimality of Gaussian states applies to the cases of von Neumann entropy, thus calculating the von Neumann entropy for a Gaussian state with the same moments as that of the actual state ρ_{AB}. Now, all that is left, is to show the method of computing the Holevo bound from a Gaussian covariance matrix, and the derivation of the covariance matrix of the state ρ_{AB} from the data obtained in the PM version of the protocol.

What we proved above is that it is always safe to assume the state ρ_{AB} to be Gaussian. This statement is equivalent to the notion of optimality of Gaussian attacks [35, 43] meaning that Gaussian attacks are optimal among the family of collective attacks.

Estimation of the covariance matrix in the entanglement-based protocol from data observed in the PM protocol

In the considered protocol, Alice encodes information in the quadratures $\hat{x}$ and $\hat{p}$ of coherent states. The random variables x and p are drawn according to a Gaussian distribution of variance $V_0 : x, p \sim \mathcal{N}_{\mathbb{C}}(0, V_0)$.

Recall that, in the corresponding EB version of the protocol, Alice starts with the two mode squeezed state (TMSS), which has the covariance matrix

$$\gamma = \begin{pmatrix} V\mathbb{I}_2 & \sqrt{V^2-1}\sigma_z \\ \sqrt{V^2-1}\sigma_z & V\mathbb{I}_2 \end{pmatrix}, \tag{3.24}$$

where $V = V_0 + 1$ and measures one of the modes with heterodyne detection, which forces the other mode to collapse in the coherent state centered at $\frac{\sqrt{2(V^2-1)}}{V+1}(x_A, -p_A)$ if Alice's measurements were on the first mode (x_A, p_A), according to Eq. (2.153).

After the quantum exchange, Alice and Bob perform a parameter estimation which is done by analyzing m pairs of correlated data $(a_i, b_i)_{1 \geq i \geq m}$. As we saw, for CV-QKD, it is sufficient to estimate the covariance matrix of the state shared by Alice and Bob.

For Gaussian modulated CV-QKD protocols, from the symmetry, we see that only two parameters need to be estimated:

- the variance of Bob's side
- the correlation between Alice and Bob

Using optimality of Gaussian attacks, we consider the quantum channel to be a Gaussian thermal noise channel of transmittance T and excess noise ξ, which models the realistic optical fibers used for experiments, then, the covariance matrix after such a channel transmission reads

$$\gamma_{AB} = \begin{pmatrix} V\mathbb{I}_2 & \sqrt{T(V^2-1)}\sigma_z \\ \sqrt{T(V^2-1)}\sigma_z & T(V+\chi)\mathbb{I}_2 \end{pmatrix}, \tag{3.25}$$

where $\chi = \frac{1-T}{T} + \xi$.

We wrote the above covariance matrix because it makes the connection between the observed transmission value T and excess noise ξ with the quadratures of the two parties, these observed quantities are linked to $\langle \hat{x}^2 \rangle, \langle \hat{y}^2 \rangle$ and $\langle \hat{x}\hat{y} \rangle$ through

$$\begin{cases} V = \langle \hat{x}^2 \rangle + 1, \\ T = \dfrac{\langle \hat{x}\hat{y} \rangle}{\langle \hat{x}^2 \rangle^2} \\ T(V+\chi) = \langle \hat{y}^2 \rangle. \end{cases} \tag{3.26}$$

Key rate

The upper bound of $\chi(b; E)$ can be computed by assuming a Gaussian state with the same covariance matrix γ_{AB}. Therefore,

$$\chi(b; E) = S(E) - S(E|b) = S(AB) - S(A|b), \tag{3.27}$$

since system E is without loss of generality a purifying system for AB, ρ_{ABE} is a pure state, thus $S(E) = S(AB)$. The von Neumann entropy for a Gaussian state is computed using the Eqs. Eqs. (2.159) and (2.160), which requires the symplectic eigenvalues from the corresponding covariance matrix, given by Eq. (2.122).

The symplectic eigenvalues for γ_{AB} are

$$v_{1,2}^2 = \frac{1}{2}\left[\Delta \pm \sqrt{\Delta^2 - 4D}\right], \tag{3.28}$$

where

$$\Delta = V^2 + T^2(V+\chi)^2 - 2T(V^2-1) \tag{3.29}$$
$$D = (TV(V+\chi) - T(V^2-1))^2. \tag{3.30}$$

To calculate $S(AB|b)$, we need the remaining covariance matrix of ρ_{AB} (in the EB version) after Bob has measured his states by a heterodyne measurement, given by Eq. (2.154),

$$\begin{aligned}\gamma_{A|b} &= V\mathbb{I}_2 - \sqrt{T(V^2-1)}\sigma_z(T(V+\chi)\mathbb{I}_2 + \mathbb{I}_2)^{-1}(\sqrt{T(V^2-1)}\sigma_z)^\top \\ &= V - \frac{T(V^2-1)}{T(V+\chi)+1}\mathbb{I}_2 = \frac{T(V\chi+1)+V}{T(V+\chi)+1}\mathbb{I}_2.\end{aligned} \tag{3.31}$$

The symplectic eigenvalue is

$$v_3 = \frac{T(V\chi+1)+V}{T(V+\chi)+1}. \tag{3.32}$$

Thus the maximum of $\chi(b;E)$ is

$$\chi(b;E) = S(AB) - S(A|b) = G\left(\frac{v_1-1}{2}\right) + G\left(\frac{v_2-1}{2}\right) - G\left(\frac{v_3-1}{2}\right) \tag{3.33}$$

where $G(x)$ is given by Eq. (2.160),

$$G(x) = (x+1)\log_2(x+1) - x\log_2 x. \tag{3.34}$$

This concludes how the supremum of the Holevo information can be computed from the covariance matrix.

To calculate the key rate, all we need to do is evaluate the mutual information between Alice and Bob's data. Note that, both Alice and Bob perform heterodyne measurement on their respective modes. Therefore the covariance matrix of the outcome reads,

$$\gamma_{ab} = \frac{1}{2}(\gamma_{AB} + \mathbb{I}_4), \tag{3.35}$$

and thus, the mutual information is given by Eq. (2.23),

$$I(a:b) = \frac{1}{2}\log\left(\frac{V_a V_b}{\det\gamma_{ab}}\right), \tag{3.36}$$

where $V_a = (V+1)/2$ and $V_b = (T(V+\chi)+1/2)$.

The secret key rate against collective attacks coincides with the secret key rate valid against arbitrary attacks in the asymptotic limit [27, 44, 72].

This concludes our discussion of CV-QKD. In chapters 4 and 5, we use the tools and techniques mentioned here to analyze the security of a two-way CV-QKD protocol and a discrete-modulated CV-QKD protocol.

3.2. Quantum Money

Another protocol of practical interest is *quantum money*. Using the theory of conjugate coding and no-cloning theorem, Wiesner, in his seminal work conceived the idea of unforgeable quantum money [46]. A quantum money scheme aims to protect the money from being counterfeited. This is accomplished by combining the money with a secret key that has been encoded onto quantum states.

A quantum money scheme involves three parties - a mint, a bank and a client. The mint generates the money, a n-qubit state. Then the n-qubit state is stored in a quantum memory, assigned with a unique serial number and finally handed to a client. This sequence of states is stored by the mint in a classical key and then shared with the bank.

Depending on whether the key is kept secret or made public, the money schemes can be categorized as:

- *Private-key money schemes*: The classical key of sequence of quantum states is stored securely by the mint in a classical key and shared only with the bank (and its branches). Since the key is known only to the mint and the banks, the banks are responsible for verifying the validity of the money.

  Two types of verification may be used in these money schemes:

  - *Quantum verification*: The client has to send the entire quantum money state to a bank for verification. Since, the states must physically reach the bank to be verified as valid, we shall refer to this money scheme as *quantum cheques*. Wiesner's money scheme falls under this category.
  - *Classical verification*: The bank verifies the validity of the money through classical communication with the measurement data performed locally by the client. Such schemes will be referred as *quantum credit card* schemes. This scheme was first introduced by Gavinsky [49].

- *Public-key money schemes*: The key according to which quantum states are generated are made known to the public. Therefore, any party (a client or a vendor) is able to verify the validity of the money without contacting the bank. These schemes are quantum analogues of classical *banknotes*. This concept of public-key quantum money scheme was introduced in [54] by Aaronson.

3.2.1 Properties

A quantum money protocol satisfies the following properties:

- Correctness: this property ensures that an honest client should always be able to successfully verify the original quantum money issued by the mint.
- Security: it refers to that fact that a dishonest client (or an adversary) trying to counterfeit the money should always fail at the verification process.

There is another property that many money schemes follow but is not necessary to ensure the proper use of the money: *reusability*. This ensures that an honest client can verify the money with different banks at different times.

In the following subsections, we will be discussing in detail private-key money schemes based on different verification processes.

3.2.2 Private-key with quantum verification money scheme: Wiesner's model

In Wiesner's original scheme, the mint generates two random bit-strings $b^{(s)}$ and $k^{(s)}$. The string $b^{(s)}$ indicates the encoding bases to be used, 0 for σ_z and 1 for σ_x, while string $k^{(s)}$ denotes the eigenstate of the bases, 0 refers to positive eigenstate and 1 refers to the negative eigenstate. Thus, the n-qubit quantum money state associated with the serial number s and the secret bit-strings $b^{(s)}$ and $k^{(s)}$ can be written as:

$$|\Psi^{(b,k)}\rangle = \otimes_{i=1}^{n} |\psi_i^{(b_i,k_i)}\rangle \,, \tag{3.37}$$

where $|\psi_i^{(b_i,k_i)}\rangle \in \{|0\rangle, |1\rangle, |+\rangle, |-\rangle\}$.

For verification, the bank asks the client to send the quantum states, which requires a quantum channel. This is termed as *quantum verification.* A major problem in the implementation of a quantum channel, is that the coherence of the states has to be maintained throughout the duration of the transmission or else the states decohere and the bank declares the money to be invalid. Also, an adversary with access to the channel might intentionally change the states by performing some measurements or can pretend to be the bank to steal the money, thus hindering the verification process for an honest client. This is one of the major drawbacks of Wiesner's scheme.

The bank measures each of the n-qubits in $|\Psi^{(b,k)}\rangle$ in the correct preparation basis according to the bit-string $b^{(s)}$ and if the result matches with the bit-string $k^{(s)}$, the money is said to be valid. In the honest scenario, considering no decoherence, the verification is always successful, $p_h = 1$.

In the original scheme, if the money sent to the bank for verification is declared to be invalid, then the bank can simply discard the money or the bank sends back the invalid money to the client. If it is the latter scenario, a dishonest client can interact adaptively with the bank, and the money will be counterfeited. To learn one of the bits of a valid money, the adversary can apply σ_x on the said qubit, send the money to the bank for verification; if the bank's response is valid then it is an eigenvector of σ_x, then σ_x measurement will reveal the state and if the response is invalid, the adversary applies σ_x to recover the original qubit and measures in σ_z basis to learn the actual bit. The adversary can now follow the same procedure to learn all of the bits and counterfeit

is successful. This interaction of the adversary with the bank, i.e., depending on the bank's answer to adapt the measurements to gain desired results, is called an adaptive attack. This is the second drawback of Wiesner's money scheme [48].

Let us consider a dishonest client interested in counterfeiting the money, i.e., producing an extra copy of the money that can be sent to two branches of the bank for verification. Due to the no-cloning theorem and the uncertainty principle, an adversary cannot copy the states without modifying some of the states, since the encoding bases (observables) are unknown to the adversary. These modifications will be revealed upon verification and the money will be declared invalid. Thus producing an extra copy of money is simply impossible, guaranteeing unconditional security.

For a single state ($n = 1$), the dishonest client can pass the verification with probability $p_d \leq 3/4$. The upper bound is achieved when the dishonest client measures the state in one of the random encoding bases. Half the time, he guessed the correct basis for which he identifies the correct state and half the time he has chosen the wrong basis and thus has a incorrect state. If this state is now sent to the bank for verification, if the chosen basis was correct the verification is successful with probability 1, but if the chosen basis is wrong the probability of successfully passing the verification is 1/2. Therefore, the successful counterfeiting probability is $\frac{1}{2}.1 + \frac{1}{2}.\frac{1}{2} = \frac{3}{4}$.

For a quantum money consisting of n qubits, the honest success probability remains 1, $p_h(n) = 1$. However, the adversary's counterfeiting probability can be made arbitrarily close to 0. This is because n individual attacks on n-qubits is indeed the optimal way of counterfeiting rather than a general attack [47, 50, 52]. Thus, for an n-qubit state, the counterfeiting probability reads $p_d(n) \leq (3/4)^n$.

In 2012, Molina *et al.* [50] presented a detailed analysis on the security bounds of Wiesner's money scheme based on semi-definite programming (SDP). As mentioned earlier, in case of Wiesner's money scheme counterfeiting equates cloning. The idea is to pass the verification test at two banks independently. Cloning of the states can be described by a quantum channel, and the verification at different banks is described by the particular state projective measurement.This problem can be then re-written in terms of an SDP problem with the constraints being that the quantum channel is a completely-positive and trace-preserving (CPTP) map. The authors generalized the scheme for other state ensembles and higher dimensional systems.

3.2.3 Private-key with classical verification money schemes

To address the two previous drawbacks, Gavinsky [49] in 2011, introduced a quantum money scheme with *classical verification*, based on quantum retrieval games, involves three rounds of classical communication between the client and the bank. The verification process involves answering randomly selected challenge questions given by the bank. A counterfeit for this scheme is considered successful, if for a given credit card, the adversary is able to answer two sets of independent challenge questions from two different banks simultaneously. The security relies on the fact that a single random challenge question can be answered with certainty, while any two randomly selected challenge questions can not be answered with unit probability. The classical communication

channel can be unencrypted, even the messages can be openly broadcasted.

The scheme also prevents against an adversary pretending to be a bank to steal the money during the process of verification. Gavinsky also shows that the scheme is secure against adaptive attacks, thus making the money scheme more realistic and secure than Wiesner's money scheme. The drawback of the protocol is that a verification of the money states implies its destruction, the states can no longer be used after a single verification process similar to the Wiesner's scheme. This protocol, is also not realistic since it uses impractical fingerprint states and only works when no experimental noise is taken into consideration.

In [50], along with providing a detailed analysis on the security bounds of Wiesner's money scheme based on SDP's. The authors also introduced a variant of Wiesner's money scheme with classical communication for verification, where the probability of a successful counterfeiting is $(3/4 + \sqrt{2}/8)^n$, n being the number of states in the credit card.

Further independent works of quantum money with classical verification based on quantum retrieval games (QRG) include works by Pastawaski et al [51], Georgiou *et al.* [52] and Amiri et al [53]. In [51], the authors extend the Wiesner's money scheme to incorporate noise for a practical implementation: the errors associated with encoding, storage and decoding of individual qubits, and provide a security proof for the new model with tighter bounds. This money scheme with classical verification uses only two rounds of communication and tolerates noise up to $(1/2 - 1/\sqrt{8}) \approx 14.6\%$. Noise tolerance is be defined as the maximum probability with which an honest client get an invalid response upon verification of a valid money. It is a measure of robustness of the scheme; the higher the noise tolerance, the higher is the robustness of the scheme.

In [52], the authors presented an improvement over Gavinsky's scheme, reducing the classical communication required for verification to a single round. Based on 1-out-of-2 QRG, this scheme tolerates noise up to 12.5%. The money scheme proposed by Amiri et al. [53] is yet another classical verification private-key money scheme with only one round of communication between the bank and the client. This scheme has a noise tolerance of 23%. The authors also claim that any hidden-matching QRG based money schemes can have maximum noise tolerance limit of 25%.

3.2.4 Public-key money schemes

In the classical world, public-key money schemes are based on the inability to copy the intricate coloring and hologram designs. Similarly, public-key quantum money schemes (or quantum banknotes) cannot base their security solely on the no-cloning theorem, since anyone who can verify the state and has a copy can produce additional copies of the state [55]. Thus, quantum banknotes require some computational assumptions such as knot problems or quantum obfuscation [56–60]. However, the schemes still boast a security advantage over classical banknotes, since there exists no notion of computational security in classical banknotes. The experimental work from [61] shows how such private-key quantum money can be constructed on-the-fly but unfortunately still forgeable.

3.2.5 Other works

Different variants of quantum money have been proposed over the years such as quantum tokens, coins, cheque, credit cards etc. Though all of these stem from the Wiesner's primitive money scheme, there are some subtleties involved with respect to the verification process. Let us consider the credit card scenario where a client needs to verify the money classically using a vendor's measurement terminal. Now, the question arises, does the client trust the vendor's terminal? Even if (s)he does not trust the terminal, is the security and verification process compromised? Is the credit card still unforgeable? Bozzio et al. in [62], address this problem in both trusted and untrusted terminal scenarios and show that implementation of such protocols is indeed possible. Another independent work by Horodecki and Stankiewicz [63] also provides a semi-device-independent quantum money scheme in a stronger threat scenario with a dishonest mint, but does not consider a practical implementation.

Kent introduced the idea of S-money [64], quantum money schemes (virtual tokens) used on a network of space-time points with an enforced causal order, based on summoning tasks. Advantages of this idea include near-instant verification and unforgeability without quantum storage. Kent with Pitalua-Garcia [65] extends the idea of S-money to allow flexible transfer between clients without any client privacy compromisation. In [66], Radian and Sattath introduces semi-quantum money, where the quantum minting process is done by the client. The verification process is classical. The security is computational (rather than information theoretic), based on the hardness of the *Learning With Errors* (LWE) problem.

There have been only two proof-of-principle experimental demonstrations of private-key quantum money to date, by Bozzio *et al.* [67] which is based on the theoretical scheme of [52] and by Guan *et al.* [68] based on the theoretical scheme of [53]. In [67], the authors encode information in polarized weak coherent states and achieves the error rate of around 4% which is well under the maximum noise tolerance of 12.5%, however this implementation does not take into account the losses, while in [68], the encoding is based on the phase parity of corresponding pairs of weak coherent states. This scheme has an error rate of 3%, making it secure with the theoretical limit being 16.6%. Unfortunately, none of these experiments implement the storage of quantum money states.

CHAPTER 4

COMPOSABLE SECURITY OF TWO-WAY CV-QKD PROTOCOLS

This chapter presents a general framework encompassing a plethora of QKD protocols, including standard one-way protocols, measurement-device-independent protocols, as well as some two-way protocols, or any other QKD protocol which involves preparation of coherent states modulated via Gaussian distribution and heterodyne detection for measurement. The main interest of this framework is that the corresponding protocols are all covariant with respect to the action of the unitary group U(n), implying that their security can be established thanks to a Gaussian de Finetti reduction. Although the main motivation for this work was to provide a composable security proof for two-way CV-QKD, since such protocols are more robust to noise than their one-way counterparts [74], the framework that we have developed is of general interest. We remark that there have been significant developments in two-way QKD protocols over the years [75–79, 93], however, a composable security proof was left as an open question.

In the QKD section of chapter 3, we have seen that symmetrization of the states or the data is a crucial part of a QKD protocol with coherent states and heterodyne detection. The symmetrization steps makes the states invariant to the unitary group which allows us to bound the covariance matrix in the parameter estimation step. This stronger unitary symmetry also paves the way for Gaussian de Finetti theorem to act and provide us with a composable security proof against general attacks. Though the symmetrization step is costly to implement and breaks the permutation symmetry of the original protocol, the benefit it provides is unquestionable. However, the benefit is actually due to the unitary invariance $U(n)$. If we are able to design a protocol that inherently possesses the unitary invariance, then our protocol might not require any active symmetrization. In this chapter, we present a composable security proof for CV-QKD protocols that inherits this symmetry.

Here we will restrict our attention to the "entanglement-based" (EB) protocols where the parties prepare bipartite pure states, and exchange optical modes through an untrusted quantum channel and an authenticated classical channel. This is without loss of generality since any prepare and-measure (PM) protocol admits an EB version with the same security (as shown in section 3.1.1), and it is therefore sufficient to analyze the

latter version. The framework include all protocols where Alice and Bob prepare two-mode squeezed states, possibly perform two-mode squeezing operations or beamsplitter transformations, and finally measure their respective modes with heterodyne detection.

4.1. Symmetry

A standard argument for establishing the security of a protocol is to consider attacks displaying the same symmetry as the protocol, generally permutation-invariance. Then the usual de Finetti theorem precisely asserts that permutation-invariant states have an independent and identically distributed (i.i.d.) structure $\rho_{AB}^n = \rho_{AB}^{\otimes n}$, where n is the number of quantum signals exchanges and we can consider collective attacks. However, for CV protocols, this method does not work on the account of infinite-dimensional Hilbert (Fock) space. But, the CV protocols considered here, show a specific unitary phase-space symmetry, which allows one to exploit the Gaussian de Finetti theorem and consider the class of Gaussian collective attacks, which are easier to manage.

These CV-QKD protocols are invariant to the action of unitary group $U(n)$. For a given n-mode Fock space with annihilation operators $\mathbf{a} = (a_1, ..., a_n)$, the unitary group acts as follows

$$\mathbf{a} \to U\mathbf{a}, \qquad \mathbf{a}^\dagger \to \bar{U}\mathbf{a}\dagger \tag{4.1}$$

where $\mathbf{a}^\dagger$ is the creation operator and $\bar{U}$ is the complex conjugate of U, an unitary matrix. The unitary group is the 3-fold intersection of the orthogonal, complex, and symplectic groups:

$$U(n) = Sp(2n, \mathbb{R}) \cap O(2n) \cap GL(n, \mathbb{C}). \tag{4.2}$$

A beamsplitter with transmittance t and a two-mode squeezing operator of gain g act on a 2-mode Hilbert space with annihilation operators a and b via the respective transformations

$$[a, a^\dagger, b, b^\dagger]^\top \to B(t)[a, a^\dagger, b, b^\dagger]^\top, \quad [a, a^\dagger, b, b^\dagger]^\top \to S(g)[a, a^\dagger, b, b^\dagger]^\top \tag{4.3}$$

with

$$B(t) = \begin{bmatrix} \sqrt{t}\mathbb{I}_2 & -\sqrt{1-t}\mathbb{I}_2 \\ \sqrt{1-t}\mathbb{I}_2 & \sqrt{t}\mathbb{I}_2 \end{bmatrix}, \quad S(g) = \begin{bmatrix} \sqrt{g}\mathbb{I}_2 & -\sqrt{g-1}\sigma_x \\ \sqrt{g-1}\sigma_x & \sqrt{g}\mathbb{I}_2 \end{bmatrix}$$

where $t \in [0, 1]$ and $g \geq 1$. This subgroup of the symplectic group $\mathrm{Sp}(2n, \mathbb{R})$ is isomorphic to the unitary group $U(n)$.

