Unconditional Security of Continuous-Variable Quantum Cryptography

Carlo Ottaviani

PhD

University of York
Computer Science

July 2015

Abstract

This thesis deals with a detailed study of the unconditional security of Continuous-Variable (CV) Quantum Key Distribution (QKD). We consider general communication architectures based on both point-to-point and end-to-end principle. For the first case we develop an extensive analysis of the unconditional security of both one-way and two-way protocol under several eavesdropping conditions.

We describe an effective post-processing strategy, to apply to one-way communications, that allows to neutralise general coherent attacks. This result motivates us to formulate the conjecture that the *de Finettization* of the classical data, typically adopted in the asymptotic limit of many signals exchanged in order to reduce the attacks from a general coherent to a collective one, may not be necessary for Gaussian one-way communication.

For what it concerns two-way protocols we show that after the reduction of the general attack using the de Finetti symmetrization, two-mode coherent attacks are the optimal eavesdropping. Our cryptanalysis shows that the parties can exploit a strategy, inspired by the results obtained on the security of one-way protocols against two-mode coherent attacks, which allows to prove explicitly that two-way communications, with Gaussian continuous variables, are immune to general coherent attacks. The core idea is that Alice and Bob exploit the random opening and closing of the circuit at Alice station (ON/OFF switching). In the limit of many uses of the channel we prove that collective attacks represent, strictly, the best strategy available to Eve, and any correlation used by the eavesdropper to perform the coherent attack can be turned into noise under the control of the parties, which can exploit it to increase their secret-key rate.

We have then studied the general security of one-way protocol considering not just lossy channel, but extending the cryptanalysis to all physically allowed canonical forms attacks. Finally we extended the study of thermal CV-QKD to two-way communication at different frequencies, in the framework of optimal collective attacks.

In the last part of this thesis we focused on CV-QKD considering a modern end-to-end configuration. We then extend CV quantum cryptography to a network configuration. We develop a detailed cryptoanalysis of a communication scheme based on an untrusted relay, assisting the parties during the preparation of the secret key. We find the optimal eavesdropping and prove, both theoretically and experimentally, the feasibility of high-rate CV-QKD over metropolitan distances with of-the-shelves devices.

Contents

List of Figures

Preface

Contribution

The main contributions of this thesis, to the field of continuous variable quantum information, can be summarised by two results. For what it concerns point-to-point architectures the main result is represented by an explicit analytical proof that the bound

$$\chi_{\text{coh}} \leq \chi_{\text{coll}}, \tag{1}$$

holds for one-way quantum cryptographic protocol with Gaussian continuous variables. This result allows to show explicitly that general coherent attacks are always strictly less effective than coherent-collective ones. Using this result we identify a general post-processing strategy, based on arranging the exchanged signals into two-mode blocks, that we show being analytically solvable. Then, within the usual assumption of point-to-point QKD, we show that the parties can always share a secret-key, also in the presence of coherent attacks, by selecting (*a posteriori* after the tomography of the quantum channel) those signal with statistical properties more advantageous for the parties. This strategy has the side effects of reducing the calls to the de Finetti symmetrization. In our case the reduction is of a factor 1/2 (because of the reduction of the general attack to a two-mode block). We conjecture that the same should be valid for blocks with a larger number of modes, and then that Gaussian CV-QKD protocols could avoid to use the de Finetti symmetrization.

We also explicitly identified, a coherent attack beating a point-to-point protocol in two-way communication. We propose an effective counteraction that the parties can exploit in order to prevent the effects of this armful, optimal eavesdropping. This is based on the implication of Eq. (1) used in combination with the random opening/closing (ON/OFF switching) of the two-way quantum circuit performed by Alice independently from Bob. This action, basically reduces the communication to and double use of one-way communication.

The second main result obtained is concerns CV-QKD protocols in the end-to-end architecture. We theoretically design a communication scheme based on an untrusted relay. This theory has been tested in a proof-of-principle experiment, performed in collaboration with researchers (Ulrik L. Andersen group) at the Danish Technical University (DTU) in Lyngby, Denmark. The study of the symmetric configuration, where the relay is placed midways the two Alice and Bob, allowed to illustrate in detail the optimal coherent attack. Then we generalised the analysis to the optimal asymmetric configuration, also implemented in the experiment. We then proved, that CV-QKD can distribute a cryptographic key, in a full network configuration, at the metropolitan scale and at a very high rate, that exceeds by three/four orders of magnitude that today achievable using discrete variables, in a setup of comparable simplicity.

Project structure

This thesis is divided in three Parts and include also five Appendices. In Part I we introduce the main mathematical tools used through this thesis, we also discuss the main protocols to implement quantum cryptography with continuous variables, and finally present the state-of-the-art implementation of CV quantum cryptography.

In Part II we present the main novel result we have obtained quantum cryptography protocols in the point-to-point configuration. We first perform a systematic study of the security of CV-QKD in one and two-way communication. In both cases we assumed a communication quantum channel with memory. We provide an explicit proof that the active exploitation of the ON/OFF switching, typical of CV two-way protocols, we can achieve the immunity against coherent attacks. In this part we also studied the performances of two-way communication using thermal state, in particular in the switching setup. We finally studied the security of one-way protocols against arbitrary canonical-form attacks, in the framework of optimal collective attacks.

In Part III we extend the field of continuous variables quantum information to an end-to-end formulation. We show that exploiting the measurement-device-independent (MDI) principle we can shift quantum communications towards a network configuration, with relatively cheap and of-the-shelves technologies available today. We describe novel theoretical and experimental results obtained to implement high-rate quantum cryptography. In this respect we prove, both theoretically and experimentally, that CV systems represents a very promising candidate for future in-field implementations of high-rate quantum cryptography at the metropolitan scale. In particular we show that the achievable secret-key rate of this technology is, at least, three order of magnitude higher than that provided by discrete variable approach, implemented with comparably cheap and practical devices.

We conclude describing future challenges for the field of CV quantum cryptography, focusing on the open problems we think should be tackled in order to improve the security proof, the performances of the protocols both in terms of rates and/or distances; we will stress, in particular, on the importance of finite size effects, the non-optimal efficiency of the classical reconciliation codes, and on the lacking of a security proof for CV protocols with coherent state, against general attacks, in the composable security framework.

Assumed Knowledge

We assume some mathematical background and a large amount of knowledge in particular on: quantum mechanics, the theory of Gaussian continuous variables systems, and quantum cryptography in both continuous and discrete variables approach. The assumed background in computer science include information and coding theory. In particular the reading and understanding of the goals and results achieved in the work presented requires to be familiar with: *(i)* general mathematical theory of Gaussian CV classical and quantum systems, with special emphasis on the technical tools needed to manipulate the covariance matrix and to perform the symplectic analysis; *(ii)* Shannon's information and coding theory, where the key concepts of Shannon entropy and mutual information are developed; *(iii)* Quantum information theory with special emphasis on the definition, properties and meaning of the von Neumann entropy.

Acknowledgments

I would like to acknowledge my supervisor, Stefano Pirandola, and advisor, Samuel L. Braunstein, for their precious hints and critical advices during the development of this thesis. I'd like to give special thanks to the persons that, during these last years, have been closer to me and that belong to my family life, personal life and musical life: Maria Renata Roscioni, Armando Ottaviani, Lucia Ottaviani and Kathrin Nitschke, for supporting me. Again Kathrin Nitschke for dispensing me with thoughtful love, and James Marshall Hendrix for his music.

Author's Declaration

The work presented in this thesis is all my own except where explicitly indicated and cited. My main research activity has been focused to the development of the analysis of the unconditional security quantum cryptography with continuous variables. The subject of the work described in Part II are of point-to-point architectures. I had a leading role in developing the subjects of Chapters 4, 5, 6, 7 and in the study described in Chapter 8. Many of the results described in this part have not been yet published but, at the time of writing of this thesis, there are drafts almost ready for submission including the studies of Chapters 4, 5, 6 and 7. The work described in Chapter 8 has been published in Physical Review A [41].

The work described in Part III focus on CV-quantum cryptography in the end-to-end architecture. The results of this part have been published in Physical Review A [18], and Nature Photonics [17]. In the research developed in Ref. [18] I had the leading role at all stages of the development of the research, with a personal deeper focus in assessing the security analysis of the protocol. In the research work connected with Ref. [17] I worked on the security analysis of the scheme, and on the implementation of the theory and the numerical codes that have been used to perform the massive data analysis and post-processing of the experimental data, crucial to determine the experimental secret-key rate.

FInally, I declare that this work has not previously been presented for an award at this, or any other, University.

Part I

Preliminaries

Chapter 1

Continuous variable quantum systems

1.1 Quantisation of the electromagnetic field

The dynamics of an electromagnetic field in vacuum, with no presence of charges distribution nor currents, are given by the following Maxwell equations [1]

$$\nabla \times \vec{E} = -\epsilon_0 \frac{\partial \vec{H}}{\partial t}, \tag{1.1}$$

$$\nabla \times \vec{H} = -\mu_0 \frac{\partial \vec{E}}{\partial t}, \tag{1.2}$$

$$\nabla \cdot \vec{E} = 0, \tag{1.3}$$

$$\nabla \cdot \vec{H} = 0, \tag{1.4}$$

where $c = \sqrt{\epsilon_0 \mu_0}$ is the speed of light in vacuum, and ϵ_0 and μ_0 describe respectively the electric and magnetic permeability constants of the vacuum [1]. The Maxwell equations interconnect the electric field $\vec{E}$ and the magnetic field $\vec{H}$, providing a description of the EM field as single physical entity. Combining Eqs. (1.1–1.4), we can write the following equation solving the space-time dynamics of the electric field

$$\nabla^2 \vec{E} - \frac{\partial^2 \vec{E}}{\partial t^2} = 0, \tag{1.5}$$

where we set $c = 1$. We then solve Eq. (1.5) in a box with edge's length L. Assuming $L \to \infty$, the electric field can be written in terms of plane waves

$$\vec{E}(\vec{r}, t) = \sum_{j=1}^{n} E_j \mathbf{u}_j \left(q_j \cos \vec{k} \cdot \vec{r} - \nu_j t) + p_j \sin(\vec{k} \cdot \vec{r} - \nu_j t) \right) \tag{1.6}$$

where, $\vec{k}$ is the wave vector of the plane waves with angular frequency ν_j relative to mode j, and $\mathbf{u}_j$ is the polarisation of the wave. All physical quantities are given by the amplitudes E_j, defined as follows,

$$E_j = \sqrt{\frac{\hbar \nu_j}{2\epsilon_0}}.$$

Each term in the sum of Eq. (1.6) defines a wave, i.e., a mode. The electromagnetic field is so described as a collection of n independent harmonic oscillators whose

states, for fixed $\overrightarrow{k}$, $\overrightarrow{r}$, ν_j, and t, is determined by the components proportional to the quadrature q_j and p_j of the field, describing respectively the in-phase and out-of-phase (momentum) component to mode j.

It is easy to pass form a classical to a quantum description of the field. It is sufficient to replace the classical canonical variables, q_j and p_j, with two non-commuting operators $\hat{q}_j$ (position-like) and $\hat{p}_j$ (momentum-like) that verify the following commutation relation

$$[\hat{q}_j, \hat{p}_j] = 2i \text{ and } [\hat{q}_j, \hat{p}_l] = 0. \tag{1.7}$$

The description in terms of the canonical quantum variable is then ideal to describe infinite-dimensional quantum bosonic systems as the electric field. In fact the commutation relation given in Eq. (1.7) can be easily obtained defining the quantum canonical variables $\hat{q}_j, \hat{p}_j$ in terms of the field's bosonic operators $\hat{a}$ and $\hat{a}^\dagger$. In fact, if we define

$$\hat{q}_j = \hat{a}_j + \hat{a}_j^\dagger \text{ and } \hat{p}_j = -i(\hat{a}_j - \hat{a}_j^\dagger), \tag{1.8}$$

from the commutator for the field operators

$$\left[\hat{a}_l, \hat{a}_m^\dagger\right] = \delta_{lm}$$

with δ_{lm} the Kronecker $\delta-$function, one straightforwardly obtains Eq. (1.7).

With this replacement the electric field can be written as follows

$$\hat{E}(\overrightarrow{r}, t) = \sum_{j=1}^{n} E_j \left[\hat{q}_j \cos\left(\overrightarrow{k} \cdot \overrightarrow{r} - \nu_j t\right) + \hat{p}_j \sin\left(\overrightarrow{k} \cdot \overrightarrow{r} - \nu_j t\right)\right], \tag{1.9}$$

where the sum is over n bosonic modes, and is composed by the in-phase and out-of-phase quantized components, proportional respectively to $\hat{q}_j$ and $\hat{p}_j$. These are named the field quadratures and represent observable quantum variables (position and momentum-like) to which corresponds an infinite-dimensional Hilbert space $\mathcal{H}_j$.

1.2 Continuous Variables

Let $\hat{\rho}$ be an arbitrary quantum state of the bosonic system, $\hat{E}(\overrightarrow{r}, t)$.This is defined as $|\psi\rangle := \sum a_k |\psi_k\rangle$, and the corresponding quantum state is given by the density matrix operator $\hat{\rho} = |\psi\rangle\langle\psi|$. One then has that the expectation values of the field quadratures $\hat{q}_j$ and $\hat{p}_j$ are given by the expressions

$$\langle \hat{q}_j \rangle = \mathrm{Tr}(\hat{\rho}\hat{q}_j),$$
$$\langle \hat{p}_j \rangle = \mathrm{Tr}(\hat{\rho}\hat{p}_j),$$

for the quadratures relative to the $j-$esime mode of the electric field. The uncertainty relative to the expectation values is obtained computing the variances

$$\Delta\hat{q}_j = \langle \hat{q}_j^2 \rangle - \langle \hat{q}_j \rangle^2,$$
$$\Delta\hat{p}_j = \langle \hat{p}_j^2 \rangle - \langle \hat{p}_j \rangle^2.$$

Now, considering that for two non commuting quantum observables, described by operators $\hat{O}_1$ and $\hat{O}_2$ [2]

$$\left[\hat{O}_1, \hat{O}_2\right] \neq 0,$$

we have that

$$\Delta\hat{O}_1, \Delta\hat{O}_2 \geq \frac{\langle\psi|\left[\hat{O}_1, \hat{O}_2\right]|\psi\rangle}{2},$$

using previous general relation with Eq. (1.7) one has that the following inequality holds

$$\Delta\hat{q}_j \Delta\hat{p}_j \geq 1. \tag{1.10}$$

This represents the uncertainty associated with the measurements performed on incompatible observable $\hat{q}_j$ and $\hat{p}_j$ of mode j. The inequality is saturated only when mode j is in the vacuum state.

1.2.1 Photon number and energy of bosonic mode.

We note that the energy of mode j can be written in terms of the position and momentum quadratures, $\hat{q}_j$ and $\hat{p}_j$, as

$$\hat{H}_j = \frac{\hat{q}_j^2 + \hat{p}_j^2}{2}. \tag{1.11}$$

Now, from the definition of the photon number operator, $\hat{n}_j = \hat{a}_j^\dagger \hat{a}_j$, and inverting Eq. (1.8), one has

$$\hat{n}_j = \frac{1}{4}\left(\hat{q}_j^2 + \hat{p}_j^2 + i\left[\hat{q}_j, \hat{p}_j\right]\right), \tag{1.12}$$

that using Eq. (1.7) gives

$$\hat{n}_j = \frac{\hat{q}_j^2 + \hat{p}_j^2}{4} - \frac{1}{2}. \tag{1.13}$$

that with Eq. (1.11) provides a general relation connecting the observable energy and the number of mode j and the corresponding number of photons

$$\hat{H}_j = 2\hat{n}_j + 1. \tag{1.14}$$

This equation shows the operator defining the observable energy can be expressed in terms of the number of photons in each mode. We stress that Eq. (1.14), implicitly, show that thorough out this thesis we will work in a natural units system[1], where the vacuum shot-noise is equal to 1, i.e., $\hbar = 2$.

Previous Eq. (1.14) can be then used to obtain the energy in the general case of an electric field made of N modes, i.e., N independent harmonic oscillators.

$$\hat{H} = \sum_{j=1}^{N} \left(2\hat{n}_j + 1\right). \tag{1.15}$$

1.2.2 The Fock basis

It is possible to associate a set of orthogonal quantum states to the Hamiltonian of Eq. (1.15). These compose the Fock's number state basis $\mathcal{B} = \{|n_j\rangle\}_{n_j=1,\ldots,\infty}$, that is defined by the number of photons n_j in mode j. The element of this set are also eigenstates of the number operator $\hat{n}_j = \hat{a}_j^\dagger \hat{a}_j$, and of the energy operator $\hat{H}_j$ of Eq. (1.14). They span the infinite-dimensional Hilbert space $\mathcal{H}_j$ describing mode j, and then they can be written as a linear combination of the form

$$|\psi\rangle_j = \sum_{n_j=1}^{\infty} c_{n_j} |n_j\rangle, \tag{1.16}$$

[1] Natural units means that we adopt a rescaling where energy is in units of ν_j and distance is in units of $1/\sqrt{m\nu_j}$.

where the coefficients of the sum are $c_{n_j} = \langle n_j|\psi\rangle_j$, i.e., the quantity $|c_{n_j}|^2$ provides the probability of projecting mode j on a quantum state with n_j photons, $|n_j\rangle$. This can formally be represented by means of the action of a positive operator-valued measure (POVM), that in this case is defines the projector $|n_j\rangle\langle n_j|$.

For a collection of n uncoupled oscillators (n independent electromagnetic modes), we have a global tensor product Hilbert space given by the following tensor product

$$\mathcal{H} = \bigotimes_{j=1}^{n} \mathcal{H}_j, \tag{1.17}$$

spanned by state vectors of the form $\otimes_{j=1}^{n} |\psi\rangle_j$, with $|\psi\rangle_j$ defined in Eq. (1.16).

To build the vectors of the Fock basis $\mathcal{B}$, one can start from the vacuum $|0_j\rangle$, describing a mode j with no photons, and then apply consecutively the creation operator $\hat{a}_j^\dagger$, that applied on an arbitrary number states $|n_j\rangle$ gives

$$\hat{a}_j^\dagger |n_j\rangle = \sqrt{n_j + 1}|n_j + 1\rangle. \tag{1.18}$$

Applying n_j times on the vacuum state $|0_j\rangle$, one has

$$|n_j\rangle = \frac{(\hat{a}_j^\dagger)^{n_j}}{\sqrt{n_j!}}|0_j\rangle. \tag{1.19}$$

In the same way the annihilation operator $\hat{a}_j$

$$\hat{a}_j|n_j\rangle = \sqrt{n_j}|n_j - 1\rangle, \text{ for } n_j \geq 1, \tag{1.20}$$

applied to $|n_j\rangle$ n_j times gives

$$|0_j\rangle = \frac{\hat{a}_j{}^{n_j}}{\sqrt{n_j!}}|n_j\rangle. \tag{1.21}$$

1.2.3 Phase Space representation

Given an $n-$mode bosonic quantum system, with quantum state

$$\hat{\rho} := \mathcal{H}^{\otimes n} \to \mathcal{H}^{\otimes n}, \tag{1.22}$$

it is possible to associate an equivalent representation on the *phase-space*. This is $2n-$dimensional vectorial space, $\mathcal{K} : \mathbb{R}^{2n} \to \mathbb{R}^{2n}$, whose elements $\hat{\mathbf{x}}$ are composed by means of the canonical field quadratures, $\hat{q}_1, ..., \hat{q}_n$ and $\hat{p}_1, ..., \hat{p}_n$. We will use the convention that the arbitrary $\hat{\mathbf{x}}$ is defined as follows

$$\hat{\mathbf{x}} = (\hat{q}_1, \hat{p}_1, \ldots, \hat{q}_n, \hat{p}_n)^T. \tag{1.23}$$

The commutation relation for the general quadrature-operator, verifies the following commutation relation

$$[\hat{x}_l, \hat{x}_m] = 2i\mathbf{\Omega}, \tag{1.24}$$

where

$$\mathbf{\Omega} = \bigoplus_{k=1}^{2n} \omega_k, \tag{1.25}$$

is the $2n-$symplectic form and each component ω_k, defined as

$$\omega_k := \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix},$$

represents the single-mode symplectic form.

The mapping between the Hilbert space representation and the phase-space representation is performed by Wigner-Weyl operators, defined by the following formula

$$D(\xi) = \exp[i\hat{\mathbf{x}}\mathbf{\Omega}\xi] \tag{1.26}$$

with $\xi \in \mathbb{R}2^n$. In terms of this operator one can define characteristic function that is defined as follows

$$\chi_s(\xi) = Tr[\hat{\rho}D(\xi)], \tag{1.27}$$

and a corresponding Wigner, defined as

$$W(\mathbf{x}) = \frac{1}{(2\pi)^{2n}} \int_{\mathbb{R}^{2n}} d^{2n}\xi e^{-i\mathbf{x}^T\ \mathbf{\Omega}\ \xi} \chi_s(\xi), \tag{1.28}$$

where $\mathbf{x} \in \mathbb{R}^{2n}$ and its elements are the eigenvalues of the quadrature operator of Eq. (1.23).

The Wigner function of Eq. (1.28) is a quasi-probability distribution function because despite being properly normalised to unity, it is in general non-positive. Its properties are determined by the statistical moments and for the specific class of Gaussian states, which we dill deal with, the first and second statistical moments are all we need to know to determine the dynamics of the quantum system [11].

1.3 Gaussian Quantum States

In CV [8] quantum information Gaussian states play a privileged role [11]. Gaussian states are defined as quantum states having a Wigner-function representation that is a Gaussian. They are interesting because are easy to implement in today quantum optics labs, and as we will see allow a simple and elegant mathematical description. This make them particularly attractive in order to study protocols and propose experimental implementation. To clarify their properties, in next sections, we introduce some basic mathematical tools.

1.3.1 General properties

Let us consider a bosonic mode of the EM field. It can be described by the set of coherent states $|\alpha\rangle$: an over-complete set of quantum states that can be defined as the eigenstates of the destruction operator,

$$\hat{a}_k|\alpha_k\rangle = \alpha|\alpha_k\rangle. \tag{1.29}$$

These states can be *generated* by applying the Weyl displacement operator to the vacuum state, $|0\rangle_k$,

$$D_k(\alpha) = e^{(\alpha_k\hat{a}_k^\dagger - \alpha_k^\star\hat{a}_k)},$$

where $\alpha_k \in \mathbb{C}$, and their expansion in number state n reads,

$$|\alpha_k\rangle = e^{\frac{|\alpha_k|^2}{2}} \sum_{k=1}^{\infty} \frac{\alpha^n}{\sqrt{n!}}|n\rangle.$$

In terms of the generalized canonical vector $\hat{\mathbf{x}}$ of Eq. (1.23), the previous relation can be written as,

$$D_\alpha = e^{i\hat{\mathbf{x}}^T\mathbf{\Omega}\ \alpha,} \text{ where } \alpha \in \mathbb{R}^{2n}. \tag{1.30}$$

For a *Gaussian states* the characteristic function of Eq. (1.27) and the corresponding Wigner function of Eq. (1.28) are a Gaussian. That allows to introduce a further reduction on the quantities to take into account to study the dynamics of Gaussian systems. Considering an $n-$mode Gaussian system, and defining the generalized quadrature vector $\hat{\mathbf{x}}$ of Eq. (1.23), we have that the dynamics of the $n-$mode system is completely determined by the first and second moments of the Wigner distribution describing the system. This means that an arbitrary quantum state of the $n-$mode Gaussian system can be defined as follows

$$\hat{\rho} \coloneqq \hat{\rho}(\langle \hat{\mathbf{x}} \rangle, \mathbf{V}), \tag{1.31}$$

i.e., in terms of the covariance matrix $\mathbf{V}$, and the the mean value of the $\langle \hat{\mathbf{x}} \rangle$. This allows a huge simplification of the mathematics and in many cases we can obtain the analytical description of properties and dynamics of Gaussian quantum systems.

The first moment $\langle \hat{\mathbf{x}} \rangle \coloneqq (\langle \hat{x_1} \rangle, \ldots, \langle \hat{x_{2n}} \rangle)$, and represents the center of the multi-dimensional Gaussian distribution describing the quantum state. The first moment does not provide critical physical and informational contents, in fact it is always possible to compensate the shift of these mean values by local operations on the single modes k. A much more crucial role is instead played by the cross-correlations between modes. These are described by the second moments, i.e., the covariance matrix whose entries are defined as follows

$$V_{i,j} \coloneqq \frac{1}{2}\langle \{\Delta \hat{\mathbf{x}}_i, \Delta \hat{\mathbf{x}}_j\} \rangle, \tag{1.32}$$

where $\Delta \hat{\mathbf{x}}_i \coloneqq \hat{\mathbf{x}}_i - \langle \hat{\mathbf{x}}_i \rangle$, and $\{.,.\}$ stands for the anti-commutation operation. One can then rewrite the CM in a more explicit form

$$V_{i,j} \coloneqq \frac{1}{2}\langle \hat{\mathbf{x}}_i \hat{\mathbf{x}}_j + \hat{\mathbf{x}}_j \hat{\mathbf{x}}_i \rangle - \langle \hat{\mathbf{x}}_i \rangle \langle \hat{\mathbf{x}}_j \rangle,$$

where the diagonal elements

$$V_{ii} = V(\hat{\mathbf{x}}_i) = \langle \hat{\mathbf{x}}_i^2 \rangle - \langle \hat{\mathbf{x}}_i \rangle^2, \tag{1.33}$$

represent the usual variance for the $i-$th mode described by the quadrature $\hat{\mathbf{x}}_i$, while the off-diagonal terms describes the cross-correlations. We can rewrite the generalized expression of the Wigner function in terms of the CM

$$W(\hat{\mathbf{x}}) = \frac{e^{-\frac{1}{2}\hat{\mathbf{x}} V^{-1} \hat{\mathbf{x}}^T}}{\pi \sqrt{\det \mathbf{V}}}.$$

From previous equation, it is clear the advantage of describing these systems in terms of the covariance matrix: the study of an infinite dimensional multimode quantum system can be reduced to study a matrix that has a finite dimension and is only required to fulfill the following condition (uncertainty principle)

$$\mathbf{V} + i\Omega \geq 0. \tag{1.34}$$

in order to be a bona-fide CM, describing physical systems. Previous relation basically imposes that the minimum phase-space volume occupied by the quantum system with CM $\mathbf{V}$, must be larger than the volume occupied by the vacuum state.

Chapter 2

One-way quantum cryptography with continuous variables

2.1 Introduction

Quantum cryptography [3] deals with communication protocols, where quantum and classical information strategies are combined. The interest in this field is motivated by the fact that, in principle, the parties (Alice and Bob) can share the same random sequence of bits. This can then be used as a cryptographic key in conventional one-time pad protocols [5], that are known to be unconditionally (informational-theoretic) secure [4]. The ground rule to make this key-distribution effective is to use non-orthogonal quantum states to encode classical information, and then share them over a quantum channel. This is assumed to deteriorate the quantum properties of the signals as a consequence of the actions of an eavesdropper (Eve) that is in control of the communication channels between the parties. Despite this, the encoding performed using non-orthogonal quantum state limits the power of the eavesdropper, who results bounded by fundamental laws of quantum physics [6]. In fact any information gain for Eve comes with a reward for Alice and Bob, in terms of unavoidable noise on the quantum state of the shared signals. The parties, taking advantage of this automatic feedback provided by natural laws, can indeed not only detect the presence of Eve on the quantum channel but also estimate the amount of error correction and privacy amplification needed, in order to arbitrarily reduce Eve's stolen information [7] to a negligible amount.

Since the first proposals to realize quantum informational tasks [9, 10] over quantum continuous variable (CV) [8] this approach, describing infinite-dimensional quantum systems, has attracted increasing attention. The main appealing aspects of this approach, with respect the traditional based on discrete variable (qubits), are the possibility of making use of bright coherent states together with highly efficient homodyne detections, and the possibility of a relatively simple development towards broadband technologies. Particularly successful has been the design of CV protocols based on Gaussian quantum states that represents, nowadays, quantum systems routinely engineered in the labs [11].

In the context of Gaussian CV-QKD [12], the progress made in the classical post-processing [13], have recently allowed in-field implementation over distances [14] closer to those achievable by discrete variable protocols [15]. Besides this success, it seems plausible [16] that we couldn't avoid to exploit quantum repeaters in order to improve the present performances of QKD. In this respect a scheme, considering the

building block of a modern end-to-end high-rate network for continuous variables, has been recently proposed theoretically [17, 18] and successfully tested in a proof-of-principle experiment [17]. We will discuss it in Part III of this dissertation.

2.2 Continuous-variable protocols

2.2.1 General mechanism

Let us consider a single-mode, bosonic, quantum system with quadrature vector defined as $\hat{\mathbf{x}} := (\hat{q}, \hat{p})$. In a general cryptographic protocol with continuous variable, the encoding is made in energy, and then Alice chooses a quantum state $\hat{\rho}(\langle\hat{\mathbf{x}}\rangle, \mathbf{V})$ from a set of possible states belonging to the ensemble $\mathcal{A} = \{p(\langle\hat{\mathbf{x}}\rangle), \hat{\rho}(\langle\hat{\mathbf{x}}\rangle, \mathbf{V})\}$. This set, in practice, encodes the classical information $\alpha = \{p(\langle\hat{\mathbf{x}}\rangle), \langle\hat{\mathbf{x}}\rangle\}$ to be sent through the noisy channel. The variable α describes the modulation of the first moment $\langle\hat{\mathbf{x}}\rangle$ to which it is appended some probability distribution $p(\langle\hat{\mathbf{x}}\rangle)$. This variable α represent the amplitude of a coherent state that is sent to Bob by means of many independent uses of the quantum channel and, eventually, measured by the receiver who is generally assumed to perform a simple incoherent measurement. After that Bob will posses a variable β correlated with α. From this discussion it is clear that in CV quantum cryptography, the encoding of information is made in energy. In the next Sections we will review the steps that brought to the present status of the research in quantum cryptography with continuous variable.

2.2.2 Basic principle of security analysis

To quantify the security of a cryptographic protocol we compute the key-rate, which is defined by the following expression

$$R := I_{AB} - I_E. \tag{2.1}$$

This quantity can be positive, negative or equal to zero. In assessing the security of a protocol, we generally study for which range of the channel's parameters[1]

$$R > 0. \tag{2.2}$$

This provides a sufficient condition to claim the security of the protocol and in order to determine the threshold of security of the protocol we solve the equation

$$R = 0, \tag{2.3}$$

which marks the range of channel's parameters for which the cryptographic protocols starts to fail in providing a secure key.

In Eq. (2.1) the function I_{AB} quantifies the correlation (mutual information) between Alice and Bob's variables α and β, while I_E accounts for Eve's accessible information on α or β, depending on the setup of the classical reconciliation procedure (see later). In a general scenario Eve's attack is coherent, that means that

[1] Usually these are transmissivity and noise properties of the quantum channel. In particular the first describe the attenuation of the signal, while the second quantifies the presence of the eavesdropper on the channel.

different uses of the channels result correlated after Eve processing. The analysis of this case is unpractical and to overcome this difficulty we need some more assumption that allows to greatly simplify the general analysis of the eavesdropping. The first is to exploit the de Finetti theorem, that holds in both discrete [19] and continuous variable protocols [20]. It states the equivalence between general coherent and collective attacks, where different uses of the quantum channel are uncorrelated. The second is that Eve is assumed to be able to perform an optimal coherent measurement of an a set of ancillary states she has make interact with the parties' quantum signals. The ability of realize an optimal coherent measurement allows Eve to achieve the Holevo bound of the channel [21], in which case the accessible information is defined by the Holevo bound

$$I_E = \chi := S(\rho_E) - S(\rho_{E|X}), \tag{2.4}$$

where $S(\cdot)$ defines the von Neumann entropy of the Eve's quantum state.

A third important assumption applies for Gaussian protocols, for which Gaussian collective attack are optimal [30, 31, 32]. This allows to simplify further the complexity of the cryptoanalysis, and in many situations we can work with analytical expressions.

2.2.3 First steps: hybrid protocols

The first protocols exploiting continuous variable have been introduced in [22, 23, 24]. For instance in ref.[23], Alice randomly chooses to squeeze one of the two quadrature in a way that is very similar to $BB84$ protocol for discrete variables. Then a displacement $\pm\alpha$ is applied and Bob performs homodyne detection one of the two quadrature $\hat{q}$ or $\hat{p}$ again switching randomly between the two basis.

The sifting of the raw key, in this family of protocols, is implemented so that the parties retain only those cases where the prepared and measured quadratures coincide. Alice's encoding is not performed by a Gaussian modulation but is a discrete encoding with Bob's binary data that can be described by a Gaussian distribution around the values $\pm\alpha$. For this difference in the encoding/decoding stage, they represent a sort of hybrid protocol and are also known as CV protocols with discrete modulation [3].

2.3 Gaussian one-way communication

In these schemes the sender modulates the amplitude α, of coherent states $|\alpha\rangle$, by means of a bivariate Gaussian distribution. The decoding realized by the receiver is performed by Gaussian measurements like homodyne and/or heterodyne detections. When the receiver use homodyne detections switching randomly between one of the possible two bases, then we say to have the *switching* protocol. If instead a measurement on both quadrature (heterodyne detection) is implemented, then the scheme is known as *no-switching* protocol and, avoiding the random switching of the measurement basis, can provide higher key-rates. When the encoding is made by modulating squeezed states and together with a decoding by homodyne detection we will call the protocol *squeezed/hom*. Finally we have the *squeezed/het* protocol, where the receiver uses heterodyne detection to decode.

Each of this cases can be implemented using two possible reconciliation strategies: direct reconciliation (DR) and reverse reconciliation (RR). In DR (RR), the classical

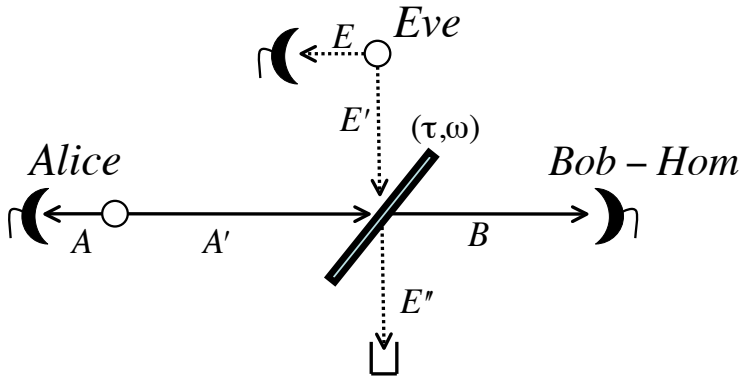

Figure 2.1: The figure shows the implementation of the one-way protocol with continuous variables, in the EB representation. Alice modulates coherent states by measuring one mode of her EPR state. The states with distinct amplitudes α, are sent to Bob who measures the received state by means of a homodyne detection by switching between the two orthogonal quadratures Q_α, and P_α. Eve attacks the line by performing an entangling cloner attack on the intercepted state.

communication steps, channel's parameter estimation and sifting of the raw key, is performed by the receiver (sender) guessing the encoding (decoding) of the sender (receiver).

2.3.1 The very first Gaussian protocol

It has been introduced in [25] and is a generalization of the protocol of ref. [23]. Now Alice prepares squeezed states modulating by a Gaussian distribution in $\hat{q}$ or $\hat{p}$ with Bob measuring the signals received via homodyne detections. The average state sent by Alice to Bob is a thermal state, while the original *BB84* make use of a mixed quantum state of the form

$$\hat{\rho} = \sum_k p_k \rho_k.$$

The unconditional security of this protocol can be found in [26]. This protocol is important from the conceptual point of view, but less interesting from the experimental implementation point of view, being infinitely squeezed state un-physical (infinite energy is needed to implement such a state).

2.3.2 The coherent state protocol

This protocol represented a major shift ahead for what it concerns the simplicity of the implementation and the security analysis of Gaussian protocols. There is in fact no need for squeezed states to grant the security of the quantum communication. In Ref. [27], a coherent states based protocol was proposed, which was able to exploit a basis of quantum states that are non-orthogonal by construction, i.e., coherent states. In this protocol, the sender encodes classical information in coherent states while the receiver decodes by performing homodyne detection. Of course the no-cloning theorem can be applied also to the coherent states, then quantum states for

which it is possible to apply the no-cloning theorem and then achieve the security performances of quantum cryptography.

Coherent states are of course much simpler to implement than squeezed states and this protocol represented a pivotal result to prove the feasibility of CVQKD by off-the-shelves optical elements. The protocol is illustrated in figure 2.1.

2.4 Cryptoanalysis in the entanglement-based representation

We give here a simplified description of the purification procedure widely used ti perform the cryptoanalysis. A more detailed description of the dilation/purification of source and communication channel is discussed in Chapter 5, in the context of general security of quantum cryptographic protocols.

The security of cryptographic protocols is often performed exploiting the entanglement based representation (EB) [26, 28]. This method of analysis is based on the assumption of performing the *purification* of both the source of quantum states and quantum channel, and is very powerful because allows a drastic simplification of the mathematics and calculations to generalize the security of a protocol. It is based on the principle [28] that if we assume the possibility of presence of entanglement in the circuit this is equivalent to the actual presence and exploitation of entanglement. In others words the entanglement can be virtual, in the sense that what really matter is the physical possibility, for the system, to support entanglement. If this is true then the standard prepare and measure description of a protocol has an equivalent entanglement based representation.

2.4.1 Source Purification

Let us consider a sender (Alice) preparing quantum states described by the canonical variables $\hat{q}_A, \hat{p}_A$, and sending these pairs of complex numbers to the receiver (Bob). From the outside Alice's device can be seen as a Black-Box, i.e., the only things coming out from it are the values of these pairs. These stage represents the quantum state preparation, i.e., the encoding. We now can assume that *(i)* inside Alice's black box an entangled pairs of modes is generated and (*ii*) that while one of this modes is sent troughs the quantum channel, the other (the *local* one) is measured by a homodyne or heterodyne detection. The law of quantum mechanics ensure that the remote mode will be projected to a coherent or a squeezed state, conditioned to the measurement applied.