Both Alice and Bob perform a heterodyne measurement of their respective n modes. A heterodyne detection is a generalized measurement where the POVM elements are the coherent states, and satisfies the resolution of identity in an n-mode Fock space

$$\mathbb{I}_{\mathcal{H}} = \frac{1}{\pi^n} \int |\alpha\rangle \langle\alpha| \, \mathrm{d}\alpha \tag{4.4}$$

$\mathrm{d}\alpha$ being the uniform measure in $\mathbb{C}^n$. The measurement can be rewritten in a quantum-classical map as follows

$$\mathcal{M}(\rho) = \frac{1}{\pi^n} \int \langle\alpha| \rho |\alpha\rangle |\alpha^{cl}\rangle \langle\alpha^{cl}| \, \mathrm{d}\alpha, \tag{4.5}$$

where the superscript "cl" indicates the classical encoding of the value α.

The probability distribution of their outcomes is given by the Q-function of the state $\rho_{AB}^n \in (\mathscr{H}_A \otimes \mathscr{H}_B)^n : Q_\rho(\mathbf{x}_A, \mathbf{p}_A, \mathbf{x}_B, \mathbf{p}_B)$. We can rewrite the unitary matrix in its real and imaginary parts as $U = V - \iota W$, where V=Re(U) and W = -Im(U). So, the displacement vector (**x**,**p**) transforms as

$$\begin{pmatrix} \mathbf{x} \\ \mathbf{p} \end{pmatrix} \to \begin{pmatrix} V & W \\ -W & V \end{pmatrix} \begin{pmatrix} \mathbf{x} \\ \mathbf{p} \end{pmatrix}. \tag{4.6}$$

Therefore, Q-function associated with the new state $\rho' = (\mathcal{U} \otimes \bar{\mathcal{U}})\rho_{AB}^n(\mathcal{U} \otimes \bar{\mathcal{U}})^\dagger$ is

$$Q_\rho(\mathbf{x}_A, \mathbf{p}_A, \mathbf{x}_B, \mathbf{p}_B) = Q_\rho(V\mathbf{x}_A - W\mathbf{p}_A, W\mathbf{x}_A + V\mathbf{p}_A, V\mathbf{x}_B + W\mathbf{p}_B, -W\mathbf{x}_B + V\mathbf{p}_B), \tag{4.7}$$

where $\mathcal{U}$ is the action of symplectic operation on the Fock space.

In other words, these protocols are covariant w.r.t the action of the unitary group $U(n)$, meaning the beamsplitters, two-mode squeezing and heterodyne detection all commute with the action of the unitary group as follows:

$$[\mathcal{S}^{\otimes n}, \mathcal{U} \otimes \bar{\mathcal{U}}] = 0, [\mathcal{B}^{\otimes n}, \mathcal{U} \otimes \mathcal{U}] = 0 \text{ and } [\mathcal{M}^{\otimes n}, \mathcal{U}] = 0 \tag{4.8}$$

where $\mathcal{S}, \mathcal{B}, \mathcal{M}$ and $\mathcal{U}$ refers to the action of the symplectic operations S, B, M and U respectively.

For this reason, protocols that start with vacuum states and where the honest parties apply two-mode squeezing (to prepare TMSSs), beamsplitters and perform heterodyne measurements will be covariant with respect to $U(n)$ acting as a product of the form $\mathcal{U}^{\otimes p} \otimes \bar{\mathcal{U}}^{\otimes q}$, where $p + q$ is the total number of modes held by Alice and Bob, for each round of the protocol. For instance, in case of one-way no-switching protocol of [30], the optical scheme is covariant to $\mathcal{U}_A \otimes \bar{\mathcal{U}}_B$.

4.2. Security proof using Gaussian de Finetti reduction

A full security proof consists of two steps: proving security against the restricted collective attacks and then applying the Gaussian de Finetti reduction to show security against general attacks. As mentioned earlier, for protocols which are invariant under the action of unitary group $U(n)$, it is sufficient to consider Gaussian collective attacks. For the implementation of the reduction theorem, we still need to truncate the Fock space so that it can be replaced by a finite-dimensional vector space such that we can consider states which are invariant under the action of unitary group but occupy a very small subspace of Fock states. More specifically, the restriction on the dimension of subspace containing K (finite number) photons grows polynomially in K, rather than exponentially as in the total Fock space.

From Eq. (3.6), we know that a protocol $\mathcal{E}$ is ϵ-secure if it is indistinguishable from an ideal protocol $\mathcal{F}$. Mathematically,

$$||\mathcal{E} - \mathcal{F}||_\diamond := \sup_{\rho_{ABE}} ||(\mathcal{E} - \mathcal{F}) \otimes \mathbb{I}_{\mathscr{K}}(\rho_{ABE})||_1 < \epsilon, \tag{4.9}$$

where the supremum is taken over all density operators on $(\mathscr{H}_A \otimes \mathscr{H}_B)^{\otimes n} \otimes \mathscr{K}$ for an arbitrary system $\mathscr{K}$.

It has been shown that for protocols displaying such symmetry, it is enough to consider a single-state; a purification of a special mixture of Gaussian i.i.d. states, $SU(p,q)$ coherent states [73], instead of optimising over the whole space.

Recall that, a QKD protocol consists of three main steps-(a) state preparation, (b) measurement and parameter estimation and (c) classical post-processing: error reconciliation and privacy amplification. Depending on the preparation we have either PM based protocols or EB protocols. Here, Alice and Bob prepare two-mode squeezed states, perform some symplectic transformations and send a mode of their choosing to the other party while keeping one for themselves. They perform heterodyne detection on their modes (all) to obtain the classical strings, X for Alice and Y for Bob, and one of them is chosen to be the raw key $Z = f(X)$ or $f(Y)$, via a key map f of choice. The size of the strings depends on the number of modes held by the parties. In one-way protocols we have one mode for each of the parties, for two-way we have two modes for Alice and Bob, $X = (X_1, X_2)$ and $Y = (Y_1, Y_2)$.

The goal of the parameter estimation procedure is to obtain a min-entropy resource [84]. It is a test $\mathcal{T}$ that checks whether the correlations between X and Y are sufficient to imply a lower bound on $H^{\epsilon}_{min}(Z|E)\rho_{ZE}$, where ϵ is the smoothing parameter, Z is the raw key, and E is the Eve's quantum register. If the test passes, the protocol continues, otherwise it aborts.

The test consists of a check which ensures that the energy measured on a small number of $k << n$ modes is below some threshold due to the truncation of Fock space and the covariance between Alice and Bob is large enough. The truncation of the Fock space can be defined by a CP map $\mathcal{P}$ which projects onto the finite dimensional subspace (corresponding to states containing at most K photons in $2n$ modes), d_A and d_B being the dimension of the finite dimensional subspace of Alice and Bob respectively. This is strictly a technical tool for security analysis, that does not need to be implemented in practice. It is to ensure the input states live in a finite-dimensional subspace.

The parameter estimation test takes the element of the Gram matrix, $\mathrm{Gram}(X,Y)$ [1] of the vectors $X_1, ..., X_{d_A}, Y_1, ..., Y_{d_B}$ or their conjugate $\bar{X}_i$ or $\bar{Y}_j$ [depending on whether the corresponding mode is transformed according to U or $\bar{U}$ through the U(n) symmetry] as input to estimate the three quantities

$$\begin{aligned}
\Sigma_a &:= \frac{1}{2n}\sum_{i=1}^{n}[\langle q_{A_i^2}\rangle + \langle p_{A_i^2}\rangle] \\
\Sigma_b &:= \frac{1}{2n}\sum_{i=1}^{n}[\langle q_{B_i^2}\rangle + \langle p_{B_i^2}\rangle] \\
\Sigma_c &:= \frac{1}{2n}\sum_{i=1}^{n}[\langle q_{A_i}, q_{B_i}\rangle + \langle p_{A_i}, p_{B_i}\rangle]
\end{aligned} \tag{4.10}$$

The test is considered to be a success if the estimated quantities follow the following

[1] m x m matrix with $m = d_A + d_B$

relations:

$$[\Sigma_a^{est} < \Sigma_a^{max}] \wedge [\Sigma_b^{est} < \Sigma_b^{max}] \wedge [\Sigma_c^{est} > \Sigma_c^{max}], \tag{4.11}$$

the superscript *est* refers to the estimated value of the respective quantities. The test can be viewed as a classical function with $\mathrm{Gram}(X, Y)$ as input and passes if it belongs to some predefined set of acceptable covariance matrices, and fails otherwise, in which case the protocol aborts. The protocol (and in particular, the acceptance region) is in general designed in order to perform well when the adversary is passive; it means that the quantum channel is expected to be a covariant bosonic thermal channel which is a good model for fiber-based quantum communication

If the test passes, then it is possible to have a lower bound on the min-entropy resource. The next logical question that arises is that after this step if the protocol is still invariant w.r.t the action of unitary group. The map $\mathcal{T}$ still preserves the symmetry of the protocol. This is due to the choice of the set of acceptable Gram matrices, which is a direct consequence of the invariance of the optical structure of the protocol. And we have already shown that the heterodyne measurement also preserves the symmetry. Therefore the map $\mathcal{T} \circ \mathcal{M}$ is also invariant w.r.t the action of unitary group.

From [84], we learn that a key distribution protocol can be divided in two parts, construction of a min-entropy resource followed by the distillation of the resource into a secret key. Resource construction is composable in nature, therefore proving security of the protocol reduces to proving that the protocol constructs a min-entropy resource. The author also proves security for a generic key distillation protocol for any min-entropy resource. So, it suffices to determine the existence of a min-entropy resource, to establish security proof of the protocol. Therefore, if $\mathcal{T} \circ \mathcal{M}$ is invariant w.r.t the action of unitary group, then the protocol is invariant w.r.t the action of the unitary group and we can establish security against collective attacks by using de Finetti states, which in our case are $SU(m, m)$ coherent states, where m is total number of modes of both parties per round.

In [72], with the de Finetti reduction theorem, it is shown that ϵ-security against Gaussian collective attacks then implies ϵ'-security against general attacks, with $\epsilon'/\epsilon = O(n^{m^2})$. In other words, it is sufficient to show that the protocol is secure when the overall initial pure state ρ_{ABE} is a mixture of such $SU(m, m)$ coherent states.

Please note that, in this security proof, there has been no mention of active symmetrization since we have restricted our analysis to $\mathcal{T} \circ \mathcal{M}$ instead of the whole QKD protocol. The latter steps of a QKD protocol do not commute with the unitary group (because of error reconciliation for instance). But, the work by Portmann [84] ensures that we only need to realize a min-entropy resource, and till that step, if we are still unitary invariant the protocol is secure.

4.3. An example: two-way CV-QKD with heterodyne detection

In this section, we apply the above-mentioned security proof to the case of two-way CV-QKD protocols. In a two-way protocol, the exchange of quantum states is bi-directional.

Both Alice and Bob send quantum states to one another. In the PM version, Alice sends coherent states with a Gaussian modulation to Bob, who performs a Gaussian displacement (via a beamsplitter) to the mode he receives and sends it back through the quantum channel. Alice measures the output mode with heterodyne detection, and computes a weighted sum of this result and the value of her initial coherent state. This serves as the raw key. The weights in the sum as well as the variances of the Gaussian distribution should be optimized to yield the maximum key rate. Note that this protocol differs a little bit from the one of Ref. [74] in that here Bob always performs a displacement, that the weights of the sum are optimized and that Bob also exploits the second output of his beamsplitter to guess the raw key. The setup of the corresponding EB version is depicted in Fig.4.1.

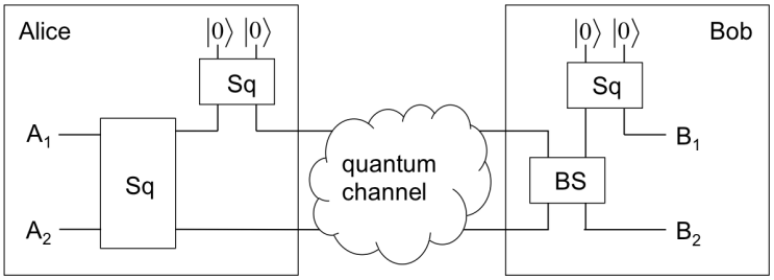
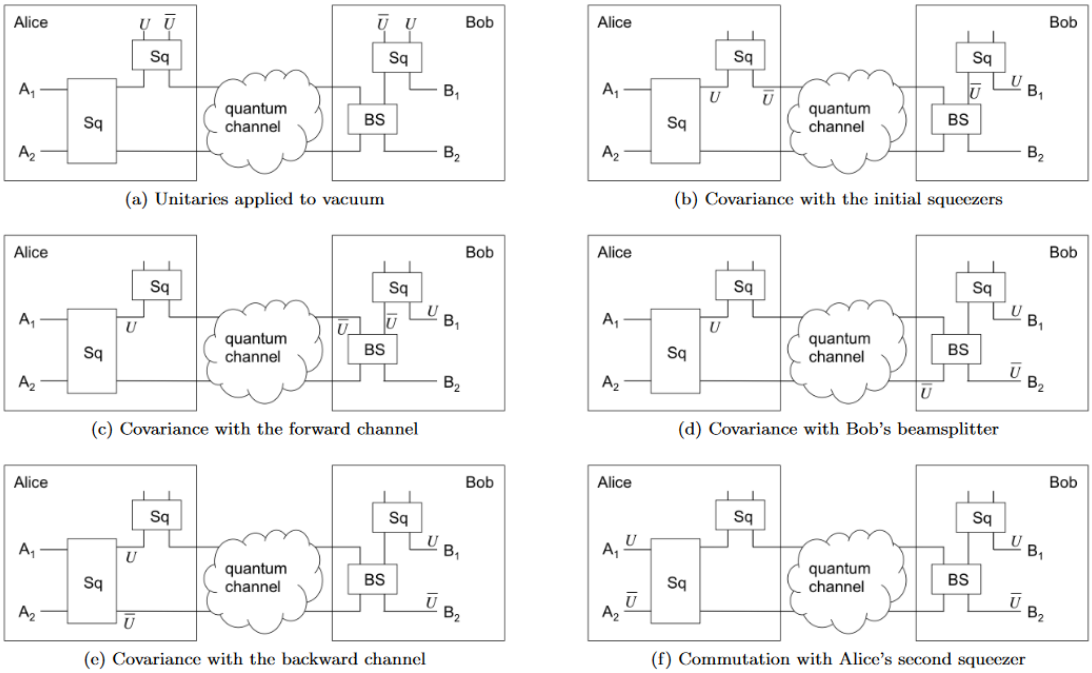


Figure 4.1: Optical scheme of the EB version of the two-way protocol: 'Sq' is a two-mode squeezer; 'BS' is a beamsplitter required to implement the random displacement by Bob.

In the EB version of the protocol, both Alice and Bob have a two-mode squeezed state. Alice keeps one of the modes and sends the other one to Bob. After receiving the mode, Bob combines one of his mode with the received mode via a beamsplitter: this effectively implements a Gaussian displacement on the received mode. The displaced mode is then sent back to Alice. Alice combines her two modes through a a two-mode squeezer. One of the output modes is then measured with heterodyne detection and the measurement result, serves as the raw key. None of the three two-mode squeezers are needed in the PM version as they can always be simulated classically.

If the quantum channel is covariant with respect to $U(n)$[2], as expected in the case of a passive adversary and a bosonic phase-insensitive channel, the quantum state held in registers A_1, A_2, B_1, B_2 by Alice and Bob is invariant under the unitary transformation $\mathcal{U}_{A_1} \otimes \bar{\mathcal{U}}_{A_2} \otimes \mathcal{U}_{B_1} \otimes \bar{\mathcal{U}}_{B_2}$ (see 4.2). For this protocol, the set of acceptable covariance matrices will therefore satisfy the same symmetry. For this reason, it is natural to choose an accepting region for the parameter estimation test that also satisfies this symmetry.

[2]We do not need to assume covariance with respect to $U(n)$ for the security proof to hold. However, if the channel isn't covariant, then the covariance matrix Alice and Bob evaluate will not be good enough to extract a key.



(a) Unitaries applied to vacuum

(b) Covariance with the initial squeezers

(c) Covariance with the forward channel

(d) Covariance with Bob's beamsplitter

(e) Covariance with the backward channel

(f) Commutation with Alice's second squeezer

Figure 4.2: Propagation of the unitaries through the circuit of the two-way protocol. 'Sq' and 'BS' stand respectively for two-mode squeezer and beamsplitter. One starts by applying unitaries U or $\bar{U}$ to the input of the protocol and propagates these operators through the setup. The input of the setup is the vacuum and therefore invariant under the action of U or $\bar{U}$. (a) Unitaries applied to vacuum, (b) Covariance with the initial squeezers, (c) Covariance with the forward channel, (d) Covariance with Bob's beamsplitter, (e) Covariance with the backward channel and (f) Commutation with Alice's second squeezer.

This means that the first part of the protocol, that realizes the min-entropy resource, is indeed covariant with respect to the action of the unitary group $U(n)$, and that one can apply the de Finetti reduction in order to prove the composable security of the protocol against general attacks. In particular, this means that Gaussian attacks, described by $SU(4,4)$ generalized coherent states, are asymptotically optimal and that the asymptotic key rate can be computed with the techniques described in chapter 3.

For the sake of completion, we find the covariance matrix of the state in some realistic scenarios. We consider the quantum channel to be the bosonic thermal noise channel of transmittance τ and excess noise ξ, as mentioned earlier. For the sake of convenience, we define a few registers, which are labelled in the following figure.

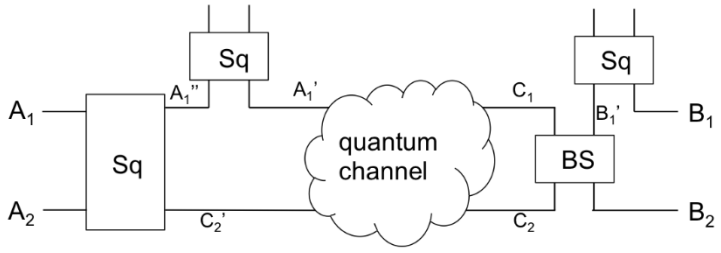


Figure 4.3: Description of the EB version of the two-way protocol along with some extra notations to help understand the steps and the modes propagation in the protocol.

Both Alice and Bob start with a TMSS with variances V_A and V_B respectively. The covariance matrix reads,

$$\gamma_{A_1''A_1'B_1'B_1} = \mathbb{I}_8 + \begin{bmatrix} v & \boldsymbol{z} & & \\ \boldsymbol{z} & v & & \\ & & v' & \boldsymbol{z}' \\ & & \boldsymbol{z}' & v' \end{bmatrix}, \tag{4.12}$$

where

$$v = V_A + 1, \quad z = \sqrt{v^2 + 2v}, \quad v' = V_B + 1, \quad z' = \sqrt{v'^2 + 2v'}$$

and all the matrices are block-matrices. We use boldface to indicate a 2×2 matrix that is proportional to σ_z. Otherwise, the block is simply proportional to $\mathbb{I}_2$.

Alice sends the mode A_1' to Bob via the quantum channel, yielding:

$$\gamma_{A_1''C_1B_1'B_1} = \mathbb{I}_8 + \begin{bmatrix} v & \sqrt{\boldsymbol{\tau}}\boldsymbol{z} & & \\ \sqrt{\boldsymbol{\tau}}\boldsymbol{z} & \tau(v+\xi) & & \\ & & v' & \boldsymbol{z}' \\ & & \boldsymbol{z}' & v' \end{bmatrix}.$$

The beamsplitter interaction is given by:

$$\begin{aligned} \gamma_{A_1''C_2B_2B_1} &= (\mathbb{I}_2 \oplus B(T) \oplus)\, \gamma_{A_1''C_1B_1'B_1} \left(\mathbb{I}_2 \oplus B(T)^\top \oplus \mathbb{I}_2\right) \\ &= \mathbb{I}_8 + \begin{bmatrix} v & \sqrt{\boldsymbol{T}\boldsymbol{\tau}}\boldsymbol{z} & -\sqrt{(\mathbf{1}-\boldsymbol{T})\boldsymbol{T}}\boldsymbol{z} & \\ * & T\tau(v+\xi) + (1-T)v' & \sqrt{(1-T)T}\tau(\tau(v+\xi) - v') & \sqrt{(\mathbf{1}-\boldsymbol{T})\boldsymbol{T}}\boldsymbol{z}' \\ * & * & Tv' + (1-T)\tau(v+\xi) & \sqrt{\boldsymbol{T}}\boldsymbol{z}' \\ * & * & * & v' \end{bmatrix}. \end{aligned}$$

Since the matrix is symmeteric, we simply write $*$ in the bottom left matrix to improve the readability.

Bob sends back the mode C_2 via the quantum channel to Bob, the covariance matrix

$\gamma_{A_1''C_2'B_2B_1}$ reads

$$\mathbb{I}_8 + \begin{bmatrix} v & \boldsymbol{\sqrt{T}\tau z} & \boldsymbol{-\sqrt{(1-T)T}z} & \\ * & T\tau^2(v+\xi)+(1-T)\tau v'+\tau\xi & \sqrt{(1-T)T\tau}(\tau(v+\xi)-v') & \boldsymbol{\sqrt{(1-T)T}z'} \\ * & * & Tv'+(1-T)\tau(v+\xi) & \boldsymbol{\sqrt{T}z'} \\ * & * & * & v' \end{bmatrix}$$

$$= \begin{bmatrix} V_A & \boldsymbol{z_1} & \boldsymbol{z_2} & \\ * & V_1 & z_{12} & \boldsymbol{z_1'} \\ * & * & V_2 & \boldsymbol{z_2'} \\ * & * & * & V_B \end{bmatrix}, \text{with} \begin{cases} V_1 = T\tau^2(v+\xi)+(1-T)\tau v'+\tau\xi+1, \\ V_2 = Tv'+(1-T)\tau(v+\xi)+1, \\ z_{12} = \sqrt{(1-T)T\tau}(\tau(v+\xi)-v'), \\ z_1 = \sqrt{T}\tau z, \quad z_2 = -\sqrt{(1-T)T}z, \\ z_1' = \sqrt{(1-T)T}z', \quad z_2' = \sqrt{T}z' \end{cases}$$

Alice upon receiving the states, process her two modes using a two-mode squeezing operator, in order to form the raw key. This is performed to get a weighted combination of the two modes. The squeezing parameter $g > 1$ is optimized so as to maximize the key rate:

$$\gamma_{A_1A_2B_2B_1} = (S(g) \oplus \mathbb{I}_4)\gamma_{A_1''C_2'B_2B_1}(S(g) \oplus \mathbb{I}_4)^\top = \begin{bmatrix} \gamma_A & \gamma_C \\ \gamma_C^\top & \gamma_B \end{bmatrix}$$

where

$$\gamma_A = \begin{bmatrix} gV_A+(g-1)V_1+2\sqrt{g(g-1)}z_1 & \boldsymbol{(2g-1)z_1-\sqrt{g(g-1)}(V+V_1)} \\ * & (g-1)V+gV_1-2\sqrt{g(g-1)}z_1 \end{bmatrix},$$

$$\gamma_B = \begin{bmatrix} V_2 & \boldsymbol{z_2'} \\ * & V_B \end{bmatrix} \quad \text{and} \quad \gamma_C = \begin{bmatrix} \boldsymbol{\sqrt{g}z_2-\sqrt{g-1}z_{12}} & -\sqrt{g-1}z_1' \\ \sqrt{g}z_{12}-\sqrt{g-1}z_2 & \boldsymbol{\sqrt{g}z_1'} \end{bmatrix}.$$

The raw key is the measurement outcome X_2 obtained by performing heterodyne detection on mode A_2. Now, one can easily obtain the key rate following the key rate calculation steps presented in section 3.1. Finally, the key rate is calculated by optimizing over the choices of the variances V_A, V_B, transmittance T and squeezing gain g. Note that, we have used the quantum channel twice in this protocol, thus to calculate the key rate per channel use, we have to introduce a factor of $1/2$ in the key rate formula given by Eq. 3.16,

$$K = \frac{1}{2}(\beta I(X_2 : (Y_1, Y_2)) - \chi(X_2; E)), \tag{4.13}$$

where β is the so-called reconciliation efficiency.

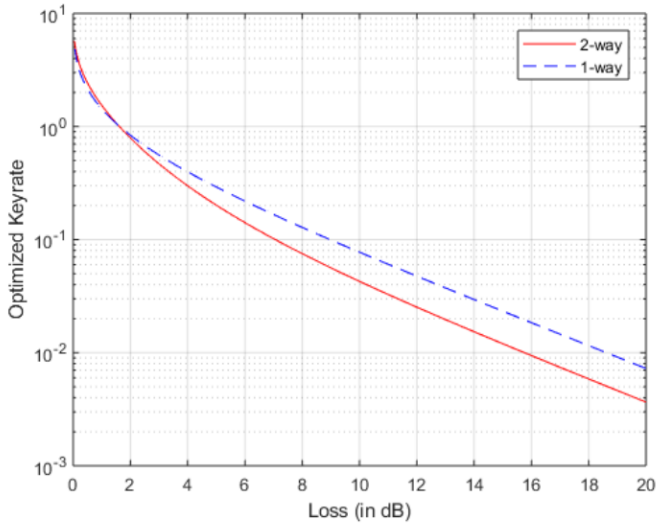


Figure 4.4: Secret key rate of the two-way CV QKD protocol (full line) and of the one-way no-switching protocol (dashed line), assuming $\xi = 0$ and $\beta = 1$.

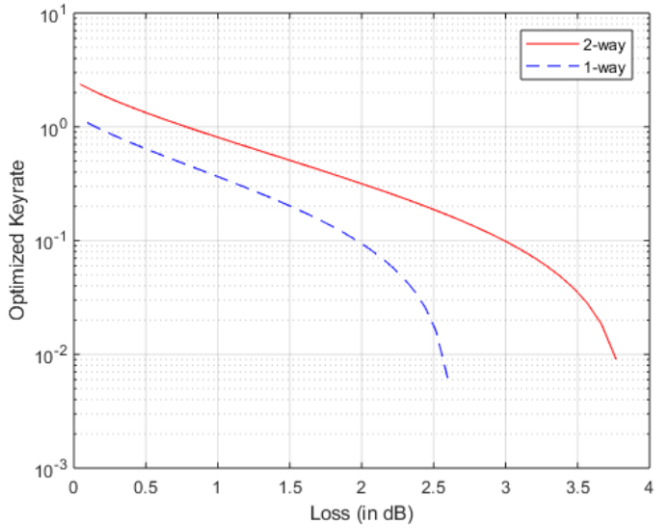


Figure 4.5: Secret key rate of the two-way CV QKD protocol (full line) and of the one-way no-switching protocol (dashed line), assuming $\xi = 0.1$ and $\beta = 0.95$.

We plot on Fig. 4.4 and Fig. 4.5, the asymptotic key rate of the two-way protocol and of the (one-way) no-switching protocol. In case of Fig. 4.4, we consider a noiseless channel ($\xi = 0$) and we also assume the reconciliation efficiency to be perfect ($\beta = 1$). One can recover the key rate of the one-way protocol similarly by imposing $V_A = 1$, i.e., Alice sends the vacuum to Bob, fixing $\tau = 0$ so that mode B_2 contains the vacuum, and getting rid of the final squeezer in Alice's lab (by choosing $g = 1$). We note that the

two-way protocol slightly outperforms the one-way protocol in the regime of ultra low loss (T close to 1). In Fig. 4.5, we choose a noisy channel with $\xi = 0.1$ and realistic reconciliation efficiency $\beta = 0.95$. The advantage of the two-way protocol is clear in this case.

In Fig. 4.6, we plot the tolerable excess noise of the two-way and one-way no-switching protocol against the channel transmittance τ, that is the value of ξ for which the key rate becomes 0. As, we can see the two-way protocol is more robust to noise than the no-switching protocol.

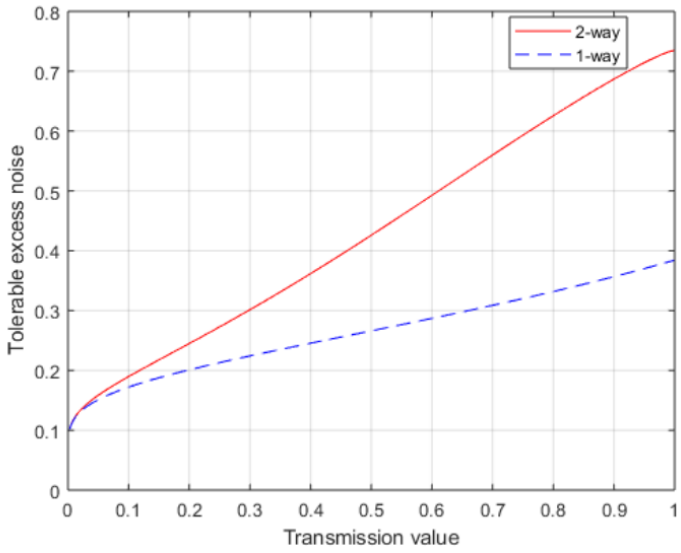


Figure 4.6: Maximum tolerable excess noise ξ for the two-way CV QKD protocol (full line) and the one-way no-switching protocol (dashed line), assuming perfect reconciliation efficiency.

4.4. Measurement-Device Independent (MDI)-QKD

At first sight, MDI-CV-QKD does not quite fit our framework since it involves a third node, controlled by Charlie, performing a Bell measurement consisting of homodyning two modes. To be precise, the idea is that both Alice and Bob prepare a TMSS, keep one mode each and send the other one to Charlie who performs entanglement swapping, publicly announces the results of his Bell measurement, allowing Alice and Bob to conditionally displace their remaining mode in order to create some correlations [82]. In this scenario, one could *a priori* consider that there are four optical modes: one for Alice, one for Bob and two measured by Charlie, hinting that one should appeal to a proof technique similar to that of two-way CV-QKD. This is for instance an approach followed in [89] where it was realized that this scheme has the advantage of not requiring much public communication for parameter estimation. However, this description doesn't seem compatible with the Gaussian de Finetti reduction since the homodyne detection

performed by Charlie breaks the invariance of the protocol under the unitary group $U(n)$.

An alternative approach is to look at this scheme as a special case of one-way CV-QKD by treating Charlie's communication as part of the state distribution: once Alice and Bob's displacements have been performed, the two honest parties are left with a bipartite two-mode quantum state. This is the same situation as after state distribution in the EB version of the no-switching protocol [30]. In this sense, while MDI-CV-QKD is implemented similarly as a two-way CV-QKD protocol, its security can be established by considering it as a one-way CV-QKD, with a Gaussian deFinetti reduction involving $SU(2,2)$ coherent states. Particularly, the reduction from Ref. [72] together with the security proof of Ref.[88] establish the security of MDI-CV-QKD against general attacks (see also [77, 91]).

4.5. Conclusions

In this work, we considered a particular framework of CV-QKD protocols which are invariant with respect to the unitary group $U(n)$ and showed that it is sufficient to establish their security against Gaussian collective attacks. This extends the results of Ref. [72] to two-way protocols which are known to display improved tolerance to noise compared to the no-switching protocol, and provides the first composable security proof for two-way CV-QKD protocols against general attacks. Furthermore, by exploiting the modularity of the QKD protocols as introduced by Portmann, we showed that active symmetrization of the data is not needed for the de Finetti reduction to act and to obtain security.

CHAPTER 5

ASYMPTOTIC SECURITY OF CV-QKD WITH A DISCRETE MODULATION

There exist CV-QKD protocols which enjoy composable security [31,32,72,88], but all of these protocols have one element in common: the protocols are modulated according to a Gaussian distribution. However, Gaussian modulation can never be perfectly achieved in practice, and in real protocols, one merely approximates such a Gaussian by some finite constellation of finite energy [100,101]. Furthermore, a discrete modulation does not only simplify the state preparation procedure [22,24,102,103]; the crucial step of error correction is dramatically simplified with a small constellation of states [104].

In a discrete modulation setup, one simply needs to generate random bits and not Gaussian random variables that would further require to be discretized with sufficient precision. Imagine a protocol where the coherent states are modulated by a discrete distribution and the states are measured by coherent detection techniques; we get the best of both worlds, simpler state preparation, and cheaper and effective measurement setup, both of which are the current industry standard in optical telecommunication. This will also be helpful deploying QKD at large scale. Therefore, establishing the security of this protocol has been a pressing open problem for a long time. The current security proofs pertaining to discrete modulation restrict Eve's possible attacks to emulate a linear quantum channel between Alice and Bob [104–106].

In this chapter, we establish a lower bound on the secure key rate valid against collective attacks in the asymptotic limit of infinitely long keys. We introduce a new proof technique and apply it to the case of quadrature phase-shift keying protocol (QPSK), then we discuss its generalization to larger constellations of quadrature amplitude modulations (QAM). In the asymptotic limit, the secret key rate against collective attacks equates to the secret key rate valid against arbitrary attacks. For a full composable security proof and finite-size key rate, one would require to fully address the parameter estimation procedure, which is not addressed in this thesis, since it needs further considerations and is left for future work. Nonetheless, we will discuss of possibilities how this can be achieved as well as other developments in this field.

5.1. The QPSK protocol

The constellation we study consists of four coherent states $\{|\alpha_k\rangle\}_{k=0...,3}$ with

$$\{|\alpha_k\rangle\} := |i^k\alpha\rangle = e^{-\frac{1}{2}|\alpha|^2}\sum_{n=1}^{\infty} e^{ikn\frac{\pi}{2}}\frac{\alpha^n}{n!}|n\rangle\,, \tag{5.1}$$

where $\alpha > 0$, which will be optimized later. The protocol goes as follows. Alice chooses a random bit-string of length $2L$ $\mathbf{x} = \{x_0, x_1, ..., x_{2L-1}\}$. The successive bit pairs (x_{2l}, x_{2l+1}) are encoded into coherent states $|\alpha_{k_L}\rangle$ with $k_l = 2x_{2l} + x_{2l+1}$. Then she sends the L coherent states to Bob, who performs heterodyne detection on each mode to output another $2L$-string $\mathbf{z} = \{z_0, z_1, ..., z_{2L-1}\}$. The string is then converted to a raw key of 2L bits $\mathbf{y} = \{y_0, y_1, ..., y_{2L-1}\}$ given by

$$(y_{2l}, y_{2l+1}) = \begin{cases} (0,0) \text{ if } z_{2l+1} < z_{2l}, z_{2l+1} \geq -z_{2l}, \\ (0,1) \text{ if } z_{2l+1} \geq z_{2l}, z_{2l+1} > -z_{2l}, \\ (1,0) \text{ if } z_{2l+1} > z_{2l}, z_{2l+1} \leq -z_{2l}, \\ (1,1) \text{ if } z_{2l+1} \leq z_{2l}, z_{2l+1} < -z_{2l}. \end{cases} \tag{5.2}$$

The following diagram makes it clear about the relation between the two bit-strings.

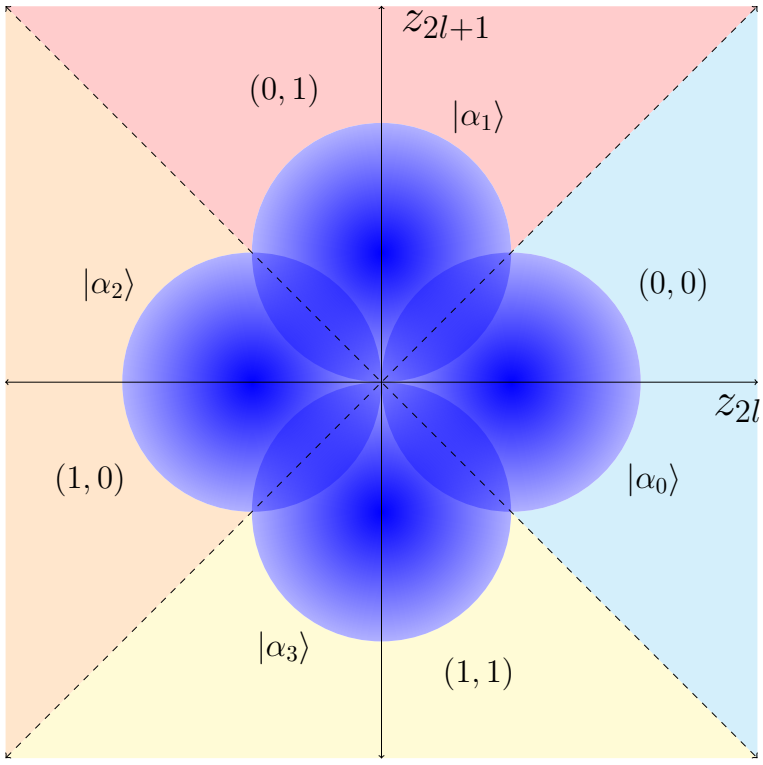


Figure 5.1: QPSk protocol

Bob discloses the values of $|z_{2l} \pm z_{2l+1}|$ on the public channel[1]. To distill a secret key from the raw key, the remaining steps of a QKD protocol are performed. In parameter estimation step, the two parties check if the correlation between the two data sets is large enough so that Eve has very little information about the raw key. As we have learnt in Chapter 3, in CV-QKD, we are interested in estimating the covariance matrix, which consists of variances of two parties and the covariance between them. More precisely, we are interested in Bob's variance v^2 and the covariance c. As already mentioned in Chapter 3, the state distribution for a PM protocol can be written as a classical-quantum state (Eq. (3.8)),

$$\rho_{AB} = \frac{1}{4}\sum_{k=0}^{3} \Pi_k \otimes \mathcal{E}(|\alpha_k\rangle \langle\alpha_k|), \tag{5.3}$$

with $\{\Pi_k\}_{k=0\ldots3}$ being four orthogonal projectors and $\mathcal{E}$ being the quantum channel from Alice to Bob. We also define the quadrature operators Bob's phase-space as

$$\hat{q}_B = \frac{1}{\sqrt{2}}(\hat{b}^\dagger + \hat{b}), \quad \text{and} \quad \hat{p}_B = \frac{i}{\sqrt{2}}(\hat{b}^\dagger - \hat{b}), \tag{5.4}$$

which satisfies $[\hat{q}_B, \hat{p}_B] = i$. Using these definitions, we can write Bob's variance v and the covariance c as:

$$\begin{aligned} c &= \mathrm{tr}[\big((\Pi_0 - \Pi_2) \otimes \hat{q}_B + (\Pi_1 - \Pi_3) \otimes \hat{p}_B\big)\rho_{AB}], \\ v &= \mathrm{tr}[\big(\mathbb{I}_4 \otimes (\hat{q}_B^2 + \hat{p}_B^2)\big)\rho_{AB}]. \end{aligned} \tag{5.5}$$

These two quantities can be obtained directly from the experiment. For instance, if the quantum channel between Alice and Bob is a bosonic phase-invariant Gaussian channel of transmittance T and excess noise ξ, under its action a coherent state $|\alpha\rangle$ is mapped to a thermal state centered at $\sqrt{T}\alpha$ with variance $1 + T\xi$. In this case, we obtain $c = 2\sqrt{T}\alpha$ and $v = 1 + 2T\alpha^2 + T\xi$. Thus, under the assumption that the channel is known (Gaussian), one can recover the values of T and ξ from the parameters c and v observed in the protocol.

Finally, one can perform the rest of classical post-processing to finally obtain the secure key; information reconciliation, where Bob sends additional information on the classical channel to help Alice guess the string $\mathbf{y}$ and privacy amplification, so that Eve has no information about the final key.

In reconciliation step, the advantage a discrete modulation scheme has over a Gaussian modulated protocol is significant. It is well known that the reconciliation of Gaussian variables (Refs.[29, 30]) is quite costly and requires decoding of classical error-correcting codes of length $2L$ [44, 115, 116]. In contrast, the binary nature of the raw key in the QPSK protocol allows Alice and Bob to aggregate the symbols in large blocks of size, say m and thus, to only decode classical codes of length $2L/m$, reducing the post processing complexity by a factor m (which usually scales like $1/T$).

[1]This information is used to turn the reconciliation problem into a channel coding problem for the binary-input additive white Gaussian noise channel (AWGN)

[2]Alice's variance is known to us

But, QPSK protocol has limitations as well. In particular, for our security proof to provide a meaningful bound on the secret key rate, the mixture of four coherent states should approximate a thermal state, which limits the possible value of α to low numbers. In the following section, we discuss the challenges one face due to discrete modulation while estimating parameters.

5.2. Challenges due to discrete modulation

The general strategy to prove security of a protocol against coherent attacks, is to use a de Finetti-type theorem to reduce the problem to the case of collective attacks. The security against collective attacks is analyzed thanks to a version of the asymptotic equipartition property [117], which states that the asymptotic secret key rate is given by the so-called Devetak-Winter rate, given by Eq. (3.16),

$$K_{coll}^{asympt} = I(\mathbf{x}:\mathbf{y}) - \sup \chi(\mathbf{y};E), \tag{5.6}$$

where the supremum is taken over all quantum channels $\mathcal{E}$ compatible with the correlations c and v observed during parameter estimation. Also, recall that bounding the quantity $\chi(\mathbf{y};E)$ is not so straightforward, since the optimization is for all states in the whole Fock space. More precisely, there are two issues that need to be addressed: (i) how to obtain a robust estimate of c and v and (ii) how to compute the supremum of $\chi(\mathbf{y};E)$ over all states compatible with c and v.

As explained previously in section 3.1, currently, the only protocols for which we are able to analyze parameter estimation (of a covariance matrix), within the proper error bounds, are those with the invariance in phase space [88]. In this case, the prime problem is that the parameters to be estimated are neither bounded (unlike BB84-type protocols where the error rate is between 0 and 1), nor the protocol is invariant under unitary transformations in phase space or some additional assumptions (for instance, that the state is Gaussian or that some moments of the variables are upper bounded by some explicit value) such that a confidence region can be computed. In this thesis, we do not address this question, and we leave it for future work.