For Gaussian systems this initial state from which Alice starts has particularity simple expression. In fact the CM describing the two-mode squeezed state is given by the following expression

$$V_{AA'} = \begin{pmatrix} \mu\mathbf{I} & \sqrt{\mu^2-1}\mathbf{Z} \\ \sqrt{\mu^2-1}\mathbf{Z} & \mu\mathbf{I} \end{pmatrix}, \tag{2.5}$$

where μ describe the classical Gaussian modulation of the amplitude of the coherent state, while $\mathbf{I}$ =diag$(1,1)$ and $\mathbf{Z}$ =diag$(1,-1)$.

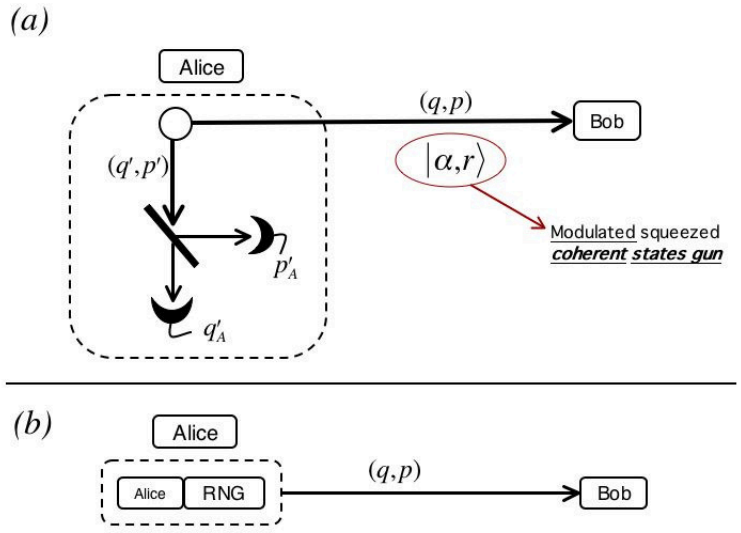

Figure 2.2: Figure 2.2*(a)* shows the Entanglement Based (EB) representation of general squeezed coherent states preparation. The measurement of one(both) quadrature(s) of the component of the entangled pair of beam, retained by Alice, induce on the entangled partner the projection onto a squeezed (coherent state).The virtual entanglement representation is widely adopted to study the security of QKD protocols by means of entanglement purification. Figure *(b)* is the equivalent representation "seen" from the outside of Alice's black-box: the EB representation is equivalent to a (Q,P) modulation obtained by means of a Random Number Generator(RNG).

2.4.2 Channel dilation

To perform the purification of the channel's state (see Fig. 2.3) one assume to process Alice-Bob quantum state, ρ_{AB}, and Eve's quantum state, ρ_E, by means of a completely positive trace-preserving (CPT) map. This makes the global quantum state, of Alice-Bob-Eve, a pure.This is obtained dilating the Hilbert space on which Alice-Bob systems evolve, including the environment. In such a larger space it is possible to define a unitary evolution **U**, acting not only on Alice-Bob modes processed by the quantum channel but also Eve's quantum state $|\psi\rangle_E$.

For Gaussian protocol we can assume that **U** operation is a Gaussian processing one mode from an EPR pairs in Alice hands and the other mode coming from Eve's EPR state (see Fig. 2.3). This makes the global quantum state of Alice, Bob and Eve's a pure quantum state, in the larger Hilbert space.

This purification procedure is crucial because we want to make as less assumption as possible on the operations performed by Eve to process the signal exchanged. Indeed, working in the EB representation, allows to say that as far as the modes' processing takes place under evolutions like source purification and POVM, the purity of the global state is preserved. To obtain information on the effects of Eve's measurements on Alice-Bob state, one has to perform a partial trace over Eve's variables

$$\rho_{AB} = Tr_E\left(\rho_{ABE}\right), \tag{2.6}$$

that, in fact is automatically realized by Eve when performs the optimal coherent

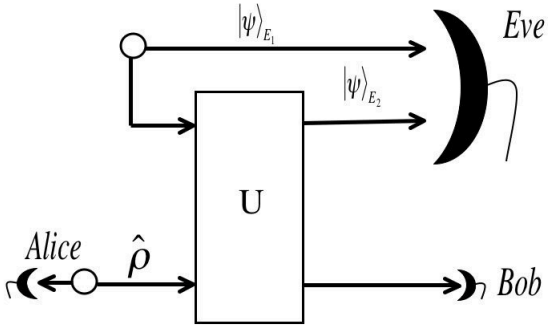

Figure 2.3: Channel Purification through entanglement . Alice and Eve both inject into the channel a mode of their respective entangled state (–◯–). This allows to have a purified global quantum state of the three systems Alice, Bob and Eve, and a simplified security analysis, because in studying the evolution of the system we can rid of the specific operations performed by the eavesdropper. This authorise to write $\chi_E = S(\rho_{AB|X}) - S(\rho_{AB})$.

measurement her quantum memory, where her ancillary states are stored. Thanks to this we have that the informational contents of the quantum state ρ_{AB} and ρ_E are identical. This means that we can write

$$S(\rho_{AB}) = S(\rho_E), \tag{2.7}$$

where the function $S(.)$ is the von Neumann entropy. It is then clear that we can retrieve Eve's accessible information on Alice-Bob quantum signals ignoring the details of the operation performed during the eavesdropping. In fact the same principle can be applied to the conditional state. If $\rho_{E|X}$ represents Eve's conditional state after Bob's measurements, where $X = (q_B, p_B)$, one has that

$$S(\rho_{AB|X}) = S(\rho_{E|X}). \tag{2.8}$$

These quantities are useful to compute Eve's accessible information I_E. We have seen that in the worst case we have to consider that Eve owns a quantum memory. In such a case we can write

$$I_E = \chi := S(\rho_E) - S(\rho_{E|X}) = S(\rho_{AB}) - S(\rho_{AB|X}), \tag{2.9}$$

where function χ is named the Holevo bound. This represent the typical scenario studied in this dissertation.

2.5 Conditioning in the asymptotic limit

For what said in previous sections, it is clear that to study the security of any Gaussian continuous-variable protocol depends on the computation of the total and conditional covariance matrix. We then give here some simple instrument to perform the *conditioning* of a variance or of a covariance matrix, meaning with this the

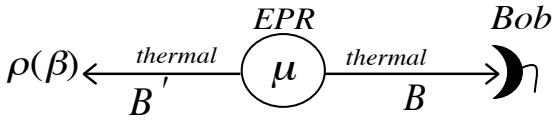

Figure 2.4: This figure describes the preparation of Gaussian states, for the one-way protocol. Bob generates a thermal state with large Gaussian modulation by measuring one component of his two-mode vacuum squeezed state (EPR pair). This measurement in one of the possible configuration (Het, Hom), performed on the local mode B, projects the remote mode, B', into a coherent or squeezed state, depending ont he measurement scheme employed.

steps to obtain the conditional CM starting from the total CM. The conditioning is specified by the type of measurement performed and by the modality in which the classical reconciliation is implemented, i.e., if we study the direct or the reverse reconciliation. Technically, we have to way to perform the conditioning of the total state. In the entanglement based representation (see next section), we can extract information on Eve's quantum state, $\hat{\rho}_E$, from Alice-Bob's state, $\hat{\rho}_{AB}$.

On the other hand, not always it is possible to have a treatable entanglement based representation. In such a case the security analysis of a protocol be performed in the prepare and measure representation, i.e., directly Eve's state $\hat{\rho}_E$. The conditioning is then performed by completing the covariance matrix describing Eve's state with the mode belonging to the party's modes with respect want to perform the conditioning. We can then assign a precise value to the Gaussian modulation μ, that mimic the measurement process. Of course this procedure can be applied also in the EB representation.

2.5.1 Conditioning in the one-way protocols in DR

With reference to Fig. 2.4, we have a sender starting from an EPR state and measuring one mode of his two-mode squeezed vacuum state, while sending the other to the channel.The sender prepares many EPR pairs and repeatedly performs measurements (heterodyne or homodyne) on mode B. After each measurement on modes B, B' will be remotely projected in a quantum state (coherent or squeezed) compatible with the type of measurement performed by the sender. In doing this, we can also modulate the amplitudes of the resulting quantum state that is sent trough the quantum channel, and at the receiver we will have a thermal states.

Coherent State protocol

In this case both the quadratures are measured, so to repeatedly prepare coherent states $|\beta\rangle$ on mode B'. The transmitted thermal state is characterized by the total

modulation

$$\mu_B = \bar{\mu}_B + 1, \tag{2.10}$$

on both quadratures $(\hat{p}, \hat{q})$, composed by the classical $\bar{\mu}_B$ modulation on the top of the quantum contribution, accounting for the variance of the vacuum shot-noise. The conditioning on the CM is performed by setting $\bar{\mu}_B = 0$, or equivalently $\mu_B = 1$.

Squeezed State protocol

In this case Bob homodynes one quadrature of mode B so to prepare squeezed coherent state $|\beta, r\rangle$ on mode B', where

$$r = \frac{1}{\mu} \tag{2.11}$$

is the squeezing parameter. The thermal state is characterized by the following relations defining the resulting modulations of quadratures $\hat{q}$ and $\hat{p}$ respectively,

$$\mu_B^q = \bar{\mu}_B + \frac{1}{\mu}, \tag{2.12}$$

$$\mu_B^p = \mu, \tag{2.13}$$

where we can distinguish again between a classical and the quantum contribution $1/\mu$. In this case the conditioning is performed again by setting $\bar{\mu}_B = 0$, but this time total modulation will have different values for the two quadratures,

$$\mu_B^q = \frac{1}{\mu}, \tag{2.14}$$

$$\mu_B^p = \mu, \tag{2.15}$$

for the usual limit of large modulation $\mu \to \infty$, we have $\mu_B^q = 0$.

2.6 The switching protocol

The protocol has been introduced in ref. [27] in the direct reconciliation, and has been tested experimentally in [12] also in reverse reconciliation.

The sender (Alice) modulates coherent states applying a bivariate Gaussian modulation of the amplitudes of the prepared coherent state, whose variance μ. Bob applies homodyne detection to the incoming coherent states in order to perform the decoding. To choose the quadrature to measure randomly switch between the basis $\hat{q}$ and $\hat{p}$. In a typical communication scenario the channel is lossy (free-space or optical fibre), so that the channel is well approximated by an entangling cloner. This is a beam splitter of transmissivity $0 \leq \tau \leq 1$, attenuating the modulation of the incoming states, on which Eve mixes her ancillary modes with the the sender's modes. During this quantum communication phase, a portion of the energy of the incoming signals beams is intercepted by Eve. depending on the transmissivity of the beam splitter. When $\tau < 1/2$, the amount of information in common between Eve and Alice becomes larger than that Alice and Bob are sharing. So we have

$$I_{AE} > I_{AB}.$$

That means that the tolerable noise of the protocol is limited by $\tau = 1/2$ ($\sim 3\ dB$), i.e., the scheme in DR is not secure for values of the transmission line below $3dB$, this value is to low to allow transmission over long distances.

The use of the protocol in reverse reconciliation can beat this limit because now Bob's variables are the reference, while Alice and Eve estimate the results of Bob's measurements. So, if the signals arrive very attenuated to Bob, this only affects the intensity of the signals, i.e., it affects symmetrically both Alice-Bob mutual information I_{AB}, and Eve's I_{BE}. But the difference $I_{AB} - I_{BE}$, that quantify the security of the protocol, is left unchanged.

2.6.1 Cryptanalysis

Alice's EPR state, modes A and A' (see Fig. 2.1), is described by the following CM matrix

$$\mathbf{V}_{AA'} = \begin{pmatrix} \mu\mathbf{I} & \sqrt{\mu^2-1}\mathbf{Z} \\ \sqrt{\mu^2-1}\mathbf{Z} & \mu\mathbf{I} \end{pmatrix}, \tag{2.16}$$

Mode A' is sent to Bob through the quantum channel. After applying the de Finetti theorem, we can reduce the general attack to the study of a single use of the channel where an entangling cloner implemented by a beam splitter with transmissivity τ, intercepts the signals of the sender that are mixed with Eve's ancillary mode E' described by a thermal noise ω. Eve's initial state is another EPR pair E, E' with covariance matrix

$$\mathbf{V}_{EE'} = \begin{pmatrix} \omega\mathbf{I} & \sqrt{\omega^2-1}\mathbf{Z} \\ \sqrt{\omega^2-1}\mathbf{Z} & \omega\mathbf{I} \end{pmatrix}. \tag{2.17}$$

Let define the general vectorial canonical variable $X := (\hat{q}_x, \hat{p}_x)$. The equations of motions, in the Heisenberg picture, are given by the following linear Bogoliubov transformation

$$B = \sqrt{\tau}A' + \sqrt{1-}E', \tag{2.18}$$

$$E' = \sqrt{\tau}E' - \sqrt{1-\tau}A'. \tag{2.19}$$

Note that in the entanglement based representation, our interest can focus on modes A and B, from which we can obtain the variances and the covariances defining covariance matrix of the joint state of Alice and Bob. Simple algebra provides the following expressions

$$\begin{aligned} \mathbf{V}_A &= \langle A^2 \rangle = \mu\mathbf{I}, \\ \mathbf{V}_B &= \langle B^2 \rangle = \tau\langle A'^2 \rangle + (1-\tau)\langle E'^2 \rangle = [\tau\mu + (1-\tau)\omega]\,\mathbf{I}, \qquad (2.20) \\ \mathbf{V}_{AB} &= \langle AB \rangle = \sqrt{\tau}\langle AB \rangle + \sqrt{1-\tau}\langle AE' \rangle = \sqrt{\tau(\mu^2-1)}\mathbf{Z} = \langle BA \rangle, \qquad (2.21) \end{aligned}$$

from which one has the covariance matrix

$$\mathbf{V}_{AB} = \begin{pmatrix} \mu\mathbf{I} & \sqrt{\tau(\mu^2-1)}\mathbf{Z} \\ \sqrt{\tau(\mu^2-1)}\mathbf{Z} & [\tau\mu + (1-\tau)\omega]\mathbf{I} \end{pmatrix}. \tag{2.22}$$

The mutual information between Alice and Bob, is given by the ratio between the signal prepared by the sender, described by the variance V_B arriving at Bob, and the noisy signals after Bob's detections, described by the conditional variance $V_{B|\alpha}$.

This is conditioned to the results of Alice measurements, i.e., from the preparation stage. We than can write the following general relation

$$I_{AB} = \frac{1}{2}\log\frac{V_B}{V_{B|\alpha}}, \tag{2.23}$$

that is valid when the receiver measure only one of the quadrature composing the coherent state sent. To compute this quantity one uses Eq. (2.20) and apply conditioning prescription of section 2.5. Form the variance of Bob's mode in $\mathbf{V}_{AB}$, one straightforwardly obtains the following general expression

$$I_{AB} = \frac{1}{2}\log\frac{\tau\mu + (1-\tau)\omega}{\tau + (1-\tau)\omega}.$$

Now, we note that clearly the ideal operative limit of these protocol is when Alice and Bob can exchange a lot of energy, i.e., to find the best performance of a protocol it is reasonable to assume the limit of large modulation ($\mu >> 1$). This simplify further the mathematical expressions and here, in particular, allows to simplify the expression of Alice-Bob mutual information, that asymptotically is given by the following formula

$$I_{AB} = \frac{1}{2}\log\frac{\tau\mu}{\tau + (1-\tau)\omega}. \tag{2.24}$$

The security is quantified by the key-rate given in general by Eq. (2.1), where Eve's accessible information is given by Eq.(2.4).

2.6.2 Direct Reconciliation

We compute now the conditional covariance and show how to obtain the Holevo bound from the symplectic analysis [11]. We first calculate the determinant of the CM of Eq. (2.22), and take the asymptotic limit $\mu >> 1$, obtaining

$$\det \mathbf{V}_{AB} = \mu^2\omega^2(1-\tau)^2.$$

The motivation to compute this is that the determinant of a covariance matrix is connected to the symplectic spectrum by the following general relation [11]

$$\sqrt{\det \mathbf{V}} = \nu_1, ..., \nu_N,$$

where $\nu_1, ..., \nu_N$ represents are the symplectic eigenvalues relative to a $N-$modes Gaussian system. This expression can then be of great help in determining the analytical expression of the symplectic spectrum. To compute the symplectic eigenvalues one calculate the absolute value of the eigenvalues of the following symplectic matrix

$$\mathbf{M} = i\mathbf{\Omega}\mathbf{V},$$

where $\mathbf{\Omega} = \oplus_j \omega_j$ with

$$\omega_j = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}.$$

We then apply the previous steps to the CM of Eq. (2.22), obtaining

$$\{\nu_1, \nu_2\} \to \{\omega, (1-\tau)\mu\}.$$

For Gaussian systems the von Neumann entropy has a simple definition in terms of the symplectic eigenvalues. This is given by the following general formula

$$S(\nu) = \sum_{\nu} h(\nu), \tag{2.25}$$

where ν are the component of the symplectic spectrum and

$$h(\nu) = \frac{\nu+1}{2}\log_2\frac{\nu+1}{2} - \frac{\nu-1}{2}\log_2\frac{\nu-1}{2}. \tag{2.26}$$

That asymptotically verifies the following equation

$$\lim_{\nu\to\infty} h(\nu) = \log_2\frac{e}{2}\nu + O(\nu^{-1}).$$

The previous equations allow to write the total von Neumann entropy in the following form

$$S_{AB} = h(\omega) + \log_2\frac{e}{2}(1-\tau)\mu. \tag{2.27}$$

The computation of the conditional spectrum, we apply the conditioning prescription described in Section 2.5, collapsing the Gaussian modulation $\mu := 1$ in one quadrature of the CM of Eq. (2.22), and obtaining $V_{AB|\alpha}$. We then compute first compute the determinant of $V_{AB|\alpha}$ and take the asymptotic limit, obtaining

$$\det V_{AB|\alpha} = \omega(1-\tau)\mu[\tau+\omega(1-\tau)].$$

We then calculate the conditional symplectic spectrum, that for large μ, and after some algebra, is given by the following mathematical expression

$$\{\bar{\nu}_1, \bar{\nu}_2\} \to \left\{\sqrt{[\tau\omega+1-\tau](1-\tau)\mu}, \sqrt{\omega\frac{(1-\tau)\omega+\tau}{\tau\omega+1-\tau}}\right\}. \tag{2.28}$$

The symplectic spectrum of Eq. (2.28) provides the conditional von Neumann entropy

$$S^{\blacktriangleright}_{AB|A} = h(\bar{\nu}_2) + \frac{1}{2}\log_2\frac{e}{2}\left(\tau\omega+1-\tau\right)(1-\tau)\mu \tag{2.29}$$

that used with the mutual information of Eq. (2.24), Eq. (2.27) and Eq.(2.29) allows to compute the key-rate

$$R^{\blacktriangleright} = I_{AB} - \chi = I_{AB} - \left(S^{\blacktriangleright}_{AB} - S^{\blacktriangleright}_{AB|A}\right),$$

and after some algebra arrive at the final expression of the key-rate give by the formula

$$R^{\blacktriangleright}(\tau,\omega) = \frac{1}{2}\log_2\frac{\tau[\tau\omega+(1-\tau)]}{[\tau+\omega(1-\tau)](1-\tau)} + h\left(\sqrt{\frac{[\tau+\omega(1-\tau)]\omega}{\tau\omega+(1-\tau)}}\right) - h(\omega). \tag{2.30}$$

2.6.3 Reverse Reconciliation

In RR, one needs only to calculate the conditional von Neumann entropy from the conditional CM, $V_{AB|\beta}$, that is now conditioned to Bob's final measurement. We

have to apply the general formula [11] for homodyne detection. First we rewrite the total CM 2.22 in the following 4×4 block-form

$$\mathbf{V} = \begin{pmatrix} \mathbf{A} & \mathbf{C} \\ \mathbf{C}^T & \mathbf{B} \end{pmatrix}, \tag{2.31}$$

where $\mathbf{A} = \mu\mathbf{I}$, $\mathbf{B} = [\tau\mu + (1-\tau)\omega]\mathbf{I}$ and $\mathbf{C} = \sqrt{\tau(\mu^2-1)}\mathbf{Z}$. We then apply the homodyne measurement of mode $\mathbf{B}$, using the following formula [33, 11]

$$\mathbf{V}_{AB|\beta} = \mathbf{A} - \mathbf{C}(\mathbf{\Pi}\mathbf{B}\mathbf{\Pi})^{-1}\mathbf{C}^T, \tag{2.32}$$

where $\mathbf{\Pi} = \mathrm{diag}(1,0)$ for measurement on quadrature $\hat{q}$ and $\mathbf{\Pi} = \mathrm{diag}(0,1)$ for measurement on quadrature $\hat{p}$ and. We obtain the following CM,

$$\mathbf{V}_{A|\beta} = \begin{pmatrix} \frac{\tau+\omega\mu-\tau\omega\mu}{\omega-\tau\omega+\tau\mu} & 0 \\ 0 & \mu \end{pmatrix}.$$

whose exact symplectic spectrum can be computed to be

$$\bar{\nu}^{\blacktriangleleft} = \sqrt{\frac{\mu[\tau+\omega\mu(1-\tau)]}{\omega(1-\tau)+\tau\mu}}.$$

This can be simplified further taking the limit of large modulation μ obtaining

$$\bar{\nu}^{\blacktriangleleft} \to \sqrt{\mu(1-\tau)]}$$

and gives the condition von Neumann entropy

$$S^{\blacktriangleleft}_{AB|\alpha} = \frac{1}{2}\log_2(1-\tau)\mu, \tag{2.33}$$

that used with Eq. (2.24) and (2.27) give the key-rate in reverse reconciliation

$$R^{\blacktriangleleft}(\tau,\omega) = \frac{1}{2}\log_2\frac{\tau}{(1-\tau)[(1-\tau)\omega+\tau]} + h(\omega).$$

2.6.4 The Excess noise

An important quantity to describe the tolerable noise of a protocol is the *excess noise*, N. This can be seen as the analogous of the efficiency of photon counting in discrete variable QKD. Assuming the worst case scenario any noise injected in the system, exceeding that to the vacuum, is assumed to be a consequence of Eve's presence on the channel. Therefore, by definition, the *excess noise* is the noise associated with channel's thermal noise, whose total equivalent noise, $\chi_{0,}$ present on the channel is given by the following relation

$$\chi_0 \coloneqq N_0 + N, \tag{2.34}$$

where N_0 is the vacuum shot-noise. To determine N, for a protocol (here we discuss the one-way case), one can use Alice-Bob mutual information, and write it in terms of the signal to noise (χ_0) ratio

$$I_{AB} = \frac{1}{2}\log_2\frac{V_A}{V_{A|\beta}} = \frac{1}{2}\log_2\frac{\tau\mu}{\tau+(1-\tau)\omega} = \frac{1}{2}\log_2\frac{\mu}{\chi_0},$$

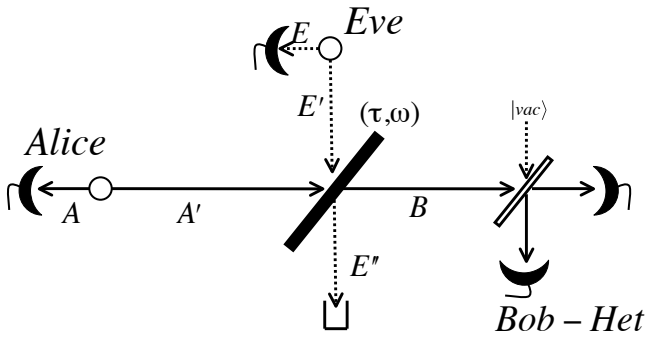

Figure 2.5: This figure shows the implementation of the one-way non-switching CV-QKD protocol, in the EB representation. Differently from the scheme of Fig. 2.1, now Bob performs an heterodyne detection, implemented measuring both outputs of a balanced beam splitter on which the incoming signals are mixed with the vacuum. This means that Bob measures both quadratures $(\hat{q}_\alpha, \hat{p}_\alpha)$. In this way although the heterodyne detection is in general a more challenging measurement scheme to perform, the random number generator for the final switching can be avoided.

where

$$\chi_0 = \frac{\tau + (1-\tau)\omega}{\tau}. \tag{2.35}$$

Setting now $\mu := 1$ and $\omega = 1$, i.e., both Alice and Eve do nothing but injecting the vacuum into the channel, we have the following expression defining the vacuum shot-noise[2]

$$N_0 = \frac{1}{\tau}, \tag{2.36}$$

that for $\tau \to 1$ gives 1. Now we subtract the shot-noise of Eq. (2.36) from Eq. (2.35) and obtain the neat effect of the presence of Eve on the line, i.e., the excess noise

$$N = \frac{\tau - 1 + (1-\tau)\omega}{\tau}. \tag{2.37}$$

We see that Eq. (2.37) depends entirely on the presence of Eve on the line via the channel parameters. For example if $\omega = 1$ then we have $N = 0$. The security thresholds as function of transmissivity τ and excess noise N are represented in figure 2.7(a).

2.7 The non-switching protocol

In this scheme, introduced in Ref. [29], Alice send coherent states to Bob who performs heterodyne detections on the incoming signals. The main advance of the scheme is technological, in fact Bob can avoid the switching of measurement basis, and can so increases the key-rate. To analyze this protocol we note that the final heterodyne detection, described in Fig. 2.6, introduces an extra-noise term with

[2]Note that the divergence we have for $\tau \to 0$ is of no interest, because in that case it is clear that the signal at the receiver would be zero.

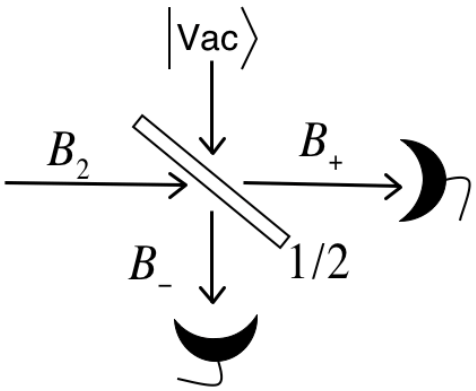

Figure 2.6: The figure shows the nonswitching scheme where the final homodyne detection is replaced by a heterodyne measurement. Bob's mode is B is mixed with the vacuum on a balanced beam splitter and both outputs are measured by conjugate homodyne detectors.

respect the switching protocol. This noise comes from the processing of the vacuum by the final balanced beam splitter. The analysis of the security of protocol is basically the same of the switching protocol, with the only change given by Bob's measurement. This modifies the expression of Alice-Bob mutual information I_{AB} and, when we study the reverse reconciliation, also the conditional state.One can compute the correct formula of Alice-Bob mutual information considering that the heterodyne detection is composed by two homodyne detection. So using the result of Eq. (2.23) and including the vacuum extra noise one has that Alice-Bob mutual information is given by the following formula

$$I_{AB} = \frac{1}{2}\log_2 \frac{V_B + 1}{V_{B|\alpha} + 1} + \frac{1}{2}\log_2 \frac{V_B + 1}{V_{B|\alpha} + 1}, \tag{2.38}$$

where we basically have the sum of the the two signals recorded at the detectors. From the block describing Bob's mode in the CM of Eq. (2.22), we obtain V_B and $V_{B|\alpha}$ and, taking the limit of large μ, we easily obtain the formula

$$I_{AB} = \log_2 \frac{\tau\mu}{1 + \tau + (1 - \tau)\omega}. \tag{2.39}$$

2.7.1 Direct Reconciliation

Now starting from the CM of Eq. (2.22), the simplest thing to do is to consider Bob's covariance matrix, that is given by the block of matrix of Eq. (2.22) describing

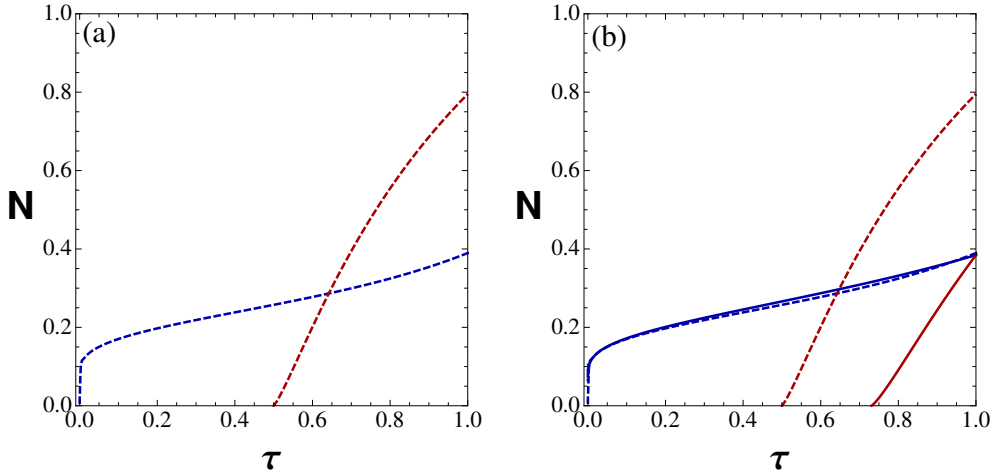

Figure 2.7: Figure (a) shows the security rates $R = I(A:B) - \chi_E$ for the one-way protocol for CV-QKD with homodyne detection. The plots give the security thresholds for both DR and RR.You can see as for $T < 1/2$ the protocol is no more secure in DR, while it continues to allow the distillation of a usable secrete key also for small transmissivity. (b) the security rates for the no-switching protocol (thick lines) compared with the performances in DR and RR (thin lines) for the standard one-way protocol.

Bob's mode and perform, by hand, the conditioning setting the modulation $\mu = 1$ in both quadratures (final heterodyne detection) of each mode. One has

$$\mathbf{V}_{AB}^{Het,\blacktriangleright} = \begin{pmatrix} [\tau + (1-\tau)\omega] & 0 \\ 0 & [\tau + (1-\tau)\omega] \end{pmatrix}.$$

It is very simple to compute the symplectic spectrum of this matrix and obtain the conditional von Neumann entropy, that is given by

$$S_{AB|\beta} = h\left[(1-\tau)\omega + \tau\right],$$

that used with Eq. (2.39) and (2.27) gives the key-rate,

$$R^{\blacktriangleright}(\tau,\omega) = \log_2 \frac{2\tau}{e(1-\tau)[1+(1-\tau)\omega+\tau]} + h\left[(1-\tau)\omega+\tau\right] - h(\omega). \tag{2.40}$$

2.7.2 Reverse Reconciliation

The computation of the key-rate in reverse reconciliation is performed by rewriting the total CM of Eq. (2.22) in the canonical form of Eq. (2.31) to which we can apply the following formula [33, 34, 11]

$$\mathbf{V}_C = \mathbf{A} - \mathbf{C}(\mathbf{B}+\mathbf{I})^{-1}\mathbf{C}^T, \tag{2.41}$$

obtaining the conditional CM

$$\mathbf{V}_{BA|B}^{Het,\blacktriangleleft} = \begin{pmatrix} \frac{\tau+\mu+w\mu-\tau w\mu}{1+w-\tau w+\tau\mu} & 0 \\ 0 & \frac{\tau+\mu+w\mu-\tau w\mu}{1+w-\tau w+\tau\mu} \end{pmatrix},$$

that provides the following asymptotic conditional von Neumann entropy

$$S^{\blacktriangleleft,Het}_{AB|\beta} = h\left[\frac{(1-\tau)\omega+1}{\tau}\right].$$

Putting together this result with those of Eq. (2.39) and Eq. (2.27) one obtains the following analytical formula for the key-rate

$$R^{\blacktriangleleft}(T,\omega) = \log_2 \frac{2\tau}{e(1-\tau)[1+(1-\tau)\omega+\tau]} + h\left[\frac{(1-\tau)\omega+1}{\tau}\right] - h(\omega). \tag{2.42}$$

The security thresholds ($R = 0$) for the non-switching protocol are represented in Fig. 2.1(b), as function of the channel's parameters, excess noise N and attenuation τ). The thresholds are also compared with the performances of the switching protocol, in both direct and reverse reconciliation.

2.7.3 Observation

The performances of the switching and the non-switching protocols are compared Fig. 2.7(b). We can note how the type of reconciliation implemented (direct or reverse reconciliation) affects the security performances of the protocols. In RR, the non-switching does a little better, than the switching protocol, not only in terms if key-rate but also in terms of security thresholds. This happens because in this configuration Eve's task is harder than in the switching protocol, having to guess the results of Bob's measurements, i.e., the results on the measurements on both quadratures. This situation is reversed in DR because in the non-switching protocol Eve can take advantage of the reconciliation protocol. In fact her detectors can count more effective clicks than those of Bob and this is reflected on the security threshold in DR, that for the non-switching protocol is lower than that of the switching protocol.

It is possible that in realistic in-field implementation the actual communication protocol used during the reconciliation procedure could not conform to either the RR or the DR. In some cases a method specific analysis could then be required.

Chapter 3

Two-way quantum cryptography

The two way protocol (see Fig. 3.1) is a communication strategy in which Alice and Bob make a double use of the quantum channel. This type a scheme has been first introduced for discrete variables [35, 37] and recently [36] in CV-QKD. In this protocol Bob send a reference quantum state $|\beta\rangle$ with modulation variance μ_B. Alice performs the encoding applying a random displacement $D(\alpha)$ on the top of the reference state, obtaining the state $|\gamma\rangle = |\beta + \alpha\rangle$ and sending the resulting state backward through the communication channel. Bob measures the state $|\gamma\rangle$ and extract Alice's encoding, by subtracting the amplitude β from the amplitude of the measured state $|\gamma\rangle$. This operation is simple to perform because it consists in classical post-processing of the type $\gamma - \tau\beta$, where τ account for the double processing by a beam splitter on each use of the channel. The eavesdropper has to attack both communication steps (the forward from Bob to Alice and backward) in order to acquire knowledge of both the reference amplitude β and the encoding α. This puts the eavesdropper in an unfavorable position, because her attack results being more noisy than in a standard single use of the quantum channel.

In addition to this we will show, in Part II, that a crucial aspect of the protocol is that it activates additional degrees of freedom available only to the parties. In fact the possibility of randomly switching between the ON (where the full double communication channels is exploited), and the OFF configuration, where the circuit is interrupted and the scheme will reduce to a double use of the one-way communication, allows to choose which data to keep and which data to discarded during the sifting of the key. This choice depends on the detection of Eve on the line, estimated after the tomography of the quantum channel. In this way the parties can minimize Eve's accessible information per use of the protocol.

3.1 Conditioning in the two-way protocols in ON and DR

As we did for the one-way protocol, we can introduce a simple set of rules to apply in order to obtain the conditional variances and the conditional covariance matrices, also for the two-way protocol. With this method we directly act on the analytical expressions of the quantities to conditioning, and we can avoid to apply the Gaussian formulas for the conditional measurement. This approach is particularly useful when we use the protocol in direct reconciliation. Let us consider the two-way com-

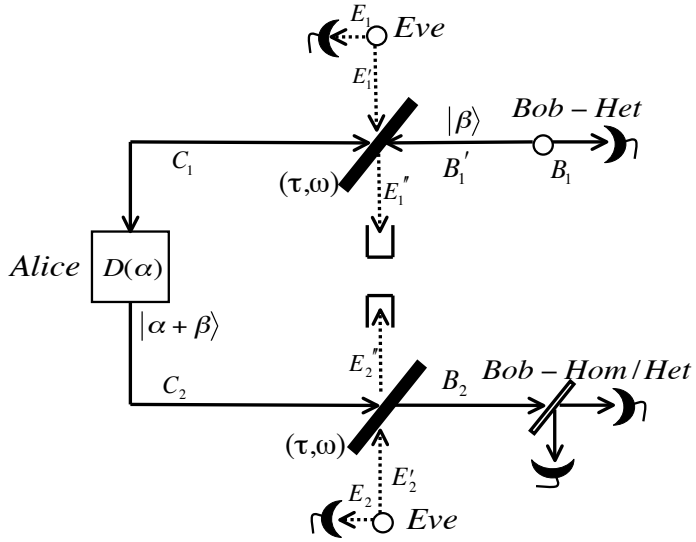

Figure 3.1: The figure shows the two-way protocol for CV-QKD, in the EB representation. Bob prepares the *reference* coherent state $|\beta\rangle$, and send it to Alice. Who applies the displacement $D(\alpha)|\beta\rangle = |\alpha + \beta\rangle$. She then sends back this state to bob who performs a measurement (Hom or Het). Knowing the reference state β, Bob can recover the information encoded in α. In the middle Eve attack both the forward and backward lines by means of two entangling cloners (T, W).

munication scheme without noise (Eve), given in Fig 3.2. The modulation of Bob's reference state has total modulation $\mu_B = \mu$, comprehensive of a classical contribution and a measure-dependent quantum contribution. Alice applies to this state an additional[1] (classical) modulation[2] $\bar{\mu}_{ON}$, representing her encoding and finally obtaining a thermal state with total modulation,

$$\mu_B + \bar{\mu}_{ON}.$$

We can distinguish the two cases where coherent state or squeezed states are used. Let discuss both situations

3.1.1 Coherent State protocol

In this case the conditioning is performed by setting

$$\bar{\mu}_{ON} = 0,$$

Assuming the same Gaussian modulation for both the reference and the encoding state, $\bar{\mu}_{ON} = \mu_B = \mu$, this means that in the formulas we will always have $\mu = 1$.

[1] This is also why the two-way scheme works for CV and not for DV. When the modulation $\mu \to \infty$ the difference between the total modulation and the reference state cannot be easily identified.

[2] $\bar{\mu}_{ON}$ should be different from μ_B. It should be equal to $\mu + 1$

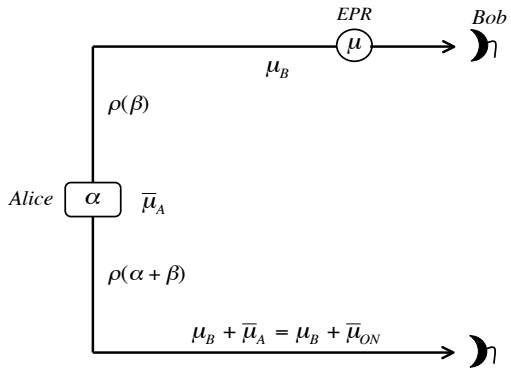

Figure 3.2: The figure shows the two-way scheme without noise. Bob prepares a thermal state and send it to Alice. After Alice'a action the final state is a new thermal state with modulation $\mu_B + \bar{\mu}_A$.

3.1.2 Squeezed State protocol

In this case the conditioning can be performed assuming

$$\bar{\mu}^q_{ON} = 1/\mu \overset{\mu\to\infty}{\to} 0,$$
$$\bar{\mu}^p_{ON} = \mu,$$

We note here that the squeezed state conditioning can be applied to all those cases of the two-way protocols where homodyne measurement is exploited, both in the preparation and/or in the decoding. More precisely we can use this approach to simplify the calculations of protocols like Hom^2, where both Bob and Alice use homodyne detection and for the asymmetric cases $Hom - Het$ (Bob uses squeezed states and Alice modulate coherent state, as well as in protocol $Het - Hom$.

3.2 Two-way protocol with coherent state and heterodyne detection

Eve performs a symmetric[3] attack on both the forward and backward communication channel. This is implemented by two identical entangling cloners of transmissivity τ and thermal noise ω. We describes the dynamics in the entanglement based representation. The processing of the channel is here illustrated step-by-step. One has (see Fig. 3.1)

$$C_1 = \sqrt{\tau}B'_1 + \sqrt{1-\tau}E'_1,$$
$$C_2 = C_1 + \alpha = \alpha + \sqrt{\tau}B'_1 + \sqrt{1-\tau}E'_1,$$

from here we get the expression of output mode B_2

$$B_2 = \tau B'_1 + \sqrt{\tau(1-\tau)}E'_1 + \sqrt{\tau}\alpha + \sqrt{1-\tau}E'_2.$$

[3]The assumption of a symmetric attack is not a problem. It is reasonable to assume that being the channel the same used twice in basically symmetric fashion the optimal attack will be a symmetric one.

In the same way we can calculate the output modes E_1'' and E_2''

$$E_1'' = \sqrt{\tau}E_1' - \sqrt{1-\tau}B_1', \tag{3.1}$$

$$E_2'' = \sqrt{\tau}E_2' - \sqrt{T(1-\tau)}B_1' - (1-\tau)E_1' - \sqrt{1-\tau}\alpha. \tag{3.2}$$

We the compute the covariance matrix describing Bob's mode B_1 and B_2, obtaining

$$\mathbf{V}_{B_1B_2} = \begin{pmatrix} \mu_B\mathbf{I} & \tau\sqrt{\omega^2-1}\mathbf{Z} \\ \tau\sqrt{\omega^2-1}\mathbf{Z} & [\tau^2\mu_B + \tau\mu_A + (1-\tau^2)\omega]\mathbf{I} \end{pmatrix}, \tag{3.3}$$

where μ_B, μ_A describe Bob and Alice's Gaussian modulation, respectively. From Eq. (3.1,3.2) we compute Eve's CM given by the following mathematical expression

$$\mathbf{V}_{E_1E_1''E_2E_2''} = \begin{pmatrix} \omega\mathbf{I} & \Phi\mathbf{Z} & & \sigma\mathbf{Z} \\ \Phi\mathbf{Z} & \Theta\mathbf{I} & & \kappa\mathbf{I} \\ & & \omega\mathbf{I} & \Phi\mathbf{Z} \\ \sigma\mathbf{Z} & \kappa\mathbf{I} & \Phi\mathbf{Z} & \Lambda\mathbf{I} \end{pmatrix} \tag{3.4}$$

where we have defined the coefficients as follows

$$\begin{aligned} \Theta &:= [\tau^2\mu_B + \tau\mu_A + (1-\tau^2)\omega], \\ \Lambda &:= [\tau\omega + \tau(1-\tau)\mu_B + (1-\tau)^2\omega + (1-\tau)\mu_A], \\ \kappa &:= [(1-\tau)\sqrt{\tau}\mu_B - \sqrt{\tau(1-\tau)}\omega], \\ \Phi &:= \sqrt{\tau(\omega^2-1)}\mathbf{Z}, \\ \sigma &:= (\tau-1)\sqrt{\omega^2-1}. \end{aligned}$$

From Eq. (3.3), from the general roles on the conditioning given in Sec. 3.1, and from the definition of the mutual information given in Eq. (2.38) for the non-switching protocol we have the following formula for Alice-Bob mutual information

$$I_{AB} = \log_2 \frac{\tau\mu}{1+\tau^2+(1-\tau^2)\omega}.$$

From Eve's CM, it is possible to calculate the symplectic spectrum for the relevant cases, heterodyne detection and DR and RR. We focus on the reverse reconciliation, with heterodyne decoding, and we find

$$\begin{aligned} \nu_E &\to \{h_1\mu, h_2\mu, \omega, \omega\} \\ \nu_{E,C}^{\blacktriangleleft} &\to \{n_1, n_2, n_3, (1-\tau^2)\mu\}, \end{aligned}$$

where $h_1h_2 = (1-T)^2$ and the three $n_{1,2,3}$ coefficients can be grouped to define the following μ-independent expression,

$$n_1n_2n_3 = \frac{[1+\tau^3+(1-\tau)(1+\tau^2)\omega]\omega}{\tau(1+\tau)},$$

where μ is the classical Gaussian modulation. Finally finding the expression of the key-rate,

$$R_{Het^2}^{\blacktriangleleft} = \log_2 \frac{2\tau(1+\tau)}{e(1-\tau)[1+\tau^2+(1-\tau^2)\omega]} + \sum_{k=1}^{3} g(n_k) - 2g(\omega).$$

Figure 3.3 compares the security threshold of the one-way and the two-way, as a function of transmissivity and excess noise τ and N. To spotlight the advantages offered by two-way communication in term of tolerable noise we show the comparison with the one-way non-switching protocol. This advantage is still present in the regime of high absorption ($\tau \ll 1$).

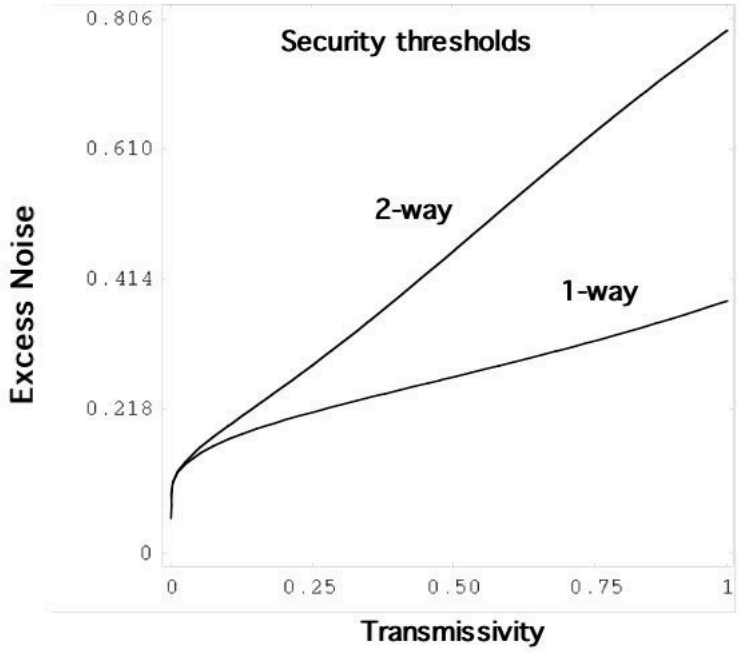

Figure 3.3: This figure shows a comparison between the one-way versus the two-way, non-switching protocol [36]. The security threshold of the two-way is the curve above, while the bottom curve describes the performances of the one-way scheme. Both plots refer to RR. Two-way communication improves the tolerance to noise. Eve is forced to attack both lines to extract only one useful information, Alice's encoding α, increasing her noise on the line. On the other hand the parties are not affected because,Bob knows his reference state $|\beta\rangle$, that is discarded at the end of the protocol. See text for more details.

Part II

Novel results on point-to-point protocols

Introduction

In this part we describe the original results obtained in studying quantum cryptographic protocols in the point-to-point scenario. We performed the security analysis of one-way protocols assuming arbitrary coherent attacks, proposing a novel reduction strategy that allows to shrink the general coherent attack to a two-mode coherent attack. We explicitly show that for Gaussian protocols, in case of independent use of the channel, the implementation of coherent attacks is, for the eavesdropper, always strictly less effective than the use of collective ones. In particular we show that, in order to achieve security, the parties need to apply the symmetric random permutation, prescribed by the quantum de Finetti theorem, only half the total use of the channel. This, in the asymptotic limit, means not only a reduction in the necessary classical processing of the data, but pose also the question if the reduced need for a de Finetti symmetrization can be extended to a $n-$coherent attack. Here we solved the problem analytically for two-mode coherent attack, and provide an interpretation of the results that make us conjecture that the same should be true also in case of $n-$mode coherent attacks, ultimately questioning the need for the de Finetti theorem to asses the security of the Gaussian point-to-point quantum cryptography.

We then studied the two-way communication scheme under general two-mode coherent attacks. In this case we found that coherent attack beating the collective ones are possible. This is the first evidence of a coherent attack outperforming the security thresholds of collective attacks, in point-to-point protocol. To close this loophole in the security of two-way communication we illustrate how combining the previous result on the security of one-way protocols combined with the active use of the ON/OFF switching, one can prove that two-way communication are even immune to coherent attack.

We conclude this part studying the two-way protocol with thermal states. We found that the exploitation of trusted thermal noise improves the performances of continuous variable quantum cryptography in reverse reconciliation. This allowed us to explore the possibility of sharing a cryptographic key at different electromagnetic frequencies, form the infrared to the microwave range. This analysis has been done considering collective attacks that, in light of the previous discussions on the security of two-way schemes, represent the optimal. The higher tolerance to noise manifested by the thermal two-way communication in reverse reconciliation, permits to improve considerably the distances over which is possible to share a secret key in the infrared regime, although remaining in the range of short-distance quantum cryptography.

Chapter 4

One-way protocols against two-mode coherent attack

4.1 Introduction

The finding that the parties can reduce the complexity of the eavesdropping of quantum cryptography, reducing general coherent attacks to collective ones [19], has been a crucial result in this field. This attack reduction is performed applying random symmetric permutation to the classical data at the input and at the output of the quantum protocol. The validity of this procedure is based on a result, known as the quantum de Finetti theorem.

Here we would like to answer the following question: *can one avoid or reduce the use of the quantum de Finetti theorem and still grant the general security of CV-QKD*? Motivated by this question we noted that the use of a coherent attack introduces correlation over different (uncorrelated) uses of the channel. This procedure should actually reduce Eve's degrees of freedom in estimating independent signal variables. If this is correct one should be able to prove that the use of coherent attack is strictly less effective, for the eavesdropper, than to implement a collective attack. Following this idea, we have studied the security of one-way Gaussian quantum cryptography, realizing a systematic investigation of the security of protocols against two-mode coherent attacks. We solved analytically this problem individuating a general post-processing strategy, proving that our initial guess is indeed true for two-mode attacks.

The basic idea is to assume that starting from a general coherent attack, the parties pack the n different uses of the one-way communication into two-mode blocks composed by two arbitrary input. Then they perform a symmetric random permutation over the label identifying these blocks. Thanks to this trick the general security analysis reduces to analytically treatable two-mode coherent attacks.Note that this methodology can always be implemented without harming the overall security of the scheme. As said we solved this problem analytically for Gaussian protocols, establishing closed formulas for the key-rates in all possible configurations of one-way quantum cryptography.

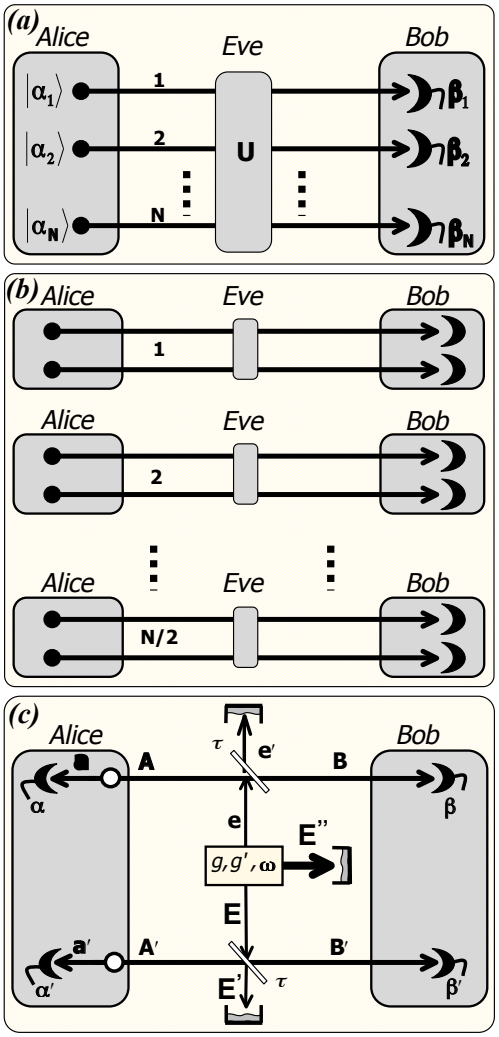

Figure 4.1: Fig.4.1(a): Alice modulates coherent states $|\alpha_k\rangle$ that are sent through the quantum channel (Eve). Bob measurements provide the classical variables β'_k for $k = 1, ..., N$. Eve's general eavesdropping is based on a global unitary operation, U, applied on the N instances of the one-way communication. Fig. 4.1(b): the residual two-mode attack after the reduction to the two-mode block. Fig. 4.1(c): the realistic scenario we have studied: the two-mode attack is simulated by two beam splitters of transmissivity τ. Eve injects two ancillary modes (e and E) whose quantum state is described by thermal noise ω and correlation matrix $\mathbf{G}$ (see main text for further details).

4.2 Protocol

Let us consider the communication scheme illustrated in Fig. 4.1(a). Alice sends to Bob coherent states $|\alpha_k\rangle$, where the amplitudes α_k are modulated by a bivariate Gaussian distribution of variance μ.

The communication channel is under Eve's control and the detections of states $|\alpha_k\rangle$ provide Bob with outcomes β_k. After N uses of the channel, the parties share two highly correlated random sequences of symbols given by the sets $\{\alpha_k\}$ and $\{\beta_k\}$ for $k = 1, ..., n$. We focus on the Reverse Reconciliation (RR) scheme, so that the key is made up from Alice's guess on Bob's variables $\{\beta_k\}$.

The decoding specifies further the protocol: if Bob applies homodynes detections, randomly switching between measurements on quadrature $\hat{q}_k$ and $\hat{p}_k$, we have the *switching* protocol [12]. While if Bob measures both quadratures, applying heterodyne detections, the protocol is named *no-switching* [29]. We discuss here this later case, remanding to the Appendix B.5 for the others.

In a general attack Eve applies a global unitary operation U that process, coherently, a set of ancillary modes together with the N modes exchanged by the parties. The output ancillas are stored in a quantum memory, which is coherently detected after the data reconciliation of the parties. At the end of this step, Alice-Bob-Eve total system is described by a quantum state of the following form

$$\rho = U(\rho_1 \otimes ... \otimes \rho_N)U^\dagger \tag{4.1}$$

where each state ρ_k, with $k = 1, ..., n$, describes the total joint state per use of the channel. This problem can be rewritten in an equivalent (much simpler) representation exploiting the quantum de Finetti theorem [20], that allows to get rid of the cross-correlations between different uses of the channel in the limit of $n \to \infty$. In particular, we here note that if the parties arrange the signals into two-mode blocks, that we call c_j with $j = 1, ..., n/2$ (see Fig. 4.1(b)), made of two arbitrary input and output. Then they apply the symmetric random permutation over the blocks c_j, so that the quantum state given in Eq. (4.1) can now be rewritten as follows

$$\rho \simeq \rho_{c_1} \otimes ... \otimes \rho_{c_M},$$

where $M = n/2$. The resulting post-de Finetti total quantum state, ρ, is now a tensor product of two-mode states ρ_{c_j}, describing the $j-$esime block, with arbitrary correlations enclosed within each block. This general reduction scheme reduces the security analysis to consider just a two-mode block. A further simplification comes from the extremality of Gaussian attacks for Gaussian protocols [11]. This property, usually proved in the context of a channel with no memory [32, 31], can easily be generalized to our two-mode case as we illustrate in the next section (see Appendix for further details).

These assumptions allow to reduce the cryptanalysis considering a single Gaussian block c_j. We solve this problem analytically, considering the most practical case where the attack is realized by means of entangling cloners, i.e., beam splitters on which Eve mixes her ancillary states with the quantum signals of the parties.

4.3 Cryptoanalysis

4.3.1 Source of coherent states

The entanglement based representation of the protocol is described in Fig. 4.1(c). As usual we assume Alice starting form an EPR source of entangled photons whose

zero mean, Gaussian quantum state is described by the usual EPR covariance matrix

$$\mathbf{V}_{EPR} = \begin{pmatrix} \mu\mathbf{I} & \sqrt{\mu^2-1}\mathbf{Z} \\ \sqrt{\mu^2-1}\mathbf{Z} & \mu\mathbf{I} \end{pmatrix},$$

were $\mu = \varphi + 1$ gives the total modulation with contribution from the classical Gaussian modulation φ on the top of the vacuum shot-noise. The matrices $\mathbf{I}$ =diag$(1,1)$, and $\mathbf{Z}$ =diag$(1,-1)$. The quantum state at the input ports of a two-mode block c_j, is then given by a zero-mean, Gaussian quantum state that we can write as the product state

$$\hat{\rho}_{aAa'A'} = \hat{\rho}_{aA} \otimes \hat{\rho}_{a'A'},$$

that is described by a CM given by $\mathbf{V}_{EPR}^{\otimes^2}$. The coherent states $|\alpha_i\rangle$ and $|\alpha_i'\rangle$, for $i = 1, .., n$, remotely projected on modes A and A', are generated applying heterodyne detections on modes a, a' of the composite state $\hat{\rho}_{aAa'A'}$.

4.3.2 General noisy channel with memory

We study the case of a lossy channel, that gives a very good description of typical communication scenarios (free-space, fibres). As usual we model the quantum channel by an entangling cloner on which Eve sends tiny Gaussian ancillary modes that typically are close to be vacuum modes. For every use of the channel, we should estimate the variances of Eve's ancillary modes at the output of the beam splitter, in order to quantify Eve's stolen information. This is not always practical, especially when cross correlation between different uses of the channel may exist, like in the case in order (two-mode coherent attack). We then dilate the Hilbert space describing the modes belonging to the quantum channel (Eve) into a larger space [39] (a larger environment), where Eve's quantum state $\hat{\rho}_E$ is a pure state. As discussed in previous Chapters, this allows to extract the entropic properties of $\hat{\rho}_E$, studying Alice-Bob quantum state $\hat{\rho}_{aa'BB'}$.

The dynamics over a noisy channel with memory is indeed well described by two correlated entangling cloners, as described in Fig. 4.1(c). Here two identical beam-splitters, with transmissivity τ, process Eve's ancillary modes e and E with modes A and A', respectively. For Gaussian protocols Gaussian attacks have been proved to be optimal so that the Gaussian state describing Eve's initial state, σ_{eE}, is completely determined by the following CM [40]

$$\mathbf{V}_{eE} = \begin{pmatrix} \omega\mathbf{I} & \mathbf{G} \\ \mathbf{G} & \omega\mathbf{I} \end{pmatrix}, \ \mathbf{G} := \begin{pmatrix} g & 0 \\ 0 & g' \end{pmatrix}, \tag{4.2}$$

where $\omega = 2\bar{n}+1$ quantifies the thermal noise injected in the two beam splitters, and $\bar{n}$ gives the mean number of thermal photons. The strength and nature of correlations between the ancillary modes e and E are described by the matrix $\mathbf{G}$. In fact for fixed transmissivity τ and thermal noise ω, affecting each use of the channel, there are additional degrees of freedom that Eve could think to exploit in a two-mode Gaussian attack. These are given by the correlation parameters g and g', which can be represented as a point on a 'correlation plane' (see Fig. 4.2). Each point of this plane describes an attack (with different amount and kind of correlations) to which will correspond a specific key rate. Here we provide a detailed comparison between these attacks, and stressing that this description is general and do not depend on the specific protocol nor communication scenario (point-to-point or end-to-end) here considered, so that the results here illustrated will remain valid also for the following.

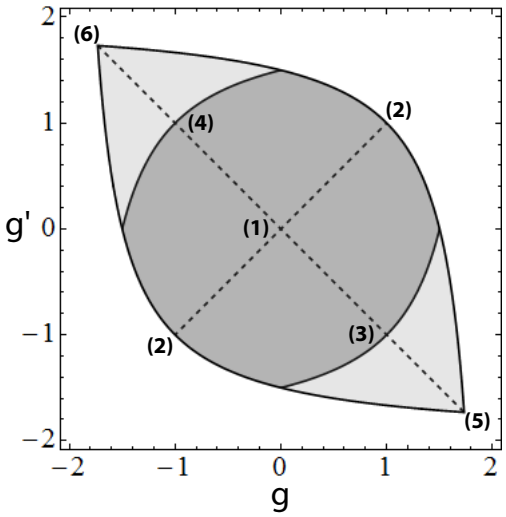

Figure 4.2: Correlation plan for a symmetric Gaussian attack. Given τ and ω (here set to 2), the attack is fully specified by the two correlation parameters (g, g'), whose accessible values are represented by the non-white area. In particular, the inner darker region represents the set of separable attacks ($\sigma_{E_1E_2}$ separable), while the two outer and lighter regions represent entangled attacks ($\sigma_{E_1E_2}$ entangled). The numbered points correspond to the specific attacks described in text.

We assume a symmetric scenario in which the parties made up the blocks c_j grouping modes for which the estimation of the parameters of the channel gives similar results, i.e., transmissivity τ and thermal noise ω are the same on each independent use of the channel. In this case it has been proved [40, 18] that we have a simple characterization of the set of possible Gaussian attacks which are accessible to Eve. Each of these eavesdropping is parameterized by the off-diagonal block in Eq. (4.2), and correspond to points in the correlation plan g, g', such that

$$|g| < \omega, \ |g'| < \omega, \tag{4.3}$$

$$\omega \left|g + g'\right| \leq \omega^2 + gg' - 1. \tag{4.4}$$

Among all these accessible attacks, those satisfying the further condition

$$\omega^2 - gg' - 1 \geq \omega|g - g'| \tag{4.5}$$

are separable attacks ($\sigma_{E_1E_2}$ separable) [40], while those violating Eq. (4.5) are entangled attacks, i.e., Eve's ancillary two-mode quantum state, $\sigma_{E_1E_2}$, is entangled. See Fig. 4.2 for a numerical representation for a fixed value of $\omega = 2$.

We can identify the following three classes of attacks:

- *Collective attack.* This is the simplest attack, represented by point (1) in Fig. 4.2, i.e., the origin of the plane ($g = g' = 0$). This corresponds to using two identical and independent entangling cloners with transmissivity τ and thermal noise ω. In fact, we have

  $$\sigma_{E_1E_2} = \sigma_{E_1} \otimes \sigma_{E_2},$$

  where σ_{E_k} $(k = 1, 2)$ is a thermal state with variance ω, whose purification $\Phi_{E_k e_k}$ is an EPR state in the hands of Eve.

- *Separable attacks.* Within the separable attacks we can identify points (2), (3), and (4) in Fig. 4.2. These are characterized by the condition $|g| = |g'| = \omega - 1$ and represent the separable attacks with the highest correlations. In particular, points (2) correspond to the cases $g = g' = \omega - 1$ or $g = g' = 1 - \omega$, point (3) corresponds to $g = -g' = \omega - 1$, and point (4) to $g = -g' = 1 - \omega$.

- *EPR attacks.* Finally, points (5) and (6) in Fig. 4.2 are the most entangled attacks, where Eve's ancillas E_1 and E_2 are described by an EPR state. Point (5) is the 'positive EPR attack' with $g = -g' = \sqrt{\omega^2 - 1}$, while (6) is the 'negative EPR attack' with $g = -g' = -\sqrt{\omega^2 - 1}$.

  Their values are bounded by the constraints

$$|g| < \omega, \ |g'| < \omega, \text{ and } \omega \left|g + g'\right| \leq \omega^2 + gg' - 1, \tag{4.6}$$

  imposed to satisfy the uncertainty principle, and the bona fide conditions for CM $\mathbf{V}_{eE}$ [40, 17]. One can note that one recovers the collective attacks scenario imposing $g = g' = 0$.

The key-rate quantifying the performances of a QKD protocol is given by the key-rate

$$R = \eta I_{AB} - I_E,$$

with in the present case the mutual information I_{AB} accounting for the correlation between variables $\{\alpha, \beta\}$ and $\{\alpha', \beta'\}$. The parameter η consider the non-ideal efficiency of the reconciliation protocol. For simplicity, in the protocol studied here, we will set to 1 this parameter. Assuming Eve owns a quantum memory, she can achieve the Holevo bound

$$\chi \geq I_E,$$

and working in the entanglement based representation we have

$$\chi = S_{AB} - S_{AB|\beta\beta'},$$

so that the final quantity we will evaluate is the key rate

$$R = I_{AB} - \chi. \tag{4.7}$$

4.3.3 Computation of the mutual information

The parties make a double use of the channel, per single use of the block c_j, so that the total Alice-Bob mutual information is given by the sum

$$I_{AB} = I + I', \tag{4.8}$$

with $I := I(\alpha, \beta)$ is the contribution from the first use of the channel, and $I' := I(\alpha', \beta')$ from the second.

For the no-switching protocol [29] each contribution to the mutual information, I' and I, is given (in bits) by the signal-to-noise ratio

$$I^{(\prime)} = \log_2 \frac{V_{Bob} + 1}{V_{Bob|\alpha(\alpha')} + 1}, \tag{4.9}$$

where variance $V_{Bob} = \tau\mu + (1 - \tau)\omega$, describes the modulation of thermal states arriving at Bob's side (the signal), while $V_{Bob|\alpha} = V_{Bob|\alpha'} = \tau + (1 - \tau)\omega$ quantify

the noise signals after the heterodyne measurements realized by Alice. Using these relations in Eq. (4.8) and (4.9), and taking the asymptotic limit $\mu \gg 1$, one easily obtain the expression of the mutual information,

$$I_{AB} = 2\log_2 \frac{\tau\mu}{1+\tau+(1-\tau)\omega}, \tag{4.10}$$

4.3.4 Computation of the Holevo bound

We now describe the general steps to obtain the Holevo bound χ, the details can be found in Appendix B. After the processing of the quantum channel on the initial state, we obtain the total CM $\mathbf{V}_{tot}$, given by Eq. (6.10) of Appendix B. This describes Alice-Bob joint quantum state $\hat{\rho}_{aa'BB'}$, whose symplectic spectrum is used to obtains Eve's total von Neumann entropy S_{AB} [11]. Taking the limit of large μ, and after basic algebra we found the following symplectic eigenvalues,

$$\begin{aligned}\nu_+ &= \sqrt{(\omega+g)(\omega+g')},\\ \nu_- &= \sqrt{(\omega-g)(\omega-g')},\\ \{\nu_1,\nu_2\} &= \{(1-\tau)\mu,(1-\tau)\mu\}.\end{aligned}$$

This spectrum and the following expansion of the entropic function $h(x)$ for $x \to \infty$

$$\lim_{x\to\infty} h(x) = \log_2 \frac{e}{2}x + O\left(x^{-1}\right), \tag{4.11}$$

allow to easily compute the total von Neumann entropy, that is indeed given by

$$S_E = h(\nu_+) + h(\nu_-) + 2\log_2 \frac{e}{2}(1-\tau)\mu.$$

The computation of the CM describing the processed quantum state $\hat{\rho}_{aa'BB'}$ is pretty simple and can be found in Appendix B (see Eq. (6.10)). We obtain the following matrix

$$\mathbf{V}_{tot} = \begin{pmatrix} (\mu+1)\mathbf{I} & & \Phi\mathbf{Z} & \\ & (\mu+1)\mathbf{I} & & \Phi\mathbf{Z} \\ \Phi\mathbf{Z} & & \Lambda\mathbf{I} & (1-\tau)\mathbf{G} \\ & \Phi\mathbf{Z} & (1-\tau)\mathbf{G} & \Lambda\mathbf{I} \end{pmatrix},$$

where we defined

$$\begin{aligned}\Lambda &= \tau(\mu+1)+(1-\tau)\omega,\\ \Phi &= \sqrt{\tau[(\mu+1)^2-1]}.\end{aligned}$$

Then, applying a partial Gaussian measurement on Bob's modes, we obtain the conditional CM describing the quantum state $\rho_{aa'|\beta\beta'}$, that is given by the expression

$$\mathbf{V}_C = \frac{1}{(\Lambda+1)^2 - g^2(1-\tau)^2} \begin{pmatrix} k & & \tilde{k} & \\ & k' & & \tilde{k}' \\ \tilde{k} & & k & \\ & \tilde{k}' & & k' \end{pmatrix} \tag{4.12}$$

where

$$k := (\mu+1)[g^2(1-\tau)^2 + (\Lambda+1)\tilde{\Lambda}] + (\Lambda+1)\tau, \tag{4.13}$$

$$\tilde{k} := -g(1-\tau)\tau\mu(\mu+2), \tag{4.14}$$

$$\tilde{\Lambda} := \Lambda - \tau, \tag{4.15}$$

with $k' = k(g \to g')$ and $\tilde{k}' = \tilde{k}(g \to g')$. The conditional spectrum is

$$\{\bar{\nu}_+, \bar{\nu}_-\} = \left\{ \frac{\sqrt{\lambda_+ \lambda'_+}}{\tau}, \frac{\sqrt{\lambda_- \lambda'_-}}{\tau} \right\}, \tag{4.16}$$

where $\lambda_+^{(\prime)} = 1 + (1-\tau)(\omega + g^{(\prime)})$ and $\lambda_-^{(\prime)} = 1 + (1-\tau)(\omega - g^{(\prime)})$. From Eq. (4.16) in the general expression of the von Neumann entropy, we obtain the following conditional entropy

$$S_{E|\beta\beta'} = h(\bar{\nu}_+) + h(\bar{\nu}_-), \tag{4.17}$$

Finally from Eq. (6.11) and (4.17) we compute the Holevo bound

$$\chi = 2\log_2 \frac{e}{2}(1-\tau)\mu + h(\nu_+) + h(\nu_-) - h(\bar{\nu}_+) - h(\bar{\nu}_-). \tag{4.18}$$

Key-rate - The secret-key rate is straightforwardly obtained using Eq. (4.18) and Eq. (4.10) in Eq.(4.7). After some algebra do not report here, we arrive at the following general expression for the no-switching protocol, under two-mode coherent attacks

$$\begin{aligned} R = 2\log_2 \frac{2}{e} \frac{\tau}{(1-\tau)[1+\tau+(1-\tau)\omega]} + \\ h(\bar{\nu}_+) + h(\bar{\nu}_-) - h(\nu_+) - h(\nu_-). \end{aligned} \tag{4.19}$$

It is easy to see that one recovers the known key-rate, under standard collective attacks, when $g = g' = 0$.

In order to prove that coherent attacks are strictly less effective than the collective ones, we studied the properties of this key rate proving the following general bound

$$R(\tau, \omega, g, g') > R(\tau, \omega), \quad \forall g, g' \neq 0. \tag{4.20}$$

The details of the calculations to obtain the general key-rate and the proof of Eq. (4.20) can be found in Appendix B. After determining the critical points of rate R, solving the equation $\nabla R = 0$ one finds (we solved this equation numerically fixing τ and ω) that only the origin, P_0, of the $g, g\prime$ plane is a critical point. To determine the nature of P_0, we compute the second order derivatives, and build the Hessian matrix H and we studied its positive definiteness. One can check that by studying the sign of $\det H$ and of the principal minors of the Hessian matrix, both evaluated in P_0, one finds that the only critical point, P_0, is also an absolute minimum point for the rate of Eq. (4.19) on the domain bounded by Eq. (4.6).

The expression of $\det H$, evaluated in P_0, is given in Eq. (B.21) of Appendix B where we show its positivity, together with the positivity of the second order derivatives given in Eq. (B.23). Finally we checked that the two-mode attacks at the boundary defined by $|g| < \omega$, $|g'| < \omega$, and $\omega\,|g + g'| = \omega^2 + gg' - 1$, gives a key rate always strictly larger than under collective attacks. This proves that the origin P_0 is a minimum for R and, consequently, any memory injected by the eavesdropper has the effect of increases the key rate. In Fig. 4.3 we plotted the behavior of the generalized key-rate of Eq. (4.19) under general attack for fixed values of the transmissivity τ and thermal noise ω, and varying the correlation between the two ancillary states. One can see that the red spot, that describes collective attack, is an absolute minimum for the general key-rate. The blue surface and the blue spots

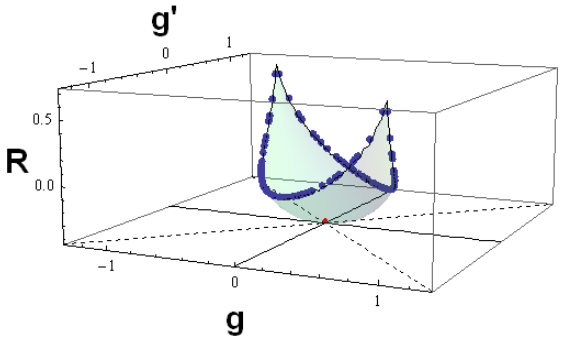

Figure 4.3: This figure shows the optimality of collective attacks for one-way communication. We computed the key-rate given by Eq. (B.19), for values of g, g' verifying the condition $\omega|g+g'| = \omega^2 + gg' - 1$, (blue points) and we compared it with the rate for collective attacks $g = g' = 0$ (Red point). We fixed the thermal noise $\omega = 1.3$ while $\tau = 0.4$ in shot-noise unit (SNU). We see that for this values of thermal noise and transmissivity the collective attacks provide a negative key-rate, this is positive for the coherent attacks at the edge of the region of physical attacks.

describe the two-mode coherent attacks for values of g and g', respectively, inside and at the boundary of the region bounded by of Eq. (4.3) and (4.4).

This analysis has been repeated for all the implementation of the one-way communication finding always the same behavior. We then have that Eq. (4.20) holds independently from the specific implementation of the one-way protocol, including the case direct as well as reverse reconciliation. It proves indeed that coherent attacks are always strictly detrimental for Eve.

4.4 Discussion

This improved security under coherent attacks, can be understood observing that the reduction to two-mode coherent attacks leaves the eavesdropper with less degrees of freedom to estimate the variables β and β'. For instance, if Eve would perform collective attacks she would have two more ancillary states in addition to e' and E' to optimize the final measurement of her quantum memory. This means a total of four ancillary modes over which perform an optimal measurement. On the other hand realizing a coherent attack, she actually helps the parties because they are now authorized to reply to the attack by means of the illustrated strategy. This forces Eve to estimate β, β' from the measurement of just e', E'. For the protocol in RR here considered, this means that Eve's accessible information χ fulfills the following inequality

$$\chi(\beta, \beta') < \chi(\beta) + \chi(\beta'), \tag{4.21}$$

while prior to our result it was only possible to say that a weaker inequality hold This block-reduction strategy can be seen also as a reactivation of the security of one-way CV quantum cryptography, activated a posteriori, in case a coherent attack is detected by the parties during the channel's tomography.

4.5 Conclusions

As one would expect, this analysis recovers the optimality of Gaussian collective attacks where Eve's ancillas share no correlations. But in addition to this we can now affirm that any correlation (memory), introduced by Eve to realize coherent attacks, can always be converted (*a posteriori*) into an advantage for the parties whose secret-key rate increases under coherent attacks. In other words we have showed that, in the context of point-to-point Gaussian quantum cryptography, coherent and collective attacks are not equivalent, but the first are always strictly less fruitful for Eve. Therefore no benefit can exist for Eve in implementing coherent attacks, as long as the parties do not prepare the key exploiting some kind of correlation as described for instance in [17, 18] (Part III), or in the next Chapter in the context of two-way communication.

An interesting side-consequence of this result is that for many use of the channel, $n \to \infty$, the parties can safely implement CVQKD reducing the total number of calls to the de Finetti symmetrization. In the case studied, the parties can apply the de Finetti symmetrization half the total runs of the protocol, reducing in this way the classical processing of the data in the hands of the parties. This finding lead us also to conjecture that the same should be true for the general case of arbitrary $n-$mode attacks. The need for less classical post-processing, could be a further simplification offered by CV systems in the quest for effective and cheap communication schemes, suitable for real-world implementation. We also stress on the fact that our strategy is general, in the sense that it can always be implemented without breaching the standard security assumptions supposing the inviolability of the parties' private spaces, typical of point-to-point quantum cryptography.

In conclusion this analysis shines a new light on the general problem of the effectiveness of coherent attacks, here specifically for independent uses of the quantum channel. This may have interesting consequences on how the de Finetti symmetrization is exploited in realistic, in-field, implementations of Gaussian quantum cryptographic protocols, and the work done could be a good starting point for further investigation to prove the general validity of our conjecture, in which case we think heavy numerical analysis will be in order.

Chapter 5

General security of one-way communication over canonical channels

5.1 Introduction

We discuss the performance of one-way quantum cryptography considering general Gaussian channels, i.e., assuming the canonical Gaussian forms described in Refs. [38, 39]. We adopt this general description to perform a systematic study one-way CV-QKD protocols extending the security analysis to any physically achievable collective attack. Despite the most typical scenario, in a realistic implementation of QKD, is to consider the quantum channel as a lossy environment, this represents only one of the possibilities available to an eavesdropper. We provide here a detailed description of the most relevant cases, focusing on the most practical protocols and attacks, and remanding to Appendix D for further discussion and details on the calculations performed and the less interesting channels.

5.2 Gaussian canonical forms

Unitary transformations $\hat{U} = \exp(i\hat{H}t)$, where the Hamiltonian operator $\hat{H}$ is bilinear in the bosonic field's quadratures $\hat{q}$ and $\hat{p}$, preserve the *Gaussianity* of the processed quantum state [11]. This happens because such a unitary evolution is also bilinear in the field operators of bosonic systems, and can be mapped to canonical linear transformations,$(\mathbf{S}, \mathbf{d})$, in the phase space. This linear maps act on the generalized quadrature vector $\hat{\mathbf{x}} = (q_1, p_1, ..., q_n, p_n)$ as follows

$$(\mathbf{S}, \mathbf{d}) : \hat{\mathbf{x}} \to \mathbf{S}\hat{\mathbf{x}} + \mathbf{d}, \tag{5.1}$$

where $\mathbf{d}$ describes the displacement of the first moment $\bar{\mathbf{x}} := \langle \hat{\mathbf{x}} \rangle$, while matrix $\mathbf{S}$ is a symplectic matrix.