To get an answer for the second question, the Holevo information is computed for the tripartite pure state ρ_{ABE} or rather a quantum-classical-quantum state ρ_{AYE}, where Bob has measured his systems with heterodyne detection. Let us give the equivalent EB version of the QPSK protocol. Alice prepares L copies of bipartite pure state

$$|\Phi\rangle = (\mathbb{I} \otimes \sqrt{\rho_{PM}})\,|EPR\rangle \tag{5.7}$$

where $\rho_{PM} = \frac{1}{4}\sum_{k=0}^{3} |\alpha_k\rangle\langle\alpha_k|$ is the mixture of the four coherent states prepared in the PM protocol and $|EPR\rangle$ is the non-normalized maximally entangled state, $|EPR\rangle = \sum_{n=0}^{\infty} |n,n\rangle$. More precisely, we have

$$|\Phi\rangle = \frac{1}{2}\sum_{k=0}^{3} |\psi_k\rangle_A\,|\alpha_k\rangle_{A'}\,, \tag{5.8}$$

where $|\psi_k\rangle = \frac{1}{2}\sum_{m=0}^{3} e^{-ikm\frac{\pi}{2}} |\phi_m\rangle$ and

$$|\phi_m\rangle = \frac{1}{\sqrt{\nu_m}} \sum_{n=0}^{\infty} (-1)^n \frac{\alpha^{4n+m}}{\sqrt{(4n+m)!}} |4n+m\rangle \tag{5.9}$$

where $\nu_{0,2} = \frac{1}{2}(\cosh(\alpha^2) \pm \cos(\alpha^2))$ and $\nu_{1,3} = \frac{1}{2}(\sinh(\alpha^2) \pm \sin(\alpha^2))$. The state is a purification of ρ_{PM} and this specific choice is made so as to optimize the correlations between Alice and Bob. She keeps the register A and sends register A' through the quantum channel to Bob. We can describe the quantum channel by a CPTP map $\mathcal{E}$ from register $A' \to B$, or equivalently by an isometry $\mathcal{U}_{A'\to BE}$, courtesy of Stinespring's dilation theorem. Then the tripartite state reads,

$$\rho_{ABE} = (\mathrm{id}_A \otimes \mathcal{U}_{A'\to BE})(|\Phi\rangle \langle\Phi|). \tag{5.10}$$

Bob measures his states by heterodyne detection and stores the measurement results in the register Y. Alternatively, we can write the classical-quantum state (Eq. (5.3)) as

$$\rho_{cq} = \mathrm{tr}_E \left[\mathcal{U}_{A'\to BE} \left(\frac{1}{4} \sum_{k=0}^{3} \Pi_k \otimes (|\alpha_k\rangle \langle\alpha_k|) \right) \right]. \tag{5.11}$$

The supremum of the Holevo information between Y and E computed for ρ_{AYE}, is optimized over all isometries $\mathcal{U}_{A'\to BE}$ yielding parameters c and v when applied to ρ_{AB}. This optimization is indeed troublesome since this is an arbitrary isometry between infinite-dimensional Fock spaces. However, recall from the optimality of Gaussian states, it is possible to compute the supremum of $\chi(\mathbf{y}; E)$ over all possible ρ_{AYE} with a fixed covariance matrix for ρ_{AB} appearing in the EB protocol. Note that, for bounding the Holevo information, using the Gaussian modulated covariance matrix, one does not need the states to be Gaussian, only the covariance of the states matter.

The problem, however, is that there is no direct way of computing the covariance matrix from c and v obtained from the experiment for discrete modulation protocols, as mentioned earlier. Therefore, we need to perform an optimization over the possible covariance matrices compatible with c and v. Prior researched solutions restrict the possible quantum channels to linear bosonic channels, as done in Ref.[104], or to add decoy states as in Ref.[118]. Neither solution is satisfactory since the former does not generate a general security proof, and the latter renders all the advantages of the discrete modulation moot (since Alice must still implement a Gaussian modulation, making the error-correction procedure quite heavy). We also note that Ref.[104] analyzed the security of a two-state protocol and Ref.[108] the security of a three-state protocol; however, the corresponding bounds are very pessimistic in term of resistance to loss, and the proof techniques in these papers are unlikely to easily generalize to more useful modulation schemes. We now present a much better solution to this problem.

5.3. A lower bound in the asymptotic limit

As remarked earlier, we do not consider composability issues in this chapter and restrict ourselves to the asymptotic scenario. As explained in the previous section, we will be

performing an optimization over covariance matrix for all possible channels with fixed c and v. Before that, we discuss the special case of pure-loss channel and then move on to the general case of arbitrary channels.

5.3.1 Pure-loss channel

For a pure-loss channel, $c = 2\sqrt{T}\alpha$ and $v = 1 + 2T\alpha^2$. From this it is easy to infer that, the coherent state $|\alpha\rangle$ is mapped to another coherent state $|\sqrt{T}\alpha\rangle$. Then, without the loss of generality, the isometry $\mathcal{U}$ is of the form: $\mathcal{U}|\alpha_k\rangle_{A'} = |\sqrt{T}\alpha_k\rangle_B |e_k\rangle_E$ for some states $\{|e_k\rangle\}_{k=0..3}$. The output states are indeed product states, else, the output in register B would not be pure and the channel would input noise. From the isometry, we can write $\langle\alpha_k|\alpha_l\rangle = \langle\sqrt{T}\alpha_k|\sqrt{T}\alpha_l\rangle\langle e_k|e_l\rangle$. And after a beamsplitter transformation on coherent states one can write, $\langle\alpha_k|\alpha_l\rangle = \langle\sqrt{T}\alpha_k|\sqrt{T}\alpha_l\rangle\langle\sqrt{1-T}\alpha_k|\sqrt{1-T}\alpha_l\rangle$. Equating both, we can see that, the Gram matrices of $\{|\sqrt{1-T}\alpha_k\rangle\}$ and $\{|e_k\rangle\}$ are equal. Under polar decomposition, if two Gram matrices of theform $M_1M_1^\dagger$ and $M_2M_2^\dagger$ coincide, then there exists some isometry V such that $M_1 = M_2V$, which essentially means, that there exists a local isometry between $|\sqrt{1-T}\alpha_k\rangle$ and $|e_k\rangle$. This proves the channel can also be modeled as

$$\mathcal{U}'|\alpha_k\rangle_{A'} = |\sqrt{T}\alpha_k\rangle_B |\sqrt{1-T}\alpha_k\rangle_E, \tag{5.12}$$

behaving like a pure-loss channel restricted to our set of states. In particular, since we know the value of c and therefore of T, it is easy to compute the covariance matrix of ρ_{AB} in the EB version of the protocol.

5.3.2 A general lower bound via SDP

In this section, we will deal with the noisy channel. We have already introduced the EB version of the QPSK protocol. In this version, the quantum state shared by Alice and Bob is

$$\rho_{AB} = (\mathrm{id}_A \otimes \mathcal{E}_{A'})|\Phi\rangle\langle\Phi| = \frac{1}{4}\sum_{k,l=0}^{3} |\psi_k\rangle\langle\psi_l| \otimes \sigma_{kl}, \tag{5.13}$$

where $\sigma_{kl} = \sum_i K_i|\alpha_k\rangle\langle\alpha_l|K_i^\dagger$ with $\{K_i\}$ being the Kraus operators characterizing the channel $\mathcal{E}$, given by Eq. (1.16).

The goal is to bound the covariance matrix for every possible quantum channel yielding some fixed values for c and v. Note that, for bounding the Holevo information, using the Gaussian modulated covariance matrix, one does not need the states to be Gaussian, only the covariance of the states matter. By symmetry, we are actually interested in 3 parameters, the variances of the parties, and the covariance. Therefore, without loss of generality, we can consider the covariance matrix to have the form: $\begin{pmatrix} V_A\mathbb{I}_2 & Z\sigma_z \\ Z\sigma_z & V_B\mathbb{I}_2 \end{pmatrix}$ with $V_A = 1 + 2\alpha^2$ and $V_B = v$. The only unknown is Z, which we need to bound. Since, Holevo bound is a decreasing function of Z when the other parameters are fixed, it is enough to get a lower bound on Z as a function of c and v. Z can be

defined as the expectation of $(\hat{q}_A\hat{q}_B - \hat{p}_A\hat{p}_B)$ of ρ_{AB}, which basically is

$$Z = \mathrm{tr}[(ab + a^\dagger b^\dagger)\rho_{AB}], \tag{5.14}$$

with $\hat{a}$ and $\hat{a}^\dagger$ being the annihilation and creation operator for register A. For a linear channel [26], the value of Z turns out to be

$$Z_{linear} = 2\alpha^2 \sum_{k=0}^{3} \frac{\nu_{k-1}^{3/2}}{\nu_k^{1/2}}. \tag{5.15}$$

Let us define two new parameters $\Pi = \sum_{k=0}^{3} |\psi_k\rangle \langle\psi_k|$, the orthogonal projector on the subspace spanned by four coherent states and $C = \Pi a \Pi \otimes b + \Pi a^\dagger \Pi \otimes b^\dagger$. Thus we have, $Z = \mathrm{tr}(CX)$, X is the unknown state ρ_{AB}, along with some constraints as $\mathrm{tr}(B_0X) = v$ and $\mathrm{tr}(B_1X) = c$ for

$$\begin{aligned} B_0 &= \Pi \otimes (\mathbb{I} + 2b^\dagger b) \\ B_1 &= (|\psi_0\rangle \langle\psi_0| - |\psi_2\rangle \langle\psi_2|) \otimes \hat{q} + (|\psi_1\rangle \langle\psi_1| - |\psi_3\rangle \langle\psi_3|) \otimes \hat{p}. \end{aligned} \tag{5.16}$$

The final constraint being $\mathrm{tr}_B X = \mathrm{tr}_B |\Phi\rangle \langle\Phi| = \frac{1}{4}\sum \langle\alpha_l|\alpha_k\rangle |\psi_k\rangle \langle\psi_l|$. So the problem now can be written as a SDP problem:

$$\min \mathrm{tr}(CX) \tag{5.17}$$

$$\text{such that} \begin{cases} \mathrm{tr}(B_0X) = v \\ \mathrm{tr}(B_1X) = c \\ \mathrm{tr}(B_{k,l}X) = \frac{1}{4}\langle\alpha_l|\alpha_k\rangle \\ X \geq 0, \end{cases} \tag{5.18}$$

where $B_{k,l} = |\psi_l\rangle \langle\psi_k|$ and the last constraint implies that X is positive semidefinite. This can be solved numerically. Once, we have obtained the $Z*$, optimum value of the program, we can compute an explicit lower bound on $\sup \chi(\mathbf{y}; E)$ by taking the value of Holevo information for a Gaussian state ρ_{AB}^* with the covariance matrix $\begin{pmatrix} 1 + 2\alpha^2\mathbb{I}_2 & Z^*\sigma_z \\ Z^*\sigma_z & v\mathbb{I}_2 \end{pmatrix}$. Following the steps described in section 3.1, one can obtain the explicit value of $\chi(\mathbf{y}; E)$. Indeed, it satisfies $\chi(\mathbf{y}; E)_{\rho_{AB}^*} \geq \sup_{A' \to BE} \chi(\mathbf{y}; E)$ for all isometries compatible with c and v.

Note that, there are no constraints on the channel except for one, which is the trace-preserving property of the map $\mathrm{tr}_B X = \mathrm{tr}_B |\Phi\rangle \langle\Phi|$, which means that all the solutions of the SDP correspond to valid quantum states for some quantum channel $\mathcal{E}$. Alternatively, one can say that, since the initial state is pure, and all purifications of ρ_A are equivalent up to an isometry on the purifying system BE, there always exists an isometry from A' to BE mapping to any valid solution X of the SDP.

5.3.3 Numerical Results

The mutual information between $\mathbf{x}$ and $\mathbf{y}$ and the parameters c and v are obtained directly from the protocol. Thus, we need no more assumptions on the channel. For the numerical results without sampled data, we consider a realistic model for a quantum channel, the noisy thermal channel with transmittance T and excess noise ξ. In this section, we calculate the key-rate for a thermal bosonic noisy channel, and all the parameters will be expressed in terms of T and ξ: $c = 2\sqrt{T}\alpha$ and $v = 1 + 2T\alpha^2 + T\xi$.

The values computed from the SDP give a lower bound on Z, which in turn provides us a lower bound the secret key rate, which we can compare with a Gaussian channel or a linear channel. For realistic implementations, we use the modified version of Devetak-Winter key rate,

$$K = \beta I(\mathbf{x} : \mathbf{y}) - \sup \chi(\mathbf{y}; E), \tag{5.19}$$

where β is the reconciliation efficiency. The mutual information is computed for a binary AWGN channel, which approximates to the capacity of an AWGN channel under an energy constraint given by Eq. (2.31),

$$I(\mathbf{x} : \mathbf{y}) \approx \log_2(1 + SNR) = \log_2\left(1 + \frac{2T\alpha^2}{2 + T\xi}\right). \tag{5.20}$$

This is the mutual information of the classical data. Due to the heterdoyne measurement, the variance of y changes to $(v + 1)/2$.

For each channel, we compute the parameters $c(T, \xi)$ and $v(T, \xi)$ that Alice and Bob would obtain during parameter estimation (in the asymptotic limit), and we solve the SDP of Eq. (5.17) to compute the upper bound on $\sup \chi(Y; E)$. Unfortunately, the SDP involves infinite-dimensional matrices and it is therefore necessary to truncate this space in order to get numerical results. It is natural to truncate the Fock space of Bob by the space spanned by the first N Fock states: $|0\rangle, |1\rangle, \ldots, |N-1\rangle$, thus obtaining a full Hilbert space of dimension $4N$ (since Alice's local space is 4-dimensional).

In practice, we observe that the results do not depend on the specific value of N provided that it is larger than 10. Note the fact that we need to truncate the Fock space is not necessarily an important issue for security proofs, solely because composable security proofs of CV-QKD usually require one to project the state onto a low-dimensional subspace of the Fock space anyway, via some energy constraints[117]. We use the solver SCS [119, 120] and set the precision below 10^{-5}.

We plot our lower bound of the key-rate for three different values of excess noise: $\xi = 0.002$ in Fig. 5.2, $\xi = 0.005$ in Fig. 5.3a and $\xi = 0.01$ in Fig. 5.3b. We note in particular that distances much larger than 100 km are possible provided that the excess noise is sufficiently small. Such values have already been obtained in experimental demonstrations [121, 122]. Note that in realistic implementations, the detectors are inevitably noisy and display limited efficiency. In such a scenario where these imperfections are possibly controlled by the eavesdropper, the secret key rate would be much lower than the ones displayed in Fig. 5.2 and 5.3. However, considering a more optimistic scenario where

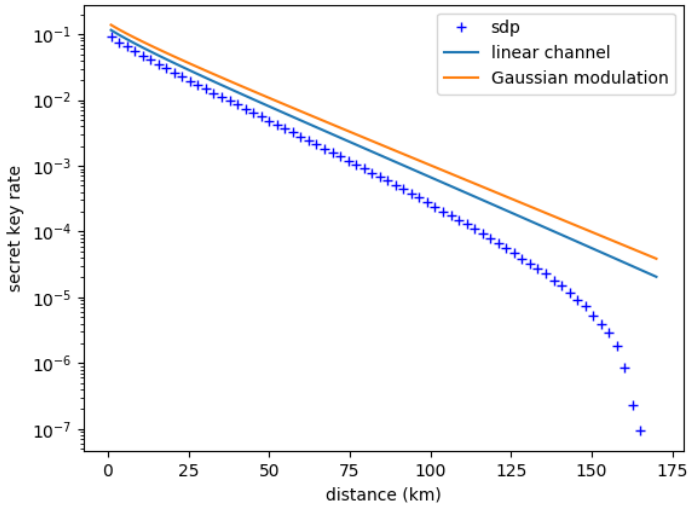
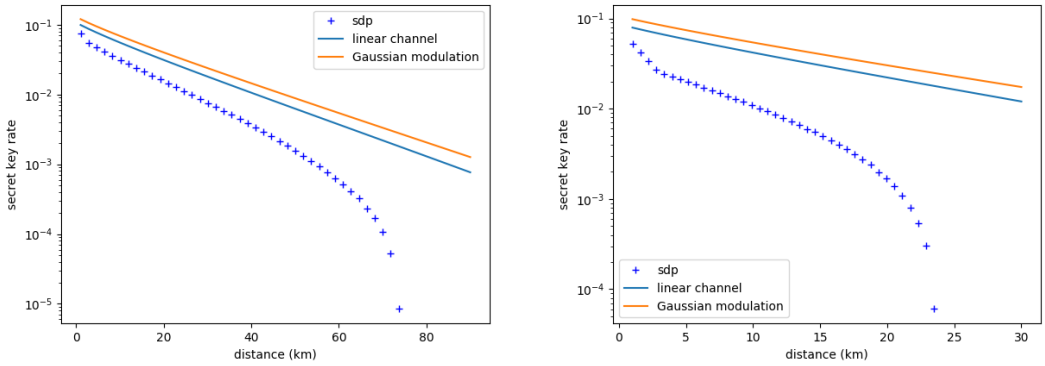


Figure 5.2: Secure key rate vs distance, for a Gaussian channel with transmittance $T = 10^{-0.02d}$ and excess noise $\xi = 0.002$. Here d is the distance between Alice and Bob in km. The value of α is 0.35. The reconciliation efficiency β is set to 0.95. The red curve corresponds to the performance of the protocol [39] with a Gaussian modulation, the lower blue curve is the performance of the QPSK protocol, assuming a linear channel [26] and the crosses correspond to the lower bound given by our sdp.



(a) For excess noise $\xi = 0.005$.

(b) For excess noise $\xi = 0.01$

Figure 5.3: Secure key rate vs distance, for a Gaussian channel of transmittance $T = 10^{-0.02d}$ and different excess noise values. Other parameters are the same as in Fig. 5.2

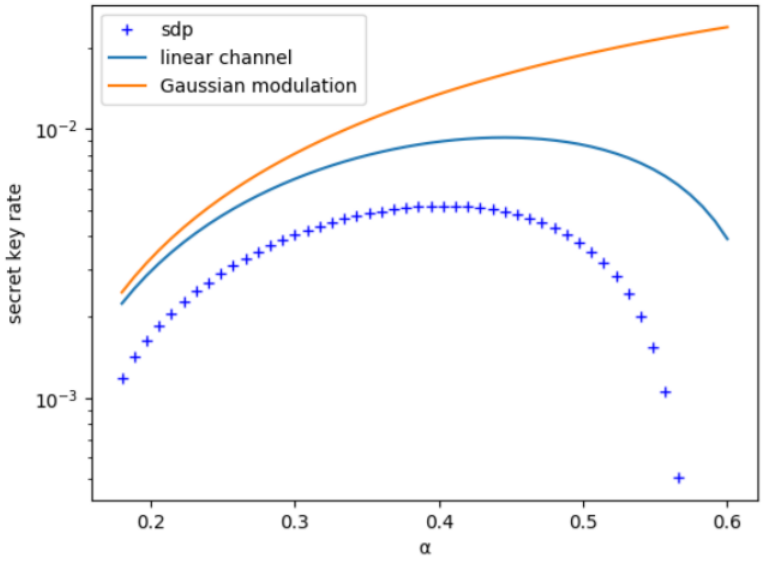


Figure 5.4: ecret key rate vs α, for a distance of 50 km and excess noise of $\xi = 0.002$. Other parameters are the same as in Fig. 5.2

the imperfections of the detectors are not assumed to be controlled by the eavesdropper [124], the secret key rate can be computed following the method of Ref.[123]. Because the effect of imperfections in the trusted-detector-noise scenario is typically quite mild [126], we choose to ignore it here and assume ideal detectors for Bob.

As mentioned earlier, the main limitation of the QPSK protocol probably concerns the small value of α. As described, our approach indeed relies on the closeness between a thermal state (corresponding to the Gaussian modulation, and for which we know the exact secret key rate) and a mixture of four coherent states. These two mixtures are only approximately indistinguishable in the regime where $\alpha << 1$, and surely the performance of the QPSK protocol degrades rapidly for $\alpha \geq 0.5$, corresponding to about 0.25 photon per pulse. Empirically, we observe that values of α below 0.3 or above 0.5 lead to worse performances in terms of maximum range of the protocol. This behavior is illustrated in Fig. 5.4.

To overcome this limitation, it is possible to exploit more complicated QAMs that will better approximate thermal states with a large variance, as discussed below. This case is notably explored in Refs.[100, 101] in the context of QKD and in Refs.[125, 127, 128] for communication over bosonic Gaussian channels.

5.4. Extension to larger constellations

We have shown our approach using the QPSK modulation. However, our technique can be generalized, in a very straightforward way, to more complex modulation schemes. We

start out with a target Gaussian modulation, described by some thermal state

$$\rho(\beta) = (1-\beta^2)\sum_{m=0}^{\infty}\beta^{2m}\left|m\right\rangle\left\langle m\right| \tag{5.21}$$

of parameter $\beta > 0$ and the aim is to find a modulation scheme that approximates this state by a mixture of finite number of coherent states.

Consider, a modulation scheme, where n coherent states $\{|\alpha_k\rangle\}_{k=1...n}$ have been prepared according to probabilities $\{p_k\}_{k=1...n}$. A possibility is to consider the n states on a circle (phase-shift keying) of the form $|\alpha e^{ik2\pi/m}\rangle$, as considered, for instance, in Refs.[106, 129], or more general QAM as in Ref.[130]. The average state prepared by Alice in the PM protocol is $\rho_n = \sum_{k=1}^{n} p_k \left|\alpha_k\right\rangle\left\langle\alpha_k\right|$. Similar to the QPSK protocol, for The EB protocol, the purified state can be written as

$$\left|\Phi_n\right\rangle = (\mathbb{I}\otimes\sqrt{\rho_n})\sum_{i=0}^{\infty}\left|i,i\right\rangle. \tag{5.22}$$

This specific choice is made so that the value of the parameter Z is maximized and thus maximizing the resulting lower bound on the secret key rate. The objective function of our SDP is $\mathrm{tr}[(ab+a^\dagger b^\dagger)\rho_{AB}]$ where $\rho_{AB} = (\mathbb{I}\otimes\mathcal{E})\left|\Phi_n\right\rangle\left\langle\Phi_n\right|$.