This description can of course be expanded in order to include open quantum system interacting with an environment described by a large, but numerable, number of modes n. In particular, a natural extension of Gaussian unitaries are Gaussian bosonic channels, i.e., a map that act on an $n-$mode quantum state $\hat{\rho}^{\otimes n}$ as follows

$$\mathcal{G}^n : \mathcal{D}(\mathcal{H}^{\otimes n}) \to \mathcal{D}(\mathcal{H}^{\otimes n}). \tag{5.2}$$

In case of a single mode Gaussian channel (basically the case we deal with in one-way quantum cryptography) a one-mode bosonic channel has received recently a complete characterization in terms of canonical forms [65]. Let us consider a Gaussian system with covariance matrix (CM) $\mathbf{V}$. We can describe the evolution in the following way

$$\mathbf{V} \to \mathbf{T}^T \mathbf{V} \mathbf{T} + \mathbf{N}, \tag{5.3}$$

$$\bar{\mathbf{x}} \to \mathbf{T}^T \bar{\mathbf{x}} + \mathbf{d}, \tag{5.4}$$

where $\mathbf{T}$ and $\mathbf{N}$ are 2×2 real matrices so that $\mathbf{N}^T = \mathbf{N} > 0$ and $\det \mathbf{N} \geq (\det \mathbf{T} - 1)^2$. Matrix $\mathbf{T}$ describes the changes induced by the channel on the covariance matrix, while $\mathbf{N}$ describe the noise added to the system. We then have that an arbitrary one-mode Gaussian channel $\mathcal{G} = \mathcal{G}[\mathbf{T}, \mathbf{N}, \mathbf{d}]$ can be transformed into a simpler canonical form via unitary transformations of the input and the output of the channel [11], and it can be written as non-unique representation via Gaussian unitaries $\hat{U}_A$ and $\hat{U}_B$ such that

$$\mathcal{G}(\rho_a) = \hat{U}_B \left[\mathcal{C}(\hat{U}_A \rho_a \hat{U}_A) \right] \hat{U}_B. \tag{5.5}$$

The canonical form $\mathcal{C}$ is a map on the characteristic function of the Gaussian state $\hat{\rho}$, defined as follows

$$\mathcal{C} : \chi(\xi) \to \chi(\mathbf{T}_c \xi) \exp\left[-\frac{1}{2} 1 \xi^T \mathbf{N}_c \xi \right], \tag{5.6}$$

with $\xi \in \mathbb{R}^{2n}$ and the matrices $\mathbf{N}_c$ and $\mathbf{T}_c$ diagonal. The symplectic invariants $\det \mathbf{T}$, $\mathrm{rank}(T)$ and $\mathrm{rank}(N)$, six different expressions for the diagonal matrices $\mathbf{N}_c$ and $\mathbf{T}_c$ have been identified in ref [38] each corresponding to a class of canonical forms $\mathcal{C} = \mathcal{C}[\mathbf{T}_c, \mathbf{N}_c]$: A_1, A_2, B_1, B_2, C and D, that are identified, in general by means of three symplectic invariants: the generalized transmissivity $\tau := \det \mathbf{T} \in \{0, 1,], 0, 1[\}$the rank of the Gaussian channel

$$r := \frac{\mathrm{rk}(\mathbf{T}) \mathrm{rk}(\mathbf{N})}{2}, \tag{5.7}$$

and the *temperature* of the channel

$$\bar{n} := \begin{cases} \frac{1}{2} \left(\frac{\sqrt{\det \mathbf{N}}}{|1-\tau|} - 1 \right), & \text{for } \tau \neq 1 \\ \sqrt{\det \mathbf{N}}, & \text{for } \tau = 1. \end{cases} \tag{5.8}$$

(see ref. [11] and [38] for a detailed discussion about the forms of these canonical forms).

5.3 General canonical form of a collective Gaussian attack

We consider now the typical cryptographic scenario where the environment is assumed to be controlled by an eavesdropper. Eve's freedom in choosing the attack is limited in space and time as well as in energy. As a consequence of that, we can consider a maximal environment which is made by a large (but numerable) set of ancilla modes $e, e', e_1, e_2, ... := e, e', \mathbf{e}$ that interact with finite energy. Then, we can extend the Stinespring dilation (see Fig. 5.1) $\{\mathbf{L}(\tau, r), |\omega\rangle\}$ of a canonical form $\mathcal{C}[\tau, r, \bar{n}]$, described in terms of a symplectic operation $\mathbf{L}$ processing Alice-Bob signal and Eve's

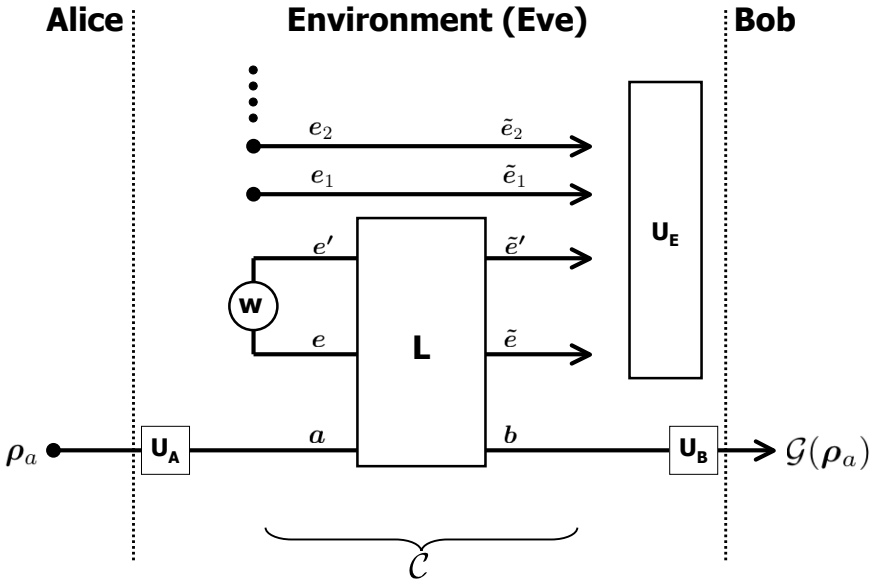

Figure 5.1: General Stinespring dilation of a canonical form. This figure describes the most general collective channel for single mode Gaussian channel.

two-mode squeezed state, $|\omega\rangle$, into the maximal dilation $\{\mathbf{L}(\tau,r)\oplus I_{\mathbf{e}}, |\omega\rangle\otimes|0\rangle_{\mathbf{e}}\}$. In this way we can provide a general description of a Gaussian channel $G[\tau,r,\bar{n},\hat{U}_A,\hat{U}_B]$ that is also unique, up to local unitary operation $\hat{U}_A,\hat{U}_B,\hat{U}_E$.

The set of elements defining the single mode attack is then given by $\{\mathbf{L}(\tau,r),|\omega\rangle,\hat{U}_A,\hat{U}_B,\hat{U}_E\}$. If we now assume that Eve has also a quantum memory, she can perform a coherent measurement of the stored ancillas, and the most general collective attack is described by the set $\{\mathbf{L}(\tau,r),|\omega\rangle,\hat{U}_A,\hat{U}_B,\hat{U}_E,\mathcal{M}^{coh}\}$.

This description can be further simplified observing that we quantify the security of a QKD protocol by computing a bound, given by the Holevo function χ, that is unitarily invariant, i.e., we can set the $\hat{U}_E \coloneqq \mathbf{I}$. The set of elements defining the general collective attack will indeed reduces to $\{\mathbf{L}(\tau,r),|\omega\rangle,\hat{U}_A,\hat{U}_B\}$ representing the case of canonical attacks, described in Fig. 5.2 and considered in this chapter, when both $\hat{U}_A \coloneqq \mathbf{I}$ and $\hat{U}_B \coloneqq \mathbf{I}$. A review about the canonical forms and the possible implementation of the attack have been summarized in ref. [11], where one can find the expression of the symplectic transformation $\mathbf{L}$ for the most relevant cases A_1, A_2, B_1, and $C(lossy)$ describing the standard case of a channel with transmissivity $0<\tau<1$, $C(amp)$ for which $\tau>1$, and D for which $\tau<0$.

5.4 Security analysis of the *non-switching* protocol

Let us consider the one-way protocol represented in Fig. 5.3. In this chapter, following the classification given in [11], we will consider the most interesting channels, described by the canonical forms $\mathcal{C}(amp)$, $\mathcal{D}$, $\mathcal{A}_2$, $\mathcal{B}_1$. Alice measure the local mode A projecting the remote mode A' on a coherent or squeezed state, depending on the measurement applied on A. The remote mode cross the quantum channel, that describes the eavesdropping. Eve make Alice remote mode A' interact with her ancillas, described by mode E' and keep E and E'' for the later optimal measure-

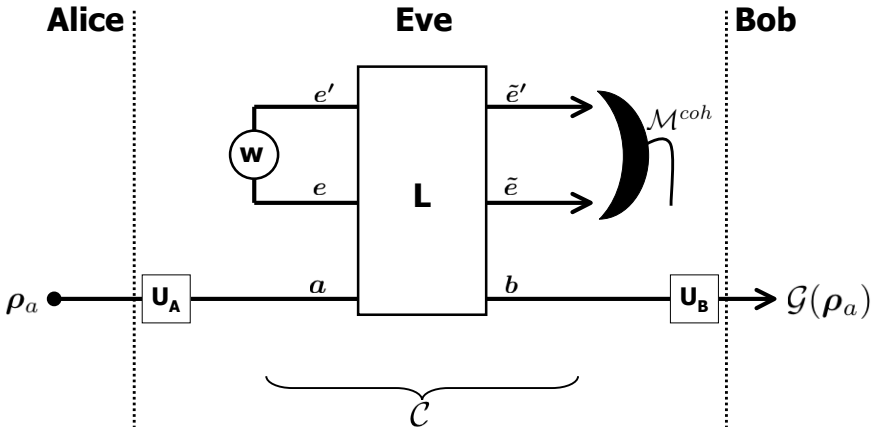

Figure 5.2: This figure represents the optimal collective attacks for single mode Gaussian channel. Mode a represent the transmitted signals.

ment as discussed in previous section. The processed remote mode B is measured by Bob, who can apply a homodyne or an heterodyne detection, specifying the protocol (switching, or non-switching). In the following section we discuss the security of this scheme assume some of the previous canonical forms. In Appendix D we complete this analysis considering the canonical forms and the protocols not discussed in this chapter.

5.4.1 Canonical form $\mathcal{C}(amp)$

This class is formally defined as $\mathcal{C}(\tau, r, \bar{n}) := \mathcal{C}(\tau > 1, 2, \bar{n})$, and it describes a quantum channel amplifying the incoming signals. Our analysis starts from the non-switching protocol. The scheme could be represented in a fashion very similar to that of Fig. 2.5 where the beam splitter, that in the typical lossy channel simulates the attenuation of the communication line, is now replaced by an amplifying device (see Fig. 5.3), whose action is described by the appropriate symplectic matrix $\mathbf{L}$, that correspond to the unitary evolution $\mathbf{U}$.The sender, Alice, prepares coherent states on mode A' that crosses the quantum channel. Mode A' is coupled with mode E', from Eve's EPR state. The total input Gaussian system $\rho_A \otimes \rho_E$, is indeed described by the following initial covariance matrix

$$\mathbf{V}_{IN} = \mathbf{V}_{AA'} \oplus \mathbf{V}_{E'E},$$

where

$$\mathbf{V}_{AA'} = \begin{pmatrix} \mu\mathbf{I} & \sqrt{\mu^2-1}\mathbf{Z} \\ \sqrt{\mu^2-1}\mathbf{Z} & \mu\mathbf{I} \end{pmatrix},$$
$$\mathbf{V}_{E'E} = \begin{pmatrix} \omega\mathbf{I} & \sqrt{\omega^2-1}\mathbf{Z} \\ \sqrt{\omega^2-1}\mathbf{Z} & \omega\mathbf{I} \end{pmatrix},$$

with as usual μ the Gaussian thermal modulation of the signals, and ω the thermal noise of the attack. The symplectic form $\mathbf{L}$ is characterized by the transmissivity

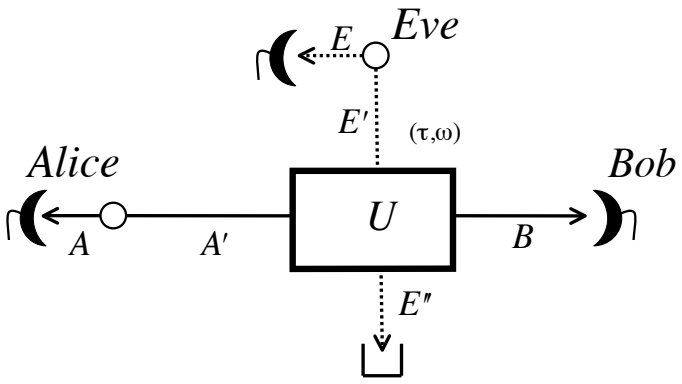

Figure 5.3: This figure represents the general one-way protocol, in the entanglement based representation. Alice modulates coherent state (or squeezed state) by measuring one modes of her EPR pair, and send the other through the channel that is modelled by some unitary operation $\mathcal{U}$ corresponding to a Gaussian canonical form $\mathbf{L}$, i.e., $\mathcal{C}(loss)$, $\mathcal{C}(amp)$, $\mathcal{D}$, $\mathcal{A}_1$, $\mathcal{A}_2$, $\mathcal{B}_1$, $\mathcal{B}_2$. Bob measures the incoming signals by an heterodyne or homodyne detection.

$\tau > 1$ [11], and is given by the following sympectic matrix

$$\mathbf{L}_{\mathcal{C}(amp)} = \begin{pmatrix} \sqrt{\tau}\mathbf{I} & \sqrt{\tau-1}\mathbf{Z} \\ \sqrt{\tau-1}\mathbf{Z} & \sqrt{\tau}\mathbf{I} \end{pmatrix}. \tag{5.9}$$

We write the total symplectic operation describing the modes' processing of the channel as

$$\mathbf{S} = \mathbf{I} \oplus \mathbf{L}_{\mathcal{C}(amp)} \oplus \mathbf{I}, \tag{5.10}$$

where $\mathbf{I}$ =diag$(1,1)$. Note that this interaction does nothing on local modes A and E, that in fact remain in Alice and Eve's hands. We then apply $\mathbf{S}$ that acts only on the remote modes $A'$and E', and we obtain the following output covariance matrix

$$V_{out} = (\mathbf{I}_2 \oplus \mathbf{L}_{\mathcal{C}(amp)} \oplus \mathbf{I}_2) \otimes \mathbf{V}_{IN} \otimes (\mathbf{I}_2 \oplus \mathbf{L}_{\mathcal{C}(amp)} \oplus \mathbf{I}_2)^T, \tag{5.11}$$

From this matrix one can extract the block describing Alice-Bob total output state, given by the matrix

$$\mathbf{V}_{AB}^{\mathcal{C}(amp)} = \begin{pmatrix} \mu\mathbf{I} & \sqrt{\tau(\mu^2-1)}\mathbf{Z} \\ \sqrt{\tau(\mu^2-1)}\mathbf{Z} & [\tau\mu + (\tau-1)\omega]\mathbf{I} \end{pmatrix}.$$

Now, we compute Alice-Bob's mutual information using Eq. (2.38), and finally obtain the asymptotic mutual information, that is

$$I_{AB}^{\mathcal{C}(amp)} = \log_2 \frac{1+\tau\mu+(\tau-1)\omega}{1+\tau+(\tau-1)\omega} \overset{\mu>>1}{\to} \log_2 \frac{\tau\mu}{1+\tau+(\tau-1)\omega} \tag{5.12}$$

From previous equation one can express Eve's thermal noise ω and in terms of τ and the excess noise N[1] (this expression is the same for all the others protocols

[1]The excess noise can also be seen as additional channel's noise not present at the source.

involving the $\mathcal{C}(amp)$ canonical form). From Eq. (5.12) and following the discussion given in Sec. 2.6.4, one easily finds that

$$\omega = \frac{\tau - 1 + N\tau}{\tau - 1}. \tag{5.13}$$

Note that this expression is the same as that of a standard lossy channel, given in Eq. (2.37), applying the transformation $\tau \to -\tau$.

Direct Reconciliation

We compute the total von Neumann entropy, which is obtained starting form Eve's block of CM $\mathbf{V}_{out}$. This is given by the expression

$$\mathbf{V}_{EE''}^{\mathcal{C}(amp)} = \begin{pmatrix} [\tau\omega+(\tau-1)\mu]\mathbf{I} & \sqrt{\tau(\omega^2-1)}\mathbf{Z} \\ \sqrt{\tau(\omega^2-1)}\mathbf{Z} & \omega\mathbf{I} \end{pmatrix}, \tag{5.14}$$

from which one can compute the total symplectic spectrum

$$\nu_{1,2}^{\mathcal{C}(amp)} = \frac{\Upsilon - \sqrt{\Upsilon^2 + 4(\tau + (\tau-1)\omega\mu)}}{2} \overset{\mu>>1}{\to} \omega, \tag{5.15}$$

$$\nu_{2}^{\mathcal{C}(amp)} = \frac{\Upsilon + \sqrt{\Upsilon^2 + 4(\tau + (\tau-1)\omega\mu)}}{2} \overset{\mu>>1}{\to} (\tau-1)\mu, \tag{5.16}$$

where $\Upsilon = (\tau-1)(\omega+\mu)$. These eigenvalues are used to compute the total Eve's von Neumann entropy

$$S_E = h(\nu_1^{\mathcal{C}(amp)}) + h(\nu_2^{\mathcal{C}(amp)}) \overset{\mu>>1}{\to} h(\omega) + \log_2 \frac{e}{2}(\tau-1)\mu, \tag{5.17}$$

with the function $h(x)$ defined as

$$h(x) \coloneqq \frac{x+1}{2}\log_2\frac{x+1}{2} - \frac{x-1}{2}\log_2\frac{x-1}{2}. \tag{5.18}$$

From Eq. (5.14) we can obtain the conditional CM collapsing the modulation $\mu = 1$ in both quadratures, and obtaining the matrix

$$\mathbf{V}_{E|\alpha}^{\mathcal{C}(amp)} = \begin{pmatrix} [\tau\omega+(\tau-1)]\mathbf{I} & \sqrt{\tau(\omega^2-1)}\mathbf{Z} \\ \sqrt{\tau(\omega^2-1)}\mathbf{Z} & \omega\mathbf{I} \end{pmatrix}, \tag{5.19}$$

that has the symplectic spectrum

$$\{\overline{\nu}_1^{\mathcal{C}(amp)}, \overline{\nu}_2^{\mathcal{C}(amp)}\} = \{1, \omega - \tau(\omega+1)\}, \tag{5.20}$$

from which one gets the conditional von Neumann entropy

$$S_{E|\alpha} = h(\overline{\nu}_2^{\mathcal{C}(amp)}) = h(|\omega - \tau(\omega+1)|). \tag{5.21}$$

Using Eq. (5.12) with Eq. (5.17) and (5.21) and finding the analytical formula

$$R_{\mathcal{C}(amp)}^{\blacktriangleright}(\mu,\tau,\omega) = \log_2\frac{1+\tau\mu+(\tau-1)\omega}{1+\tau+(\tau-1)\omega} + h(|\omega-\tau(\omega+1)|) - h(\nu_1^{\mathcal{C}(amp)}) + h(\nu_2^{\mathcal{C}(amp)}), \tag{5.22}$$

$$\overset{\mu>>1}{\to} h(|\omega-\tau(\omega+1)|) - h(\omega) + \log_2\frac{2}{e}\frac{\tau}{(\tau-1)[1+\tau+(\tau-1)\omega]}. \tag{5.23}$$

Reverse reconciliation

To compute the key-rate in reverse reconciliation we fully exploit the entanglement based representation and, after rearranging the CM $\mathbf{V}_{out}$ in the form

$$V_{out}\begin{pmatrix} \mathbf{A} & \mathbf{C} \\ \mathbf{C}^T & \mathbf{B} \end{pmatrix}, \tag{5.24}$$

where the $\mathbf{B}$ describes Bob's mode, on which we apply the heterodyne measurement. The resulting matrix provides two symplectic eigenvalues that for $\mu >> 1$, are

$$\{\bar{\nu}_1^r, \bar{\nu}_2^r\} \to \left\{1, \frac{1+\omega(\tau-1)}{\tau}\right\}, \tag{5.25}$$

from which we obtain the conditional von Neumann entropy

$$S_{E|\beta} = h(\bar{\nu}_2^r) = h\left(\frac{1+\omega(\tau-1)}{\tau}\right). \tag{5.26}$$

This equation used with Eq.(5.12) and (5.17), gives the following asymptotic key-rate

$$R_{\mathcal{C}}^{\blacktriangleleft}(\mu,\tau,\omega) \overset{\mu>>1}{\to} h\left(\frac{1+\omega(\tau-1)}{\tau}\right) - h(\omega) + \log_2\frac{2}{e}\frac{\tau}{(\tau-1)[1+\tau+(\tau-1)\omega]} \tag{5.27}$$

The security thresholds of the rate of Eq.(5.23) and (5.27) are summarized in Fig (5.4. Here we show the security thresholds of both the lossy channel for $\tau < 1$ and for an $\tau > 1$. One can note that, when compared with the standard lossy channel, the action of $\mathcal{C}(amp)$ makes the RR much less effective than the DR. This is not surprising because in DR is Bob that infers the preparation of Alice's variables. So Eve amplifying the signals actually helps the parties, increasing their mutual information.

5.4.2 Canonical form $\mathcal{D}$

This channel describes the complementary output channel of an amplifier $\mathcal{C}(amp)$. It can then be parameterized by a $\tau < 0$. The steps of the analysis performed in previous section can be repeated for the canonical form $\mathcal{D}(\tau < 0, 2)$, by replacing the symplectic matrix $\mathbf{L}$ [11] with that describing the canonical form $\mathcal{D}$. This is given by the following expression [11]

$$\mathbf{L}_{\mathcal{D}} = \begin{pmatrix} \sqrt{-\tau}\mathbf{Z} & \sqrt{1-\tau}\mathbf{I} \\ -\sqrt{1-\tau}\mathbf{I} & -\sqrt{-\tau}\mathbf{Z} \end{pmatrix}, \tag{5.28}$$

with $\tau < 0$, and the Alice-Bob mutual information given by the formula

$$I_{AB}^{\mathcal{D}} = \log_2\frac{1-\tau\mu+(1-\tau)\omega}{1-\tau+(1-\tau)\omega} \overset{\mu>>1}{\to} \log_2\frac{-\tau\mu}{1-\tau+(1-\tau)\omega}. \tag{5.29}$$

As we did before, we can compute the expression of the excess of noise on the channel obtaining

$$\omega = \frac{1-\tau-N\tau}{1-\tau}, \tag{5.30}$$

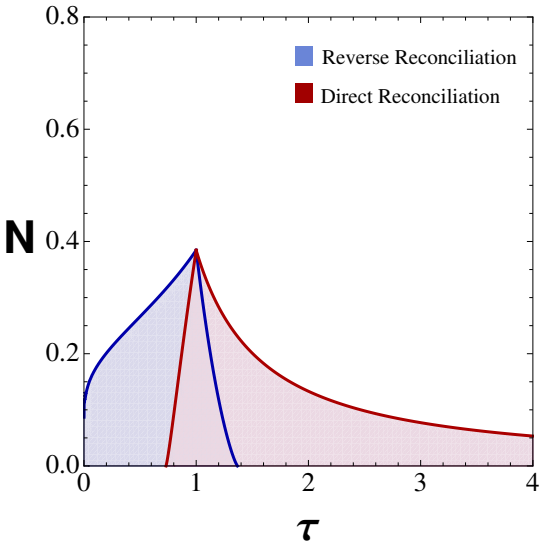

Figure 5.4: This figure shows the asymptotic security thresholds, for the one-way protocol with coherent state, used in the non-switching configuration. It summarizes the security performance of the communication channel in both cases of $C(loss)$ and $C(amp)$. The red lines and parameter region describe the direct reconciliation, while the blue one correspond to the reverse reconciliation. When the parameter $\tau \in [0, 1[$, the figures describes the attenuation channel modeled by a beam-splitter with transmissivity τ. For values of $\tau > 1$ the figure describes the security of the an amplifying channel, where now the parameter τ describes the gain in the signal obtained as a result of the action of the channel. We see that in this case the behavior of DR and RR is inverted with respect the case of attenuation.

and, repeat the same steps illustrated in the previous section to obtain the Holevo bound. We compute the total symplectic spectrum, from Eve's total CM

$$\mathbf{V}_E^{\mathcal{D}} = \begin{pmatrix} [(1-\tau)\mu - \tau\omega]\mathbf{I} & -\sqrt{-\tau}\sqrt{\omega^2-1}\mathbf{I} \\ -\sqrt{-\tau}\sqrt{\omega^2-1}\mathbf{I} & \omega\mathbf{I} \end{pmatrix}, \tag{5.31}$$

obtaining

$$\{\omega, (1-\tau)\mu\},$$

and the total von Neumann entropy

$$S_E^{\mathcal{D}} = h(\omega) + \log_2 \frac{e}{2}(1-\tau)\mu. \tag{5.32}$$

We then can compute the conditional symplectic spectra in DR, starting from Eq. (5.31). We collapse both modulations $\mu \to 1$, for both quadratures, and in the asymptotic limit we can obtain the conditional spectrum

$$\{1, \omega - \tau(\omega+1)\},$$

that gives the conditional von Neumann entropy in DR

$$S_{E|\alpha}^{\mathcal{D}} = h\left[\omega - \tau(\omega+1)\right]. \tag{5.33}$$

For the RR, we can start from Alice-Bob CM

$$\mathbf{V}_{AB|\beta}^{\mathcal{D}} = \begin{pmatrix} \mu\mathbf{I} & \sqrt{-\tau}\sqrt{\mu^2-1}\mathbf{Z} \\ \sqrt{-\tau}\sqrt{\mu^2-1}\mathbf{Z} & [(1-\tau)\omega - \tau\mu]\mathbf{I} \end{pmatrix},$$

and apply the formula for heterodyne detection $\mathbf{V}_{out} = \mathbf{A} - \mathbf{C}(\mathbf{B}+\mathbf{I})^{-1}\mathbf{C}^T$ where

$$\begin{aligned} \mathbf{A} &= \mu\mathbf{I}, \\ \mathbf{B} &= [(1-\tau)\omega - \tau\mu]\mathbf{I}, \\ \mathbf{C} &= \sqrt{-\tau}\sqrt{\mu^2-1}\mathbf{Z}. \end{aligned}$$

We compute the asymptotic limit, and obtain the simple expression for the only conditional eigenvalue

$$\frac{1+(1-\tau)\omega}{\tau},$$

that gives the following conditional von Neumann entropy

$$S_{E|\beta}^{\mathcal{D}} = h\left(\frac{1+(1-\tau)\omega}{\tau}\right). \tag{5.34}$$

From these results and using Eq. (5.29), (5.32) and Eqs.(5.33,5.34) one finally arrives at the expression of the key-rates that in direct reconciliation is given by the formula

$$R_{\mathcal{D}}^{\blacktriangleright}(\tau,\omega) = h\left[-\tau + (1-\tau)\omega\right] - h(\omega) + \log_2 \frac{2}{e}\frac{-\tau}{(1-\tau)[1-\tau+(1-\tau)\omega]}, \tag{5.35}$$

while reverse reconciliation is

$$R_{\mathcal{D}}^{\blacktriangleleft}(\tau,\omega) = h\left[\frac{1+(1-\tau)\omega}{\tau}\right] - h(\omega) + \log_2 \frac{2}{e}\frac{-\tau}{(1-\tau)(1-\tau+(1-\tau)\omega)}. \tag{5.36}$$

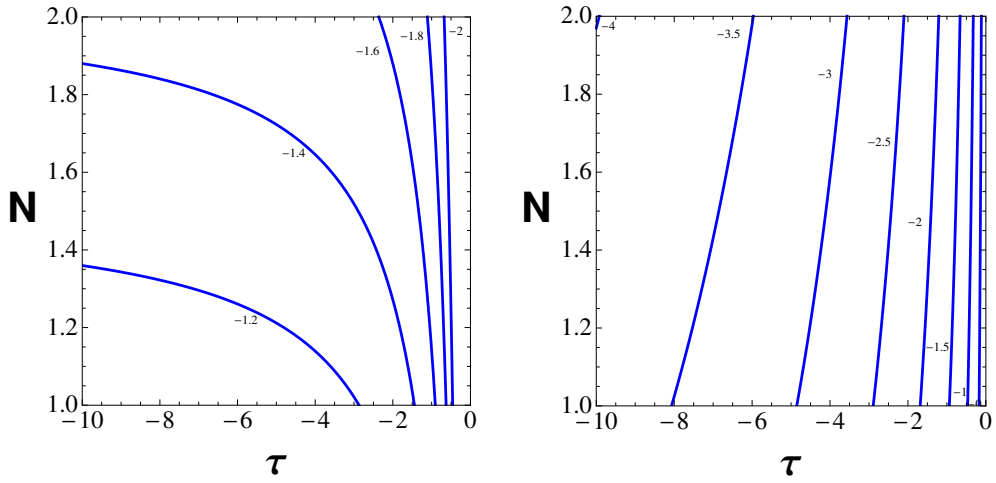

Figure 5.5: The left panel shows the key rate as a function of transmissivity and thermal noise in DR,as given in Eq. (5.35). The right panel shows the key-rate in RR, from Eq. (5.36). In both cases the quantum channel can not provide a positive key-rate, for the range of physically available of the channel's parameters. Therefore the canonical form D, used with the no-switching protocol, is equivalent to a denial-of-service attack.The values of the parameter $\tau < 0$ because the canonical form $\mathcal{D}(amp)$ represents the complementary channel of the amplifier $\mathcal{C}(amp)$.

The security thresholds of this protocol, in direct and reverse reconciliation, is plotted in Fig. 5.5(left panel) for the direct and Fig. 5.5(right panel) for the reverse reconciliation. We have that this canonical form forbid the possibility of secure communication, resulting always $R^{\blacktriangleright}_{\mathcal{D}} < 0$. One indeed concludes that an attack implemented by means of the canonical form $\mathcal{D}$, against a non-switching protocol, is equivalent to a denial-of-service attack. The the security of the non-switching protocol, against attacks implemented with the remaining canonical forms (A_1,A_2,B_1) are discussed in Appendix D.

5.5 Security analysis of the *switching* protocol

The computation to determine the key-rates goes as illustrated in previous sections. Now, in order to perform the conditioning by collapsing the Gaussian modulation μ, we have to apply this procedure only to one quadrature. To compute the conditional CM, applying the formula for partial Gaussian detection [11], we have to consider homodyne detection. Here we present the final analytical expression of the key-rate in direct and reverse reconciliation. Again we focus on the canonical forms $\mathcal{C}(amp)$ and $\mathcal{D}$, and in Fig. 5.7 we summarize and compare the results obtained for both the switching (dashed) and non-switching (continuous) protocols for any value of the the transmissivity parameter τ.

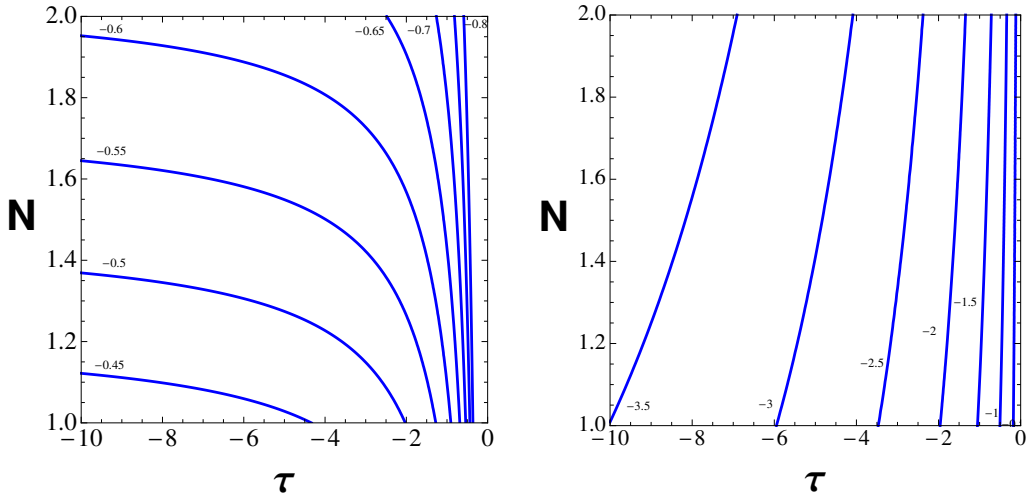

Figure 5.6: We plot the security thresholds of the switching protocol, as function of the channel's parameters, transmissivity τ and thermal noise ω for the class $\mathcal{D}$. As in the non-switching case, we found that for an attack implemented by class $\mathcal{D}$ the key-rate is always negative.

5.5.1 $\mathcal{C}(amp)$ canonical form

In this case the parties use coherent state to encode and homodyne to decode so the mutual information between Alice and Bob is given by the quantity

$$I_{AB}^{\mathcal{C}(amp)} = \frac{1}{2}\log_2 \frac{\tau\mu}{\tau + (\tau-1)\omega}. \tag{5.37}$$

After performing the symplectic analysis of the total and conditional CM, we arrived at the following expressions for the key rates. From the direct reconciliation we found

$$\tilde{R}^{\blacktriangleright}_{\mathcal{C}(amp)}(\tau,\omega) = h\left(\sqrt{\frac{\omega[\tau+(\tau-1)\omega]}{\tau-1+\tau\omega}}\right) - h(\omega) + \log_2 \frac{\tau(\tau-1+\tau\omega)}{(\tau-1)[\tau+(\tau-1)\omega]}, \tag{5.38}$$

and for RR we have

$$\tilde{R}^{\blacktriangleleft}_{\mathcal{C}(amp)}(\tau,\omega) = \frac{1}{2}\log_2 \frac{\omega}{(\tau-1)(\tau+(\tau-1)\omega)} - h(\omega). \tag{5.39}$$

These key-rates are summarized in Fig. 5.7 where we include also the performances under $C(loss)$ attacks and the threshold (continuous lines) computed in previous section for the non-switching protocols. The area below the curves describes the region of channel's parameters where the switching protocol is secure.

The class $\mathcal{D}$, also for the switching protocol does not allow the preparation of a secret key rate,, for any value of $\tau < 0$. We do not provide the calculations, being very similar to the previous case. We limit to represent, in Fig. 5.6, the thresholds as function of τ and the excess noise N. The analytical expressions of the key-rates in DR and RR for class $\mathcal{D}$, where $\tau < 0$, are given in Eq. (5.40) and (5.41).

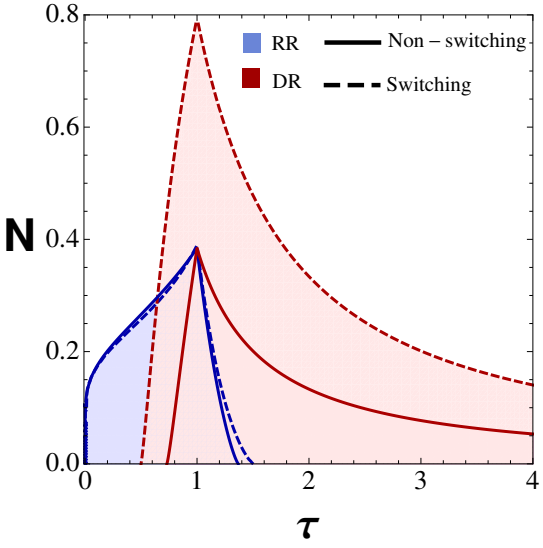

Figure 5.7: We plot the security thresholds as function of the channel's parameters, transmissivity τ and excess noise N. The figure describes the security thresholds and the security region (area below the curves) comparing the performances of the non-switching protocol and the switching protocol. We considered the classes $\mathcal{C}(loss)$ and $\mathcal{C}(amp)$. The class $\mathcal{D}$ for the switching protocol, as well as for the non-switching, results being a denial-of-service channel.

5.5.2 Summary of $\mathcal{C}(loss)$, $\mathcal{C}(amp)$ and $\mathcal{D}$ canonical forms

For the class $\mathcal{C}(amp)$ we found non-trivial results, that show that it is possible to distinguish range of channel's parameters (τ and N) for which it is possible to prepare a secret-key. We summarize the results obtained in previous section writing general expressions for the key-rate of the switching protocol, in the asymptotic limit. With this results we can then consistently write a generalized key-rate for any value of the τ parameter so that $\tau \in [-\infty, \infty]$. In direct reconciliation, we have the following general expression

$$\bar{R}^{\blacktriangleright}_{\mathcal{C}\&\mathcal{D}} = \begin{cases} h\left(\sqrt{\frac{\omega[\tau+(|1-\tau|)\omega]}{|1-\tau|+\tau\omega}}\right) - h(\omega) + \frac{1}{2}\log_2 \frac{\tau(|1-\tau|+\tau\omega)}{|1-\tau|[\tau+(|1-\tau|)\omega]}, & \text{for } \tau > 0 \\ h\left(\sqrt{\frac{\omega[(1+\tau)\omega+\tau]}{1+|\tau|(\omega+1)}}\right) - h(\omega) + \frac{1}{2}\log_2 \frac{|\tau|(1+|\tau|(\omega+1))}{(1+|\tau|)((1+|\tau|)\omega+|\tau|)}, & \text{for } \tau < 0 \end{cases} \tag{5.40}$$

while in reverse reconciliation we have

$$\bar{R}^{\blacktriangleleft}_{\mathcal{C}\&\mathcal{D}} = \begin{cases} -h(\omega) + \frac{1}{2}\log_2 \frac{\omega}{|1-\tau|(\tau+|1-\tau|\omega)}, & \text{for } \tau > 0 \\ -h(\omega) + \frac{1}{2}\log_2 \frac{(1+2|\tau|)^2(1+|\tau|)\omega}{(1+|\tau|)^2[|\tau|+(1+|\tau|)\omega]}, & \text{for } \tau < 0. \end{cases} \tag{5.41}$$

Previous key rate are summarized in the following Fig. 5.7, where we also make a comparison between the switching and non-switching protocol.

5.6 Conclusions

In this chapter we have presented some of the results obtained assessing the general security of one-way protocols, considering non-typical eavesdropping. This study extended the security of CV-protocol to all physically possible canonical forms. We illustrated the security regions for the most interesting classes $\mathcal{C}(\tau > 1, 2, \hat{n})$ and $\mathcal{D}(\tau < 0, 2, \hat{n})$. Both the switching and non-switching protocols, can allow the preparation of a secret-key for the attacks implemented assuming an amplifying communication channel $\mathcal{C}(\tau > 1, 2, \hat{n})$, while the class $\mathcal{D}(\tau < 0, 2, \hat{n})$ does not allow the preparation of the secure key, and the attack is basically a denial-of-service. All others protocols based on squeezed state preparation are discussed in Appendix D, where also others canonical forms, i.e., $\mathcal{A}_2$ and $\mathcal{B}_1$, are discussed. The analysis of these last cases show that it is always trivially possible to prepare a secret key in case of the canonical form $\mathcal{B}_1$, while for the case of canonical form $\mathcal{A}_2$ the quantum channel is always a denial-of-service.

We conclude that the channels described by the canonical forms $\mathcal{C}(loss)$, $\mathcal{C}(amp)$ and $\mathcal{B}_1$ can allow the preparation of a secret key, while the channels described by canonical from like $\mathcal{D}$ and $\mathcal{A}_2$ basically behave always as a denial-of-service channel, not allowing, especially in the asymptotic regime, the preparation of a secret-key.

Chapter 6

Two-way protocol in ON configuration against coherent attacks

6.1 Introduction

The security of the full two-way communication [36] has been studied under the standard assumption of Gaussian collective attacks [32, 31]. In ref. [36] it is proved one can obtain the security also against coherent attack by switching randomly ON and OFF the circuit (ON/OFF switching).

In this Chapter we focus on a more challenging case to study, where Eve's ancillary states are correlated. In this way we obtain the first complete cryptanalysis of a two-way communication protocol against coherent attacks. Our security analysis is based upon the conventional assumption that the parties exchange a large number of signals ($n >> 1$). In this case as we did in Chapter 4, we can reduce the general attack to a simpler two-mode coherent attack where, for each use of the protocol, Eve's ancillas share non-zero two-mode correlations. In addition to this we considered the case of asymptotically large Gaussian modulation of the amplitudes α and β. This allowed us to work with analytical mathematical expressions, and to found the optimal two-mode coherent attack, which is realized when Eve injects symmetric separable correlation [40].

We obtained analytical expressions of all relevant quantities needed to study the performance of the protocol and, thanks to this, we achieved a detailed cryptanalysis in terms of security thresholds. The results for the two-way protocol here studied, are compared with the performances of the one-way version of the no-switching protocol, and show that tempering two-mode communication with two-mode coherent attack can reduce the performances below the one-way security threshold. This represents the first example of a coherent attack overcoming the performances of collective ones, in point-to-point protocols. We discuss why this happens, in the context considered here, and finally we compare our results with others recent studies [17, 18] where two-mode optimal coherent attacks have been identified for end-to-end cryptographic protocols. Our results are important from both the general perspective of the development of the security analysis of continuous variable protocols, and to identify the general challenges to implement secure point-to-point communications. From this perspective our results suggest that the ON/OFF switching of the quantum link operated by Alice, described in Chapter 4, represents a necessary

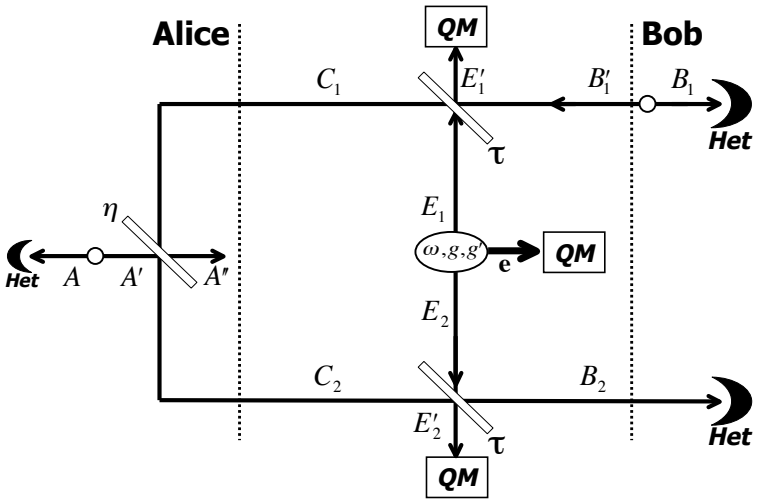

Figure 6.1: The figure describes the two-way quantum communication protocol. Bob prepares reference coherent states $|\beta\rangle$, from a source of entangled beams. One mode is measured (B_1), while the other, B_1' is sent to Alice through an insecure quantum channel. Alice applies a random displacement of the reference state $D(\alpha)$, implemented by a a source of entangled photons and a beam splitter with transmissivity η. Choosing appropriately the transmissivity η, and the classical Gaussian modulation, Alice send back to Bob coherent states of the form $|\alpha+\beta\rangle$. This is heterodyned and classical post-processed by Bob, that in this way recover Alice's encoding by subtracting the known reference amplitudes β from states $|\alpha+\beta\rangle$. The information encoded in the amplitudes α are then used to obtain the raw key.

countermeasure to overcome the problem of realistic coherent attack in two-way point-to-point quantum cryptography.

The structure of this chapter goes as follows: in Sec. 6.2 we introduced the protocol and illustrate the reduction of the general eavesdropping to two-mode coherent attack. In Sec. 6.3 we provide the definition of the key-rate and we show how to compute the Holevo bound and Alice-Bob mutual information, arriving at the analytical expression of the secret-key rate. In Sec. 6.4 we give the security thresholds and the study of the behavior of relevant quantities as function of Eve's injected thermal noise and degree of two-mode correlation. In Sec. 6.5 we discuss the result obtained and Sec. 6.6 is for conclusions.

6.2 Protocol and eavesdropping

We use the entanglement based representation described by Fig. 6.1. We reduce the general coherent eavesdropping to two mode coherent attacks, and we illustrate the steps to compute the total and conditional covariance matrices, from which in the next section we provide the calculated symplectic spectra that are used to compute the Holevo bound.

6.2.1 Entanglement based representation

Let us consider the scheme of Fig. 6.1. Bob modulates coherent states, $|\beta\rangle$, varying the amplitude β accordingly to a bivariate Gaussian distribution with variance μ_B. This states are sent to Alice that encodes the information to share, applying a random displacement $D(\alpha)$ and obtaining the coherent states $|\beta+\alpha\rangle$. These are then sent backward to Bob who post-process subtracting the information on the reference state (β) in his hands.

In a general (coherent) eavesdropping, Eve process all the N uses of the quantum channel applying a global coherent unitary operation that correlates all the modes involved in the different uses of the quantum channel. However, exploiting the quantum de Finetti theorem [20], this general scenario can be reduced to a two-mode coherent attack. The parties can apply a symmetric random permutation of the classical data in their hands, and doing so for $N >> 1$, the cross correlations between distinct uses of the two-way communication can be neglected, while the global coherence of the attack is reduced to a two-mode coherence shared between the forward and backward steps of the quantum communication.

The study of the general case can then be reduced to analyze the security against this residual two-mode coherent attack that, in the most typical case, is implemented by two entangling cloners of transmissivity τ [40], where Eve mixes two ancillary modes E_1 and E_2, (see Fig. 6.1). These two ancillas belong generally to a larger set of modes, $\{E_1,\ E_2, \mathbf{e}\}$, defining the pure initial quantum state owned by the eavesdropper. As described in the previous Chapter 4 sec. 4.3.2, the two-mode Gaussian state $\rho_{E_1E_2}$, is completely described by the following covariance Matrix (CM)

$$\mathbf{V}_{E_1E_2} = \begin{pmatrix} \omega\mathbf{I} & \mathbf{G} \\ \mathbf{G} & \omega\mathbf{I} \end{pmatrix},\ \mathbf{G} := \begin{pmatrix} g & 0 \\ 0 & g' \end{pmatrix}, \tag{6.1}$$

where the parameter ω describes the variance of the thermal noise injected by Eve in the beam splitters, $\mathbf{I} = \mathrm{diag}(1,1)$, $\mathbf{Z} = \mathrm{diag}(1,-1)$, and matrix $\mathbf{G}$ account for the specific two-mode coherence exploited by Eve to eavesdrop. We here recall the classification of the different attacks given Sec. 4.3.2. We can distinguish between three possible extremal cases: *collective attacks* when $g = g; = 0$ corresponding to the standard collective eavesdropping, *separable attacks* defined by the condition $|g| = |g'| = \omega - 1$, representing coherent attacks with separable correlations injected and, finally, *EPR attacks* when $g = -g' = \sqrt{\omega^2-1}$ and $g = -g' = -\sqrt{\omega^2-1}$.

Besides previous description of Eve's quantum state, that purifies the quantum channel, we need to provide the purification of the sources of coherent states (Bob and Alice's devices). To this end let assume that Bob's coherent states originates from two-mode squeezed states (EPR states), whose zero mean Gaussian states is described by the covariance matrix given by the following expression

$$\mathbf{V}_{B_1B_1'} = \begin{pmatrix} \mu_B\mathbf{I} & \sqrt{\mu_B^2-1}\mathbf{Z} \\ \sqrt{\mu_B^2-1}\mathbf{Z} & \mu_B\mathbf{I} \end{pmatrix}. \tag{6.2}$$

The parameter $\mu_B = \mu+1$ accounts for Bob's global (classical plus quantum) Gaussian modulation. The heterodyne measurement performed by Bob on mode B_1, see Fig. 6.1, remotely projects mode B_1' on a coherent state traveling forward (from Bob to Alice) through the quantum channel.

At Alice's station the random displacement $D(\alpha)$ can be implemented by means of a beam splitter of transmissivity η. This mixes mode C_1 with mode A', coming

from Alice's source of the EPR pairs A, A', whose Gaussian quantum state, $\rho_{AA'}$, is described by the following CM

$$\mathbf{V}_{AA'} = \begin{pmatrix} \mu_A \mathbf{I} & \sqrt{\mu_A^2 - 1}\mathbf{Z} \\ \sqrt{\mu_A^2 - 1}\mathbf{Z} & \mu_A \mathbf{I} \end{pmatrix}. \tag{6.3}$$

While Alice's mode A' is sent through the beam splitter η, the other mode A is heterodyne detected, in order to project mode A' on a coherent state $|\gamma\rangle$ that is modulated with variance μ_γ. This quantity defines Alice's total modulation

$$\mu_A = \mu_\gamma + 1, \tag{6.4}$$

and mode C_2, after the processing of Alice's beam splitter, is given by the following coherent state

$$|\sqrt{\eta}\beta + \sqrt{1-\eta}\gamma\rangle. \tag{6.5}$$

Now, in order to obtain a coherent state of the form $|\beta+\alpha\rangle$ from Eq. (6.5), we design Alice's beam splitter to have transmissivity $\eta \to 1$, and we assume that the coherent amplitude $\gamma \to \infty$. In this way the modulation of μ_γ, of coherent state $|\gamma\rangle$, can be defined as

$$\mu_\gamma := \frac{\mu}{1-\eta}, \tag{6.6}$$

and the amplitude γ can be chosen as follows

$$\gamma := \frac{\alpha}{\sqrt{1-\eta}}. \tag{6.7}$$

Designing in the way described the purification of the protocol, we have that when $\eta \to 1$, the coherent state of Eq. (6.5) obtained on mode B_2 traveling backward to Bob, verifies the following relation

$$|\sqrt{\eta}\beta + \sqrt{1-\eta}\gamma\rangle \sim |\beta + \alpha\rangle.$$

6.3 Key-rate, Holevo function and mutual information.

If we use the no-switching protocol in direct reconciliation the parties use the coherent amplitudes α to prepare the secret key. This means that, during the classical procedures of parameter estimation, error correction and privacy amplification, Bob guesses Alice's variables α from the results of his measurements. The security performances are then quantified by the secret-key rate defined as follows

$$R := I_{AB} - \chi_{EA} \tag{6.8}$$

that, assuming a large number of signals exchanged ($n >> 1$), is defined as the difference between Alice-Bob mutual information I_{AB} and the Holevo bound χ_{EA}, that quantifies the information shared between Alice and the eavesdropper.

The advantage of using the entanglement based representation relies on the fact that we do not need to know the details of the coherent operations performed by Eve to globally process her set of modes given by $\{E_1, E_2, \mathbf{e}\}$. Instead, we can compute the function χ_{EA} from the total and conditional quantum state of the Alice-Bob Gaussian system [11]. This means that we can use the following definition of the Holevo bound

$$\chi_{EA} = S_E - S_{E|\alpha}, \tag{6.9}$$

where S_E represents the von Neumann entropy, corresponding to the pure quantum state $\rho_{B_1AA''B_2}$, describing the total Alice-Bob Gaussian system. Here A'' describes the mode processed by Alice's beam splitter, that remain in Alice hands. The quantity $S_{E|\alpha}$, gives the conditional von Neumann entropy that can be computed from the conditional state $\rho_{B_1B_2|\alpha}$, i.e., the quantum state after Bob's and Alice detections on mode B_1 and A.

In next subsection we provide the total and conditional covariance matrices corresponding to $\rho_{B_1AA''B_2}$ and $\rho_{B_1B_2|\alpha}$ and the respective symplectic spectra, that are then used to compute the Holevo bound χ_{EA}.

6.3.1 Total symplectic spectrum

The global Alice-Bob quantum state, $\rho_{B_1AA''B_2}$, is a Gaussian state whose properties are described by the following CM (we used the following modes ordering: $B_1AA''B_2$)

$$V_T = \begin{pmatrix} \mu_B\mathbf{I} & & \phi\mathbf{Z} & \theta\mathbf{Z} \\ & \mu_A\mathbf{I} & \xi\mathbf{Z} & \kappa\mathbf{Z} \\ \phi\mathbf{Z} & \xi\mathbf{Z} & k\mathbf{I} & \delta\mathbf{I} \\ \theta\mathbf{Z} & \kappa\mathbf{Z} & \delta\mathbf{I} & \varepsilon\mathbf{I} \end{pmatrix} + \begin{pmatrix} & & & \\ & & & \\ & & & g_\delta\mathbf{G} \\ & & g_\delta\mathbf{G} & g_\varepsilon\mathbf{G} \end{pmatrix}, \tag{6.10}$$

where we have define

$$\begin{aligned} \phi &:= -\sqrt{\tau(1-\eta)}\sqrt{\mu_B^2-1}, \\ \theta &:= \tau\sqrt{\eta(\mu_B^2-1)}, \\ k &:= \eta\mu_A + (1-\eta)[\tau\mu_B + (1-\tau)\omega], \\ \xi &:= \sqrt{\eta(\mu_A^2-1)}, \\ \kappa &:= \sqrt{\tau(1-\eta)(\mu_A^2-1)}, \\ \varepsilon &:= \tau^2\eta\mu_B + \tau(1-\eta)\mu_A + (\tau\eta+1)(1-\tau)\omega, \\ g_\varepsilon &:= 2(1-\tau)\sqrt{\eta\tau}, \\ \delta &:= \sqrt{\tau\eta(1-\eta)}[\mu_A - \tau\mu_B - (1-\tau)\omega], \\ g_\delta &:= -(1-\tau)\sqrt{(1-\eta)}. \end{aligned}$$

The symplectic spectrum of the CM given in Eq. (6.10), is obtained from the "standard" eigenvalues of matrix

$$\mathbf{M}_T = i\mathbf{\Omega}\mathbf{V}_T.$$

For $\mu >> 1$, we find the following general expressions for the symplectic spectrum

$$\begin{aligned} \nu_1 &= \sqrt{(\omega-g)(\omega-g')}, \\ \nu_2 &= \sqrt{(\omega+g)(\omega+g')}, \\ \nu_3\nu_4 &= (1-T)^2\mu^2, \end{aligned}$$

where we note that the dependency from the correlation parameters, g, g', generalizes the known total symplectic spectrum under collective attack, that in our notation correspond to the case $g = g' = 0$. Using the previous symplectic spectrum with we arrive at the asymptotic total von Neumann entropy, that we can write as follows

$$S_E = h(\nu_1) + h(\nu_2) + \log_2\frac{e^2}{4}(1-T)^2\mu^2. \tag{6.11}$$

6.3.2 Conditional symplectic spectrum and Holevo bound

When the protocol is used in direct reconciliation we note that, in order to obtain the conditional covariance matrix, we do not need to start from the total CM of Eq. (6.10) and apply the appropriate measurements. Instead, the conditional covariance matrix can be obtained straightforwardly considering the CM involving Bob's modes, obtained from Eq. (6.10) tracing Alice's modes. This approach considerably simplifies the problem, and starting from the following matrix

$$\mathbf{V}_{B_1B_2} = \begin{pmatrix} \mu_B\mathbf{I} & \theta\mathbf{Z} \\ \theta\mathbf{Z} & \varepsilon\mathbf{I} + g_\varepsilon\mathbf{G} \end{pmatrix}, \tag{6.12}$$

in which we set $\mu_A \coloneqq 1$ to simulate the conditioning after Alice's measurements, we straightforwardly arrive at the conditional CM given by

$$\mathbf{V}_C = \mathbf{V}_{B_1B_2}(\mu_A \coloneqq 1). \tag{6.13}$$

From here we compute the matrix

$$\mathbf{M}_C = i\mathbf{\Omega}\mathbf{V}_C,$$

where $\mathbf{\Omega} = \bigoplus_{k=1}^{2} \tilde{\omega}_k$, and from here the the eigenvalues of $\mathbf{M}_C$. Again considering the asymptotic limit we obtain the following pair of symplectic eigenvalues

$$\begin{aligned} \bar{\nu}_1 &= \sqrt{\omega + 2g\frac{\sqrt{\tau}}{1+\tau}}\sqrt{\omega + 2g'\frac{\sqrt{\tau}}{1+\tau}}, \\ \bar{\nu}_2 &= (1-\tau^2)\mu, \end{aligned}$$

from which we have the conditional von Neumann entropy that we write in the following expression

$$\begin{aligned} S_{E|\alpha} &= h(\bar{\nu}_1) + h(\bar{\nu}_2), \\ &= h(\bar{\nu}_1) + \log_2\frac{e}{2}(1-\tau^2)\mu. \end{aligned} \tag{6.14}$$

Finally, putting together the results of Eq. (6.11) and Eq. (6.14) in the definition of the Holevo function, Eq. (6.9), we have the analytic expression of the Holevo bound

$$\chi_{EA} = h(\nu_1) + h(\nu_2) - h(\bar{\nu}_1) + \log_2\frac{e}{2}\frac{1-\tau}{1+\tau}\mu. \tag{6.15}$$

6.3.3 Mutual Information

To obtain the secret-key rate we need Alice-Bob mutual information. In the non-switching protocol both quadratures of mode B_2 are measured, and the mutual information I_{AB} is given by the following expression

$$\begin{aligned} I_{AB} &= \frac{1}{2}\log_2\frac{V_B^q+1}{V_{B|\alpha\beta}^q+1} + \frac{1}{2}\log_2\frac{V_B^p+1}{V_{B|\alpha\beta}^p+1}, \\ I_{AB} &= \frac{1}{2}\log_2\frac{(V_B^q+1)(V_B^p+1)}{(V_{B|\alpha\beta}^q+1)(V_{B|\alpha\beta}^p+1)}, \end{aligned} \tag{6.16}$$

where V_B^q, V_B^p are the variances for quadratures $\hat{q}$ and $\hat{p}$ of mode B_2, while $V_{B|\alpha\beta}^q$ and $V_{B|\alpha\beta}^p$ describe the conditional variance after Bob and Alice's measurements. The

latter can be obtained from the diagonal block of the CM given in Eq. (6.12), that describing mode B_2. This is given by the expression

$$\langle B_2^2 \rangle = \varepsilon \mathbf{I} + g_\varepsilon \mathbf{G},$$

from which, taking the limit $\eta \to 1$ and setting $\mu_B := 1$, we obtain

$$V_B^q = \tau^2 + \tau\mu + (1-\tau^2)\omega + 2g(1-\tau)\sqrt{\tau},$$
$$V_B^p = \tau^2 + \tau\mu + (1-\tau^2)\omega + 2g'(1-\tau)\sqrt{\tau}.$$

The conditional variances, $V_{B|\alpha\beta}^q$ and $V_{B|\alpha\beta}^p$, can now be obtained setting $\mu = 0$ in the previous equations, and collapsing the classical Gaussian modulation we simulate the guessing of Bob on Alice's variables α. From Eq. (6.16) taking the limit of large modulation $\mu >> 1$, we get the asymptotic Alice-Bob mutual information

$$I_{AB} = \frac{1}{2}\log_2 \frac{T^2\mu^2}{\sigma\sigma'}, \tag{6.17}$$

where

$$\sigma = V_{B|\alpha\beta}^q + 1 = 1 + \tau^2 + (1-\tau^2)\omega + 2g(1-\tau)\sqrt{\tau},$$
$$\sigma' = V_{B|\alpha\beta}^p + 1 = 1 + \tau^2 + (1-\tau^2)\omega + 2g'(1-\tau)\sqrt{\tau}.$$

6.3.4 Secret-key rate

We have now all the quantities needed to compute the secret-key rate defined in Eq. (6.8). From the expressions for the asymptotic mutual information given in Eq. (6.17), and the Holevo bound of Eq. (6.9), one has the following expression of the key-rate

$$R = \frac{1}{2}\log_2 \frac{\tau^2\mu^2}{\sigma\sigma'} - \log_2 \frac{e}{2}\frac{1-\tau}{1+\tau}\mu - h(\nu_1) - h(\nu_2) + h(\bar{\nu}_1),$$

that can be easily simplified obtaining the following formula

$$R = \log_2 \frac{2\tau(1+\tau)}{e(1-\tau)\sqrt{\sigma\sigma'}} - h(\nu_1) - h(\nu_2) + h(\bar{\nu}_1), \tag{6.18}$$

6.4 Results

The security thresholds that describe the performances of the considered protocol for all possible attacks are plotted in Fig. 6.2. The plots represents the tolerable excess of thermal noise, defined as $N = [\tau - 1 + (1-\tau)\omega]/(1-\tau)$, as a function of the channel transmissivity τ. The tolerable excess of noise N is defined as that portion of the thermal noise, in units of vacuum shot-noise (SNU), injected by Eve into the quantum channel, exceeding the vacuum shot-noise limit. We then express the rate of Eq. (6.18) in terms of transmissivity τ and excess noise N, and we solve the equation

$$R(\tau, N) = 0,$$

that provides a curve $N(\tau)$ establishing the security threshold.

Fig. 6.2 compares the two-way security thresholds (thick lines) with the corresponding no-switching protocol in direct reconciliation, implemented by means of one-way communication, for which the optimal attack is the standard collective one

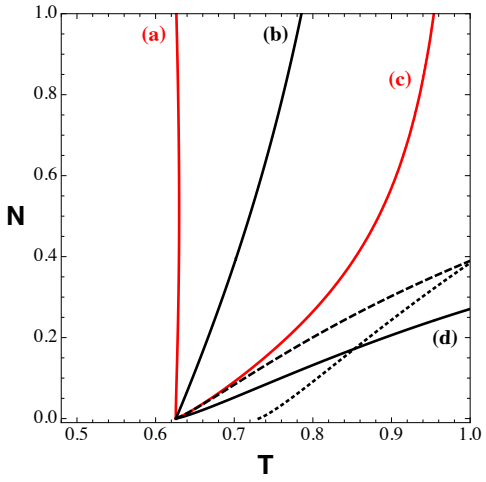

Figure 6.2: We plot the security thresholds for the case of two-way, no-switching protocol, in direct reconciliation, against two-mode coherent attacks. The y-axis is in vacuum shot-noise units (SNU). Curves (a) and (c), describe two-mode attacks for which $g = -g'$. In particular (a) is the threshold obtained when Eve eavesdrops making use of maximally entangled ancillas E_1 and E_2. This case is given by the two equivalent conditions on the correlation parameters $g = \sqrt{\omega^2 - 1} = - g'$ and $g = -\sqrt{\omega^2 - 1} = - g'$. Curve (c) describes the cases $g = \omega - 1 = - g'$ and $g = 1 - \omega = - g'$. The curves (b) and (d) correspond to the thresholds for $g = g'$. In curve (b) we have $g = \omega - 1 = g'$and $g = 1 - \omega = g'$ (d). The dashed line is the threshold for standard collective attacks, $g = g' = 0$. The black dotted line is the security threshold for the corresponding one-way protocol for which only collective attacks can be considered.

(dotted line). In particular the red lines, labeled (a) and (c), describe the thresholds of the two-way protocol obtained when the correlation parameters of the attack fulfill the condition $g = -g'$. In this case curve (a) describes the security threshold for maximally entangled ancillary modes E_1, E_2. This situation is described by two distinct (despite equivalent) setup of the coherent attack, for which $|g| = \sqrt{\omega^2 - 1} = -|g'|$. Curve (c), obtained when $|g| = \omega - 1 = -|g'|$, gives the extremal case of separable and maximally correlated ancillas.The black lines are the security thresholds when Eve exploits correlation of the type $g = g'$. In this group of attacks, modes E_1 and E_2 can only share separable correlation, and for $g = \omega - 1 = g'$ we have curve (b) while for $g = 1 - \omega = g'$ we obtained curve (d).

Finally the dashed line provides the two-way threshold, under standard collective attacks, i.e., when $g = g' = 0$. All these cases have been compared with the security threshold of the one-way, no-switching protocol, in direct reconciliation (dotted line), for which the collective attacks are known to be optimal. We note that for standard collective attack, the two-way no-switching protocol (dashed) always overcome the performances of the one-way (dotted). On the contrary, in case Eve exploit correlated ancillas, she can perform a more profitable eavesdropping challenging the two-way protocol studied. In this case curve (d) is clearly below that security threshold corresponding collective attacks (dashed), and one can note that for $\tau \gtrsim 0.86$ the security of two-way communication can be lower than the one-way performances for which collective attacks are optimal. In particular for the protocol described in this

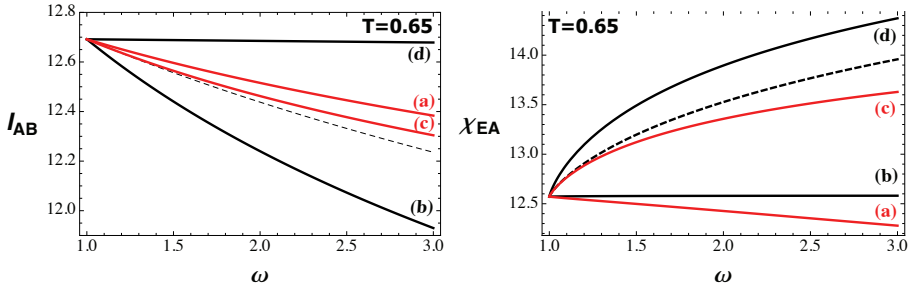

Figure 6.3: This figure shows the behavior of the asymptotic mutual information I_{AB} and of the Holevo function χ_{EA} as a function of Eve's thermal noise ω (SNU). We fixed the Gaussian modulation $\mu = 10^6$, value for which we checked the asymptotic limit is achieved. We then have the transmissivity $T = 0.65$, for which the parties start obtain a positive key-rate (see curves (a) and (b) in Fig. 6.2). The labelling corresponds to that adopted for the thresholds of Fig. 6.2. We have that (a) describes two-mode attacks for which $g = \sqrt{\omega^2 - 1} = - g'$, $g = -\sqrt{\omega^2 - 1} = - g'$ and curve (c) describes the cases $g = \omega - 1 = - g'$ and $g = 1 - \omega = - g'$. The curve (b) corresponds to the case $g = \omega - 1 = g'$and (d) is for $g = 1 - \omega = g'$ represents the optimal attack. The dashed line refers to standard collective attacks, $g = g' = 0$. We see that for the optimal attack (d) while the mutual information decreases increasing ω, the curve corresponding to the Holevo bound, χ_{EA}, increases and with a larger rate than in any other attack, coherent as well as collective. This cause the reduction of the key-rate in case (d).

paper, we found that the two-mode coherent attack,given by curve (d), is optimal. In the next section we deepen the discussion about this result.

6.5 Discussion

The result of Fig. 6.2 shows that differently from the one-way protocol, the use of correlated ancillas are useful for the eavesdropper. To investigate further this behavior we studied the behavior of the quantities defining the key-rate of Eq. (6.18) as function of the thermal noise ω given in vacuum shot noise units (SNU).We fixed the classical Gaussian modulation $\mu = 10^6$ (SNU), for which we have verified that the asymptotic limit is largely fulfilled, and the transmissivity to the value $\tau = 0.65$. In Fig. 6.3, left panel, we plotted the mutual information I_{AB}, given in Eq. 6.17, and in the right panel the Holevo function χ_{EA} given by Eq. (6.15). First, as one would expect, we note that the mutual information (left panel) always decrease for increasing thermal noise. In addition to this we have that while the Holevo bound χ_{EA} (left panel) corresponding to the two-mode attack (d), for which $g = g' = 1 - \omega$, is the largest of the others four extremal cases $(a - c)$, increases its value for increasing ω. This means that Eve can extract more and more information while increasing the thermal noise injected. On the opposite, under the same conditions, the mutual information I_{AB} remains basically constant (just a very small reduction). As a consequences this attack is highly profitable for Eve that is able to increase the gap between her information on Alice variable, at an higher rate than Bob on α. Consequently there is a lower rate for the parties. The dashed line represents the case of two-way protocol in case of collective attacks.

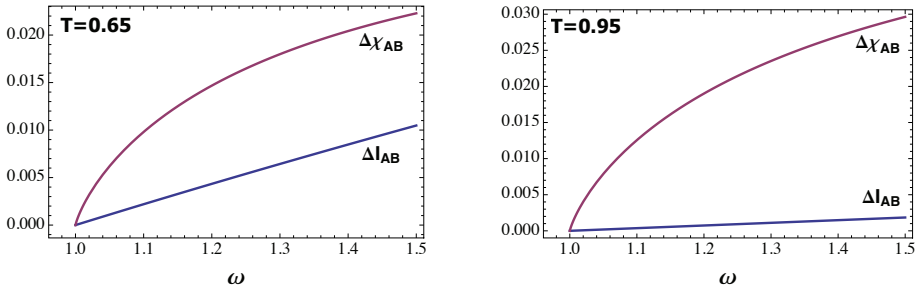

Figure 6.4: This figure analyzes the relative variation of the Holevo bound, $\Delta\chi_{EA} \coloneqq (\chi_{EA} - \chi_c)/\chi_c$, and of the mutual information $\Delta I_{EA} \coloneqq (I_{EA} - I_c)/I_c$, as functions of the thermal noise for fixed values of the transmissivity $T = 0.65$ (left) and $T = 0.95$ (right). The function χ_c describes the Holevo function for $g = g' = 0$, when we have collective attacks.

The cause, for this behavior of the security of two-way protocol under coherent attack, is that the double use of the quantum channel gives the eavesdropper the opportunity to take advantage of her final detection of the ancillas. In fact, she can perform an optimized coherent measurement on the ancillary states stored in her quantum memory, whereas the parties are limited to local measurement to determine the tolerable thermal noise. In general this advantage is no longer valid in case of one-way communication protocol, for this reason the two-way threshold against the optimal attack can even be worse than the one-way (dotted curve in Fig. 6.2).

To illustrate further this behavior we have plotted in Fig. 6.4 the variation of Alice-Bob mutual information, $\Delta I_{AB} = (I_{AB} - I_{c)}/I_c$ and of the Holevo function $\Delta\chi_{EA} = (\chi_{EA} - \chi_c)/\chi_c$, re-scaled with respect the expressions of the mutual information and of the Holevo function under collective attacks ($g = g' = 0$), given by I_c and χ_c respectively. In the left panel we plotted the case for $\tau = 0.65$, while the right panel shows the evolution of the mutual information and of the Holevo bound for $\tau = 0.95$.We note that increasing the transmissivity τ, the gap existing between the mutual information (blue line) and the Holevo function (red line) increases, with respect the case for $\tau = 0.65$, from this it we have the divergences between curves (d) and the black-dashed one, in Fig. 6.3, describing the collective attack.

6.6 Conclusions

In conclusion, the results obtained are important for the general assessment of quantum cryptography with continuous variable. In particular we have studied the case of two-way communication, focusing on the security of the protocol under two-mode coherent attack. This represents the first study of this type for this kind of communication scheme in which coherent attack can be explicitly considered and analytically solved. The analysis spotlighted the first evidence of existing coherent attacks beating the collective ones, in point-to-point protocols. This represents important finding for the research community working on quantum cryptography.

A similar result has been obtained from the analysis developed in our previous investigations, focused on the alternative approach to quantum cryptography, based on the end-to-end paradigm. As we will show in Part III, when the parties estab-

lish the key exploiting some kind of correlation, then Eve can obtain an advantage over the parties exploiting correlated ancillary modes, in order to optimize her final coherent measurement. Here something similar happens, despite the optimal attack is different because here we do not employ any Bell measurement.

Finally we emphasize that our analysis is also important to stress on the importance of the ON/OFF switching strategy. We conclude that the active exploitation of the additional degrees of freedom, activated by the ON/OFF switching, represent a necessary solution to avoid the possibility of powerful coherent attacks.

Chapter 7

Immunity of two-way communication against coherent attacks

In Chapter 4 we showed that one-way point-to-point communication, Eve has strictly no benefits in using a coherent attack: the key-rate is in fact increased in this case. In Chapter 6 we found instead that when the two-way communication is used in the ON configuration, then coherent attacks can outperform collective attacks.

In light of this result here we study the security of the two-way communication against coherent attacks, and show that exploiting the ON/OFF switching (i.e. the possibility of keeping closed or randomly opening the two-way communication), the two-way communication is immune against two-mode general coherent attacks. In [36] it was showed that the ON/OFF switching can be used to select the security thresholds of the channel in OFF, in which case the reduction of the general attack grant the optimality of collective attack. Here we go further because using the result of Chapter 4, we know that in case of coherent attacks the security thresholds of one-way protocol are always higher than under collective ones. On the other hand in previous Chapter we have seen that optimal two-mode coherent attacks, overcoming the collective attacks, can exist. Here we show that the ON/OFF switching neutralizes this two-mode optimal attacks so that, combining the super-additivity of the double communication and the control on the random opening and closing of the two-way circuit, we can convert the memory used by Eve into noise on which Eve has no control.

7.1 Security against coherent attacks

The quantum communication of the two-way non-switching protocol has been already discussed. After this first communication stage, the parties perform the tomography of the quantum channel in order to determine the presence of Eve on the line. They use part of their exchanged data to reconstruct the covariance matrix of the attack determining, in particular, the matrix $\mathbf{G}$. Then, they retain the data exchanged with the circuit in ON if $\mathbf{G} = \mathbf{0}$ while if they find $\mathbf{G} \neq \mathbf{0}$ then they select the data exchanged with the circuit set in OFF. Let us consider the reverse

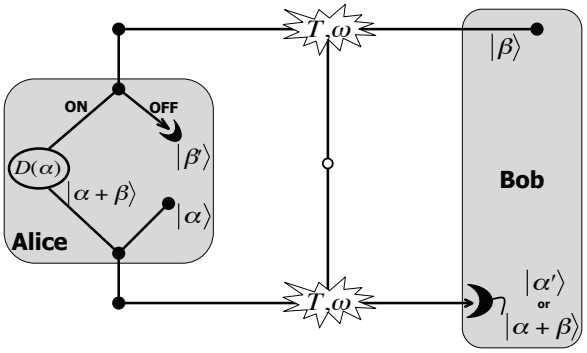

Figure 7.1: The two-way CV-QKD protocol versus coherent attacks. Steps: *forward*, Bob prepares coherent states $|\beta\rangle$ and send it through the noisy channel. *Backward*, in ON configuration Alice applies a random displacement $D(\alpha)$ on $|\beta\rangle$ encoding information in α. Bob heterodynes the coherent $|\alpha+\beta\rangle$ and finally subtracts β, recovering α . In OFF configuration, the circuit is randomly opened at Alice's station. She then *heterodynes* the reference state, obtaining the variable β'. She then prepares a new coherent state α that is sent back to Bob who performs an *heterodyne* or an *homodyne* detection depending on the decoding scheme) it obtaining the variable α'. Eve, ignoring which setup has been adopted (as well as Bob), needs to recover both the reference amplitude and Alice's encoding α, so she's forced to attack both communication lines. The reduction of the general attack in a two-way scenario, by means of the de Finetti theorem, configures the residual two-mode coherent attack, where E_1 and E_2 share some kind of correlation. The ON/OFF setting of the circuit commute this correlation into pure noise.

reconciliation case. We define the key rate as

$$R \coloneqq \max_{\mathbf{G}}\{R_{ON},\, R_{OFF}\},$$

where the rate in ON is known and already computed in [36]. The rate in OFF is, in practice that one computed in Chapter 4, in the context of the one-way protocol against two-mode coherent attack, where we have

$$R_{OFF} = I_{AB}^{OFF} - \chi(\varepsilon : \alpha, \beta, \alpha', \beta'),$$

where $I_{AB}^{OFF} = (I(\alpha:\alpha') + I(\beta:\beta'))/2$. Reverse reconciliation the parties can indeed choose between the following two thresholds

$$R_{ON} = \log_2 \frac{2\tau(1+\tau)}{e(1-\tau)(1+\Lambda)} + \sum_{i=1}^{3} h(\bar{\nu}_i) - 2h(\omega), \tag{7.1}$$

$$R_{OFF} = \frac{1}{2}\log_2 \frac{2\tau}{e(1-\tau)(1+\tilde{\Lambda})} + \sum_{j=\pm} \frac{h(\bar{\nu}'_j) - h(\nu_j)}{2}, \tag{7.2}$$

where, for this protocol, the symplectic eigenvalues $\bar{\nu}_i$ can only be computed numerically, with $\Lambda = \tau^2 + (1-\tau^2)\omega$ and $\tilde{\Lambda} = \tau + (1-\tau)\omega$. The symplectic eigenvalues in OFF have been computed in Chapter 4, and we rewrite here their expressions

$$\nu_{\pm} \to \sqrt{(\omega \pm g)(\omega \pm g')}, \tag{7.3}$$

$$\bar{\nu}'_{\pm} \to \frac{\sqrt{[\lambda_{\pm} + 1 - \tau][\lambda'_{\pm} + 1 - \tau)]}}{\tau},$$

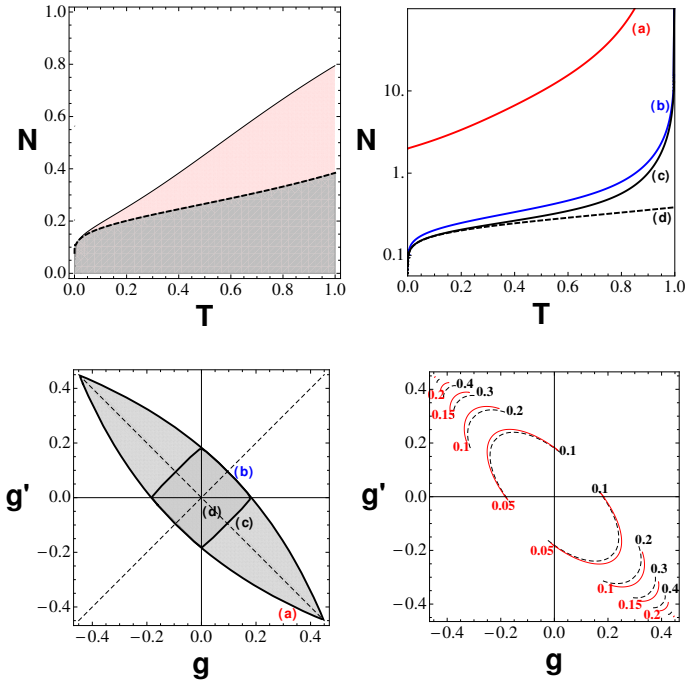

Figure 7.2: Top-left panel represents the tolerable excess noise (N) Vs. transmissivity (τ). The one-way threshold (dashed line) under collective attacks ($g = 0$), is compared with the thresholds $R_{ON} = 0$ (black thick line) for the two-way against collective attacks. In top-right panel we study the case OFF, comparing the thresholds for collective attack, (d), and others cases for increasing values of the correlation parameter $g' = -g$ and $g = \pm(\omega - 1)$(c), $g = \pm\sqrt{\omega^2 - 1}$ (a), corresponding to maximally entangled states, and $g' = g$ with $g = \pm(\omega - 1)$ (b) The curves correspond to the the values of the correlations labeled in panel bottom-left. Finally the bottom-right panel we plot the security thresholds as a function of the correlation parameters g, g', computed for values of the transmissivity $\tau = \tau_{fix} = 0.3$ and thermal noise $\omega = \omega_{fix} \simeq 1.097$, for which the rate against collective attack of the nonswitching one-way protocol is zero. For the same parameters we also plot the two-way secret-key rate in OFF, when Eve is performing a coherent attack and we apply the ON/OFF switching.

where $\lambda_{\pm} = \tau + (\omega \pm g)(1 - \tau)$ and $\lambda'_{\pm} = \tau + (\omega \pm g')(1 - \tau)$.