Next, follows the constraints of the SDP. The first constraint is that the partial trace of the final state over system B, $\mathrm{tr}_B[\rho_{AB}]$, should coincide with the partial trace of the initial state $\mathrm{tr}_B[\left|\Phi_n\right\rangle\left\langle\Phi_n\right|] = \rho_n$. The second constraint corresponds to the variance of Bob's reduced state, given $\mathrm{tr}[\mathbb{I}\otimes(\mathbb{I}+2b^\dagger b)\rho_{AB}] = v$. The third constraint requires a bit more work. One needs to provide a relation between the covariance c from the PM protocol and a measurement applied on ρ_{AB}

For a general QAM, the best way to define c is to define in a similar way the protocols with a Gaussian modulation does. It should be the average of the dot product between the L-dimensional complex vector $(\alpha_{k_1},...,\alpha_{k_L})$ states sent by Alice and the L-dimensional complex vector $(\beta_1,...,\beta_L)$ of measurement results of Bob, where, β_l the outcome of the heterodyne detection of $\mathcal{E}(\left|\alpha_{k_l}\right\rangle\left\langle\alpha_{k_l}\right|)$, the state received by Bob for the l^{th} use of the channel. This dot product can be alternatively written as the expectation of $\bar{\alpha_k}\beta_k$, where the conjugation is a consequence of working with complex variables. We define M_∞^1 as the observable corresponding to heterodyne detection (the usual definition):

$$M_\infty^1 = \frac{1}{\pi}\int_{\mathbb{C}}\alpha\left|\alpha\right\rangle\left\langle\alpha\right| d\alpha.$$

Therefore, c can be defined as

$$c := \sum_{k=1}^{n} p_k\bar{\alpha_k}\mathrm{tr}[M_\infty^1\mathcal{E}(\left|\alpha_k\right\rangle\left\langle\alpha_k\right|)]. \tag{5.23}$$

However, as mentioned earlier we need c to be the expectation of an observable on the state ρ_{AB}. By construction, we can see that there exists an $n-$outcome measurement

on system A, such that outcome k prepares the state $|\alpha_k\rangle$ on the second mode. To understand this, let us define another purification of the ρ_n,

$$|\Phi'_n\rangle_{CB} = \sum_{k=1}^{n} \sqrt{p_k}\, |\phi_k\rangle \otimes |\alpha_k\rangle\,, \tag{5.24}$$

for an arbitrary orthonormal basis $\{|\phi_k\rangle\}_{k=1\ldots n}$. Since, both the states are purification of ρ_n, there exists an isometry $\mathcal{V} : C \to A$ such that $(\mathcal{V} \otimes \mathbb{I})\,|\Phi'_n\rangle_{CB} = |\Phi_n\rangle_{AB}$. Then, we can choose $F_k = \mathcal{V}\,|\phi_k\rangle\,\langle\phi_k|\,\mathcal{V}^\dagger$. F_k satisfies, $\sum_{k=1}^{n} F_k = \mathbb{I}$ and $\langle\Phi_n|F_k \otimes \mathbb{I}|\Phi_n\rangle = p_k$. we define another complex-valued observable: $M_n = \sum_k \alpha_k F_k$, which correctly yields α_k when Alice sends $|\alpha_k\rangle$ through the quantum channel. We can finally use the fact that $\mathrm{tr}[M_n^\dagger \rho_{AB}] = \sum_{k=1}^{n} p_k \bar{\alpha_k} \mathcal{E}(|\alpha_k\rangle\,\langle\alpha_k|)$ to express c as

$$c = \mathrm{tr}[(M_n^\dagger \otimes M_\infty^1)\rho_{AB}]. \tag{5.25}$$

Finally, we write the SDP problem as follows:

$$\min\ \mathrm{tr}[(ab + a^\dagger b^\dagger)\rho_{AB}] \tag{5.26}$$

$$\text{such that} \begin{cases} \mathrm{tr}_B[\rho_{AB}] = \rho_n \\ \mathrm{tr}[(\mathbb{I} \otimes (\mathbb{I} + 2b^\dagger b))\rho_{AB}] = v \\ \mathrm{tr}[(M_n^\dagger \otimes M_\infty^1)\rho_{AB}] = c \\ \rho_{AB} \geq 0. \end{cases} \tag{5.27}$$

The solution $Z*$ returns a covariance matrix $\begin{pmatrix} V_A\mathbb{I}_2 & Z^*\sigma_z \\ Z^*\sigma_z & v\mathbb{I}_2 \end{pmatrix}$ with V_A being the variance of ρ_n. Similar to the steps in section 5.3.2, we compute the the upper bound of the Holevo information.

Such a SDP can be solved efficiently, although its size appears to grow quite rapidly with the number n of states in the constellation. This is because the state ρ_{AB} is represented by an $nNxnN$ matrix, with n being the dimension of Alice's space (spanned by n coherent states) and an N-dimensional truncation of Bob's Fock space. For large constellations, a better idea might be to truncate Alice's Hilbert space to the first N Fock states, which would yield a matrix of size $N^2 \times N^2$.

Now, comes the question, what happens in the limit $n \to \infty$? The constellation becomes exactly Gaussian, i.e., $\rho_n \to \rho(\beta)$ and the purification of the thermal state ρ_{beta} turns out to be the two-mode squeezed vacuum state (TMSS).

$$(\mathbb{I} \otimes \sqrt{\rho(\beta)}) \sum_{i=0}^{\infty} |i, i\rangle = (1-\beta^2) \sum_{k=0}^{\infty} \beta^k\, |k\rangle\, |k\rangle \tag{5.28}$$

Because of this purification, the observable M_n tends to the (rescaled and conjugated) heterodyne detection

$$(M_\infty^\beta)^\dagger = \frac{1}{\pi} \int_{\mathbb{C}} \beta\bar{\alpha}\, |\alpha\rangle\,\langle\alpha|\, d\alpha,$$

since a heterodyne detection on the first mode (corresponding to M_∞^1) prepares a coherent state $|\beta\bar{\alpha}\rangle$ for the second mode upon the measurement result α. Therefore, the third constraint becomes $\mathrm{tr}[((M_\infty^\beta)^\dagger \otimes M_\infty^1)X] = c$, where X is the unknown state ρ_{AB}. Note that, $M_\infty^\beta = \beta M_\infty^1$. Using the fact that a heterodyne detection is nothing but two noisy homodyne detections, we get

$$\begin{aligned}\mathrm{tr}[((M_\infty^\beta)^\dagger \otimes M_\infty^1)X] &= \beta \mathrm{tr}[((M_\infty^1)^\dagger \otimes M_\infty^1)X] \\ &= \beta \mathrm{tr}[(\hat{q}_A \otimes \hat{q}_B - \hat{p}_A \otimes \hat{p}_B)X] \\ &= \beta \mathrm{tr}[((ab + a^\dagger b^\dagger))X]. \end{aligned} \tag{5.29}$$

Put differently, the objective function of the SDP (when $n \to \infty$) is a scalar multiple of the third constraint. Thus, the solution turns out to be $\beta^{-1}c$, which is indeed the covariance for a CV-QKD protocol with Gaussian modulation.

Since the limit of the SDP for large constellations ($n \to \infty$) recovers the value of the secret key rate for protocols with a Gaussian modulation, it is tempting to exploit continuity arguments to show that the secret key rate of CV-QKD protocols with large constellations is close to that of Gaussian protocols. To make this case quantitative, one must study the stability of the SDP of Eq. (5.26)against small perturbations in the constraints, namely, when ρ_n approximates $\rho(\beta)$ and M_n approximates M_∞^β in the first and third constraints, respectively. Such questions have been studied in the literature on complex optimization [131].

5.5. Discussions and Perspectives

We have provided a general technique to derive a lower bound on the secret key rate of CV-QKD with a discrete modulation and applied it to the case of the QPSK modulation. The bound is rather loose since it relies on Gaussian optimality, meaning that $\chi(\mathbf{y}; E)$ is computed for the Gaussian state with the same covariance matrix as the one returned by the SDP. However, the state is a mixture of four coherent states, thus non-Gaussian. Thus, the quantity $\chi(\mathbf{y}; E)$ is overestimated. The issue is that the SDP is not looking for a state that would yield the maximized $\chi(\mathbf{y}; E)$ but instead for a state with a very specific covariance matrix. This isn't the right optimization for an attacker. Ideally, one would like to optimize for $\chi(Y; E)$ instead of $Z = \mathrm{tr}\left[(ab + a^\dagger b^\dagger)\rho_{AB}\right]$, but it is unlikely that such an optimization can be performed efficiently. At the same time, this restriction disappears when the size of the constellation increases since the SDP bound converges to the optimal secret key rate in the limit of a Gaussian modulation. While our bounds are likely not tight, they already show that secret key rates can be distributed over more than 100 km for realistic values of the excess noise.

A promising approach to improve our results would be to better understand the structure of the SDP and maybe to find analytical bounds by exploiting the dual problem

of Eq. (5.17) which reads:

$$\max_{\mathbf{y}} \quad y_0 v + y_1 c + \sum_{k,\ell=0}^{3} y_{k,\ell} \langle \alpha_\ell | \, \alpha_k \rangle$$

such that :

$$C - y_0 B_0 - y_1 B_1 - \sum_{\ell,k=0}^{3} y_{k,\ell} B_{k,\ell} \geq 0.$$

With an analytical bound, it might become possible to understand which quantum channel yields the state with optimal covariance matrix and decide whether it corresponds to a good attack or not. Another advantage of obtaining an analytical bound is that it wouldn't depend on the dimension of the truncated Fock space anymore.

The question of composable security is left unanswered in this chapter, and would require proper analysis of parameter estimation step. While parameter estimation is rather straightforward for BB84-like protocols, the situation is more complicated for continuous variables because we need to obtain a confidence region for parameters, such as the variance of Bob's state, which are unbounded. Because of that, standard statistical tools to get tail bounds on distributions of random variables such as the Chernoff bound or variants do not apply anymore. An alternative approach to simplify the error-correction procedure is to rely on postselection [103, 109, 110], but security proofs for such protocols are currently restricted to Gaussian attacks, which are not believed to be optimal [90, 105, 111]. Gaussian postselection has also been investigated in the literature mainly because security proofs are easier to obtain [112, 113], but the performance of these variants is still not well understood.

A solution is to exploit some specific symmetry of the protocol in phase space as in Ref. [88]; however, discrete modulations break this symmetry, and a new approach is therefore needed. At the same time, the fact that Bob's detection is rotationally invariant gives us hope that a rigorous analysis of the parameter estimation procedure should be possible. Combining such an analysis with our results would then yield a composable security proof that is valid against collective attacks, and the exponential de Finetti theorem of Renner and Cirac would then imply a composable security proof that is valid against general attacks [117], albeit with pessimistic bounds in the finite-size regime. This result points to two important directions for future work: analyzing the parameter estimation procedure of protocols with a discrete modulation and improving on the exponential de Finetti theorem of Ref.[117].

CHAPTER 6

CONTINUOUS-VARIABLE QUANTUM MONEY WITH CLASSICAL VERIFICATION

Wiesner, in the early '70s, proposed the idea of unforgeable quantum money [46]. Wiesner's private-key quantum money scheme involves three parties - a mint, a bank, and a client. The mint is responsible for generating a random n-qubit state, each state chosen randomly from $\{|0\rangle, |1\rangle, |+\rangle, |-\rangle\}$. Then the n-qubit state is stored in a quantum memory, assigned with a unique serial number, and finally handed to a client. This sequence of n chosen states is stored securely by the mint in a classical key and then shared with the bank. Whenever a client wishes to verify the validity of the money, the client can send the money to the bank for validity verification, and following the secret sequence, the bank can perform the correct projective measurement. The bank maintains a secret database of the encoded random states corresponding to each serial number.

A quantum money scheme with classical verification was introduced by Gavinsky to address the drawback of Wiesner's money scheme [49]: the verification process involves answering randomly selected challenge questions given by the bank instead of sending the money to the bank for verification as in Wiesner's scheme. Over the years, there have been significant developments in this cryptographic protocol (and its variants) both theoretically and experimentally, see section 3.2 for details. In [51], the authors incorporated noise in the protocol for practical implementation. The protocol had a noise tolerance of 14.6%. The work was further improved in [52] by reducing the classical communication exchanges to a single round. In [53], the authors present another classical verification scheme, with an increased noise tolerance of 23%. A common element of all these protocols is the use of qubits to encodes information which necessitates the use of single-photon detectors for verification. Instead of using this costly and specific equipment for verification, we can use coherent detection, which is the current industry standard in optical telecommunication. In this chapter, we present a CV model of a private-key quantum money scheme with classical verification.

A quantum money scheme is *correct* if the original quantum money issued by the mint is verified as valid by the bank with unit probability. A quantum money scheme is information-theoretically *secure* if no adversarial client with unlimited power can

pass verification with two different branches of the bank at the same time with high probability. This prevents any dishonest client from trying to spend double the amount than intended for the same serial number.

For a private-key quantum money scheme with classical verification, counterfeiting is considered successful, if, for a given credit card, the adversary can answer two sets of independent challenge questions from two different banks simultaneously. The security relies on the fact that a single random challenge question can be answered with certainty, while any two randomly selected challenge questions can not be answered with unit probability.

Let us denote p_{hon} as the probability of successfully verifying the quantum money by an honest client and p_{counter} as the probability of successful counterfeiting by an adversary. The bank can now pre-determine a quantity p_{bank} such that:

$$p_{\text{hon}} > p_{\text{bank}} > p_{counter}, \tag{6.1}$$

where p_{bank} is the fraction of states that has to successfully pass the bank's verification process for the bank to declare the money as valid. Therefore, as long as the probabilities follow the above relation, an honest client is always successful in verifying his original quantum money state and a counterfeiter always fails. Thus, the above Eq. (6.1) is sufficient to show both properties of a quantum money scheme.

In this chapter, we present a one-time use private-key money scheme with classical verification, which will be referred to as *quantum tickets*. We start with a small ensemble of 4 states. Care must be taken when choosing the ensemble of states, we need non-orthogonal states such that there does not exist a single-shot measurement that distinguishes the states. Our set of 4 coherent states are on a circle (phase-shift keying) similar to the constellation considered in chapter 5. We analyze the security of the protocol by computing the honest and the counterfeiter scenario. Then, we propose a money scheme with a larger ensemble of 8 states. We compute the probabilities in the honest and the counterfeiting scenario as well as compute the loss tolerance of the money scheme. We then generalize the money scheme to a higher ensemble of $4N$ coherent states.

6.1. 4-state money scheme

We first consider a very simple scheme with a small ensemble of 4 states which is not secure but allows us to present the main ideas of the scheme and the security analysis. In the following sections, we consider schemes with more states.

Our classical verification quantum ticket exploit a set of 4 coherent states: $\{|\alpha_k\rangle\}_{k=0\ldots,3}$ with

$$\{|\alpha_k\rangle\} := |i^k\alpha\rangle = e^{-\frac{1}{2}|\alpha|^2} \sum_{n=1}^{\infty} e^{ikn\frac{\pi}{2}} \frac{\alpha^n}{n!} |n\rangle\,, \tag{6.2}$$

for some $\alpha > 0$, which will be optimized later. A given quantum ticket consists of n quantum registers, each one of them containing a state from $\{|\alpha_k\rangle\}_{k=0,\ldots,3}$, chosen

at random. For each quantum ticket, the mint shares the string $\mathbf{k}_4 = (k_1, \ldots, k_n) \in \{0, 1, 2, 3\}^n$ with the banks, which will be required later for verification.

After the preparation of the quantum ticket, it is handed over to the client. The client may choose to spend it wherever. The *transaction* process involves another party, the vendor. During the transaction, the ticket needs to be verified and the verification result (valid/invalid) should be known to the holder as well as the the vendor, which would then require a (classical) communication between the vendor and the bank.

To verify the validity of the quantum ticket, the client answers a challenge consisting of n random questions asked by the bank. The questions will ask for the sign of a quadrature ($\hat{x}$ or $\hat{p}$) for each quantum register. Therefore, for instance if the state is $|\alpha_0\rangle$, the correct response for the x-quadrature is $+$, while any answer in $\{+, -\}$ is considered to be correct for the p-quadrature.

The correct answers for all the states are tabulated below:

State	Sign of x-quadrature	Sign of p-quadrature
$\|\alpha_0\rangle$	+	+/-
$\|\alpha_1\rangle$	+/-	+
$\|\alpha_2\rangle$	-	+/-
$\|\alpha_3\rangle$	+/-	-

Note in particular that by replying random answers to each question, one obtains a fraction of correct answers of 3/4 on average. This is because both answers are correct for one of the two quadratures, and because there is a probability 1/2 of being correct for the second question.

After the client sends the answers of the challenge questions, the bank checks the answers with the string $\mathbf{k}_4$ and calculates the number of correct answers. If the fraction of correct answers exceeds some fixed value, say $\bar{\eta}$, the bank declares the ticket to be valid. The quantity $\bar{\eta}$ is fixed for a particular protocol. Note that, a client who does not have an access to the money physically is unable to perform the required measurements and thus guesses the correct answer. Therefore, the client can never pass the verification test.

In a transaction verification, the client sends the serial number to the bank and asks for challenge questions. On receiving the questions, the client sends back the answers of the challenge questions. Now, the vendor sends the serial number to ask for the validity of the ticket and the bank responds with either valid or invalid. If the ticket is valid, the transaction is completed with the exchange of the goods and the payment. The client can let the bank know the vendor's bank account number for instant credit similar to *point-of-sale* (POS) transactions or *online shopping*.

In this protocol an honest client will simply try to answer say a x-question by measuring the x-quadrature of the state with homodyne detection. One could also imagine performing the optimal Helström measurement, but a more practical protocol that only requires honest parties to perform coherent detection is preferable. By contrast, a dishonest party trying to prove the validity of a ticket to two distinct entities will sometimes need to correctly determine both quadratures of the state, a task that cannot be won with the same probability as determining a single quadrature. Therefore, the

money scheme is considered to be secure if the honest probability is greater than the counterfeiting probability. The bank can then set the value $\bar{\eta}$ between the honest probability and the counterfeiting probability. This implies that an honest client will always succeed, while a dishonest client trying to validate the same ticket twice will fail at this task with overwhelming probability.

Let us investigate the expected fraction of correct answers obtained by an honest party using homodyne measurement. By symmetry of the protocol, one only needs to analyse the case where the state is $|\alpha_0\rangle$. First, with probability 1/2, the question asks for the sign of the x-quadrature, to obtain the correct answer we need to distinguish between the coherent states $|\alpha\rangle$ and $|-\alpha\rangle$. The probability of correctly distinguishing the states using a homodyne measurement is $\frac{1}{2}(1+\mathrm{erf}(\sqrt{2}\alpha))$[132]. Second, if the question concerns the p-quadrature, any answer is considered as correct. This gives a probability p_{hon} of correct answers for a honest client with homodyne detection equal to:

$$p_{\mathrm{hon}} = \frac{3}{4} + \frac{1}{4}\mathrm{erf}(\sqrt{2}\alpha). \tag{6.3}$$

The question that we must answer now is whether this strategy outperforms the optimal strategy of a counterfeiter (dishonest client), considering the vendor is honest and the payment terminal functions perfectly.

To find out the counterfeiting probability, we consider a dishonest client that wants to validate the ticket with two external banks B_0 and B_1. He receives two challenges, one for verification at each bank. There are only two scenarios to consider:

- when both questions coincide, then the client can simply perform the appropriate Helström measurement, distinguishing between $|\alpha_0\rangle$ and $|\alpha_2\rangle$ in the case of a question about the sign of x-quadrature (or between $|\alpha_1\rangle$ and $|\alpha_3\rangle$ for a p-question). Note that we do not want to restrict the dishonest client to coherent detection. The success probability for the Helström measurement is given by Eq. (1.34), which in this case equates to $\frac{1}{2}(1+\sqrt{1-e^{-4\alpha^2}})$.

  In the situation, where the state is either $|\alpha_1\rangle$ or $|\alpha_3\rangle$ and the sign of x-quadrature is asked, performing the appropriate Helström measurement outputs either $|\alpha_0\rangle$ or $|\alpha_2\rangle$. However, both the answers are correct as stated earlier.

  This yields an expected fraction p_{Hel} of correct answers equal to:

$$p_{\mathrm{Hel}} = \frac{3}{4} + \frac{1}{4}\sqrt{1-e^{-4\alpha^2}}. \tag{6.4}$$

- when the questions differ, the only possible strategy is to apply a general measurement Π, with a 4-outcome measurement $\Pi_{01}, \Pi_{12}, \Pi_{23}, \Pi_{30}$, where for outcome Π_{ij}, the dishonest client answers the sign of the corresponding quadratures considering $|\alpha_i\rangle$ and $|\alpha_j\rangle$ as the actual state. For instance, if the outcome is Π_{01}, then the dishonest party's answer to x-question is + (considers $|\alpha_0\rangle$ as the actual state) and answer to p-question is + (considers $|\alpha_1\rangle$ as the actual state).

Let us introduce some notations. We define $\sigma_k = |\alpha_k\rangle\langle\alpha_k|$. Without loss of generality, we assume that the bank B_0 asks question x and the bank B_1 asks question p.

For bank B_0, possible answers are + and − (for $|\alpha_0\rangle$ and $|\alpha_2\rangle$ respectively). The answer + is given by both outcomes Π_{01} and Π_{30}. The probability that the answer + is correct is given by $\frac{1}{2}\mathrm{tr}[\sigma_0(\Pi_{01}+\Pi_{30})]$. Therefore, the average fraction of correct answers for B_0 is

$$p_{B_0} = \frac{1}{2}\mathrm{tr}[\sigma_0(\Pi_{01}+\Pi_{30}) + \sigma_2(\Pi_{12}+\Pi_{23})]. \tag{6.5}$$

Similarly, the average fraction of correct answers, for B_1 is given by

$$p_{B_1} = \frac{1}{2}\mathrm{tr}[\sigma_1(\Pi_{01}+\Pi_{12}) + \sigma_3(\Pi_{23}+\Pi_{30})]. \tag{6.6}$$

Therefore the fraction of correct answers when two different questions are asked is $\frac{1}{2}(p_{B_0}+p_{B_1})$. We optimize this quantity over the set of POVM's to obtain the optimal cheating probability for the different question scenario:

$$\max \frac{1}{2}(p_{B_0}+p_{B_1}) \tag{6.7}$$

$$\text{such that} \begin{cases} \Pi_{01},\Pi_{12},\Pi_{23},\Pi_{30} \geq 0 \\ \Pi_{01}+\Pi_{12}+\Pi_{23}+\Pi_{30} = \mathbb{I} \end{cases}. \tag{6.8}$$

Let us denote p_Π as the optimized solution to the above sdp problem.

Therefore the average counterfeiting probability is given by $p_{\text{counter}} = \frac{1}{2}(p_{\text{Hel}} + \frac{p_\Pi+1}{2})$. A money scheme is correct and secure if

$$p_{\text{hon}} > p_{\text{counter}}. \tag{6.9}$$

However for the considered 4-state ensemble money scheme, this is not the case even if the honest party has a perfect homodyne measurement equipment.