7.2 Discussion

The thresholds of Eqs. (7.1) and (7.2) in case $\mathbf{G} = 0$, are plotted in Fig.7.2 as a function of the transmissivity τ and of the tolerable excess noise $N = (\omega - 1)(1 - \tau)/\tau$. In Figure (7.2)(top-right) we plot the thresholds for the case OFF, showing the role played by Eve's correlations. We compared the cases for $g' = g = 0$ (dashed), that coincide with the threshold of the one-way protocol, with the cases given by $g' = -g = \pm(\omega - 1)$ (black), $g' = -g = -\sqrt{\omega^2 - 1}$ for ancillas in the maximally entangled states (red curve), and finally we considered the case $g' = g = \pm(\omega - 1)$ (blue). The Fig.7.2(bottom-left) and (bottom-right), show the link between the improved security provided by the ON/OFF switching with respect the one-way, and the amount and type of correlation used to prepare the attack. We fixed τ to a value for which the one-way rate is zero ($\tau_{fix} = 0.2$), we then compute the corresponding thermal

noise ω_{fix} from Eq. (4.3) and (4.4), and we plot the rate $R_{OFF}(\tau_{fix}, \omega_{fix}, g, g')$ as a function of the correlation parameters (g, g'). In Fig.7.2(bottom-left) the correlation plan (g, g') is linked with the curves of figure 7.2(top-right) by the labels *(a),(b),(c)* and *(a)*. In particular in Fig.7.2(bottom-right) with the black-dashed curve we plot the quantum mutual information, quantifying the correlation between Eve's ancillas, while the red curves, always positive and increasing, represent the rate of the two-way protocol in OFF (red curves), given by eq.(7.1), for the case $g' = -g = \pm(\omega - 1)$, that represent also the worst case scenario described curve *(c)* in Fig. 7.2(top-right).

This behavior is general and then independent from the encoding/decoding configurations. We then see that the degrees of freedom activated by the ON/OFF switching can be used to transform the two-way communication into a protocol that is immune to coherent attacks. In fact, in light of this result, Eve will limit herself to collective attacks despite being non-optimal to avoid to help the parties in sharing the secret-key. In fact the mechanism described in Chapter 4, can here be seen as an *a-posteriori* conversion of the memory injected by Eve into pure noise, when the circuit is opened. This noise is not deleterious for the parties that control it, so it cannot affect Alice-Bob mutual information, but it is for Eve that has no power on the activation of the ON/OFF switching. This is responsible for a reduction in Eve's accessible information.

7.3 Switching protocol

We describe now the results of the same analysis applied to the switching protocol (encoding in coherent states, and detection by homodyne measurements). This thresholds are new and never presented for the case of two-way communication in ON. Again the global key-rate, $\tilde{R}$, available for the parties can be defined as

$$\tilde{R} \coloneqq \max_{\mathbf{G}} \{\tilde{R}_{ON},\, \tilde{R}_{OFF}\}, \tag{7.4}$$

where we have found the following expression for the case ON and OFF, respectively

$$\tilde{R}_{ON} = \log_2 \frac{\tau^2 + \omega + \tau^3(\omega - 1)}{(1-\tau)\Lambda} + h(\widetilde{\nu}) - 2h(\omega), \tag{7.5}$$

$$\tilde{R}_{OFF} = \frac{1}{2}\log_2 \frac{\sqrt[4]{(\omega^2 - g^2)(\omega^2 - g'^2)}}{(1-\tau)\tilde{\Lambda}} - \sum_{i=\pm} \frac{h(\nu_i)}{2}, \tag{7.6}$$

where,

$$\widetilde{\nu} = \sqrt{\frac{\omega[1 + \tau^2\omega(1-\tau) + \tau^3]}{\tau^2 + \omega + \tau^3(\omega - 1)}}, \tag{7.7}$$

and the total symplectic spectrum ν_i has been determined before, in Eq.

7.4 Conclusions

In this chapter we studied the two-way communication protocol for CVQKD under a general eavesdropping scenario. We found that the additional degree of freedom activated by a random switching of the two-way communication line, while the eavesdropper is performing a coherent attack, allows to take advantage of Eve's injected memory converting it into noise eluding Eve's control. The result of this

strategy are improved security thresholds with respect one-way scheme, and allows to conclude that a coherent attack against a CV two-way communication is ineffective from Eve's perspective, disclosing the immunity of two-way protocol against general attacks.

The optimal strategy for the eavesdropper, with the circuit in ON, would be to perform a coherent attack. But because of Eve cannot control the opening and closing of the circuit, if she realizes a coherent attack, the parties can choose to use the data exchanged with the circuit in OFF, increasing in this way the security of their transmission. We can indeed conclude that Eve will not perform coherent attacks against Gaussian quantum cryptography in two-way communication.

Chapter 8

Two-way quantum cryptography with thermal states

8.1 Introduction

Recently there has been some interest in thermal quantum cryptography [49, 51, 50, 52]. These protocols consider the effect of unknown preparation noise on Alice's signal states. One of the applications of thermal quantum cryptography is the possibility to generate secure keys at different wavelengths of the electromagnetic field [51, 52], from optical range down to the infrared and microwave regimes. Investigations in this sense can have important applications in communications technologies. In fact secure communication at different wavelengths is ubiquitous in today's communication environment. From the optical telecommunication wavelength of 1550 nm down into the GHz microwave regime, utilized by technologies such as Wi-Fi and cellular phones.

In this chapter, we show that it is possible to improve the security of thermal QKD at different wavelengths, using two-way quantum communication, which can tolerate higher levels of loss and noise [36] with respect one-way communication. Variants of the two-way quantum communication protocol also exist [53, 54], including some schemes [55, 56] related to the mechanism of quantum illumination [57, 58].

The idea of using additional preparation noise for two-way quantum communication was preliminarily investigated in [59]. Here they showed the 'fighting noise with noise' effect, an effect first seen in discrete-variable QKD [60] and later in CV one-way protocols [61, 62, 63]. The basic mechanisms is that if extra noise (trusted) is added in the appropriate way, then the performance of the protocol can be improved, in terms of secret-key rate and security threshold [52]. In this chapter we consider the two-way protocol in the presence of considerably large levels of preparation noise, corresponding to the use of different communication wavelengths. We show that the two-way communication is extremely robust in reverse reconciliation, such as to beat one-way protocols for any value of the preparation noise, a feature which allows us to improve the performance of quantum cryptography at the infrared regime.

The model we use to describe the thermal noise simplifies the mathematical description of the system, but will require further improvements to provide a definitive and accurate evaluation of the performances of QKD at different frequencies, in particular in those regimes far from the optical range. We will discuss further this

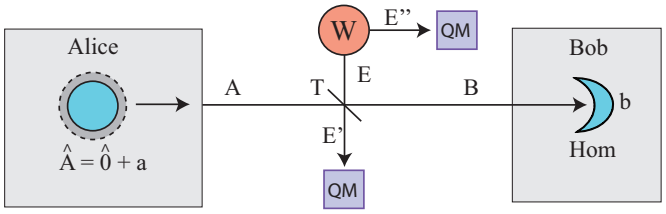

Figure 8.1: One-way thermal QKD protocol. See text for details.

limitation of the model we have adopted, in the conclusion to this chapter.

8.2 From one-way to two-way thermal quantum communication

8.2.1 One-way thermal quantum cryptography

In a thermal protocol the sender (Alice) randomly modulates thermal states, that are sent to the receiver, Bob (see Fig. 8.1). On average, we can write the generic quadrature $\hat{A}$ of Alice's input mode A as $\hat{A} = \hat{0} + a$, where the real number a is the Gaussian encoding variable with variance μ_a, and $\hat{0}$ is a quadrature operator accounting for the thermal 'preparation noise', with variance $V_0 \geq 1$. The overall variance of Alice's average state is therefore given by $\mu_A = V_0 + \mu_a$.

The variance V_0 can be broken down as $V_0 = 1 + \eta$, where 1 is the variance of the vacuum noise, and $\eta \geq 0$ is the variance of an extra noise which is confined in Alice's station and not known to either Eve, Alice or Bob. At the output of the channel, Bob homodynes the incoming mode B, randomly switching between position and momentum detections, as well as in a no-switching setup. In this way, Bob collects an output variable b which is correlated to Alice's encoding a.

The above thermal protocol is still Gaussian and its security can be tested against collective Gaussian attacks. As usual we consider the most practical collective attack, represented by the entangling cloner collective attack [28], where Eve's ancillary mode E interacts with the signal mode A by means of a beam splitter with transmission $\tau \in [0,1]$. The mode E is as usual one of the two component of an Einstein-Podolsky-Rosen (EPR) state $\rho_{EE''}$, with covariance matrix

$$\mathbf{V}_{EE''} = \begin{pmatrix} \omega\mathbf{I} & \sqrt{\omega^2-1}\mathbf{Z} \\ \sqrt{\omega^2-1}\mathbf{Z} & \omega\mathbf{I} \end{pmatrix},$$

where ω, $\mathbf{I}$ and $\mathbf{Z}$ as been previously defined. Both the kept mode E'' and the transmitted mode E' are collected in Eve's quantum memory which is coherently measured at the end of the protocol. For a thermal QKD protocol based on modulated thermal states and homodyne detection, the key rates are functions of the input parameters, namely the variance of the thermal noise V_0 and the variance of the classical signal modulation μ_a, plus the parameters of the attack, τ the thermal variance ω.

In the typical limit of high modulation ($\mu_a \gg 1$), one gets the two analytical expressions for the asymptotic secret-key rates

$$R^{\blacktriangleright}(V_0,\tau,\omega) = \frac{1}{2}\log_2\frac{\tau\Lambda(\omega,V_0)}{(1-\tau)\Lambda(V_0,\omega)} + h\left[\sqrt{\frac{\omega\Lambda(1,\omega V_0)}{\Lambda(\omega,V_0)}}\right] - h(\omega), \tag{8.1}$$

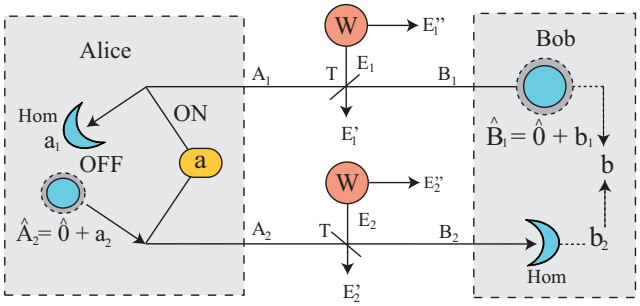

Figure 8.2: Two-way thermal QKD protocol. See text for explanations. A collective entangling-cloner attack is also shown, where Eve uses two beam splitters with transmission T and two EPR states with variance W. The output modes E_1', E_1'', E_2', E_2'' are collected in a quantum memory which is coherently measured at the end of the protocol.

and

$$R^{\blacktriangleleft}(V_0,\tau,\omega) = \frac{1}{2}\log_2 \frac{\omega}{(1-\tau)\Lambda(V_0,\omega)} - h(\omega), \tag{8.2}$$

where we have used the two functions

$$\Lambda(x,y) := \tau x + (1-\tau)y, \tag{8.3}$$

and $h(x)$ previously defined in Eq. (5.18). By setting these key rates to zero, we can derive the two security thresholds that expressed in terms of tolerable excess noise are $N^{\blacktriangleright} = N^{\blacktriangleright}(V_0,\tau)$ and $N^{\blacktriangleleft} = N^{\blacktriangleleft}(V_0,\tau)$, where N is the excess noise given in Eq. (2.37).

8.2.2 Two-way thermal protocol

For the sake of clarity we describe here the two-way protocol in the thermal setup. As depicted in Fig. 8.2, Bob has an input mode B_1 where now a thermal state with preparation variance V_0 is modulated by a bivariate Gaussian distribution with signal variance $\mu_{b_1} := \mu$. On average, we have the input quadrature $\hat{B}_1 = \hat{0} + b_1$, encoding the Gaussian variable b_1. In the first quantum communication through the insecure channel, mode B_1 is sent to Alice, who receives the noisy mode A_1 and randomly switches between two configurations [36]:

(i) ON configuration, where Alice encodes a Gaussian variable a with variance $\mu_a = \mu$, randomly displacing the quadrature of the incoming mode $\hat{A}_1 \to \hat{A}_2 = \hat{A}_1 + a$;

(ii) OFF configuration, where Alice homodynes the incoming mode A_1 with classical output a_1, and prepares another Gaussian-modulated thermal state $\hat{A}_2 = \hat{0} + a_2$, with the same preparation and signal variances as Bob, i.e., V_0 and $\mu_{a_2} = \mu$.

In both cases, the processed mode A_2 is sent back to Bob in the second quantum communication through the channel. At the output, Bob homodynes the incoming mode B_2 with classical output b_2.

As in the standard two-way protocol, after the quantum communication, Alice reveals which configuration of the circuit, between the ON or OFF, was chosen in each round of the protocol, and both the parties declare which quadratures were detected by their homodyne measurement. After this stage, Alice and Bob possess

a set of correlated variables, which are $a_1 \approx b_1$ and $a_2 \approx b_2$ in OFF configuration, and $a \approx b$ in ON configuration, where b is post-processed from b_1 and b_2.

In this way the parties can detect the presence of memory between the first and the second use of the channel. If a memory is present (as in case of the two-mode coherent attack described in previous Chapter), then Alice and Bob use the OFF configuration, extracting a secret-key from $a_1 \approx b_1$ and $a_2 \approx b_2$. By contrast, if the memory is absent (one-mode collective attack), then they use the ON configuration and they post-process a and b. Once Alice and Bob have decided which configuration to use, they post-process their remaining data using standard one-way algorithms of classical error correction and privacy amplification, therefore extracting a secret-key in direct or reverse reconciliation.

As we discussed in the previous Chapter, the use of two-mode coherent attacks against the two-way protocol is not advantageous for Eve. In fact, using the OFF configuration against such attacks, Alice and Bob can reach security thresholds which are much higher than those of one-way protocols. Thus, we consider here the analysis of collective one-mode attacks, in particular, those based on entangling cloners, which are the most practical benchmark to test CV-QKD. We show that, using the ON configuration against these attacks, Alice and Bob are able to extract a secret-key in conditions so noisy that any one-way protocol would fail. In particular, this happens in reverse reconciliation which turns out to be extremely robust in the preparation noise, therefore allowing us to improve the performance of CV-QKD in the very noisy regime of infrared frequencies.

8.3 Cryptanalysis

We study now the security of the two-way thermal quantum cryptographic protocol, against collective entangling-cloner attacks. Adopting the ON configuration, we derive the analytical expressions of the asymptotic secret-key rates (i.e., for high modulation $\mu \to +\infty$), first in DR and then in RR. Such rates are explicitly plotted in the transmission τ for $\omega = 1$ (pure-loss channel) and studied in terms of the preparation noise V_0. In the specific case of RR, we also analyze the behavior of the security threshold for different values of τ and V_0, comparing this threshold with that of the corresponding one-way thermal protocol.

As shown in Fig. 8.2, a collective entangling-cloner attack against the two-way protocol consists of Eve performing two independent and identical beam-splitter attacks (transmission T), one for each use of the channel. For each beam splitter $i = 1$ or 2, Eve prepares two ancillas whose modes E_i and E_i'' are in an EPR state with variance ω. Eve keeps mode E_i'' while injecting the other mode E_i into one port of the beam splitter, leading to the transmitted mode E_i'. These operations are repeated identically and independently for each signal mode sent by Bob as well as the return mode sent back to Bob by Alice. All of Eve's output modes E_i' and E_i'' are stored in a quantum memory which is coherently detected at the end of the two-way protocol. Eve's final measurement is optimized based on Alice and Bob's classical communication.

For such an attack, Bob's post-processing of his classical variables is just given by $b = b_2 - \tau b_1$. This variable is the optimal linear estimator of Alice's variable a in the limit of high modulation $\mu \to +\infty$. Note that this classical post-processing can be equivalently realized by constructing a displaced mode B with generic quadrature $\hat{B} = \hat{B}_2 - \tau b_1$ which is then homodyned by Bob. Despite being useful for the theo-

retical analysis of the protocol in RR, such a physical representation is not practical since it involves the use of a quantum memory to store mode B_2 whose displacement $-\tau b_1$ can only be applied once Bob has estimated the channel transmission τ. Finally we remark that this equivalent representation is realized by Gaussian operations, so that the global output state of Bob (B-mode) and Eve (E-modes) is Gaussian (this is true for both b_1 fixed or Gaussian-modulated).

8.3.1 Secret-key rate in direct reconciliation

Let us start our security analysis considering direct reconciliation [68]. For one-way protocols this setup is very robust [51], which were in principle able to tolerate an infinite amount of preparation noise and still have a finite secret key, albeit very small [52]. As we show below, such a behavior is not typical of two-way thermal protocols.

As we know, the secret key rate for DR is given by $R^{\blacktriangleright} := I_{ab} - I_{aE}$. The mutual information between Alice and Bob is derived from the differential Shannon entropy [69] and is simply given by

$$I_{ab} = \frac{1}{2}\log_2 \frac{V_b}{V_{b|a}} \ ,$$

where V_b is the variance of Bob's post-processed variable b, and $V_{b|a}$ its variance conditioned to Alice's encoding a. These variances are easy to compute once we write the Bogoliubov transformations for the quadratures.

The output mode B_2 has generic quadrature

$$\hat{B}_2 = \tau\hat{B}_1 + \sqrt{\tau}a + \sqrt{1-\tau}(\sqrt{\tau}\hat{E}_1 + \hat{E}_2) \ .$$

Subtracting off the input modulation b_1 (known to only Bob), we get the processed quadrature $\hat{B} = \hat{B}_2 - \tau b_1$ equal to

$$\hat{B} = \tau\hat{0} + \sqrt{\tau}a + \sqrt{1-\tau}(\sqrt{\tau}\hat{E}_1 + \hat{E}_2) \ ,$$

with variance $V_B = \tau^2 V_0 + \tau\mu_a + (1-\tau^2)\omega$. Since $V_B = V_b$ and $\mu_a = \mu$, we get

$$V_b = \tau^2 V_0 + \tau\mu + (1-\tau^2)\omega \ , \tag{8.4}$$

which gives $V_b \to \tau\mu$ in the limit of high modulation.

In the same limit, the conditional variance $V_{b|a}$ is given by setting $\mu = 0$ in the previous equation for V_b, i.e., we have

$$V_{b|a} = V_b|_{\mu=0} = \tau^2 V_0 + (1-\tau^2)\omega \ .$$

Therefore, the mutual information between Alice and Bob is given by

$$I_{ab} = \frac{1}{2}\log_2 \frac{\tau^2 V_0 + \tau\mu + (1-\tau^2)\omega}{\tau^2 V_0 + (1-\tau^2)\omega} \to \frac{1}{2}\log_2 \frac{\tau\mu}{\tau^2 V_0 + (1-\tau^2)\omega} \ . \tag{8.5}$$

Eve's Holevo information on Alice's encoding variable a is defined as

$$I_{aE} := S(E) - S(E|a) \ ,$$

where $S(\cdot)$ is as usual the von Neumann entropy of Eve's multimode output state ρ_E (modes $E_1' E_1'' E_2' E_2''$) and $S(E|a)$ the entropy of the conditional state $\rho_{E|a}$ for

fixed values of Alice's encoding variable a. Since these states are Gaussian, their entropies can be computed from the symplectic spectra of their covariance matrices, $\mathbf{V}_E$ and $\mathbf{V}_{E|a}$, respectively [11].

By generalizing the derivation in Ref. [65] to include the presence of preparation noise ($V_0 \geq 1$) we get the following expression of Eve's CM for the Gaussian state ρ_E of modes $E_1' E_1'' E_2' E_2''$

$$\mathbf{V}_E(\mu_a, \mu_a) = \left(\begin{array}{cc|cc} \varepsilon \mathbf{I} & \varphi \mathbf{Z} & \chi \mathbf{I} & \mathbf{0} \\ \varphi \mathbf{Z} & \omega \mathbf{I} & \theta \mathbf{Z} & \mathbf{0} \\ \hline \chi \mathbf{I} & \theta \mathbf{Z} & \mathbf{\Delta}(\mu_a, \mu_a) & \varphi \mathbf{Z} \\ \mathbf{0} & \mathbf{0} & \varphi \mathbf{Z} & \omega \mathbf{I} \end{array} \right), \tag{8.6}$$

where $\mathbf{0} \coloneqq \mathrm{diag}(0,0)$ and the parameters are defined as

$$\varepsilon \coloneqq (1-\tau)\mu_{B_1} + \tau\omega, \tag{8.7}$$

$$\chi \coloneqq -\sqrt{\tau}(1-\tau)(\omega - \mu_{B_1}), \tag{8.8}$$

$$\theta \coloneqq -(1-\tau)(\omega^2 - 1), \tag{8.9}$$

$$\gamma \coloneqq \tau(1-\tau)\mu_{B_1} + (1 - \tau + \tau^2)\omega \tag{8.10}$$

$$\varphi \coloneqq \sqrt{\tau(\omega^2 - 1)}, \tag{8.11}$$

$$\mathbf{\Delta}(\mu_a, \mu_a) \coloneqq \gamma \mathbf{I} + (1-\tau)\ \mathrm{diag}(\mu_a, \mu_a)\ . \tag{8.12}$$

In the previous parameters, we set $\mu_{B_1} = V_0 + \mu$ and $\mu_a = \mu$, and we consider the limit of high modulation ($\mu \to +\infty$). Thus, we are able to compute the asymptotic symplectic spectrum of the CM which is given by the four eigenvalues $\nu_1 \to \omega$, $\nu_2 \to \omega$ and $\{\nu_3, \nu_4\}$ such that $\nu_3 \nu_4 \to (1-\tau)^2 \mu^2$. Using these eigenvalues, we compute the entropy of Eve's state ρ_E which is given by [70]

$$S_E = \sum_{k=1}^{4} h(\nu_k) \to 2h(\omega) + \log_2 \left(\frac{e}{2}\right)^2 (1-\tau)^2 \mu^2.$$

Now we consider the conditional CM $\mathbf{V}_{E|a}$ which is given by $\mathbf{V}_E(0, \mu)$ [65] As a result, $\mathbf{V}_{E|a}$ is the same as $\mathbf{V}_E$ except for the adjustment of the variable $\mathbf{\Delta}(\mu, \mu) \to \mathbf{\Delta}(0, \mu)$. In the usual limit ($\mu \to +\infty$) we compute the conditional spectrum $\bar{\nu}_1 \to 1$, $\bar{\nu}_2 \to \omega$ and $\{\bar{\nu}_3, \bar{\nu}_4\}$ such that $\bar{\nu}_3 \bar{\nu}_4 \to (1-\tau)\sqrt{(1-\tau^2)\omega\mu^3}$. Such eigenvalues allow us to derive the conditional entropy $S(E|a)$ and, therefore, to compute Eve's Holevo information

$$I_{aE} \to h(\omega) + \frac{1}{2} \log_2 \frac{(1-\tau)\mu}{(1+\tau)\omega}\ . \tag{8.13}$$

Combining Eqs. (8.5) and (8.13), we get following asymptotic expression for the DR secret-key rate

$$R^{\blacktriangleright}(V_0, \tau, \omega) = \frac{1}{2} \log_2 \frac{\tau(1+\tau)\omega}{(1-\tau)(\tau^2 V_0 + (1-\tau^2)\omega)} - h(\omega). \tag{8.14}$$

In order to study the performance of the two-way thermal protocol, we plot in Fig. 8.3 the DR secret-key rate in the presence of a pure-loss channel (corresponding to an entangling-cloner attack with $\omega = 1$) as a function of the channel transmission τ, and for different values of the preparation noise V_0. As we can see from the figure, two-way quantum communication with modulated pure states ($V_0 = 1$) is able to

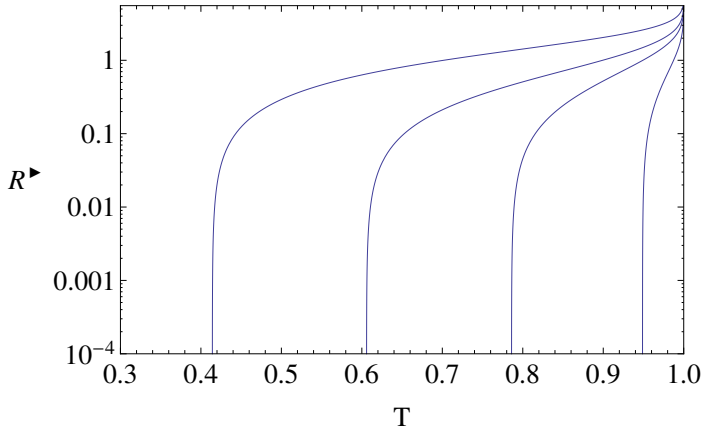

Figure 8.3: Plot of the DR secret-key rate of the two-way thermal protocol for a pure-loss channel ($\omega = 1$) as a function of the channel transmissivity, for different values of the preparation noise $V_0 = 1, 5, 10$, and 40 shot noise units (from left to right).

beat the 3 dB loss limit (corresponding to the threshold $\tau = 1/2$). However, as the preparation noise is increased, we see a fairly rapid deterioration in the security of the protocol. Such a behavior is different from what happens in DR for the corresponding one-way thermal protocol [51, 52]. In fact, despite one-way thermal QKD being secure only within the 3 dB loss limit, such limit is not affected by the preparation noise V_0, so that high values of V_0 are tolerable in the range $0.5 < \tau < 1$ with the DR secret-key rate remaining positive even if close to zero.

However, contrarily to what happens in DR, we show below that two-way thermal QKD is very robust to the preparation noise in RR, such that its security threshold outperforms both the thresholds (in DR and RR) of the one-way thermal QKD at any value of the preparation noise V_0. This is the feature that we will exploit to improve the security at the infrared regime.

8.3.2 Secret-key rate in reverse reconciliation

Let us derive the RR secret-key rate $R^{\blacktriangleleft} := I_{ab} - I_{Eb}$ [68]. Here we need to compute Eve's Holevo information on Bob's processed variable b, i.e., $I_{Eb} = S(E) - S(E|b)$. From the formula, it is clear that we need to compute the entropy $S(E|b)$ of Eve's output state $\rho_{E|b}$ conditioned to Bob's variable b. To compute the CM $\mathbf{V}_{E|b}$ of this state, we first derive the global CM

$$\mathbf{V}_{EB} = \begin{pmatrix} \mathbf{V}_E & \mathbf{D} \\ \mathbf{D}^T & \mu_b \mathbf{I} \end{pmatrix}, \tag{8.15}$$

describing Eve's modes $E_1' E_1'' E_2' E_2''$, with reduced CM $\mathbf{V}_E$ given in Eq. (8.6), plus Bob's virtual mode B, with reduced CM $V_b \mathbf{I}$, with the variance V_b computed in Eq. (8.4). Then, we apply homodyne detection on mode B, which provides [33, 34, 51, 71] $\mathbf{V}_{E|b} = \mathbf{V}_E - (1/V_b)\mathbf{D}\mathbf{\Pi}\mathbf{D}^T$, where $\mathbf{\Pi} := \mathrm{diag}(1, 0, 0, 0)$. Here the off-diagonal block $\mathbf{D}$ describes the correlations between Eve's and Bob's modes, and is given by

$$\mathbf{D}^T = \begin{pmatrix} \xi_1 \mathbf{I}, & \phi_1 \mathbf{Z}, & \xi_2 \mathbf{I}, & \phi_2 \mathbf{Z} \end{pmatrix}, \tag{8.16}$$

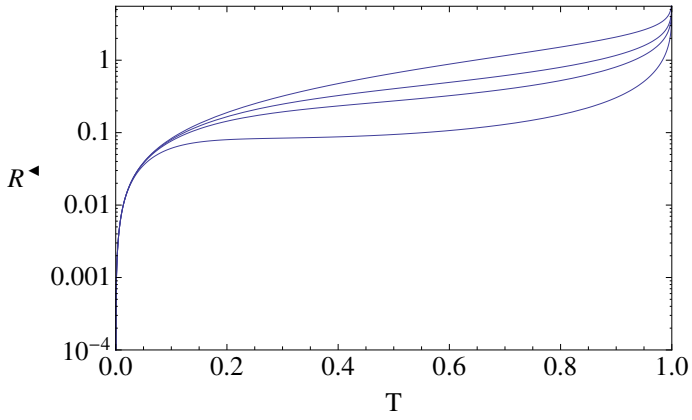

Figure 8.4: Plot of the RR secret-key rate of the two-way thermal protocol for a pure-loss channel ($\omega = 1$) as a function of the transmissivity, for different values of the preparation noise $V_0 = 1, 5, 10$, and 40 (from top to bottom). As the preparation noise is increased, the rate decreases but remains positive for any $\tau > 0$.

where

$$\xi_1 = -\tau\sqrt{1-\tau}(V_0 - \omega), \tag{8.17}$$

$$\phi_1 = \sqrt{\tau(1-\tau)}\sqrt{\omega^2 - 1}, \tag{8.18}$$

$$\xi_2 = -\sqrt{\tau(1-\tau)}(\tau V_0 + \mu_a) + \tau\omega\sqrt{\tau(1-\tau)}, \tag{8.19}$$

$$\phi_2 = \sqrt{1-\tau}\sqrt{\omega^2 - 1}\ . \tag{8.20}$$

In the previous formulas, we set $\mu_a = \mu_{b_1} = \mu$ and we consider the limit of high modulation $\mu \to +\infty$. In this limit, we derive the asymptotic expression of the conditional symplectic spectrum $\{\tilde{\nu}_1, \tilde{\nu}_2, \tilde{\nu}_3, \tilde{\nu}_4\}$, which is given by $\tilde{\nu}_1 \to \omega$,

$$\tilde{\nu}_2 \to \sqrt{\frac{\omega\left[1 + \tau^2 V_0\omega + \tau^3(1 - V_0\omega)\right]}{\tau^2 V_0 + \omega + \tau^3(\omega - V_0)}}\ , \tag{8.21}$$

and

$$\tilde{\nu}_3\tilde{\nu}_4 \to \sqrt{\frac{(1-\tau)^3\left[\tau^2 V_0 + \omega + \tau^3\left(\omega - V_0\right)\right]\mu^3}{\tau}}\ . \tag{8.22}$$

Using this spectrum we compute the conditional entropy $S(E|b)$ and, therefore, the RR secret-key rate, whose asymptotic expression is equal to

$$\begin{aligned} R^{\blacktriangleleft}(V_0, \tau, \omega) = \frac{1}{2}\log_2 \frac{\tau^2 V_0 + \omega + \tau^3\left(\omega - V_0\right)}{\left[V_0\tau^2 + \left(1-\tau^2\right)\omega\right](1-\tau)} \\ + h\left(\tilde{\nu}_2\right) - h(\omega) \end{aligned} \tag{8.23}$$

In Fig. 8.4 we plot the RR secret-key rate $R^{\blacktriangleleft}$ in the presence of a pure-loss channel ($\omega = 1$) as a function of the channel transmissivity τ for values of the preparation noise from $V_0 = 1$ to $V_0 = 40$. As we can see, there is no reduction in the security of the protocol, in the sense that all the curves originate from the common threshold $\tau = 0$ for any value of the preparation noise V_0, even if the rate is decreasing for

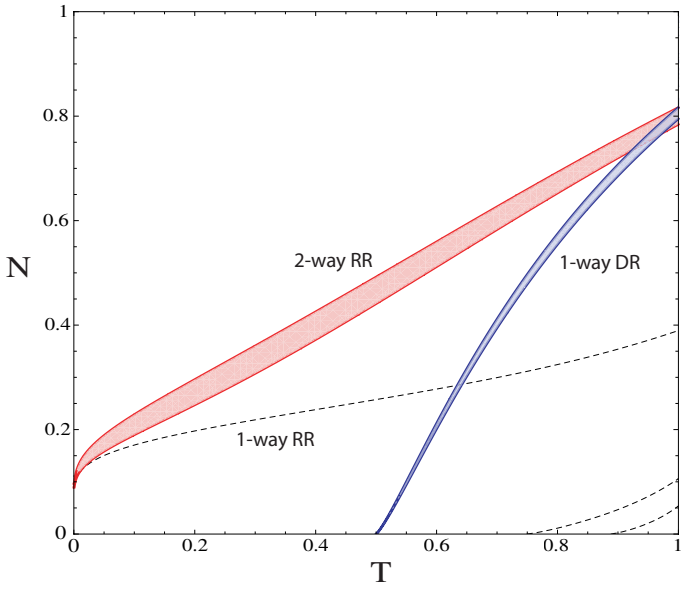

Figure 8.5: Two-way thermal protocol in the presence of an arbitrary entangling-cloner attack ($\omega \geq 1$). We plot the RR security threshold, expressed as tolerable excess noise $N^{\blacktriangleleft}$ as a function of the channel transmissivity for different values of the preparation noise from $V_0 = 1$ to 10^6 (illustrated by the shaded regions). This threshold is compared with the DR threshold of the one-way thermal protocol for $V_0 = 1$ to 10^6. The plot also shows the RR threshold of the one-way protocol (dashed curves) for $V_0 = 1, 5, 10$ (from left to right).

increasing V_0. This is clearly in contrast to what happened before for DR (with the transmission threshold τ approaching 1 for high values of V_0).

Next, we analyze the security of the two-way thermal protocol against an arbitrary entangling-cloner attack (with $\omega \geq 1$). In Fig. 8.5, we plot its RR security threshold, expressed as tolerable excess noise $N^{\blacktriangleleft} = N^{\blacktriangleleft}(V_0, \tau)$ as a function of the transmissivity τ, for a wide range of values of the preparation noise V_0. As we can see, $N^{\blacktriangleleft}$ is very robust with respect to the preparation noise V_0, with all the curves, from $V_0 = 1$ up to $V_0 = 10^6$, being included in the region shown in the figure. Thus, despite the RR secret-key rate $R^{\blacktriangleleft}$ being decreasing for increasing V_0, it remains positive up to the excess noise $N^{\blacktriangleleft}$ shown in Fig. 8.5. (Furthermore, the threshold value $N^{\blacktriangleleft}$ turns out to be slightly increasing in V_0, as a result of the 'fighting noise with noise' effect of QKD).

From the same figure, we can see that the two-way thermal protocol outperforms the one-way thermal protocol in the transmission range $0 < \tau < 1$ for any value of the preparation noise V_0 (up to 10^6). In fact, the one-way protocol is not robust in RR (see dashed curves in the figure), and its DR security threshold $N^{\blacktriangleright}_{\text{1-way}}$ is well below the two-way RR threshold $N^{\blacktriangleleft}_{\text{2-way}}$, apart from a small overlapping region very close to $\tau = 1$. By exploiting this robustness and better performance of the two-way thermal protocol, we can improve the security of CV-QKD at the infrared regime as discussed in the following section.

8.4 Performances at different wavelengths

By exploiting its robustness to the preparation noise, we can think to use the two-way thermal protocol to improve the security of CV-QKD at longer wavelengths. Given a bosonic mode with frequency f in a thermal bath with temperature t, it is described by a thermal state with mean number of photons $\bar{n} = [\exp(hf/k_B t) - 1]^{-1}$, where h is Planck's constant and k_B is Boltzmann's constant [72]. This number gives the noise-variance of the thermal state $V_0 = 2\bar{n} + 1$, i.e., the preparation noise, which is therefore function of the frequency and the temperature, i.e., $V_0 = V_0(f, t)$. In our study we consider a fixed value of the temperature $t = 15$ °C, so that V_0 is one-to-one with the frequency f. We underline that this description of the distribution of thermal photons could not be accurate in the microwave regime, so we already say that in that regime our prediction could be affected by inherent limitations of the model adopted.

Eve's attack is a collective entangling-cloner attack (as before) which is thought to be performed inside a cryostat. The purpose of this is to remove Eve from the background preparation noise at any wavelength, therefore making her ancillary modes pure. In order to cover her tracks, Eve uses an entangling cloner with channel noise equal to the preparation noise, i.e., $W = V_0$. For more information on how to implement an entangling-cloner attack in thermal QKD, see the details given in [52].

Thus, at fixed temperature ($t = 15$ °C), we can express the RR secret-key rate $R^{\blacktriangleleft}(V_0, \tau, W)$ as a function of f and τ, i.e., $R^{\blacktriangleleft} = R^{\blacktriangleleft}(f, \tau)$. By setting $R^{\blacktriangleleft} = 0$, we get the security threshold $f^{\blacktriangleleft} = f^{\blacktriangleleft}(\tau)$, giving the minimum tolerable frequency $f^{\blacktriangleleft}$ which can be used at any channel transmission τ or, equivalently, the maximum tolerable wavelength $\lambda^{\blacktriangleleft} = c/f^{\blacktriangleleft}$, with c being the speed of light. The threshold $f^{\blacktriangleleft}(\tau)$ is plotted in Fig. 8.6 and compared with the thresholds of the one-way thermal protocol in DR and RR [51, 52]. As we can see from the figure, two-way QKD allows us to use a broader range of frequencies than one-way QKD. In particular, this happens for $0.2 \lesssim \tau \lesssim 0.8$, where the two-way threshold is well below the other thresholds in the infrared regime.

From Fig. 8.6, we see a crossing point between the DR and RR thresholds of the one-way protocol, for $\tau \simeq 0.6$ and $f \simeq 1.2{\times}10^{13}$ Hz. This point identifies the maximum gap from the two-way configuration, which remains secure for channel transmissions as low as $\tau \simeq 0.4$ at the same crossing frequency $f \simeq 1.2 \times 10^{13}$ Hz. Such a frequency corresponds to a wavelength of about $\lambda = 24$ μm, an infrared region where quantum communication is very demanding, with free-space losses around 9.7 dB/m under ideal atmospheric conditions (with humidity equal to 1mm of water vapor column and temperature of 15 °C [73]).

As a result, one-way QKD ($\tau = 0.4$) is secure up to a distance of 22 cm, while two-way QKD ($\tau = 0.6$) remains secure up to 41 cm. Despite being a very short distance, this represents an improvement close to 100%, which could be extremely useful in short-range cryptography, e.g., for connecting close computers through infrared ports or interfacing mobile devices with ATM machines.

Note that the infrared regime is less challenging in the 10 μm window, for instance at $\lambda = 12$ μm. At this wavelength, the atmospheric absorption is dominated by carbon dioxide, methane, and ozone, with an attenuation which is much smaller (about 0.53 dB/km). In this case, one-way QKD is secure up to 14.6 Km, while two-way QKD allows the parties to distribute secret-keys up to 15.8 Km, corresponding to an 8% improvement in the distance.

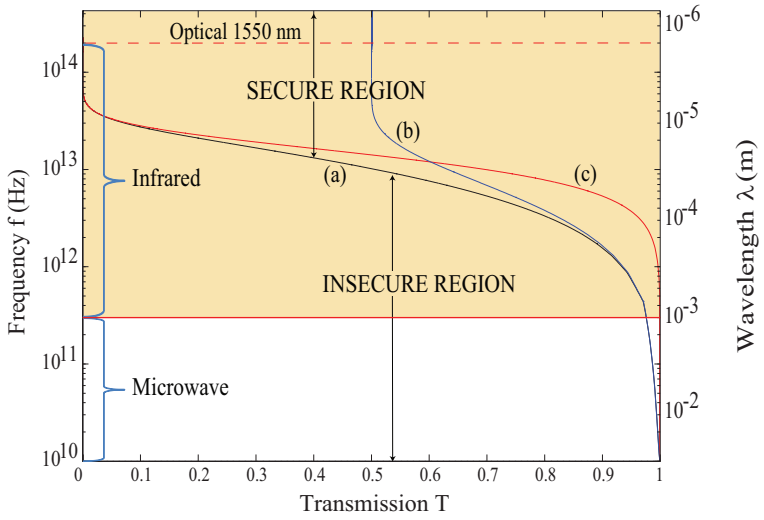

Figure 8.6: Security threshold of the two-way thermal protocol in RR (a) compared to the security thresholds of the one-way thermal protocol in DR (b) and RR (c). Thresholds are expressed as minimum tolerable frequency (or maximum tolerable wavelengths) as a function of the channel transmission. Note how the two-way threshold is deeper in the infrared regime. Environmental temperature is $t = 15$ °C.

As we said at the beginning of this section, for what it concerns the use of the two-way (and also one-way) thermal scheme in the microwave regime, we think that our model needs some improvement in order to provide a definitive answer about the viability of CV-QKD at these frequencies. In fact, we think that we should underline several points about the accuracy of our model in this regime. First of all, the detection scheme adopted in optical regime is different from that one adopted in microwave regime [42, 43]. So a complete, and more rigorous, description of the performances at microwave frequencies should take into account the viability and the efficiency of such a detection scheme, designed for microwave signals. In addition to this point we also note that the thermal noise structure is different to Gaussian noise. In particular being the thermal noise estimated using the Plank's formula, we have that the cavity photons/mode emission rate needs to be taken into account. We think that all these deficiencies our model of thermal noise could provide a too pessimistic prediction of the performances at the microwave regime. Our model is certainly accurate for Gaussian optical mode while, in case of microwaves, we could have overestimated the amount of untrusted noise. We think indeed that further analysis should be considered, in order to take into account the points discussed in the previous lines, and provide a better description of the performances of microwave QKD.

8.5 Conclusion

This chapter focused on the study of the two-way protocol in the thermal setup. We found that the parties can improve the security of thermal QKD, where (inaccessible to Eve) preparation noise is added to the signal states. Considering both types of reconciliation procedures, we have analyzed the secret-key rates and the security thresholds of a two-way protocol which is based on Gaussian-modulated thermal states, random Gaussian displacements and homodyne detections. We have tested

its security against collective Gaussian (entangling-cloner) attacks, showing how the security threshold in reverse reconciliation is very robust with respect to the preparation noise, and is able to outperform the security thresholds (in direct and reverse reconciliation) of one-way thermal QKD.

We have so successfully extended two-way thermal QKD to longer wavelengths, where thermal background naturally provides very high values of preparation noise. In particular, we have shown the superiority of two-way quantum communication in the infrared regime, improving the security distances which can be reached by the use of thermal sources at such frequencies.

Despite these results we think that further investigation regarding the performances at the microwave regime should be performed. The model adopted for the generation of thermal photons doesn't describe appropriately the situation in the microwave regime, and the existing detection schemes implemented for this regime have not been included in our study. These and other aspects make us conclude that very likely our basically negative predictions about the security performances in the range of wavelength of 10^{-4}, 10^{-3}, 10^{-2} μm, as described in Fig. (8.6), should be too pessimistic. This leave the open the possibility of implementing quantum cryptography at the very interesting regime of microwaves.

Part III

Novel results on end-to-end quantum cryptography

Introduction

This third part of the thesis is devoted to the analysis of a novel quantum cryptographic protocol for continuous variables designed thinking to the end-to-end architecture. The work presented extends the field of quantum cryptography to a modern network configuration where the users, Alice and Bob, cannot access to a direct link to communicate. We proof, both theoretically and experimentally, that they can exploit a third player (Charlie or the relay) having the duties of assisting the parties to successfully complete the cryptographic protocol.

In quantum cryptography we can hail the end-to-end principle from the seminal work by Ekert [76]. In this approach to quantum cryptography the parties exploit a fundamental property of quantum particles, the entanglement, as the quantum resource to certify the security of the shared quantum signals. From related ideas, recently [77], the concept of Device Independent (DI) protocols has been developed and investigated, with several results on the quantification of the security of this approach to quantum cryptography [78, 79, 80, 81]. In DI-QKD the parties make ideal no assumption on the trustability of the devices, and exploit the action operated by the intermediate station, to establish quantum correlations between the parties. Charlie indeed performs a Bell measurement and if the Bell test is passed, i.e., the result of the measurement violate the Bell inequalities, then the parties get entangled and can trust that the exchanged signals have not been intercepted by the eavesdropper.

Unfortunately, despite the recent results on the unconditional security of DI-QKD [83], this approach suffer of a major practical drawback. In order to prevent Eve exploiting inefficiencies of the detections (detection loop-holes) the DI protocols have to abort if the number of missed detections is too high. In Ref. [83] it is computed that in order to achieve a usable key rate, the required noise rate has to be of 2%. This efficiency is still far to be reached in today labs [82].

A solution to this problem comes relaxing the assumption on the trustability of the parties' private space. Moreover Charlie's measurement is still a Bell measurement, but the violation of the Bell inequalities is not needed. In fact just assuming that Alice and Bob's measurement devices are trusted, the parties can efficiently share a secret-key at a high rate, safe from any side-channel attack [74]. This novel approach has been introduced for general quantum system in [74] and for qubits systems in [75]. It is named Measurement-Device Independent QKD (MDI-QKD). In the next chapters we exploit this principle, developing the theory of a novel CV protocol with coherent state, and describing its experimental test under optimal attacks.

Chapter 9

Measurement-device-independence quantum cryptography

9.1 Introduction

We first consider the symmetric scenario described in Fig. 9.1(a), that is a special case of the general configuration studied in Ref. [17]. The relay is assumed to be placed midway between Alice and Bob, and the motivation to study this setup is that despite being non-optimal, in particular in terms of achievable security distances, it is easier to perform the cryptanalysis of the protocol. Beside this we remark that this configuration still represents a possible realistic network scenario where two parties are roughly equidistant from a public server or access point. We provide a detailed comparison between the most important Gaussian attacks against the quantum links, and we also show (see Appendix E the impact of several experimental imperfections on the security performance.

In a general eavesdropping of this scheme Eve injects thermal noise on the links connecting the parties to the relay in the same fashion as described in previous chapter, i.e., exploiting correlated ancillas prepared in a suitable Einstein-Podolsky-Rosen (EPR) state, and combined with Alice's and Bob's modes. We will show that for this family of protocols, such a strategy greatly outperforms the single-mode collective attack based on two independent entangling cloners which was assumed in some recent investigations[1] [84, 85]. Any such security analysis relying on independent attacks on the channels is therefore incomplete and opens security loopholes, in the context of end-to-end quantum cryptography with continuous variables.

The Chapter is organized as follows: In Section 9.2 we describe the setup in the symmetric scenario. In Section 9.3 we analyze its security and provide a formula for the key rate. In Section 9.5 we compare the various Gaussian attacks, identifying the optimal attack and the corresponding minimum key rate of the protocol. We then discuss the optimal configuration of the relay, in Section 9.6, and in Section 9.7

[1] Note that Ref. [85] computed the rate of the protocol at fixed transmissivity τ and thermal noise ω, since they fixed both τ and $\varepsilon = (\omega - 1)(1 - \tau)/\tau$. However, while the latter formula provides the excess noise for standard one-way protocols [11] it does not for the considered relay-based protocol (see Ref. [17] for the correct definition of excess noise in this more complex case).

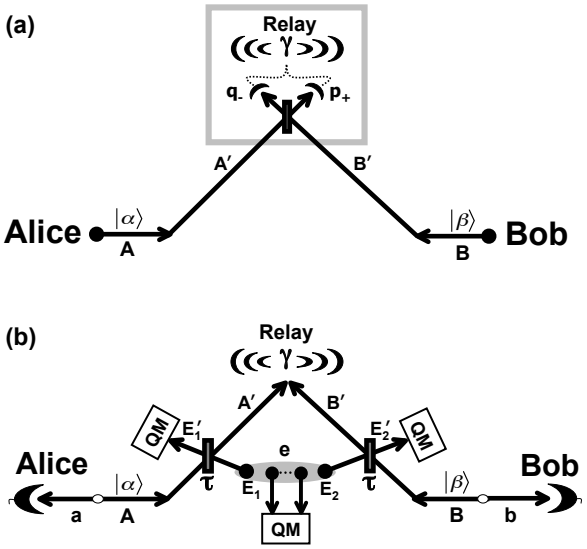

Figure 9.1: (a) Relay-based protocol performed in the symmetric configuration with the untrusted relay perfectly in the middle between the parties. Alice and Bob prepare coherent states with Gaussianly-modulated amplitudes, α and β, respectively. The relay performs a continuous-variable Bell measurement with complex outcome $\gamma := (q_- + ip_+)/\sqrt{2}$, which is publicly broadcast. From the knowledge of γ each party can infer the variable of the other party. (b) Entanglement-based representation of the protocol under two-mode Gaussian attack. Using two beam splitters with transmissivity τ, Eve injects to ancillary modes, E_1 and E_2, prepared in a two-mode Gaussian state with zero mean and CM in the symmetric normal form of Eq. (4.2). See text for details.

we discuss the results of the implementation of our scheme, in a proof-of-principle experiment. Finally, in Section 9.8 we draw our conclusions.

9.2 Protocol

Alice and Bob do not have access to a direct communication link. Instead they connect to a perfectly-in-the-middle relay via insecure quantum links, as shown in Fig. 9.1(a). The relay is untrusted, meaning that it is assumed to be operated by Eve in the worst case scenario.

The protocol proceeds as follows: Alice and Bob possess two modes, A and B, which are prepared in coherent states, $|\alpha\rangle$ and $|\beta\rangle$, with randomly-modulated amplitudes (according to a complex Gaussian distribution with large variance). They send these modes to the intermediate relay where the output modes, A' and B', are subject to a continuous-variable Bell detection [71]. This means that A' and B' are mixed on a balanced beam splitter and the output ports are conjugately homodyned: one output is homodyned in the $\hat{q}$-quadrature and gives the outcome q_-, while the other output port is homodyned in the $\hat{p}$-quadrature with outcome p_+. Compactly, the measurement provides the complex outcome

$$\gamma := \frac{q_- + ip_+}{\sqrt{2}} \tag{9.1}$$

which is then broadcast over a public channel.

To understand the working mechanism of the relay, first suppose there is no loss and noise in the links. In such a case, we have $\gamma \simeq \alpha - \beta^*$,. The public communication of γ creates *a posteriori* correlations between Alice's and Bob's variables, so that each party can easily infer the variable of the other. For instance, Alice could compute the quantity $\alpha - \gamma \simeq \beta^*$ recovering Bob's encoding β up to detection noise. This procedure partly recalls the post-processing of the two-way QKD protocols discussed in previous chapters.

Note that Eve's knowledge of variable γ would be of no help to extract information on the individual variables α and β, i.e., we have $I(\alpha : \gamma) = I(\beta : \gamma) = 0$ in terms of mutual information. By contrast, as a result of the broadcast of γ, the conditional mutual information of Alice and Bob becomes non-zero so we can write

$$I(\alpha : \beta|\gamma) > I(\alpha : \beta).$$

Thus, if Eve wants to steal information, she needs to introduce loss and noise.

Assuming a general eavesdropping, the action of Eve may involve a global unitary operation correlating all the uses of the protocols. However, using random permutations of their data [19, 20], Alice and Bob can always reduce this scenario to an attack which is coherent within the single use of protocol. This can be a joint attack of both the links and the relay. The parties can further reduce this eavesdropping to consider a coherent attack of the links only, assuming a properly-working relay, i.e., a relay implementing a continuous-variable Bell detection. In particular, since the protocol is based on the Gaussian modulation and Gaussian detection of Gaussian states, the optimal coherent attack of the links will be based on a Gaussian unitary interaction [11, 32, 31].

9.3 Description of the two-mode coherent attack

As we discussed in previous Chapters 4 and 6, the general scenario of coherent attacks can be reduced to a much simpler scenario where just two-mode Gaussian coherent attack, against the two quantum links, can be consider. We then have two entangling cloner combining Alice's and Bob's signals with ancillary modes E_1 and E_2 prepared in a correlated Gaussian state. As we are considering the symmetric configuration the parameters of the quantum channel, describing Eve's action on the quantum links, are identical so that the performances of the protocol are invariant under exchange of Alice and Bob. Adopting the entanglement based representation of the protocol, we can consider Alice's and Bob's ensembles of coherent states that are simulated using two EPR states subject to local heterodyne detections. We then have that Alice's and Bob's modes A and B are mixed with the ancillary modes, E_1 and E_2, respectively. This is done by two beam-splitters with the same transmissivity τ, and the ancillas belong to an environmental set $\{E_1, E_2, \mathbf{e}\}$ in the hands of Eve. The reduced state of E_1 and E_2 is the zero-mean Gaussian state $\sigma_{E_1E_2}$ discussed in Sec. 4.3.2, i.e., we have the same covariance matrix described by Eq. (4.2). The output modes, A' and B', are subject to the continuous-variable Bell detection (with the outcome broadcast), while Eve's output modes, E_1' and E_2', together with all the other ancillary modes $\mathbf{e}$ are stored in a quantum memory, which is detected by an optimal coherent measurement at the end of the protocol.

Note that in a general asymmetric configuration of the protocol, we may consider different transmissivities τ_A and τ_B, for the beam splitters, and an asymmetric CM with different thermal variances, ω_A and ω_B. This is the general asymmetric case

considered in Sec. 9.6. However, when the relay is midway between the two parties, the amount of loss and noise present in the links is realistically expected to be identical, and for this it is reasonable to consider here a symmetric attack as the one previously described, which has

$$\tau_A = \tau_B := \tau, \ \omega_A = \omega_B := \omega \ . \tag{9.2}$$

Exploiting this symmetry, we can reduce the number of parameters and derive a simple analytical expression for the secret-key rate, which allows us to perform a detailed analysis of the various specific symmetric attacks which are possible against our protocol. In particular, we can easily study the performances of these attacks in terms of the correlation parameters, g and g', and identify the optimal one which minimizes key rate and security threshold. Furthermore, due to the symmetry, Alice and Bob can be interchanged, which implies that there is no difference between direct and reverse reconciliation [11]. In other words, we can consider a unique secret-key rate for the protocol (assuming one-way classical communication for error correction and privacy amplification).

9.4 Secret-key rate

Without loss of generality, we assume that Alice is the encoder of information (variable α) while Bob is the decoder, so that he post-processes his variable β to infer α. In the EB-representation, these variables are informationally equivalent to the outcomes of the heterodyne detections. To derive the rate, we note that the Bell detection at the relay and the heterodyne detections of the two parties commute with each other. For this reason, we can equivalently compute the rate from the conditional state $\rho_{ab|\gamma}$ of modes a and b after the communication of the outcome γ. The rate is given by

$$R = I_{ab|\gamma} - I_{E|\gamma}, \tag{9.3}$$

where $I_{ab|\gamma}$ is Alice and Bob's conditional mutual information, while $I_{E|\gamma}$ is Eve's Holevo information [86] on Alice's variable (which can be computed from the state of the output ancillas).

Since all output modes are in a global pure state and the various detections are rank-1, we can apply safely the entanglement-based representation and write

$$I_{E|\gamma} = S(\rho_{ab|\gamma}) - S(\rho_{b|\gamma\alpha}), \tag{9.4}$$

where as usual the function $S(.)$ is the von Neumann entropy [86], now computed on the post-relay state $\rho_{ab|\gamma}$ of Alice and Bob, and the double-conditional state $\rho_{b|\gamma\alpha}$ of Bob, conditioned to relay's and Alice's detections (computable from $\rho_{ab|\gamma}$).

9.4.1 Computation of the key rate

Both the mutual information $I_{ab|\gamma}$ and Eve's Holevo entropy $I_{E|\gamma}$ can be computed from the post-relay state $\rho_{ab|\gamma}$, in particular, from its CM $\mathbf{V}_{ab|\gamma}$. Imposing the symmetry conditions of Eq. (9.2) in the general expression of $\mathbf{V}_{ab|\gamma}$ one obtains the

following post-relay covariance matrix

$$\mathbf{V}_{ab|\gamma} = \begin{pmatrix} \mu\mathbf{I} & \mathbf{0} \\ \mathbf{0} & \mu\mathbf{I} \end{pmatrix} - \frac{\tau(\mu^2-1)}{2}\times \times \begin{pmatrix} \frac{1}{\tau\mu+\lambda} & & -\frac{1}{\tau\mu+\lambda} & \\ & \frac{1}{\tau\mu+\lambda'} & & \frac{1}{\tau\mu+\lambda'} \\ -\frac{1}{\tau\mu+\lambda} & & \frac{1}{\tau\mu+\lambda} & \\ & \frac{1}{\tau\mu+\lambda'} & & \frac{1}{\tau\mu+\lambda'} \end{pmatrix}, \tag{9.5}$$

where

$$\lambda := (1-\tau)(\omega - g),\ \lambda' := (1-\tau)(\omega + g'). \tag{9.6}$$

Note that Eq. (9.5) represents a particular case of the general CM of Eq. (E.10), whose derivation is described in Appendix E, where non-unit quantum efficiencies of the detectors are also included.

Now, we can easily compute [11] the symplectic spectrum of eq.(9.5) in the limit of large modulation $\mu \gg 1$, obtaining

$$\nu_1 \to \sqrt{\frac{\lambda\mu}{\tau}}\ , \nu_2 \to \sqrt{\frac{\lambda'\mu}{\tau}}. \tag{9.7}$$

Then, entropy term $S(\rho_{ab|\gamma})$ in Eq. (9.4) can be computed to have

$$S(\rho_{ab|\gamma}) = h(\nu_1) + h(\nu_2) \to \log\frac{e^2}{4\tau}\sqrt{\lambda\lambda'}\mu. \tag{9.8}$$

To compute $S(\rho_{b|\gamma\alpha})$ we derive the double-conditional CM $\mathbf{V}_{b|\gamma\alpha}$. We put Eq. (9.5) in the block-form

$$\mathbf{V}_{ab|\gamma} = \begin{pmatrix} \mathbf{A} & \mathbf{C} \\ \mathbf{C}^T & \mathbf{B} \end{pmatrix}, \tag{9.9}$$

and we apply a partial Gaussian heterodyne measurement on Alice's remote mode a,given by [11, 87, 71],

$$\mathbf{V}_{b|\gamma\alpha} = \mathbf{B} - \mathbf{C}^T(\mathbf{A}+\mathbf{I})^{-1}\mathbf{C}, \tag{9.10}$$

which gives

$$\mathbf{V}_{b|\gamma\alpha} = \begin{pmatrix} \mu - \frac{(\mu^2-1)\tau}{\tau(\mu+1)+2\lambda} & 0 \\ 0 & \mu - \frac{(\mu^2-1)\tau}{\tau(\mu+1)+2\lambda'} \end{pmatrix}. \tag{9.11}$$

For $\mu \gg 1$, its symplectic eigenvalue is given by

$$\nu \to \frac{\sqrt{(\tau+2\lambda)(\tau+2\lambda')}}{\tau}, \tag{9.12}$$

and we have $S(\rho_{b|\gamma\alpha}) = h(\nu)$. We can then compute Eve's Holevo information, asymptotically given by

$$I_{E|\gamma} = \log_2\frac{e^2\sqrt{\lambda\lambda'}\mu}{4\tau} - h\left[\frac{\sqrt{(\tau+2\lambda)(\tau+2\lambda')}}{\tau}\right]. \tag{9.13}$$

Alice and Bob's conditional mutual information $I_{ab|\gamma}$ can be computed from the classical CM $\mathbf{V}(\alpha,\beta|\gamma) = (\mathbf{V}_{ab|\gamma} + \mathbf{I})/2$ describing their outcomes. After simple algebra, we get the asymptotic expression

$$I_{AB|\gamma} = \log_2\frac{\tau\mu}{4\sqrt{(\tau+\lambda)(\tau+\lambda')}}. \tag{9.14}$$

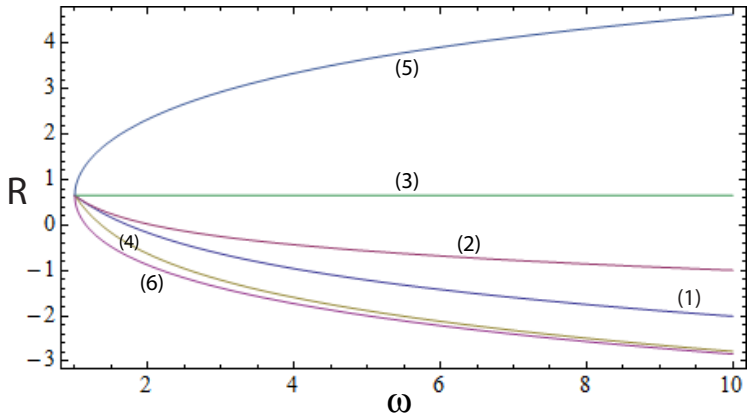

Figure 9.2: Secret-key rate R (bits) versus thermal noise ω for the various symmetric attacks (1)-(6) classified in Sec. 4.3.2 and displayed in Fig. 4.2. Link-transmissivity is set to $\tau = 0.9$. Note that the negative EPR attack (6) is the optimal attack minimizing the rate of the protocol.

As a result, we computed the following asymptotic secret-key rate for the symmetric Gaussian attack

$$R_{sym} = \log_2\left[\frac{\tau^2}{e^2\sqrt{\lambda\lambda'(\tau+\lambda)(\tau+\lambda')}}\right] + h\left[\frac{\sqrt{(\tau+2\lambda)(\tau+2\lambda')}}{\tau}\right], \tag{9.15}$$

which is function of the parameters τ, ω, g and g'.

A complete analysis of the performances of the scheme in presence of non-ideal experimental conditions is described in Appendix E.

9.5 Comparison between possible attacks

We now compare the performances of the previous attacks in Figs. 9.2 and 9.3. In Fig. 9.2 we fix the transmissivity $\tau = 0.9$ and we study the corresponding rates R as function of the thermal noise ω. In Fig. 9.3 we plot the security thresholds. These are given by the condition $R = 0$, and they are expressed in terms of maximum tolerable thermal noise versus transmissivity $\omega = \omega(\tau)$.

Our analysis identifies "good" and "bad" entanglement for the security of the protocol. Good entanglement refers to the entangled attacks in the bottom right area of Fig. 4.2, with $g = -g' > 0$, of which the attacks (3) and (5) are border points. This entanglement is good because it injects correlations of the type $\hat{q}_{E_1} \approx \hat{q}_{E_2}$ and $\hat{p}_{E_1} \approx -\hat{p}_{E_2}$, therefore helping the Bell detection (which projects on $\hat{q}_{A'} \approx \hat{q}_{B'}$ and $\hat{p}_{A'} \approx -\hat{p}_{B'}$). As a result, Eve actively helps the key distribution.

This is evident from the performance of the positive EPR attack (5) both in terms of rate (Fig. 9.2) and security threshold (Fig. 9.3). In fact, from Fig. 9.2, we see that the rate is *increasing* in the thermal noise ω and, in Fig. 9.3, we see a peculiar inversion of the security threshold so that thermal noise *above* the threshold is tolerable. These features are typical of all entangled attacks with $\omega - 1 < g \leq \sqrt{\omega^2 - 1}$

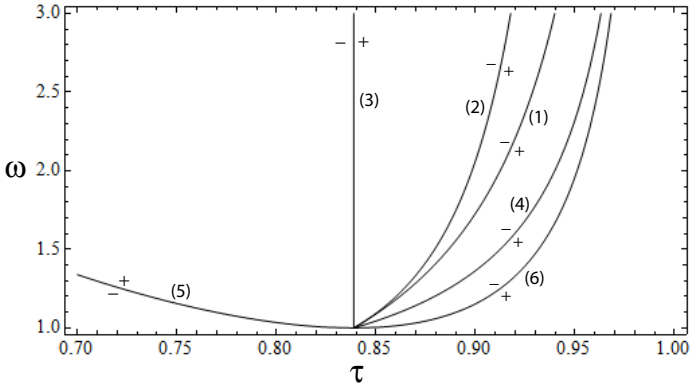

Figure 9.3: Security threshold ($R = 0$) expressed as maximum tolerable thermal noise ω versus link-transmissivity τ. We compare the various symmetric attacks (1)-(6) classified in Sec. 4.3.2 and displayed in Fig. 4.2. The negative EPR attack (6) is the optimal corresponding to the lowest security threshold. Also note the peculiar inversion of the threshold for the positive EPR attack (5), for which the rate is positive for values of thermal noise *above* the threshold.

and $g' = -g$, corresponding to the segment of points between (3) (excluded) and (5) (included). In Figs. 9.2 and 9.3, these attacks have curves which are intermediate between those of (3) and (5).

By contrast, bad entanglement refers to the entangled attacks in the top left area of Fig. 4.2, with $g = -g' < 0$ and having the attacks (4) and (6) as border points. This entanglement is instead bad because it injects correlations of the type $\hat{q}_{E_1} \approx -\hat{q}_{E_2}$ and $\hat{p}_{E_1} \approx \hat{p}_{E_2}$, which are opposite to those established by the Bell detection. In this case, Eve decreases the correlations between Alice's and Bob's variables, and she is able to eavesdrop more information, with the optimal strategy achieved by the negative EPR attack (6) as clear from the rates of Fig. 9.2 and the security thresholds of Fig. 9.3. The asymmetric version of this attack is optimal in case of asymmetric setups, as has been proved in general in [17], and we will give a brief discussion in the next section.

By comparing the curves (6) and (1) in Figs. 9.2 and 9.3, we clearly see the substantial advantage given by this optimal attack with respect to the standard collective attack based on independent entangling cloners. Analytically, the minimum key rate associated with the optimal attack is given by

$$R_{\min} = h\left(\frac{\tau + 2\lambda_{\text{opt}}}{\tau}\right) + \log_2\left[\frac{\tau^2}{e^2\lambda_{\text{opt}}(\tau + \lambda_{\text{opt}})}\right], \tag{9.16}$$

with $\lambda_{\text{opt}} = (1-\tau)(\omega + \sqrt{\omega^2 - 1})$. One can easily check this is numerically much less than the rate of the collective attack

$$R_{\text{coll}} = h\left[\frac{\tau + 2(1-\tau)\omega}{\tau}\right] + \log_2\left\{\frac{\tau^2}{e^2(1-\tau)[\tau + (1-\tau)\omega]\omega}\right\}.$$

Thus, the security analysis which is valid for one-way continuous-variable QKD protocols [11], and based on the study of collective (single-mode) entangling-cloner attacks, cannot be applied to our relay-based protocol. For this reason, we remark here that the recent studies, provided by Refs. [84, 85], are incomplete and cannot

prove the unconditional security of the relay-based (measurement-device independent) QKD with continuous variables.

9.6 Optimal configuration of the relay

The optimal implementation of the relay is asymmetric. This means that to achieve the maximal performance of the protocol, we have the consider one of the parties in proximity of the relay. This, of course, requires to consider an asymmetric attack, where the parameters of the attack on the link to the relay (transmissivity and thermal noise injected by Eve) are different and defined τ_A, ω_A for Alice's and τ_B, ω_B for Bob's link. The reduced state $\sigma_{E_1E_2}$ describing this general attack is then described by a zero mean thermal state with covariance matrix

$$\mathbf{V}_{E_1E_2} = \begin{pmatrix} \omega_A\mathbf{I} & \mathbf{G} \\ \mathbf{G} & \omega_B\mathbf{I} \end{pmatrix}, \text{with } \mathbf{G} \coloneqq \begin{pmatrix} g & 0 \\ 0 & g' \end{pmatrix}, \tag{9.17}$$

where $\omega_A, \omega_B \geq 1$.

In the same way that for the symmetric case, Alice is the encoder and Bob is the decoder. We then have that the variable α, inferred by processing β, can be obtained considering the following optimal estimator using the broadcast relay's variable

$$\gamma \simeq \sqrt{\tau_A}\alpha - \sqrt{\tau_B}\beta^*,$$

as described in Fig. 9.1. The empirical values of the transmissivities τ_A and τ_B are in fact accessible to the parties from the first-order moments of the probability distribution $p(\alpha, \beta, \gamma)$, that describes the global system. Then, from the second-order moments of $p(\alpha, \beta, \gamma)$, Alice and Bob can derive their mutual information

$$I_{AB} = \log_2(\varphi\chi_{AS}^{-1}), \tag{9.18}$$

where χ_{AS} is the equivalent noise, decomposable as

$$\chi_{AS} = \chi_{\text{loss}} + \varepsilon,$$

with $\chi_{\text{loss}}(\tau_A, \tau_B)$ being the pure-loss noise and $\varepsilon(\tau_A, \tau_B, \omega_A, \omega_B, g, g')$ the 'excess noise'. From the second-order moments, the remote parties can also compute the secret-key rate $R_{\varphi,\xi}(\tau_A, \tau_B, \varepsilon)$ which depends on the modulation φ and the reconciliation efficiency ξ , besides the main parameters of the attack, i.e., transmissivities, τ_A and τ_B, and excess noise ε.

Assuming the asymptotic limit of large modulation $\varphi \gg 1$ and ideal reconciliation $\xi = 1$, we found the following key-rate

$$R(\tau_A, \tau_B, \varepsilon) = \log_2\left[\frac{2(\tau_A+\tau_B)}{e|\tau_A-\tau_B|\chi}\right] + h\left[\frac{\tau_A\chi}{\tau_A+\tau_B} - 1\right] - h\left[\frac{\tau_A\tau_B\chi-(\tau_A+\tau_B)^2}{|\tau_A-\tau_B|(\tau_A+\tau_B)}\right], \tag{9.19}$$

where $\chi = \chi(\tau_A, \tau_B, \varepsilon) \coloneqq 2(\tau_A + \tau_B)/\tau_A\tau_B + \varepsilon$. The behavior of this ideal rate is plotted in Fig. 9.4.

As we can see from Fig. 9.4, extremely high rates ($\simeq$ 1bit/use) can theoretically be achieved by our protocol. The symmetric configurations $\tau_A \simeq \tau_B$ studied in previous section, are not the best solution, since they are secure only for transmissivity > 0.84, as we can see from the thresholds plotted in Fig. 9.3, and corresponding to links < 3.8 km in standard fibres (0.2dB/km). The optimal configuration is asymmetric

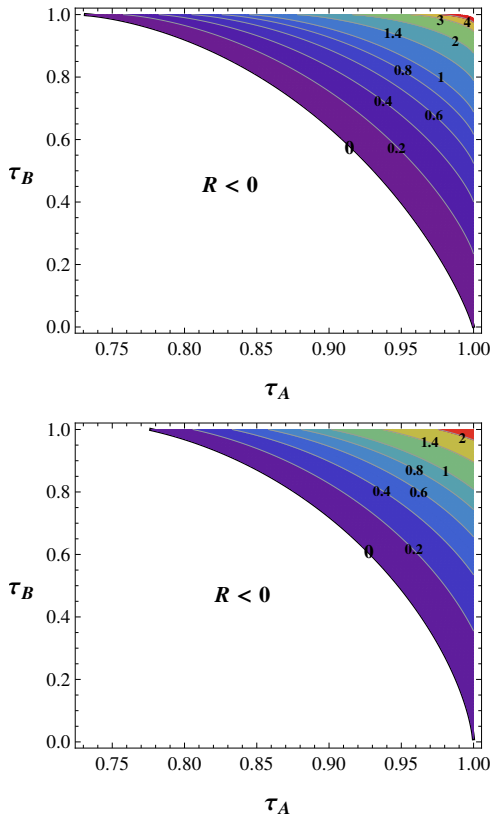

Figure 9.4: Ideal rate $R(\tau_A, \tau_B, \varepsilon)$ in terms of the links' transmissivities τ_A and τ_B, in the pure-loss case ($\varepsilon = 0$, top panel) and non-zero excess noise ($\varepsilon = 0.1$, bottom panel). We can see that, when Alice's link has small loss ($\tau_A \gtrsim 0.9$), Bob's link can become very lossy (up to $\tau_B \simeq 0$).

and corresponds to small loss in Alice's link, in which case the transmissivity of Bob's link can be close to zero. These features are robust to the presence of excess noise, for instance at $\varepsilon = 0.1$, which is higher than the typical values appearing in experiments ($\varepsilon \lesssim 0.008$ in Ref. [14]).

The asymmetry of our protocol comes from the term $h\left[\tau_A \chi (\tau_A + \tau_B)^{-1} - 1\right]$ in Eq. (9.19), which is clearly asymmetric in the transmissivities. Physically, it comes from the difference between direct and reverse reconciliation in continuous variable QKD. In fact, if one link is loss-less, the Bell detection is done locally and our scheme reduces to a point-to-point protocol in direct reconciliation (for $\tau_B = 1$) or reverse reconciliation (for $\tau_A = 1$). See Supplementary Information for details.