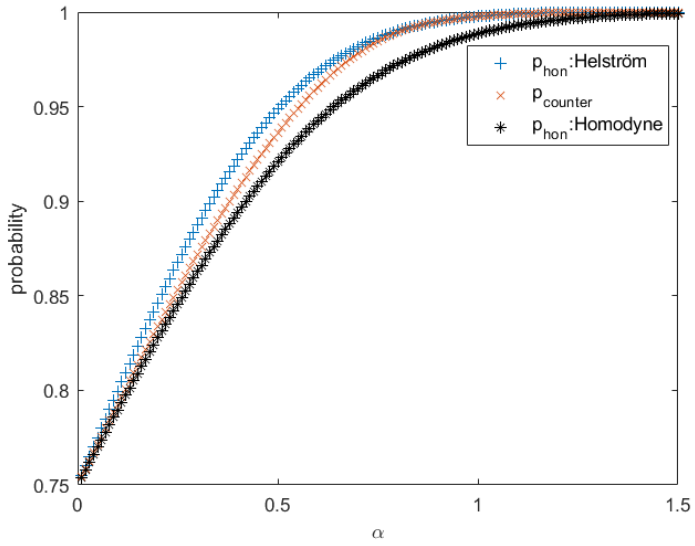


Figure 6.1: Plot of counterfeiting probability and honest probability against the amplitude of the coherent states, α. The blue and the black curves correspond to the honest probability when the client answers the challenge questions using homodyne measurement and Helström measurement respectively. The counterfeiting probability is represented by the red curve.

In Fig. 6.1, we see that when the honest client performs homodyne measurement to answer the challenge questions there does not exist any region of α for which the security condition Eq. (6.9) holds. Therefore, the 4-state money is not secure. However, if the honest client performs the Helström measurement to get the answers of the challenge questions, then the protocol is secure for small values of $\alpha \in [0.01, 0.85]$. Nonetheless, including the Helström measurement in the verification procedure is rather impractical, since our focus is on the ease of implementation.

Next, we consider a larger ensemble of states and compute the respective honest and counterfeiting probability to check if increasing the ensemble size results in a secure money scheme. In the following section, we try to analyze the security of the money scheme with an ensemble of 8 states.

6.2. 8-state money scheme

Here, we analyze a quantum money protocol with 8 coherent states $\{|\alpha_k\rangle\}_{k=0\ldots7}$ with $\alpha_k = \alpha e^{ik\pi/4}$, for some $\alpha > 0$, to be determined later. Similar to the 4-state money scheme, the n states are chosen at random from the ensemble and the mint holds a copy of the classical values $\mathbf{k}_8 = (k_1, \ldots, k_n) \in \{0, \ldots, 7\}^n$.

For each state, the bank asks a random question among $\{Q_0, Q_1, Q_2, Q_3\}$ where question Q_j means that the honest party performs a homodyne detection of the quadrature

$\hat{x}\cos(j\pi/4) + \hat{p}\sin(j\pi/4)$ and returns the sign of the outcome.

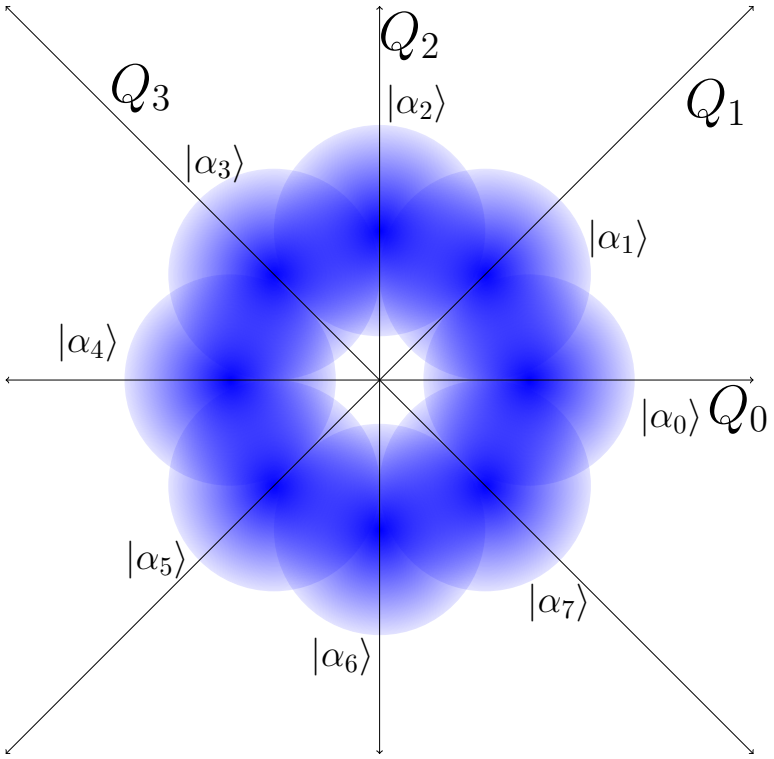


Figure 6.2: A constellation of eight coherent states and the question bases in phase space.

If the quantum state lies perpendicular to the question basis, then any answer in {+,-} to the question is considered to be correct. Therefore, the bank is interested in only two quantities:

- η_1: the fraction of correct answers when the "correct" question was asked, i.e. if question Q_j was asked for a coherent state $|\alpha_j\rangle$ or $|\alpha_{j+4}\rangle$,
- η_2: the fraction of correct answers when the question asked was biased, i.e. if question Q_j was asked for a coherent state $|\alpha_k\rangle$, $k \in \{j \pm 1, j \pm 3\}$.

Finally, the bank computes a final parameter $\eta = f(\eta_1, \eta_2)$ and validates the ticket if $\eta \geq \bar{\eta}$, for some threshold $\bar{\eta}$.

The choice of f is crucial, only those f should be chosen which does not allow the counterfeiter to achieve $\bar{\eta}$. One such choice is the linear combination of η_1 and η_2:

$$\eta = q\eta_1 + (1-q)\eta_2, \tag{6.10}$$

for some value of $q \in [0, 1]$ to be optimized later. Note that the set of all straight lines corresponding to maximum values of $q\eta_1 + (1-q)\eta_2$ gives the convex envelope of achievable values (η_1, η_2) (see Fig.6.3).

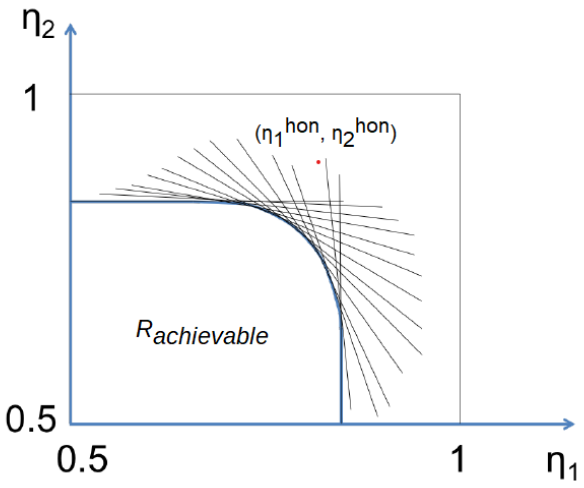


Figure 6.3: Region of achievable values for (η_1, η_2). Note that by construction $(\eta_1, \eta_2) = (1/2, 1/2)$ is achieved by answering the challenges randomly. The red point corresponds to the honest probabilities (Eq. (6.11)). If the honest probabilities lies outside the $R_{achievable}$ for a counterfeiter, the money scheme is secure.

If the quantum state and the question basis differs by an angle of θ, the probability of answering correctly the challenge question with a homodyne measurement is $\frac{1}{2}(1 + \text{erf}(\sqrt{2}\alpha\cos\theta))$.

The honest probabilities $(\eta_1^{\text{hon}}, \eta_2^{\text{hon}})$ read

$$(\eta_1^{\text{hon}}, \eta_2^{\text{hon}}) = \left(\frac{1}{2}(1 + \text{erf}(\sqrt{2}\alpha)), \frac{1}{2}(1 + \text{erf}(\alpha))\right). \tag{6.11}$$

Similar to the 4-state money scheme, to find out the counterfeiting probability, we consider a dishonest client trying to validate the ticket with two external banks B_0 and B_1.

By symmetry, we only have three scenarios to consider:

1. Both banks ask the same question, which occurs with probability 1/4. Without any loss of generality, let us assume the questions asked to be C, Q_0). We introduce a 2-outcome measurement $\{\Pi_0, \Pi_4\}$ with $\Pi_0 + \Pi_4 = \mathbb{I}$, where the outcome Π_i corresponds to the coherent state $|\alpha_i\rangle$ as the actual state for that quantum register.

   The values of η_1 and η_2 for this case is given by

$$\eta_1 = \frac{1}{2}\text{tr}[\sigma_0\Pi_0 + \sigma_4\Pi_4], \tag{6.12}$$

$$\eta_2 = \frac{1}{2}\text{tr}\left[\frac{(\sigma_1 + \sigma_7)}{2}\Pi_0 + \frac{(\sigma_3 + \sigma_5)}{2}\Pi_4\right], \tag{6.13}$$

   where $\sigma_k = |\alpha_k\rangle\langle\alpha_k|$.

To obtain the counterfeiting probability, we optimize η over POVM's:

$$\max\ q\eta_1 + (1-q)\eta_2 \tag{6.14}$$

$$\text{such that} \begin{cases} \Pi_0 \geq 0 \\ \mathbb{I} - \Pi_0 \geq 0. \end{cases} \tag{6.15}$$

For a fixed value of q, denote by (η_1^1, η_2^1) the values corresponding to the optimum in the SDP. Here, the superscript 1 refers to the first scenario.

The set of all the couples $(\eta_1^1(q), \eta_2^1(q))$ describes an achievable region in the plane (η_1, η_2).

2. The banks ask adjacent questions, which occurs with a probability of 1/2. Without any loss of generality, we can assume the questions asked to be (Q_0, Q_1). We consider a 4-outcome measurement $\Pi_{01}, \Pi_{14}, \Pi_{45}, \Pi_{50}$, where for outcome Π_{ij}, the dishonest client the sign of the corresponding quadratures considering $|\alpha_i\rangle$ and $|\alpha_j\rangle$ as the actual state. For instance, if the outcome is Π_{01}, then the dishonest party's answer to Q_0 is + (considers $|\alpha_0\rangle$ as the actual state) and answer to Q_1 is + (considers $|\alpha_1\rangle$ as the actual state).

   The bank B_0 asks question Q_0, then we have

$$\eta_{1,B_0} = \frac{1}{2}\text{tr}\left[\sigma_0(\Pi_{01} + \Pi_{50}) + \sigma_4(\Pi_{14} + \Pi_{45})\right], \tag{6.16}$$

$$\eta_{2,B_0} = \frac{1}{2}\text{tr}\left[\frac{(\sigma_1 + \sigma_7)}{2}(\Pi_{01} + \Pi_{50}) + \frac{(\sigma_3 + \sigma_5)}{2}(\Pi_{14} + \Pi_{45})\right]. \tag{6.17}$$

   The bank B_1 asks question Q_1, then we have

$$\eta_{1,B_1} = \frac{1}{2}\text{tr}\left[\sigma_1(\Pi_{01} + \Pi_{14}) + \sigma_5(\Pi_{45} + \Pi_{50})\right], \tag{6.18}$$

$$\eta_{2,B_1} = \frac{1}{2}\text{tr}\left[\frac{(\sigma_0 + \sigma_2)}{2}(\Pi_{01} + \Pi_{14}) + \frac{(\sigma_4 + \sigma_6)}{2}(\Pi_{45} + \Pi_{50})\right]. \tag{6.19}$$

   Overall, this yields a value of (η_1, η_2), given by

$$\eta_1 = \frac{1}{2}(\eta_{1,B_0} + \eta_{1,B_1}), \quad \eta_2 = \frac{1}{2}(\eta_{2,B_0} + \eta_{2,B_1}) \tag{6.20}$$

   This yields the following SDP:

$$\max\ q\eta_1 + (1-q)\eta_2 \tag{6.21}$$

$$\text{such that} \begin{cases} \Pi_{01}, \Pi_{14}, \Pi_{45}, \Pi_{50} \geq 0 \\ \Pi_{01} + \Pi_{14} + \Pi_{45} + \Pi_{50} = \mathbb{I}. \end{cases} \tag{6.22}$$

   For a fixed value of q, denote by (η_1^2, η_2^2) the values corresponding to the optimum in this SDP. Here, the superscript 2 refers to the second scenario.

   The set of all the couples $(\eta_1^2(q), \eta_2^2(q))$ describes an achievable region in the plane (η_1, η_2).

3. The banks ask orthogonal questions, questions differing by $\pi/2$. This event occurs with a probability 1/4. Without loss of generality, we can assume the questions asked to be (Q_0, Q_2). We consider a 4-outcome measurement $\Pi_{02}, \Pi_{24}, \Pi_{46}, \Pi_{60}$.

   The bank B_0 asks question Q_0, then

$$\eta_{1,B_0} = \frac{1}{2}\text{tr}\left[\sigma_0(\Pi_{02}+\Pi_{60}) + \sigma_4(\Pi_{24}+\Pi_{46})\right], \tag{6.23}$$

$$\eta_{2,B_0} = \frac{1}{2}\text{tr}\left[\frac{(\sigma_1+\sigma_7)}{2}(\Pi_{02}+\Pi_{60}) + \frac{(\sigma_3+\sigma_5)}{2}(\Pi_{24}+\Pi_{46})\right]. \tag{6.24}$$

   The bank B_1 asks question Q_2, then

$$\eta_{1,B_1} = \frac{1}{2}\text{tr}\left[\sigma_2(\Pi_{02}+\Pi_{24}) + \sigma_6(\Pi_{46}+\Pi_{60})\right], \tag{6.25}$$

$$\eta_{2,B_1} = \frac{1}{2}\text{tr}\left[\frac{(\sigma_1+\sigma_3)}{2}(\Pi_{02}+\Pi_{24}) + \frac{(\sigma_4+\sigma_5)}{2}(\Pi_{46}+\Pi_{60})\right]. \tag{6.26}$$

   Combining, yields a value of (η_1, η_2), given by

$$\eta_1 = \frac{1}{2}(\eta_{1,B_0}+\eta_{1,B_1}), \quad \eta_2 = \frac{1}{2}(\eta_{2,B_0}+\eta_{2,B_1}) \tag{6.27}$$

   This yields the following SDP:

$$\max\ q\eta_1 + (1-q)\eta_2 \tag{6.28}$$

$$\text{such that} \begin{cases} \Pi_{02}, \Pi_{24}, \Pi_{46}, \Pi_{60} \geq 0 \\ \Pi_{02}+\Pi_{24}+\Pi_{46}+\Pi_{60} = \mathbb{I}. \end{cases} \tag{6.29}$$

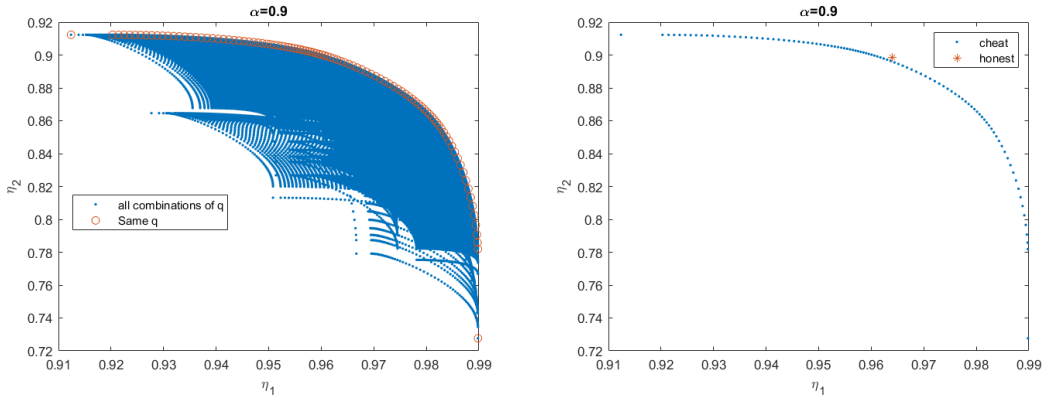
   For a fixed value of q, denote by (η_1^3, η_2^3) the values corresponding to the optimum in the SDP. Here, the superscript 3 refers to the third scenario.

   The set of all the couples $(\eta_1^3(q), \eta_2^3(q))$ describes an achievable region in the plane (η_1, η_2).

Combining the results, we obtain that the value for any achievable couple $(\eta_1^{\text{counter}}, \eta_2^{\text{counter}})$ must have the form:

$$(\eta_1^{\text{counter}}, \eta_2^{\text{counter}}) = \frac{1}{4}(\eta_1^1(q_1), \eta_2^1(q_1)) + \frac{1}{2}(\eta_1^2(q_2), \eta_2^2(q_2)) + \frac{1}{4}(\eta_1^3(q_3), \eta_2^3(q_3)), \tag{6.30}$$

where $q_1, q_2, q_3 \in [0,1]$ and the superscript "counter" denotes the counterfeiting probability. The counterfeiter considers different q_i's for different question scenarios, so as to optimize different linear quantities of η_1 and η_2. However, note that, there is only a particular value of q, which is set by the bank. Fig. 6.4a shows that considering different q_i's for different question scenarios is indeed not useful, $q_1 = q_2 = q_3$ marks the boundary of the achievable region i.e., provides the maximal counterfeiting probability.



(a) (b) $\alpha = 0.9$

Figure 6.4: (a)Achievable region: The blue dots represents all possible combination of q_1, q_2 and q_3 and red circle represents same q for all (η_1^k, η_2^k). (b) Plot of counterfeiting probability and honest probability in the plane (η_1, η_2) for $\alpha = 0.9$

Comparing the counterfeiting probability with the honest probability we find out that the protocol is secure only for a limited range of $\alpha \in [0.85, 1.14]$, see Table 6.1.

Memory model. The previous analysis is restricted to a perfect implementation. Now, we look at a more realistic scenario. The quantum states chosen from the ensemble are stored in a quantum memory. We consider the memory to be similar to a pure loss Gaussian channel of transmittance T. When a coherent state is sent through such a Gaussian channel, the new received state is a coherent state centered at $\sqrt{T}\alpha$.

$$|\alpha_k\rangle \xrightarrow{Channel} |\sqrt{T}\alpha_k\rangle \tag{6.31}$$

Under the action of such a Gaussian channel, the probability of measuring the correct quadrature with homodyne measurement is:

$$p = \frac{1}{2}\left(1 + \text{erf}\left(\sqrt{2T}\alpha\right)\right). \tag{6.32}$$

Our memory also acts in a similar way when coherent states are stored in it. We compute the honest probabilities under such imperfections:

$$(\eta_1^{\text{hon, l}}, \eta_2^{\text{hon, l}}) = \left(\frac{1}{2}(1 + \text{erf}(\sqrt{2T}\alpha)), \frac{1}{2}(1 + \text{erf}(\sqrt{T}\alpha))\right), \tag{6.33}$$

the superscript l is introduced to denote the pure loss probability. Here, we define the *losses* as the transmission loss similar to a QKD protocol.

We are now able to find the minimum value of transmission coefficient, T, for which Eq. (6.9) holds. The following table shows the minimum value of T for different values of α for which the scheme is secure:

α	T_{min}
0.85	1
0.9	0.987
1.0	0.98
1.1	0.987
1.14	1

Table 6.1: Minimum T for different values of α for which the scheme is secure

The minimum value of T is obtained for $\alpha = 1.0$, and the this minimum is obtained for $q = 0.57$. For this value of q, we plot the minimal value of T versus α to obtain the following curve:

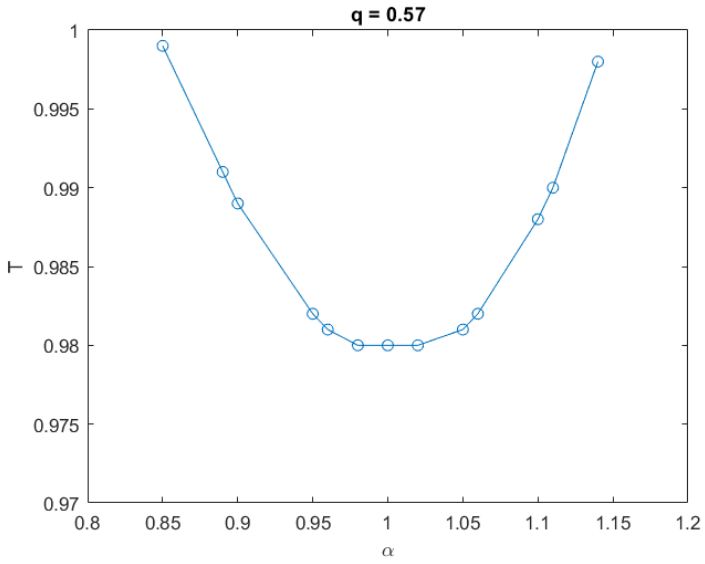


Figure 6.5: Loss tolerance for different values of α for a fixed $q = 0.57$.

We conclude from the plot that for the 8-state money scheme considered here can tolerate losses up to 2%. $\alpha \in [0.98, 1.02]$ is the optimal region of operation i.e., the region of α where the protocol tolerates the maximum loss.

The bank can set the parameter q at 0.57, which in turn determines the threshold $\bar{\eta}$ as

$$\bar{\eta} = 0.57\eta_1^{\text{counter}}(0.57) + (1 - 0.57)\eta_2^{\text{counter}}(0.57) + \delta. \tag{6.34}$$

for some small $\delta > 0$. This choice of q is made such that, a counterfeiter trying to verify the ticket at two different branches of the bank can never achieve $\bar{\eta}$. The ticket is valid if $\eta \geq \bar{\eta}$.

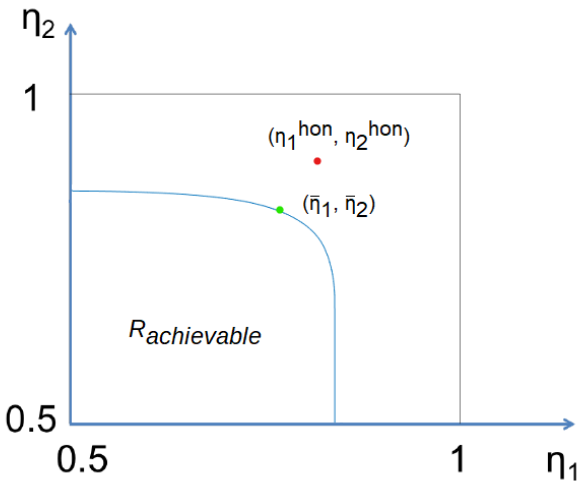


Figure 6.6: Pictorial representation of the probabilities of a correct and secure money scheme. $R_{achievable}$ describes the achievable region of (η_1, η_2) for a counterfeiter, the green point corresponds to the threshold $\bar{\eta}$ and the red point corresponds to the honest probabilities.

6.3. Generalization to higher ensembles

In this section, we generalize our CV model for the quantum money scheme to higher ensembles and compute the secure region of operation, optimal α for implementation and optimal probabilities for $\bar{\eta}$, which is required for verification.

We can consider an ensemble of $4N$ coherent states $\{|\alpha_k\rangle\}_{k=0\ldots,4N}$ with $\alpha_k = \alpha e^{ik\pi/(2N)}$, for some $\alpha > 0$. The states are chosen from this ensemble randomly i.e., with equal probability.

For verification, the bank asks a random question among $2N$ questions, $\{Q_0, \ldots, Q_{2N-1}\}$, where on asking question Q_j, honest party performs a homodyne detection of the quadrature $\hat{x}\cos(j\pi/(2N)) + \hat{p}\sin(j\pi/(2N))$ and return the sign of the outcome.

The bank is now interested in evaluating a total of N quantities, $(\eta_0, \ldots, \eta_{N-1})$, where η_m is the fraction of correct answers when the basis of the question and the state differs by an angle of $m\pi/(2N)$. Finally, the bank computes the quantity

$$\eta = \sum_{m=0}^{N-2} q_m \eta_m + \left(1 - \sum_{m=0}^{N-2} q_m\right) \eta_{N-1}. \tag{6.35}$$

The set of probabilities is denoted by $\mathbf{q} = \{q_0, \ldots, q_{N-1}\}$.

Then, the honest probability is given by

$$\eta_m^{\text{hon}} = \frac{1}{2}\left[1 + \text{erf}\left(\sqrt{2}\alpha\cos\left(\frac{m\pi}{2N}\right)\right)\right], \tag{6.36}$$

where $m \in \{0, 1, \ldots N-1\}$.

To find the counterfeiting probability, by the virtue of symmetry we only need to look at $2N+1$ scenarios. The corresponding cheating probabilities can be obtained by using the same SDP forms as derived in the 8-state money scheme and we can compute the counterfeiting probabilities and the loss tolerance for each money scheme.

- **Scenario: When the banks ask the same question**

  Without loss of generality, let us assume that the banks ask the question Q_0. We introduce a two-outcome measurement $\{\Pi_0, \Pi_{2N}\}$ with $\Pi_0 + \Pi_{2N} = \mathbb{I}$.

  The values of η_m's is given by

$$\eta_0 = \frac{1}{2}[\sigma_0 \Pi_0 + \sigma_{2N} \Pi_{2N}] \tag{6.37}$$

$$\eta_j = \frac{1}{2}[\frac{(\sigma_j + \sigma_{4N-j})}{2} \Pi_0 + \frac{(\sigma_{2N-j} + \sigma_{2N+j})}{2} \Pi_{2N}], \tag{6.38}$$

  where $j \in \{1, \ldots, N-1\}$.

  We optimize the following SDP to obtain the maximum cheating probability:

$$\max\ q_0 \eta_0 + \sum_{j=1}^{N-2} q_j \eta_j + \left(1 - \sum_{j=0}^{N-2} q_j\right) \eta_{N-1} \tag{6.39}$$

$$\text{such that} \begin{cases} \Pi_0, \Pi_{2N} \geq 0 \\ \Pi_0 + \Pi_{2N} = \mathbb{I}. \end{cases} \tag{6.40}$$

- **Generalized scenario: When the banks ask questions differing by $m\pi/(2N)$, $m \in \{1, \ldots, N-1\}$**

  Without loss of generality, we assume that the banks ask the questions (Q_0, Q_m). We consider a 4-outcome measurement $\Pi_{0,m}, \Pi_{m,2N}, \Pi_{2N,2N+m}$ and $\Pi_{2N+m,0}$.

  The values of η_j's is given by

$$\eta_0 = \frac{1}{4}[\sigma_0(\Pi_{0,m} + \Pi_{2N+m,0}) + \sigma_m(\Pi_{0,m} + \Pi_{m,2N}) + \sigma_{2N}(\Pi_{m,2N} + \Pi_{2N,2N+m}) + \sigma_{2N+m}(\Pi_{2N,2N+m} + \Pi_{2N+m,0})], \tag{6.41}$$

$$\eta_j = \frac{1}{4}[\frac{(\sigma_j + \sigma_{4N-j})}{2}(\Pi_{0,m} + \Pi_{2N+m,0}) + \frac{(\sigma_{2N-j} + \sigma_{2N+j})}{2}(\Pi_{m,2N} + \Pi_{2N,2N+m}) + \frac{(\sigma_{m+j} + \sigma_{m-j})}{2}(\Pi_{0,m} + \Pi_{m,2N}) + \frac{(\sigma_{2N+m-j} + \sigma_{2N+m+j})}{2}(\Pi_{2N,2N+m} + \Pi_{2N+m,0})], \tag{6.42}$$

where $j \in \{1, \ldots, N-1\}$. This yields the following SDP:

$$\max\ q_0\eta_0 + \sum_{j=1}^{N-2} q_j\eta_j + \left(1 - \sum_{j=0}^{N-2} q_j\right)\eta_{N-1} \tag{6.43}$$

$$\text{such that } \begin{cases} \Pi_{0,m}, \Pi_{m,2N}, \Pi_{2N,2N+m}, \Pi_{2N+m,0} \geq 0 \\ \Pi_{0,m} + \Pi_{m,2N} + \Pi_{2N,2N+m} + \Pi_{2N+m,0} = \mathbb{I}. \end{cases} \tag{6.44}$$

Numerically, we have analyzed the cases for 8, 12, 16, 20 and 24 state ensembles (for $N = 2$, 3, 4, 5 and 6). The following table includes ranges of α for which the money schemes are correct and secure along with the maximum loss tolerance and the optimal combination of the correct answer probabilities for each scheme.

$4N$	Range of alpha	T_{min}	Optimal α	**q**
8	0.85-1.14	0.980	1.0(0.98-1.02)	0.57, 0.43
12	0.85-1.6	0.923	1.35(1.31-1.39)	0.49, 0.44, 0.07
16	0.85-1.9	0.892	1.59(1.58-1.61)	0.44, 0.47 , 0.08, 0.01
20	0.85-2.1	0.877	1.85(1.83-1.9)	0.41, 0.48, 0.1, 0.01, 0
24	0.85-2.2	0.869	2.05(2.0-2.1)	0.35, 0.45, 0.14, 0.02, 0, 0.04

Table 6.2: **Numerical results for CV money schemes of varying ensemble size.**

From the table, it is clear that, on increasing ensemble size ($4N$) the scheme's tolerance to loss improves and seems to tend towards a limit. We infer the limit to be 0.86. The next figure shows the relation between loss tolerance and the ensemble size.

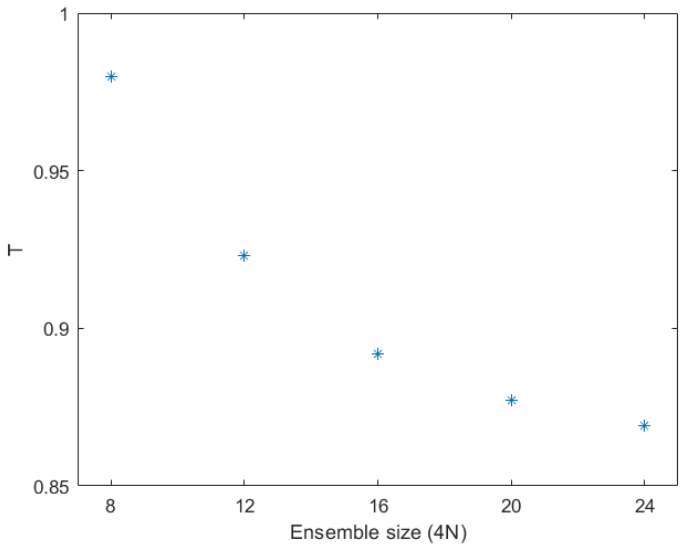


Figure 6.7: Minimal T vs ensemble size

The region of operation (range of α) for the money scheme also improves as we increase the ensemble size, i.e., the schemes are secure for a larger region of α. We also note that, on increasing the ensemble size, the optimal region of operation increases with respect to α. We plot the relation between the ensemble size and the optimal region of operation in Fig.(6.8).

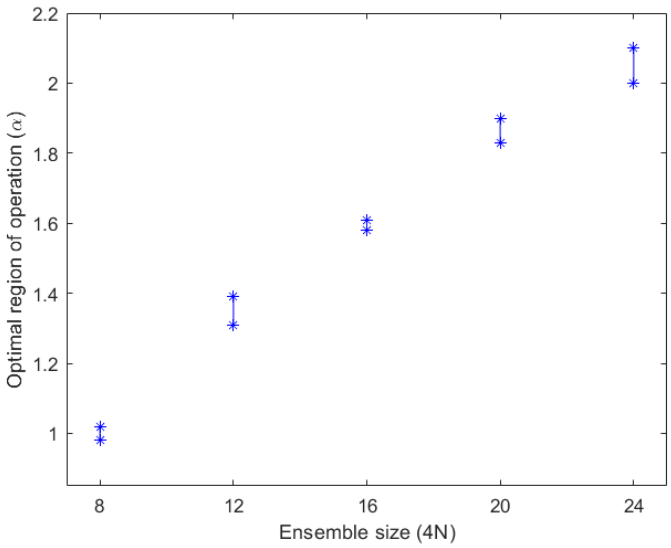


Figure 6.8: Optimal region of operation vs ensemble size

From the figures and the table, it is clear that to get money schemes with better loss tolerance; we need to consider schemes with larger ensemble sizes. However, a money scheme with an ensemble size of 20, looks like an excellent choice for a protocol. The region of operation, $\alpha \in [0.85, 2.1]$ is almost the same as in the money scheme with the ensemble size of 24. As we increase the ensemble size, the set of probabilities $\mathbf{q}$ contains smaller q_i's (close or equal to zero). As observed from the table, the money scheme with an ensemble size of 20 states, has two such smaller q_i's while for 24, has three such quantities. These smaller q_i's contribute little to the calculation of η, therefore, it is best if we choose protocols with fewer small values in the set $\mathbf{q}$.

6.4. Conclusion

In this chapter, we have introduced a continuous-variable money scheme framework with classical verification. We compute the honest and counterfeiting probabilities and prove that the money schemes are correct and secure except for the 4-state ensemble. We also notice that as we increase the ensemble size ($4N$) the loss tolerance of the scheme improves as well as the optimal α region of operation. We also show that we have money schemes with 13% of loss tolerance. Note that, in this chapter, the probabilities have been evaluated in the asymptotic limit.

CHAPTER 7

CONCLUSIONS

In this thesis, we study two continuous-variable quantum cryptographic protocols, quantum key distribution and unforgeable quantum money. Although we examine these protocols from a theoretical point of view, we design them in a way that facilitates their implementation. The easiness of the generation and manipulation of Gaussian states coupled with the availability and performance of coherent detection makes the protocols considered here relatively easy to implement with current technology.

Chapter 4 provides answers to two open questions in the field of CV-QKD. First, we prove the composable security of two-way CV-QKD against general attacks. In particular, we establish composable security for a class of CV-QKD protocols that involve a Gaussian modulation of coherent states and heterodyne detection. This class of protocols includes standard one-way protocols, measurement-device-independent protocols, and some two-way protocols. We exploit the invariance of Unitary group $U(n)$ to reduce the security proof against general attacks to collective attacks. Second, we prove that active symmetrization of the data is not needed to apply the de Finetti reduction theorem by exploiting the modularity of QKD protocols.

Chapter 5 answers another pressing open question in the field of CV-QKD with a discrete modulation by establishing a lower bound on the asymptotic secret key rate against collective attacks. The bound is obtained by formulating the problem as a semidefinite program. This bound is rather loose since we base it on the optimality of Gaussian states, but the state in the QPSK modulation scheme is a mixture of four coherent states, thus non-Gaussian. As a result, we overestimate the Holevo bound. Nonetheless, our analysis shows that we can distribute secret keys over 100 km for realistic values of the excess noise. We also discuss the generalization of the scheme to higher constellation sizes and show that the same technique could be used to analyze the security of more complicated QAM.

Another issue with our analysis is that we optimize the covariance matrix rather than the Holevo bound, which is not optimal for an attacker. However, this restriction disappears when the size of the constellation increases since the SDP bound converges to the optimal secret key rate in the limit of a Gaussian modulation. In this thesis, we do not analyze the parameter estimation procedure for the composable security proof.

Unlike the Gaussian-modulated protocols, a discrete modulation breaks the phase-space symmetry and thus requires a new approach to obtain the confidence region. Bob's detection is rotationally invariant, which gives us hope that a rigorous analysis of the parameter estimation procedure should be possible, and combining this with our result would then imply a full composable security proof. This question is left for future work.

Chapter 6 presents a CV private-key money scheme with classical verification. The motivation behind this protocol is to facilitate the process of practical implementation. Previous classical verification money schemes use single-photon detectors for verification, while our protocols require coherent detection. Our money scheme exploits a set of coherent states, where we encode information on its quadratures. To verify the quantum ticket, the bank asks for the sign of a quadrature (either $\hat{x}$ or $\hat{p}$) for all registers. An honest client simply measures the corresponding quadrature (as asked by the bank) with a homodyne detection and answers the sign of the value obtained. We analyze the correctness and security parameters of the money scheme for a varying ensemble size of $4N$. We note that the loss tolerance of the scheme improves with higher ensemble size. Our analysis shows CV money schemes with 13% loss tolerance is feasible. This opens up a new door to more practically feasible quantum money schemes.

CHAPTER A

RELATION BETWEEN TMSS, SQUEEZED STATES AND COHERENT STATES

The two-mode squeezed state (TMSS) plays a very important role in EB version of CV-QKD protocols. As mentioned earlier, if one of the mode is measured with homodyne detection, the other mode collapses to a squeezed state, while if the mode is measured via a heterodyne detection, we get coherent states on the other mode. In this section, we prove the same.

TMSS is characterized by a null displacement vector and a covariance matrix given by Eq. (2.123),

$$\gamma = \begin{pmatrix} \gamma_A & C \\ C^\top & \gamma_B \end{pmatrix} = \begin{pmatrix} \cosh 2s\, \mathbb{I}_2 & \sinh 2s\, \sigma_z \\ \sinh 2s\, \sigma_z & \cosh 2s\, \mathbb{I}_2 \end{pmatrix}, \tag{A.1}$$

for $s > 0$.

Let us first consider the case where one measures the B-part of the state with a homodyne measurement obtaining the result $m_1 = (x, 0)$. Therefore, the A-part of the state transforms into a state which is characterized by the displacement vector given by Eq. (2.149):

$$\begin{aligned} d' &= d_A + C(X\gamma_B X)^{MP}(m_1 - d_B) \\ &= \begin{pmatrix} \sinh 2s & 0 \\ 0 & -\sinh 2s \end{pmatrix} \left(\begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix} \begin{pmatrix} \cosh 2s & 0 \\ 0 & \cosh 2s \end{pmatrix} \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix} \right)^{MP} \begin{pmatrix} x \\ 0 \end{pmatrix} \\ &= \begin{pmatrix} \sinh 2s & 0 \\ 0 & -\sinh 2s \end{pmatrix} \begin{pmatrix} \operatorname{sech} 2s & 0 \\ 0 & 0 \end{pmatrix} \begin{pmatrix} x \\ 0 \end{pmatrix} = \begin{pmatrix} x \tanh 2s \\ 0 \end{pmatrix}, \end{aligned} \tag{A.2}$$

and the covariance matrix, given by Eq. (2.150):

$$\begin{aligned} \gamma' &= \gamma_A - C(X\gamma_B X)^{MP} C^\top \\ &= \begin{pmatrix} \cosh 2s & 0 \\ 0 & \cosh 2s \end{pmatrix} - \begin{pmatrix} \sinh 2s & 0 \\ 0 & -\sinh 2s \end{pmatrix} \begin{pmatrix} \operatorname{sech} 2s & 0 \\ 0 & 0 \end{pmatrix} \begin{pmatrix} \sinh 2s & 0 \\ 0 & -\sinh 2s \end{pmatrix} \\ &= \begin{pmatrix} \cosh 2s & 0 \\ 0 & \cosh 2s \end{pmatrix} - \begin{pmatrix} \sinh 2s \tanh 2s & 0 \\ 0 & 0 \end{pmatrix} = \begin{pmatrix} \operatorname{sech} 2s & 0 \\ 0 & \cosh 2s \end{pmatrix}, \end{aligned} \tag{A.3}$$

where $X = \mathrm{diag}(1,0)$. The covariance matrix of the new state (Eq. (A.3)) matches to that of a covarince matrix of a $\hat{x}$-squeezed state given by Eq. (2.114). The displacement vector is also non-zero for the $\hat{x}$-quadrature, confirming that the state is indeed a squeezed state.

Let us now consider the scenario where the B-part of the state with a heterodyne measurement obtaining the result $m_2 = (x, p)$. Thus, the A-part of the state transforms into a state, whose displacement vector is given by Eq. (2.153), which reads,

$$\begin{aligned} d'' &= d_A + \sqrt{2}C(\gamma_B + \mathbb{I}_2)^{-1}(m_2 - d_B) \\ &= \sqrt{2}\begin{pmatrix} \sinh 2s & 0 \\ 0 & -\sinh 2s \end{pmatrix}\begin{pmatrix} 1+\cosh 2s & 0 \\ 0 & 1+\cosh 2s \end{pmatrix}^{-1}\begin{pmatrix} x \\ p \end{pmatrix} \\ &= \sqrt{2}\begin{pmatrix} \tanh s & 0 \\ 0 & -\tanh s \end{pmatrix}\begin{pmatrix} x \\ p \end{pmatrix} = \sqrt{2}\begin{pmatrix} x\tanh s \\ -p\tanh s \end{pmatrix}, \end{aligned} \tag{A.4}$$

and the covariance matrix is given by Eq. (2.154),

$$\begin{aligned} \gamma'' &= \gamma_A - C(\gamma_B + \mathbb{I}_{2N_B})^{-1}C^\top \\ &= \begin{pmatrix} \cosh 2s & 0 \\ 0 & \cosh 2s \end{pmatrix} - \begin{pmatrix} \sinh 2s & 0 \\ 0 & -\sinh 2s \end{pmatrix}\begin{pmatrix} 1+\cosh 2s & 0 \\ 0 & 1+\cosh 2s \end{pmatrix}^{-1}\begin{pmatrix} \sinh 2s & 0 \\ 0 & -\sinh 2s \end{pmatrix} \\ &= (\cosh 2s - \sinh 2s \tanh s)\mathbb{I}_2 = \mathbb{I}_2. \end{aligned} \tag{A.5}$$

Since non-zero displacement vectors and a identity covariance matrix characterizes a coherent state, the new state is a coherent state.

BIBLIOGRAPHY

[1] M. A. Nielsen and I. L. Chuang. Quantum computation and quantum information. *Cambridge University Press*, 2000.

[2] K. Kraus. States, Effects, and Operations: Fundamental Notions of Quantum Theory. *Lecture Notes in Physics,* Volume 190, Springer-Verlag, Berlin, 1983.

[3] D. Aharonov, A. Kitaev, N. Nisan. Quantum Circuits with Mixed States. *Proceedings of the Thirtieth Annual ACM Symposium on Theory of Computation (STOC)*, pages 20–30, 1997.

[4] M.-Choi. Completely positive linear maps on complex matrices. *Linear Algebra and Its Applications*, 10(3), pages 285-290, 1975.

[5] T. M. Cover and J. A. Thomas. Elements of information theory. *Wiley-Interscience*, 2006.

[6] D. J. C. MacKay. Information theory, inference and learning algorithms. *Cambridge University Press*, 2003.

[7] C. Gerry and P. Knight. Introductory Quantum Optics. *Cambridge University Press*, 2004.

[8] U. Leonhardt. Essential Quantum Optics. *Cambridge University Press*, 2010.

[9] U. Leonhardt. Measuring the quantum state of light. *Cambridge University Press*, 1997.

[10] R. Simon, E. C. G. Sudarshan, and N. Mukunda. Gaussian-Wigner distributions in quantum mechanics and optics. *Physical Review A* 36, 3868, 1987; R. Simon, N. Mukunda, and B. Dutta. Quantum-noise matrix for multimode systems: $U(n)$ invariance, squeezing, and normal forms. *Physical Review A* 49, 1567, 1994.

[11] R. Simon, S. Chaturvedi, and V. Srinivasan. Congruences and canonical forms for a positive matrix: Application to the Schweinler-Wigner extremum principle. *Journal of Mathematical Physics*, 40(7), pages 3632–3642, 1999.

[12] R. Simon. Peres-Horodecki separability criterion for continuous variable systems. *Physical Review Letters* 84(12):2726, 2000.

[13] Alessio Serafini. Multimode Uncertainty Relations and Separability of Continuous Variable States. *Physical Review Letters*, 96(11):110402, 2006.

[14] A. I. Lvovsky and M. G. Raymer. Continuous-variable optical quantum-state tomography. *Reviews of Modern Physics*, 81(1):299, 2009.

[15] H. Yuen and J. Shapiro. Optical communication with two-photon coherent states–Part III: Quantum measurements realizable with photoemissive detectors. *IEEE Transactions on Information Theory*, Volume 26, Issue 1, 1980.

[16] F. Marsili, V. Verma, J. A. Stern *et al.*. Detecting single infrared photons with 93% system efficiency. *Nature Photonics* 7, pages 210–214, 2013.

[17] R. König, R. Renner, and C. Schaffner. The operational meaning of min-and max-entropy. *IEEE Transactions on Information Theory*, Volume 55, Issue 9, 2009.

[18] J. Watrous. Semidefinite Programming, ch. 7. *University of Waterloo*, 2011.

[19] L. Vandenberghe and S. Boyd. Semidefinite programming. *SIAM Review*, Volume 38, no. 1, pp. 49–95, 1996.

[20] C. H. Bennett and G. Brassard. Quantum cryptography: Public key distribution and coin tossing. *In Proceedings of IEEE International Conference on Computers, Systems and Signal Processing*, Bangalore, India, pages 175-179, 1984.

[21] A. K. Ekert. Quantum cryptography based on Bell's theorem. *Physical Review Letters*, 67(6):661–663, 1991.

[22] T. C. Ralph. Continuous variable quantum cryptography. *Physical Review A*, 61(1):010303(R), 1999.

[23] M. Hillery. Quantum cryptography with squeezed states. *Physical Review A*, 61(2):022309, 2000.

[24] M. D. Reid. Quantum cryptography with a predetermined key, using continuous-variable Einstein-Podolsky-Rosen correlations. *Physical Review A*, 62(6):062308, 2000.

[25] R. Renner. Security of quantum key distribution. PhD thesis. *International Journal of Quantum Information*, 06(01):1-127, 2008.

[26] I. Gerhardt, Q. Liu, A. Lamas-Linares, J. Skaar, C. Kurtsiefer and V. Makarov. Full-field implementation of a perfect eavesdropper on a quantum cryptography system. *Nature Communications*, 2:349, 2011.

[27] N. J. Cerf, M. Levy, and G. V. Assche. Quantum distribution of Gaussian keys using squeezed states. *Physical Review A*, 63(5):52311, 2001.

[28] E. Diamanti and A. Leverrier. Distributing Secret Keys with Quantum Continuous Variables: Principle, Security and Implementations. *Entropy* 2015, 17(9):6072-6092.

[29] F. Grosshans and P. Grangier. Continuous Variable Quantum Cryptography Using Coherent States. *Physical Review Letters*, 88(5):057902, 2002.

[30] C. Weedbrook, A. M. Lance, W. P. Bowen, T. Symul, T. C. Ralph, and P. K. Lam. Quantum Cryptography Without Switching. *Physical Review Letters*, 93(17):170504, 2004.

[31] 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. *Physical Review Letters*, 109(10):100502, 2012.

[32] F. Furrer. Reverse-reconciliation continuous-variable quantum key distribution based on the uncertainty principle. *Physical Review A*, 90(4):042325, 2014.

[33] F. Furrer, M. Berta, M. Tomamichel, V. B. Scholz, M. Christandl. Position-momentumuncertainty relations in the presence of quantum memory. *Journal of Mathematical Physics*, Volume 55, 122205, 2014.

[34] 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 Information & Computation*, Volume 3, Issue 7, pages 535–552, 2003.

[35] R. García-Patrón and N. J. Cerf. Unconditional Optimality of Gaussian Attacks against Continuous-Variable Quantum Key Distribution. *Physical Review Letters*, 97(19):190503, 2006.

[36] R. García-Patrón. Quantum Information with Optical Continuous Variables: from Bell Tests to Key Distribution. Ph.D. thesis. *Université Libre de Bruxelles*, 2007.

[37] P. J. Coles, M. Berta, M. Tomamichel, and S. Wehner. Entropic uncertainty relations and their applications. *Reviews of Modern Physics*, 89(1):015002, 2017.

[38] M. Christandl, R. König, G. Mitchison, and R. Renner. One-and-a-half quantum de Finetti theorems. *Communications in Mathematical Physics*, 273(2):473–498, 2007.

[39] R. Renner. Symmetry of large physical systems implies independence of subsystems. *Nature Physics*, 3:645–649, 2007.

[40] M. Christandl, R. König, and R. Renner. Postselection Technique for Quantum Channels with Applications to Quantum Cryptography. *Physical Review Letters*, 102(2):020504, 2009.

[41] I. Devetak and A. Winter. Distillation of secret key and entanglement from quantum states. *Proceedings of Royal Society A*, 461:207–235, 2005.

[42] M. M. Wolf, G. Giedke, and J. I. Cirac. Extremality of Gaussian Quantum States. *Physical Review Letters*, 96(8):080502, 2006.

[43] M. Navascués, F. Grosshans, and A. Acín. Optimality of Gaussian Attacks in Continuous-Variable Quantum Cryptography. *Physical Review Letters*, 97(19):190502, 2006.

[44] P. Jouguet, D. Elkouss, and S. Kunz-Jacques. High-bit-rate continuous-variable quantum key distribution. *Physical Review A*, 90(4):042329, 2014.

[45] M. Ohya and D. Petz. Quantum entropy and its use. *Springer*, Verlag, 2004.

[46] S. Wiesner. Conjugate coding. *ACM Sigact News*, Volume 15, Issue 1, pages 78-88, 1983.

[47] R. Mittal and M. Szegedy. Product rules in semidefinite programming. *In Proceedings of Fundamentals of Computation Theory (FCT)*, pages 435–445, 2007.

[48] A. Lutomirski. An online attack against Wiesner's quantum money. arXiv:1010.0256, 2010.

[49] D. Gavinsky. Quantum money with classical verification. *In Proceedings of IEEE 27th Annual Conference on Computational Complexity (CCC)*, pages 42–52, 2012.

[50] A. Molina, T. Vidick, and J. Watrous. Optimal counterfeiting attacks and generalizations for Wiesner's quantum money. *In Proceeding of Theory of Quantum Computation, Communication, and Cryptography (TQC) (K. Iwama, Y. Kawano, and M. Murao, eds.)*, Volume 7582 of Lecture Notes in Computer Science, Springer, 2013.

[51] F. Pastawski, N. Y. Yao, L. Jiang, M. D. Lukin, and J. I. Cirac. Unforgeable noise tolerant quantum tokens. *Proceedings of the National Academy of Sciences of the United States of America (PNAS)*, Volume 109, no. 40, pages 16079–16082, 2012.

[52] M. Georgiou and I. Kerenidis. New constructions for quantum money. *In Proceedings of 10th Conference on the Theory of Quantum Computation, Communication and Cryptography (TQC) (S. Beigi and R. König, eds.)*, Volume 44, pages 92–110, Schloß Dagstuhl–Leibniz-Zentrum für Informatik, 2015.

[53] R. Amiri and J. M. Arrazola. Quantum money with nearly optimal error tolerance. *Physical Review A*, 95(6):062334, 2017.

[54] S. Aaronson. Quantum copy-protection and quantum money. *In Proceedings of Annual IEEE Conference on Computational Complexity*, pages 229–242, 2009.

[55] E. Farhi, D. Gosset, A. Hassidim, A. Lutomirski, D. Nagaj and P. Shor. Quantum state restoration and single-copy tomography for ground states of Hamiltonians. *Physical Review Letters*, 105(19):190503, 2010.

[56] A. Lutomirski, S. Aaronson, E. Farhi, D. Gosset, A. Hassidim, J. Kelner, and P. Shor. Breaking and making quantum money: towards a new quantum cryptographic protocol. *In Proceeding of Innovations in Computer Science (ICS)*, pages 20–31, 2010.

[57] M. Mosca and D. Stebila. Quantum coins. *Error-Correcting Codes, Finite Geometries and Cryptography,* Vol. 523, pages 35–47, 2010.

[58] S. Aaronson and P. Christiano. Quantum money from hidden subspaces. *Theory of Computing*, Volume 9, Issue 9, pages 349–401, 2013.

[59] G. Alagic and B. Fefferman. On quantum obfuscation. *Arxiv preprint*, arXiv:1602.01771 [quant-ph], 2017.

[60] E. Farhi, D. Gosset, A. Hassidim, A. Lutomirski, and P. Shor. Quantum money from knots. *In Proceedings of 3rd Innovations in Theoretical Computer Science Conference (ITCS)* pages 276–289, 2012.

[61] K. Bartkiewicz, A. Cernoch, G. Chimczak, K. Lemr, A. Miranowicz, and F. Nori. Experimental quantum forgery of quantum optical money. *npj Quantum Information*, 3:7, 2017.

[62] M. Bozzio, E. Diamanti, and F. Grosshans. Semi-device-independent quantum money with coherent states. *Physical Review A*, 99(2):022336, 2019.

[63] K. Horodecki and M. Stankiewicz. Semi-device independent quantum money. *New Journal of Physics*, 22:023007, 2020.

[64] A. Kent. S-money: virtual tokens for a relativistic economy. *Proceedings of the Royal Society A*, 475(2225):20190170 2019.

[65] A. Kent and D. Pitalúa-García. Flexible quantum tokens in spacetime. *Physical Review A*, 101(2):022309, 2019.

[66] R. Radian and O. Sattath. Semi-Quantum Money. *In Proceedings of the 1st ACM Conference on Advances in Financial Technologies (AFT)*, pages 132-146, 2019.

[67] M. Bozzio, A. Orieux, L. T. Vidarte, I. Zaquine, I. Kerenidis, and E. Diamanti. Experimental investigation of practical unforgeable quantum money. *npj Quantum Information*, 4:5, 2018.

[68] J.-Y. Guan, J.-M. Arrazola, R. Amiri, W. Zhang, H. Li, L. You, Z. Wang, Q. Zhang, and J.-W. Pan, "Experimental preparation and verification of quantum money. *Physical Review A*, 97(3):032338, 2018.

[69] K. Jiráková, K. Bartkiewicz, A. Černoch, and K. Lemr. Experimentally attacking quantum money schemes based on quantum retrieval games. *Scientific Reports*, 9:16318, 2016.

[70] M. Tomamichel and R. Renner. Uncertainty Relation for Smooth Entropies. *Physical Review Letters*, 106(11):110506, 2011.

[71] F. Dupuis, O. Fawzi, and R. Renner. Entropy accumulation. *Communication in Mathematical Physics*, Volume 379, pages 867-913, 2020.

[72] A. Leverrier. Security of Continuous-Variable Quantum Key Distribution via a Gaussian de Finetti Reduction. *Physical Review Letters*, 118(20):200501, 2017.

[73] A. Leverrier. *SU(p,q)* coherent states and a Gaussian de Finetti theorem. *Journal of Mathematical Physics*, 59(4):042202, 2018.

[74] S. Pirandola, S. Mancini, S. Lloyd, and S. L. Braunstein. Continuous-variable quantum cryptography using two-way quantum communication. *Nature Physics*, 4:726–730, 2008.

[75] M. Sun, X. Peng, Y. Shen, and H. Guo. Security of a new two-way continuous-variable quantum key distribution protocol. *International Journal of Quantum Information*, 10(05):1250059, 2012.

[76] Y.-C. Zhang, Z. Li, C. Weedbrook, S. Yu, W. Gu, M. Sun, X. Peng, and H. Guo. Improvement of two-way continuous-variable quantum key distribution using optical amplifiers. *Journal of Physics B: Atomic, Molecular and Optical Physics*, 47(3):035501, 2014.

[77] Y. Zhang, Z. Li, Y. Zhao, S. Yu, and H. Guo. Numerical simulation of the optimal two-mode attacks for two-way continuous-variable quantum cryptography in reverse reconciliation. *Journal of Physics B: Atomic, Molecular and Optical Physics*, 50(3):035501, 2017.

[78] C. Ottaviani, S. Mancini, and S. Pirandola. Two-way Gaussian quantum cryptography against coherent attacks in direct reconciliation. *Physical Review A*, 92(6):062323, 2015.

[79] C. Ottaviani and S. Pirandola. General immunity and superadditivity of two-way Gaussian quantum cryptography. *Scientific Reports*, 6:22225, 2016.

[80] Q. Zhuang, E. Y. Zhu, and P. W. Shor. Additive Classical Capacity of Quantum Channels Assisted by Noisy Entanglement. *Physical Review Letters*, 118(20):200503, 2017.

[81] Q. Zhuang, Z. Zhang, N. Lütkenhaus, and J. H. Shapiro. Distributed quantum sensing using continuous-variable multipartite entanglement. *Physical Review A*, 98(3):032332, 2018.

[82] S. Pirandola, C. Ottaviani, G. Spedalieri, C. Weedbrook, S. L. Braunstein, S. Lloyd, T. Gehring, C. S. Jacobsen, and U. L. Andersen. High-rate measurement-device-independent quantum cryptography. *Nature Photonics*, 9:397-402, 2015.

[83] Z. Li, Y.-C. Zhang, F. Xu, X. Peng, and H. Guo. Continuous-variable measurement-device-independent quantum key distribution. *Physical Review A*, 89(5):052301, 2014.

[84] C. Portmann. (Quantum) Min-Entropy Resources. *Arxiv preprint*, arXiv:1705.10595 [quant-ph], 2017.

[85] S. Ghorai, E. Diamanti, and A. Leverrier . Composable Security of Two-Way Continuous-Variable Quantum Key Distribution without Active Symmetrization. *Physical Review A*, 99(1):012311, 2019.

[86] C. Weedbrook, S. Pirandola, R. García-Patrón, N. J. Cerf, T. C. Ralph, J. H. Shapiro, and S. Lloyd. Gaussian quantum information. *Reviews of Modern Physics*, 84(2):621-699, 2012.

[87] P. J. Coles, E. M. Metodiev, and N. Lütkenhaus. Numerical approach for unstructured quantum key distribution. *Nature Communications*, 7:11712, 2016.

[88] A. Leverrier. Composable Security Proof for Continuous-Variable Quantum Key Distribution with Coherent States. *Physical Review Letters*, 114(7):070501, 2015.

[89] C. Lupo, C. Ottaviani, P. Papanastasiou, and S. Pirandola. Parameter Estimation with Almost No Public Communication for Continuous-Variable Quantum Key Distribution. *Physical Review Letters*, 120(22):220505, 2018.

[90] X. Zhang, Y. Zhang, Y. Zhao, X. Wang, S. Yu, and H. Guo. Finite-size analysis of continuous-variable measurement-device-independent quantum key distribution. *Physical Review A*, 96(4):042334, 2017.

[91] C. Lupo, C. Ottaviani, P. Papanastasiou, and S. Pirandola. Continuous-variable measurement-device-independent quantum key distribution: Composable security against coherent attacks. *Physical Review A*, 97(5):052327, 2018.

[92] R. Renner and J.I. Cirac. de Finetti Representation Theorem for Infinite-Dimensional Quantum Systems and Applications to Quantum Cryptography. *Physical Review Letters*, 102(11):110504, 2009.

[93] C. Weedbrook, C. Ottaviani, and S. Pirandola. Two-way quantum cryptography at different wavelengths. *Physical Review A*, 89(1):012309, 2014.

[94] J. Eisert, S. Scheel, and M.B. Plenio. Distilling Gaussian states with Gaussian operations is impossible. *Physical Review Letters*, 89(13):137903, 2002.

[95] F. Grosshans, G. Van Assche, J. Wenger, R. Brouri, N. Cerf, and P. Grangier. Quantum key distribution using Gaussian-modulated coherent states. *Nature (London)*, 421:238-241, 2003.

[96] S. Pirandola, R. Laurenza, C. Ottaviani, and L. Banchi. Fundamental limits of repeaterless quantum communications. *Nature Communications*, 8:15043, 2017.

[97] M. Tomamichel, C. Lim, N. Gisin, and R. Renner. Tight finite-key analysis for quantum cryptography. *Nature Communications*, 3:634, 2012.

[98] M. Tomamichel and A. Leverrier. A Largely Self-Contained and Complete Security Proof for Quantum Key Distribution. *Quantum* 1:14, 2017.

[99] R. Arnon-Friedman, F. Dupuis, O. Fawzi, R. Renner, and T. Vidick. Practical device-independent quantum cryptography via entropy accumulation. *Nature Communications*, 9:459, 2018.

[100] P. Jouguet, S. Kunz-Jacques, E. Diamanti, and A. Leverrier. Analysis of imperfections in practical continuous-variable quantum key distribution. *Physical Review A*, 86(3):032309, 2012.

[101] E. Kaur, S. Guha, and M. M. Wilde. Asymptotic security of discrete-modulation protocols for continuous-variable quantum key distribution. *Arxiv preprint*, arXiv:1901.10099 [quant-ph], 2019. Accepted in *Physical Review A*.

[102] T. Hirano, H. Yamanaka, M. Ashikaga, T. Konishi, and R. Namiki. Quantum cryptography using pulsed homodyne detection. *Physical Review A*, 68(4):042331, 2003.

[103] S. Lorenz, N. Korolkova, and G. Leuchs. Continuous-variable quantum key distribution using polarization encoding and post selection. *Applied Physics B*, 79:273-277, 2004.

[104] A. Leverrier and P. Grangier. Unconditional Security Proof of Long-Distance Continuous-Variable Quantum Key Distribution with Discrete Modulation. *Physical Review Letters*, 102(18):180504, 2009.

[105] M. Heid and N. Lütkenhaus. Security of coherent-state quantum cryptography in the presence of Gaussian noise. *Physical Review A*, 76(2):022313, 2007.

[106] D. Sych and G. Leuchs. Coherent state quantum key distribution with multi letter phase-shift keying. *New Journal of Physics*, 12:053019, 2010.

[107] Y.-B. Zhao, M. Heid, J. Rigas, and N. Lütkenhaus. Asymptotic security of binary modulated continuous-variable quantum key distribution under collective attacks. *Physical Review A*, 79(1):012307, 2009.

[108] K. Brádler and C. Weedbrook. Security proof of continuous-variable quantum key distribution using three coherent states. *Physical Review A*, 97(2):022310, 2018.

[109] C. Silberhorn, T. C. Ralph, N. Lütkenhaus, and G. Leuchs. Continuous Variable Quantum Cryptography: Beating the 3 dB Loss Limit. *Physical Review Letters*, 89(16):167901, 2002.

[110] A. M. Lance, T. Symul, V. Sharma, C. Weedbrook, T. C. Ralph, and P. K. Lam. No-Switching Quantum Key Distribution Using Broadband Modulated Coherent Light. *Physical Review Letters*, 95(18):180503, 2005.

[111] T. Symul, D. J. Alton, S. M. Assad, A. M. Lance, C. Weedbrook, T. C. Ralph, and P. K. Lam. Experimental demonstration of post-selection-based continuous-variable quantum key distribution in the presence of Gaussian noise. *Physical Review A*, 76(3):030303(R), 2007.

[112] J. Fiurášek and N. J. Cerf. Gaussian postselection and virtual noiseless amplification in continuous-variable quantum key distribution. *Physical Review A*, 86(6):060302(R), 2012.

[113] N. Walk, T. C. Ralph, T. Symul, and P. K. Lam. Security of continuous-variable quantum cryptography with Gaussian postselection. *Physical Review A*, 87(2):020303(R), 2013.

[114] A. Leverrier. Theoretical study of continuous-variable quantum key distribution. Ph.D. thesis. *Ecole Nationale Supèrieure des Télécommunications*, 2009.

[115] P. Jouguet, S. Kunz-Jacques, and A. Leverrier. Long-distance continuous-variable quantum key distribution with a Gaussian modulation. *Physical Review A*, 84(6):062317, 2011.

[116] P. Jouguet and S. Kunz-Jacques. High performance error correction for quantum key distribution using polar codes. *Quantum Information & Computation*, volume 14, issue 3-4, pages 0329-0338, 2013.

[117] M. Tomamichel, R. Colbeck, and R. Renner, A Fully Quantum Asymptotic Equipartition Property. *IEEE Transactions on Information Theory*, 55(12):5840-5847, 2009.

[118] A. Leverrier and P. Grangier, Continuous-variable quantum-key-distribution protocols with a non-Gaussian modulation, *Physical Review A*, 83(4):042312, 2011.

[119] B. O'Donoghue, E. Chu, N. Parikh, and S. Boyd. Conic Optimization via Operator Splitting and Homogeneous Self-Dual Embedding. Journal of Optimization Theory and Applications, 169(3):1042-1068, 2016.

[120] B. O'Donoghue, E. Chu, N. Parikh, and S. Boyd. SCS: Splitting Conic Solver, Version 2.0.2, https://github.com/cvxgrp/scs.

[121] P. Jouguet, S. Kunz-Jacques, A. Leverrier, P. Grangier, and E. Diamanti. Experimental demonstration of long-distance continuous-variable quantum key distribution. *Nature Photonics*, 7:378-381, 2013.

[122] 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 Science and Technology*, 2(2):024010, 2017.

[123] 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. *Physical Review A*, 76(4):042305, 2007.

[124] V. Scarani, H. Bechmann-Pasquinucci, N. J. Cerf, M. Dušek, N. Lütkenhaus, and M. Peev. The Security of Practical Quantum Key Distribution. *Reviews of Modern Physics*, 81(3):1301-1350, 2009.

[125] A. Ghazisaeidi, I. F. de Jauregui Ruiz, R. Rios-Müller, L. Schmalen, P. Tran, P. Brindel, A. C. Meseguer, Q. Hu, F. Buchali, G. Charlet and J. Renaudier. Advanced C+L-Band Transoceanic Transmission Systems Based on Probabilistically Shaped PDM-64QAM. *Journal of Lightwave Technology*, 35(7):1291, 2017.

[126] V. C. Usenko and R. Filip. Trusted Noise in Continuous- Variable Quantum Key Distribution: A Threat and a Defense. *Entropy* 2016, 18(1):20.

[127] F. Jardel, T. A. Eriksson, C. Méasson, A. Ghazisaeidi, F. Buchali, W. Idler, and J. J. Boutros. Exploring and Experimenting with Shaping Designs for Next-Generation Optical Communications. *Journal of Lightwave Technology*, 36(22):5298, 2018.

[128] F. Lacerda, J. M. Renes, and V. B. Scholz. Coherent-state constellations and polar codes for thermal Gaussian channels. *Physical Review A*, 95(6):062343, 2017.

[129] P. Papanastasiou, C. Lupo, C. Weedbrook, and S. Pirandola. Quantum key distribution with phase-encoded coherent states: Asymptotic security analysis in thermal-loss channels. *Physical Review A*, 98(1):012340, 2018.

[130] Z. Li, Y.-C. Zhang, and H. Guo. User-defined quantum key distribution. *Arxiv preprint*, arXiv:1805.04249 [quant-ph].

[131] J. F. Bonnans and A. Shapiro. Perturbation Analysis of Optimization Problems. Springer-Verlag, Berlin, 2000.

[132] S. Olivares and M. G. A. Paris. Binary optical communication in single-mode and entangled quantum noisy channels. *Journal of Optics B: Quantum and Semiclassical Optics,* 6, 69, 2004.