9.7 Experimental implementation

We tested our theory in a proof-of-principle experiment in the free-space setup depicted in Fig. 9.5. We have reproduced the asymmetric configuration where Alice's transmissivity τ_A is sufficiently high (Alice close to the relay), while Bob's transmissivity τ_B has been progressively decreased to simulate the increasing distance of Bob from the relay. In particular, we have simulated four different scenarios for Alice: (i) the ideal limit condition where Alice-relay global transmissivity is set to unity, $\tau_A = 1$, in which case we assumed also ideal detection efficiency at the relay. This case, despite being unrealistic allows to explore the ideal limit of the scheme;

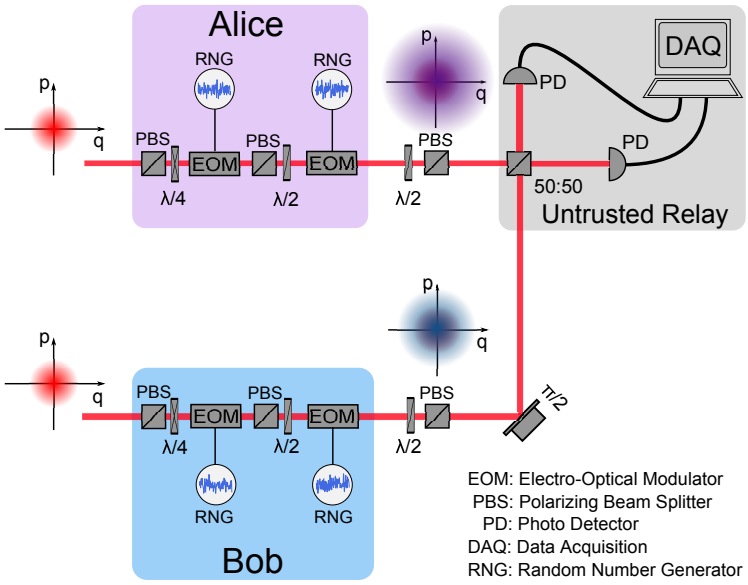

Figure 9.5: Free-space experimental setup. Alice and Bob apply amplitude and phase modulators to a pair of identical classical phase-locked bright coherent beams (coming from a common local oscillator at 1064nm). Alice's and Bob's stations are private spaces whose internal noise is trusted. This feature allows us to neglect unwanted internal loss and set the signal levels at the output of the stations. From these stations, the modes emerge randomly-displaced in the phase space according to a Gaussian distribution with high modulation variance $\varphi \simeq 60$. Losses in the links are simulated by suitably attenuating the variances of the modulations. At the relay, the modes are mixed in a balanced beam splitter and the output ports photo-detected. Photocurrents are finally processed to realize a continuous-variable Bell measurement.

(ii) Alice connected to the relay by a short free-space link, so that her loss are only due to the global detection efficiency at the relay ($\tau_A \simeq 0.98$); (iii) Alice connected to the relay at an equivalent distance of 100m in standard fiber ($\tau_A \simeq 0.975$); and (iv) Alice at an equivalent distance of 1km in standard fiber ($\tau_A \simeq 0.935$). For every experimental point, we have evaluated the second-order moments of $p(\alpha, \beta, \gamma)$ and computed the experimental key rate R, assuming different values of the reconciliation efficiency: $\xi = 1$ (ideal), $\xi \simeq 0.97$ (currently achievable [14]) and $\xi \simeq 0.95$.

Experimental results are plotted in Fig. 9.6 and compared with theoretical predictions. Assuming ideal reconciliation ($\xi = 1$), the extrapolated experimental rate is not far from the theoretical rate of a pure-loss attack $R_{\varphi\simeq 60,\xi=1}(\tau_A, \tau_B, 0)$, which provides the maximum performance achievable at the considered links' transmissivities. It is important to note that, due to inevitable experimental imperfections, there is some excess noise $\varepsilon \simeq 0.01$ entering our data, which is assumed to come from a two-mode Gaussian attack in our experiment.

Considering realistic reconciliation performances, the experimental rates are not far from the maximum theoretical predictions. In particular, for $\xi \simeq 0.97$, the experimental rate can reach remarkably high rates over typical connection lengths of a public network. For instance, if Alice connects to a public hot spot via a free-space link, she can distill $R \simeq 10^{-2}$ secret bits per relay use with Bob being 25km far in standard fiber (distance equivalent of 5dB loss). Similarly, if Alice connects to a

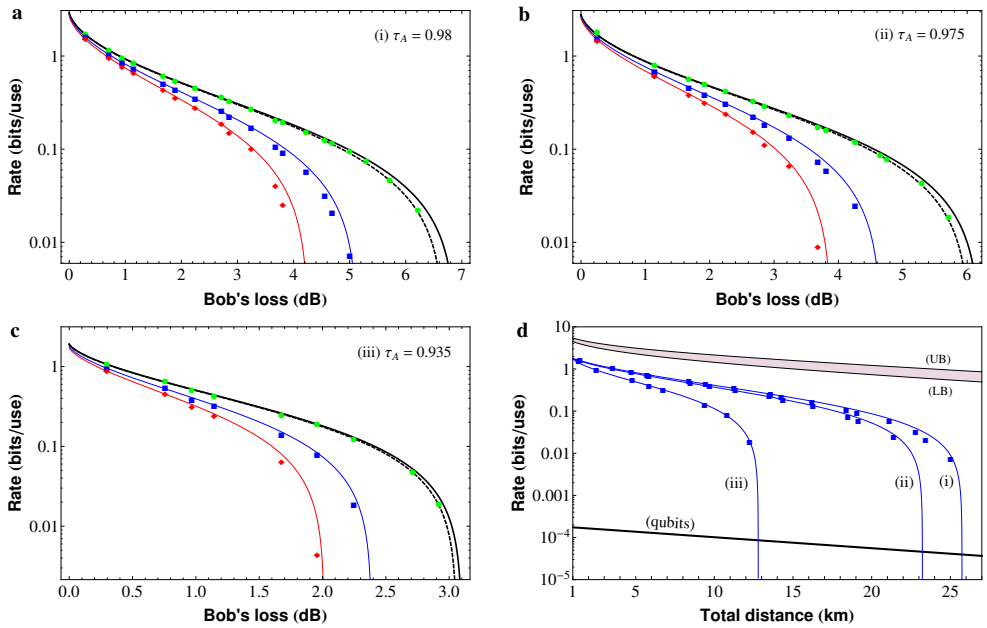

Figure 9.6: Panel **(a)**, **(b)** and **(a)** show the secret-key rate R (bits/use) versus Bob's loss (dB) for different loss in Alice's link $\tau_A \simeq 0.98$ **(a)**, 0.975 **(b)** and 0.935 **(c)**. In each panel, experimental points refer to ideal reconciliation ($\xi = 1$, green circles), achievable reconciliation ($\xi \simeq 0.97$, blue squares) and lower reconciliation ($\xi \simeq 0.95$, red diamonds). In each panel we also plot the theoretical rate $R_{\varphi,\xi}(\tau_A, \tau_B, \varepsilon)$ with $\varphi \simeq 60$. For ideal reconciliation ($\xi = 1$) we show both pure-loss $\varepsilon = 0$ (solid black line) and excess noise $\varepsilon \simeq 0.01$ (dashed black line). Then, we plot the pure-loss rate for realistic reconciliation efficiencies $\xi \simeq 0.97$ (blue line) and $\xi \simeq 0.95$ (red line). The pure-loss theoretical rates represent the maximum performances achievable at the considered links' transmissivities. Finally in panel **(d)** we show the secret key rate versus the total distance between Alice and Bob in simulated fibre. Experimental key rates ($\xi \simeq 0.97$, blue squares) for the three configurations (i) to (iii) are compared with the rate achievable by MDI-QKD with qubits [75] (thick solid line) and the secret key capacity of a direct fibre link between Alice and Bob, which lies between the lower bound (LB) of ref. [63] and the upper bound (UB) of ref. 45. At metropolitan distances, we outperform qubit-based protocols by (at least) three orders of magnitude, missing the secret key capacity by approximately one order of magnitude.

network router using a 100m fiber (as it may happen within a building), then she can distill $\gtrsim 10^{-2}$ bits/use with Bob being at 21km in fiber. If Alice is 1km far (as it may happen in a metropolitan fiber-optic network), then she extracts $\gtrsim 10^{-2}$ bits/use with Bob being at 11km.

These experimental rates are three orders of magnitude higher than those achievable with discrete-variable protocols over comparable medium-range distances, for which one has $\simeq 10^{-5}$ bits/use at $\simeq$ 25km [88, 89, 90]. For instance, implementing our protocol with a 75MHz clock rate over $\simeq$ 25km would provide a key rate of about 0.7Mbit/s, which is remarkably higher than the $\simeq$ 100bit/s achievable by the most recent qubit-based experiment [90]. We are therefore able to achieve the high-rate performances of continuous variable QKD despite the fact we are removing any direct connection between the remote parties.

9.8 Conclusion

This chapter described the theory and the experimental implementation of continuous-variable quantum cryptography in a network configuration, where two end-users do not access a direct quantum communication channel, but are forced to connect to an untrusted relay via insecure quantum links. We proved that, despite assuming a full corruption of the intermediate station and the optimal coherent eavesdropping of its links with the parties, the end-users can still extract a secret key.

An important feature of the study described is the simplicity of the relay, which does not possess any quantum source but just performs a standard optical measurement, with all the heavy procedures of data post-processing left to the end-users, fulfilling the idea behind the end-to-end principle. In particular, the relay implements a continuous-variable Bell detection which involves highly efficient photodetectors plus linear optics, whereas the discrete-variable version of this measurement needs nonlinear elements to operate deterministically. This feature combined with the use of coherent states makes the scheme very attractive, guaranteeing both cheap implementation and high rates.

We have found that the optimal eavesdropping is a two-mode coherent attack where Eve injects correlated ancillas, sharing "negative WPE-correlations". The optimal configuration of the network, with the untrusted relay acting as a proxy server near to one of the parties. In this case we have experimentally proven that remarkable rates can be reached, several orders of magnitude higher than those achievable with qubit-based protocols over comparable distances. From this point of view, our protocol can already be used for setting up very efficient star networks based on public access points.

The results described could be useful also to reduce the complexity of the implementation of future quantum networks, for instance decomposing any chain between two end-users into trusted nodes alternated by untrusted relays. We may consider chains like Alice-relay1-Charlie1-relay2-Charlie2-relay3-Bob, where only the Charlies are trusted nodes. This would reduce, proportionally to the number of Charlies implemented, the number of temporary keys to be distributed.

Chapter 10

Conclusions, further work and outlook

In this thesis, we developed a comprehensive study of the unconditional security of quantum cryptography implemented with quantum continuous variables. In order to achieve this goal we considered the two possible architectures by which quantum cryptography can be implemented: point-to-point and end-to-end. In both cases we performed a detailed analysis of the eavesdropping. We accomplished, for the first time, an explicit study of the performances of CV-QKD under coherent attacks (two-mode coherent). To achieve this goal we generally worked in the asymptotic limit, that allows to fully exploit the result of the quantum de Finetti theorem in order to reduce the general attack to simpler scenarios. A pivotal element of our study has been the explicit analysis of Gaussian quantum channels with memory described, in particular, by the CM of the form

$$\begin{pmatrix} \omega\mathbf{I} & \mathbf{G} \\ \mathbf{G} & \omega\mathbf{I} \end{pmatrix}, \text{ with } \mathbf{G} = \begin{pmatrix} g & 0 \\ 0 & g' \end{pmatrix}, \tag{10.1}$$

where the parameters ω and g, g' quantify, respectively, the energy (ω) of the ancillary states used by Eve during the eavesdropping, and g, g' the nature and degree of their correlations.

Using this approach we have been able to propose a novel, and general, security analysis for point-to-point protocols. In particular, for the one-way schemes we proved that Gaussian coherent attack are not equivalent to collective ones. We have explicitly proven that a simple classical post-processing applied on the exchanged signals, the secret-key rate under coherent attack is always strictly higher than that obtain if Eve apply just collective attacks. This motivated us to conjecture that, for point-to-point one-way protocols, the use of the de Finetti symmetrization could be avoided [91].

Studying two-way communication protocols under general coherent attack, we have identified the optimal eavesdropping that is a two-mode coherent attack with separable correlations. We proposed the effective counteraction to this case, and proved that two-way communication are immune to coherent attacks [67, 92].

In the framework of end-to-end architecture, we performed a detailed general analysis of CV-MDI protocol with coherent states, providing also the proof-of-principle experimental test of our theory. Our study open the possibility of implementing high-rate secure communication, at the metropolitan scale, in a network communication, exploiting extremely simple operation and cheap technologies.

10.1 Future work and Outlook

The work presented in this thesis beside providing several general important and novel results, in the context of unconditional security of CV-QKD, is open to several improvements of which it is worth to mention the possible developments.

The recent bounds for the secret-key capacity found in Ref. [63] and [16], suggest that for what it concerns long distance quantum cryptography it is necessary to work to refine the present limitation connected with technological imperfections. I would then divide the main challenges into two main class: a first including all the work to be done to improve the performances of error correction and the tolerance of the protocols to finite size effects. A second, maybe at a more fundamental level, where relay-based communication are exploited and in particular composable security proofs have to be developed. The research activity in this respect is quite recent and we think there should be vast rooms for improvements.

10.1.1 Finite-size effects and development of more efficient classical error correction codes

The main bottleneck limiting the present, in-field, implementations of CV-QKD, is that for Alice and Bob is in practice very difficult to extract efficiently all the information available by the encoding performed by the Gaussian modulation of quantum continuous variables. To overcome this problem it will be necessary to develop more efficient classical error correction codes. At present they have been implemented, with limited efficiency of 95% in real time QKD experiments (see Ref. [14]), and with a state-of-the-art performance of 97% [13]. This error correction protocols are generally implemented using Low-Density-Parity-Check (LDPC) coding. The Gaussian variables are then mapped into a binary input additive white Gaussian noise channel (BIAWGNC), for which the efficiency are high, but at a high signal-to-noise ratio, and at the price of very large size of the block of signals used. In practice this means that a large portion of the signals exchanged by the parties have to be used for the classical error correction and reconciliation procedures. It could be interesting to explore the possibility of using TURBO codes [95] to implement the classical communication steps of QKD protocols. The performances of these codes are close to the channel capacity, and moreover have recently also found application in 3G/4G communications. They appear indeed very promising also for the interfacing with existing Wi-Fi technologies.

In fact, we think that even an improvement by a small 1% or 2%, in the efficiency of the classical reconciliation codes, could have a remarkable effects on the rate and achievable distance at which it is possible to share a secret-key. In fact present experimental implementations of CV-QKD must use an optimal modulation in order to limit the detrimental effects of this non-ideal efficiency [93, 94]. We think that work on the aspects related with the classical coding will be one of the main research field on which the community working on CV-QKD should focus its efforts.

Further research in point-to-point architectures, for example in one-way communication, could be focused on the explicit cryptanalysis of multi-mode coherent attack. Right now we proved that the case where the exchanged signals are packed into two-mode blocks is analytically solvable, and that this allows to reduce the call to the quantum de Finetti theorem to one half of the total N uses of the communication channel. Solve the general problem of packing the signals in larger blocks, would provide an explicit proof of the validity of our conjecture that Gaussian CV-

QKD does not need de Finetti symmetrization to achieve unconditional security. The main difficulty dealing with the general case, is that increasing the number of signals that compose the blocks, we have to perform the analysis of a much more complex coherent-attack scenario, whose characterization is likely to need heavy numerical analysis.

10.1.2 Multi-way point-to-point communication

Now that we have a better picture of the optimal attacks for one and two-way protocol, we think that it worth to explore the possibility and performances of multi-way communication schemes (not just two-way), where also multi-mode-coherent attack should be considered. As in this case we need to analyze multi-mode-coherent attacks, research in this sense could be useful both to provide a complete picture of point-to-point communications and, as said in previous section, to extend the validity of our conjecture on the inequivalence between collective and coherent attacks described in Chapter 4 [91].

For what it concerns the experimental implementations of CV-QKD, it would be interesting to test the two-way communication protocol. In this respect our group is already actively involved in the realization of such experimental test, in collaboration with Andersen's group at the Danish Technical University (DTU). This will be the first implementation of a two-way CV protocol and is expected to prove the advantage of using the double communication in noisy environments, in order to allow the sharing of a usable secret-key when the level of noise on the channel prevent the use of one-way protocol.

Finally, we think that a very hot research topic will be to achieve a security proof of CV protocols based on coherent states, against general attacks and in the composable security framework. This has been introduced in QKD very recently by Ref.[96] for DV, and represents the ultimate security analysis of a QKD protocol. In this general perspective, the performances of a scheme are evaluated considering the ability of sharing secret-bit in the limit of infinite signals, and also the probability of correctness when we consider a finite number of signals exchanged. In fact the proof techniques recently developed for CV-QKD [97], have been effective to proof composable security only for CV protocols based on squeezed states. According to this work, when we deal with coherent state protocols, the size of the block-signals needed to achieve security is impractically large. On the other hand we believe that this fast convergence obtained for squeezed-state protocols, suggests that a similar result may be possible, possibly with proof techniques to be discovered, also for coherent-state protocols.

10.1.3 End-to-end multiple-nodes networks and composable security of CV-MDI QKD

For what it concerns end-to-end QKD, a natural extension of our protocol will be to consider more complex and general network structures, starting with a star-network configuration. We think that this will be one of our main research topics.

Coherently with what said in previous section, we think that our efforts will be also focused on the study of CV MDI-QKD in the composable security framework. For DV-MDI QKD a proof of the composable security of the protocols has been developed in Ref. [98]. This analysis seems to be very demanding for DV MDI

QKD, in terms of the size of the signals-blocks to use to successfully accomplish error correction (10^{12} signals).

An interesting future challenge for the theoretical research in CV-QKD will then be to extend and complete the study of Ref. [97], in particular for the end-to-end architectures and then generalise the results to the most general network topology as possible.

Appendix A

Source purification: details

Let us consider Alice preparing a two-mode vacuum squeezed state (EPR pairs), described by the field's quadratures (q',p') and (q,p) as illustrated in figure 2.2 in Part I of this thesis. The local mode (q',p') is measured by Alice, while the other is sent to Bob through a quantum channel. These two modes have a symmetrically distributed uncertainty on the two quadratures, described by the following relation,

$$\langle q^2 \rangle = \langle q'^2 \rangle = \mu N_0, \tag{A.1}$$

$$\langle p^2 \rangle = \langle p'^2 \rangle = \mu N_0, \tag{A.2}$$

where μ is the variance of the classical Gaussian modulation, and $N_0 = 1$ is the variance of the vacuum shot-noise. Measuring mode (q', p'), Alice obtain the pairs (q'_A, p'_A), that in general will differ from the true prepared quadratures (q',p'), so that we can write the following relations

$$\delta q'_A = q' - q'_A, \tag{A.3}$$

$$\delta p'_A = p' - p'_A. \tag{A.4}$$

From this equations, we see that q' and q'_A have the same commutation relation $[q', p'] = 2i$, so we can write the same uncertainty relation for the measured quadratures,

$$\langle \delta q'^2_A \rangle \langle \delta p'^2_A \rangle \geq N_0^2, \tag{A.5}$$

with previous inequality saturated when the prepared quantum state is coherent. In case Alice encoding is performed on squeezed states, we can parameterize the previous errors on the measured quadratures writing,

$$\langle \delta q'^2_A \rangle = \eta N_0, \text{ and } \langle \delta p'^2_A \rangle = \frac{N_0}{\eta}, \tag{A.6}$$

where $\eta = (1-\tau_A)/\tau_A$ is a parameter depending on the transmissivity τ_A of the beam splitter adopted to modulate the measurement procedure between the homodyne $(\tau_A = 1)$ and the heterodyne $(\tau_A = 1/2)$ detection schemes.

To quantify the conditional variances of the quantum states sent to Bob, $V_{q|q_\alpha}$ and $V_{p|p_\alpha}$, conditioned to the result of the measurement performed by Alice. One can observe that the measured values q_A of the quadrature q can be estimated by means of the values q'_A obtained by Alice,

$$q_A = \alpha q'_A, \tag{A.7}$$

where the expression of the α coefficient can be derived first evaluating the difference,

$$\delta q_A = q - \alpha q'_A, \tag{A.8}$$

where the label A is to underline that the value of q is conditioned to the measurement performed by Alice. We can calculate its variance,

$$\langle \delta q_A^2 \rangle = \langle q^2 \rangle + \alpha^2 \langle q_A'^2 \rangle - 2\alpha \langle q q'_A \rangle. \tag{A.9}$$

deriving with respect α and equating to zero to minimize. We obtain

$$\alpha = \frac{\langle q q'_A \rangle}{\langle q_A'^2 \rangle} \tag{A.10}$$

and the variance of the variable q, conditioned to the measurement of Alice is

$$\langle \delta q_A^2 \rangle = \langle q^2 \rangle - \frac{\langle q q'_A \rangle^2}{\langle q_A'^2 \rangle}. \tag{A.11}$$

Now we can calculate the previous equation considering that $q'_A = q - \delta q'_A$ and recalling that $\langle q^2 \rangle = N_0 V$ and $\delta q'_A = \eta N_0$,$\delta p'_A = N_0/\eta$ we obtain the following relations

$$V_{q|q_A} = \langle \delta q_A^2 \rangle = \frac{\eta V + 1}{V + \eta} \tag{A.12}$$

$$V_{p|p_A} = \langle \delta p_A^2 \rangle = \frac{V + \eta}{V\eta + 1}. \tag{A.13}$$

Depending on the values assumed by the transmissivity T we have different encodings. For example:

- in the case $\tau \to 1$, $\eta \to 0$ Alice gets information only on the $\hat{q}$ quadrature, so sending $\hat{q}$–squeezed states, $V_{q|q_A} = N_0/V$.
- For $\tau = 1/2$ Alice encodes coherent states, because the indetermination is equally shared between the two quadratures.
- Finally, if $\tau \to 0$, $\eta \to \infty$, and Alice will encode $\hat{p}$–squeezed states with variance $V_{p|p_A} = N_0/V$,

after normalizing with respect the shot-noise N_0.

Appendix B

One-way protocols against coherent attacks

B.1 Total covariance matrix

Let $\mathbf{X} = (q_X, p_X)$ be the vectorial quadratures operators describing a general mode X. The impact of the attenuation on the signal modes A and A' traveling through the communication channel, is obtained by the Bogoliubov equations, where two identical beam splitters of transmissivity τ simulate the loss on the channel. The amplitudes of the processed signal modes, are given by the following expressions

$$\mathbf{B} = \sqrt{\tau}\mathbf{A} + \sqrt{1-\tau}\mathbf{e}, \tag{B.1}$$

$$\mathbf{B}' = \sqrt{\tau}\mathbf{A}' + \sqrt{1-\tau}\mathbf{E}, \tag{B.2}$$

where **e, E** are the vectorial quadrature operators describing Eve's ancillary modes, mixed at the beam splitters with modes A and A', respectively. We order Alice-Bob modes as follows a, a', B, B', and we use Eq. (B.1) and (B.2) to compute the CM describing the Alice-Bob total state $\rho_{aa'BB'}$. It is simple to arrive at the following expression

$$\mathbf{V}_{tot} = \begin{pmatrix} (\mu+1)\mathbf{I} & & \Phi\mathbf{Z} & \\ & (\mu+1)\mathbf{I} & & \Phi\mathbf{Z} \\ \Phi\mathbf{Z} & & \Lambda\mathbf{I} & (1-\tau)\mathbf{G} \\ & \Phi\mathbf{Z} & (1-\tau)\mathbf{G} & \Lambda\mathbf{I} \end{pmatrix}, \tag{B.3}$$

where μ is the classical Gaussian modulation, we defined

$$\begin{aligned} \Lambda &= \tau(\mu+1) + (1-\tau)\omega, \\ \Phi &= \sqrt{\tau[(\mu+1)^2 - 1]}, \end{aligned} \tag{B.4}$$

and $\mathbf{G}$ is given by Eq. (4.2) with its matrix elements g, g' fulfilling the constraints of Eq. (4.3) and (4.4) in order to describe a physical attack.

B.2 Alice-Bob mutual information

In order to describe the information shared between the parties, we start from the following general signal-to-noise relation

$$I := \frac{1}{2}\log\frac{signal}{noise},$$

that describes the information content per quadrature, $\hat{q}$ and $\hat{p}$, used in the protocol. In practice this general formula accounts for the ratio between the signals sent through the channel and the noise added by the channel. We then note that for each use of the two-mode block, the parties share twice the signal exchanged per single use of the one-way communication. If we assume for simplicity that the variances relative to the quadratures of Bob's modes, B and B', are identical and given by Eq. (8.3), we have the following relations

$$signal := V_B = \tau(\mu + 1) + (1 - \tau)\omega = \Lambda, \tag{B.5}$$

$$noise := V_{B|\alpha,\alpha'} = \tau + (1 - \tau)\omega =, \tag{B.6}$$

where the conditional variances $V_{B|\alpha}$ and $V_{B|\alpha'}$ can be obtained from V_B, by collapsing the classical Gaussian modulation $\varphi \to 0$, to simulate Bob's gain of knowledge on Alice's variables. In the no-switching protocol the receiver performs heterodyne detections, measuring both quadratures $\hat{q}$ and $\hat{p}$, at the outputs of a balanced beam splitter. In order to include the contribution from the vacuum shot-noise, and the double use of the channel within each block, the total mutual information is given by the following expression

$$\begin{aligned} I := I + I' &:= 2\left(\frac{1}{2}\log\frac{V_{Bob}+1}{V_{Bob|\alpha,\alpha'}} + \frac{1}{2}\log\frac{V_{Bob}+1}{V_{Bob|\alpha,\alpha'}}\right) = \\ &= 2\log\frac{V_{Bob}+1}{V_{Bob|\alpha,\alpha'}}. \end{aligned}$$

From this relation, using Eq. (B.5) and Eq. (B.6) and taking the limit of large modulation ($\mu \gg 1$), one gets the asymptotic mutual information of Eq. (4.10)

$$\begin{aligned} I_{AB} &= 2\log_2\frac{\tau\mu + (1-\tau)\omega + 1}{1 + \tau + (1-\tau)\omega} \\ &\to 2\log_2\frac{\tau\mu}{1 + \tau + (1-\tau)\omega}. \end{aligned} \tag{B.7}$$

B.3 Holevo bound

The dilation of the two-mode channel allows us to describe the joint Alice-Bob-Eve quantum state as a pure. Now, we note that this quantum state is always processed by rank 1 operations (beam splitters and homodyne detections), that preserve its purity through the evolution and detection. The assumption of working in the limit of a very large number of signals exchanged ($N >> 1$) between the parties, and the fact that we are assuming that Eve is computationally unbounded, authorize also to use the Holevo bound, χ, to quantify the accessible information I_E describing the correlation of Eve with Bob. This bound can be explicitly obtained from the knowledge of Alice-Bob total state, $\rho_{aa'BB'}$, and from the conditional one, $\rho_{aa'|\beta\beta'}$. In fact when Eve perform the optimized measurement of her quantum memory, she automatically traced out herself from the global pure state ρ_{ABE}. We have indeed that Alice-Bob joint state, ρ_{AB}, provides the same entropic information of ρ_E. The Holevo bound is then given by the following relation

$$\chi = S(\rho_{aa'BB'}) - S(\rho_{aa'BB'|\beta\beta'}), \tag{B.8}$$

where $S(.)$ is the von Neumann entropy.

We need the function χ, in terms of the relevant parameters of the protocol τ, ω, g, g'. We then compute the symplectic spectrum of the total CM given by Eq. (B.3), from the absolute value of the eigenvalues of matrix

$$\mathbf{M} = i\mathbf{\Omega}\mathbf{V}_{tot}, \tag{B.9}$$

where $\mathbf{\Omega} = \oplus_{k=1}^{4}\omega_k$ is the 8×8 (four modes) symplectic form [11], and $\omega_k = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}$. For large μ, one easily obtains the following expressions

$$\nu_+ = \sqrt{(\omega + g)(\omega + g')}, \tag{B.10}$$

$$\nu_- = \sqrt{(\omega - g)(\omega - g')}, \tag{B.11}$$

$$\{\nu_1, \nu_2\} = \{(1-\tau)\mu, (1-\tau)\mu\}, \tag{B.12}$$

that together with the definition $S = \sum_x h(x)$ and Eq. (4.11) can now be used to get the expression for Eve's total von Neumann entropy, given by the following formula

$$S_E = h(\nu_+) + h(\nu_-) + \log\frac{e^2}{4}(1-\tau)^2\mu^2. \tag{B.13}$$

The conditional state, described by the conditional CM, can be obtained after Bob's heterodyne detections on modes B and B' of CM of Eq. (B.3). We arrange the total CM V_{tot} in the canonical form

$$\mathbf{V}_{tot} = \begin{pmatrix} \gamma & \mathbf{C} \\ \mathbf{C}^T & \gamma_B \end{pmatrix}, \tag{B.14}$$

and then apply partial Gaussian measurement, on modes B and B', by processing V_{tot} by means of the following formula

$$\mathbf{V}_C = \gamma - \mathbf{C}(\gamma_B + \mathbf{I})^{-1}\mathbf{C}^T. \tag{B.15}$$

After some algebra can be written the conditional CM in the following form

$$\mathbf{V}_C = \frac{1}{(\Lambda+1)^2 - g^2(1-\tau)^2}\begin{pmatrix} k & & \tilde{k} & \\ & k' & & \tilde{k}' \\ \tilde{k} & & k & \\ & \tilde{k}' & & k' \end{pmatrix} \tag{B.16}$$

where

$$\begin{aligned} k &:= (\mu+1)[g^2(1-\tau)^2 + (\Lambda+1)\tilde{\Lambda}] + (\Lambda+1)\tau, \\ \tilde{k} &:= -g(1-\tau)\tau\mu(\mu+2), \\ \tilde{\Lambda} &:= \Lambda - \tau, \end{aligned}$$

with $k' = k(g \to g')$ and $\tilde{k}' = \tilde{k}(g \to g')$. This conditional CM has the following asymptotic spectrum

$$\tilde{\nu}_+ = \frac{\sqrt{\lambda_+\lambda'_+}}{\tau}, \quad \tilde{\nu}_- = \frac{\sqrt{\lambda_-\lambda'_-}}{\tau}, \tag{B.17}$$

where we have defined

$$\begin{aligned} \lambda_+^{(\prime)} &= 1 + (1-\tau)(\omega + g^{(\prime)}), \\ \lambda_-^{(\prime)} &= 1 + (1-\tau)(\omega - g^{(\prime)}). \end{aligned}$$

Note that this spectrum does not depend on the modulation μ, and for $g = g\prime = 0$ we recover the conditional eigenvalue of Ref. [29].

Now, one can use Eq. (B.17) with definition $S = \sum_x h(x)$ and Eq. (6.11) to obtain the Holevo bound, whose final expression is given by the following formula

$$\chi = h(\nu_+) + h(\nu_-) - h(\tilde{\nu}_+) - h(\tilde{\nu}_-) + \log \frac{e^2}{4}(1-\tau)^2\mu^2. \tag{B.18}$$

Finally from Eq. (B.7) and (B.18), one has the the key-rate for the non-switching protocol in the presence of general two-mode coherent attacks

$$R = \log_2 \frac{e^2}{4} \frac{\tau^2}{(1-\tau)^2[1+\tau+(1-\tau)\omega]^2} + h(\tilde{\nu}_+) + h(\tilde{\nu}_-) - h(\nu_+) - h(\nu_-). \tag{B.19}$$

B.4 Study of the critical point

We compute the first order derivatives $\partial_g R$ and $\partial_{g'} R$, and solve the equation $\nabla R = 0$. We found that this equation, $\forall\ \tau$ and ω, admits a single critical point P_0, given by the origin $g = g' = 0$, of the the surface parameterized by those g, and g' fulfilling the constrains given by Eq. (4.3) and (4.4).

We then take the second order derivative with respect the correlation parameters, g, g', and build the Hessian matrix

$$H = \begin{pmatrix} \partial_g^2 R & \partial_{g,g'}^2 R \\ \partial_{g',g}^2 R & \partial_{g'}^2 R \end{pmatrix}. \tag{B.20}$$

From the positive definiteness of this matrix, evaluated in the critical point P_0, one can determine that P_0 is an absolute minimum. We then study the sign of the determinant evaluated in P_0, whose expression simplifies to the following

$$\det H = \frac{\left[\tau\bar{\lambda} f\left(\omega^{-1}\right) - \omega(1-\tau)^2 f\left(\tau\bar{\lambda}^{-1}\right)\right]}{\tau\left[\bar{\lambda}+\tau\right]\bar{\lambda}\omega(\omega^2-1)}, \tag{B.21}$$

where we have defined

$$f(x) \coloneqq \log_2 \frac{1+x}{1-x}, \tag{B.22}$$

and $\bar{\lambda} \coloneqq 1 + \omega(1-\tau)$. Now, one can check that the function $f\left(\tau\bar{\lambda}^{-1}\right) \geq 0$ for any $0 \leq \tau \leq 1$, $\omega \geq 1$, and that we also have

$$\tau\bar{\lambda} f\left(\omega^{-1}\right) > \omega(1-\tau)^2 f\left(\tau\bar{\lambda}^{-1}\right).$$

Now, being τ and ω both positive quantities as well as $\bar{\lambda}$, we have that

$$\det H > 0,$$

for any possible value of the transmissivity τ and of Eve's thermal noise ω. To complete the proof we need to study the second order derivatives $\ddot{R}$ evaluated in the critical point P_0 (the first minor of the Hessian matrix of Eq. (B.20)). It is very easy to check the validity of the following chain of inequalities. In fact, considering the definition function $f(.)$ given in Eq. (B.22) and that we have $\omega > 1$ and $0 \leq \tau \leq 1$, one gets

$$\begin{aligned} \partial_g^2 R = \partial_{g'}^2 R &= \frac{1}{\left(\tau+\bar{\lambda}\right)(\omega^2-1)} + \frac{f(\omega^{-1})}{4\omega} + \frac{(1-\tau)^2}{4\tau\bar{\lambda}} f(\tau) > \frac{1}{\left(\tau+\bar{\lambda}\right)(\omega^2-1)} + \frac{f(\omega^{-1})}{4\omega} \\ &> \frac{1}{(\tau+\bar{\lambda})(\omega^2-1)} > 0. \end{aligned} \tag{B.23}$$

The positivity of the first minor given by $\partial_g^2 R$, certifies that P_0 is a minimum point for the key-rate of the *no-switching* protocol.

Note that the previous analysis is valid only for those points, of the correlation plan, within the domain bounded by the constraints of Eq. (4.3) and (4.4) for which it is possible to define the derivative. In order to complete this analysis we need to check that also the points belonging to the boundary, of this domain, the rate under two-mode coherent attacks is larger than that for $g = g' = 0$. We have considered these cases numerically, computing the rate for the defined by the equation $\omega\,|g + g'| = \omega^2 + gg' - 1$. In 4.3 we provide an example of this computation, for the case with transmissivity fixed at $\tau = 0.4$ and the thermal noise $\omega = 1.3$ shot-noise unit (SNU). We see that the rate for collective attacks (red spot) lies at the bottom of the ship-shaped surface. The blue points describe the key-rate at the boundary and the semi-transparent region gives the (extremal) key rate for non zero correlations, g, g', between the ancillas (coherent attack). Analogous results can be obtained for any other value of $0 \leq \tau \leq 1$ and $\omega \geq 1$, with the surface vanishing into a point as $\omega \to 1$ and consequently, for Eq. (4.3) and (4.4), $g, g' \to 0$.□

B.5 Others protocols

In this section we focus on the details of the computations to perform the same analysis previously describe for the *switching* protocol for which we arrive at the same conclusion obtained for the no-switching protocol. Finally, for the sake of completeness, we discuss also the two remaining cases where Alice replaces the preparation of coherent states by the squeezed states. These two cases are named *squeezed/Hom* and *squeezed/Het* protocols. They represent an instructive example useful to complete this study, despite being less interesting from the point of view of a realistic implementation. In fact they are based on the ideal assumption of using infinitely squeezed state. Nevertheless also in these cases the origin, P_0, of the correlation plan is an absolute minimum for the key rates.

B.5.1 *Switching* protocol

In order to obtain the conditional CM for this case, we can starting from Eq. (B.14) and apply a homodyne detection on Bob's modes, that is we use the following formula for partial homodyne detection

$$\mathbf{V}_c = \gamma - \mathbf{C}(\mathbf{\Pi}\gamma_B\mathbf{\Pi})\mathbf{C}^T, \tag{B.24}$$

where $\mathbf{\Pi}$ =diag$(1, 0)$, for measurement performed on quadrature $\hat{q}$ and $\mathbf{\Pi}$ =diag$(0, 1)$ for measurements on quadrature $\hat{p}$.

We apply Eq. (B.24) first on mode B' and then on mode B, obtaining the conditional CM $\mathbf{V}_c$. Note that we have to make a distinction about the measurement strategy applied by Bob. Within each block c_j, Bob can decide to apply the same homodyne detection on both modes B, B', or measure on two distinct bases ($\hat{q}$ and $\hat{p}$).

When the detection of Bob's modes are both on quadrature $\hat{q}$ we have

$$\mathbf{V}_c^q = \mu\mathbf{I} - \frac{\tau(\mu^2-1)}{\tilde{\Lambda}[g^2(1-\tau)^2 - \tilde{\Lambda}^2]} \times \begin{pmatrix} 2g^2(1-\tau)^2 - \tilde{\Lambda}^2 & & g(1-\tau)\tilde{\Lambda} & \\ & 1 & & \\ g(1-\tau)\tilde{\Lambda} & & \tilde{\Lambda}^2 & \\ & & & 1 \end{pmatrix},$$

while for measurements on mode $\hat{p}$ we obtain

$$\mathbf{V}_c^p = \mu\mathbf{I} - \frac{\tau(\mu^2-1)}{\tilde{\Lambda}[g'^2(1-\tau)^2-\tilde{\Lambda}^2]} \times \begin{pmatrix} 1 & & \\ & 2g'^2(1-\tau)^2-\tilde{\Lambda}^2 & g'(1-\tau)\tilde{\Lambda} \\ & g'(1-\tau)\tilde{\Lambda} & \tilde{\Lambda}^2 \end{pmatrix}, \quad \text{(B.25)}$$

where $\tilde{\Lambda} = \tau\mu + (1-\tau)\omega = \Lambda - \tau$.

In the first case, for large μ, we have two following symplectic eigenvalues

$$\bar{\nu}_\pm = \sqrt{\frac{(1-\tau)(\omega \pm g)\mu}{\tau}}, \quad \text{(B.26)}$$

note that they depend only on the correlation parameter g, relative to the $\hat{q}$. In the second case, we have the following symplectic spectrum

$$\bar{\nu}'_\pm = \sqrt{\frac{(1-\tau)(\omega \pm g')\mu}{\tau}}, \quad \text{(B.27)}$$

depending on correlation parameter g'.

From this spectra we have two distinct conditional von Neumann entropies,

$$\begin{aligned} S_{E|\beta_q\beta'_q} &= h(\bar{\nu}_+) + h(\bar{\nu}_-) \\ &\overset{\mu\to\infty}{=} \log_2 \frac{e^2}{4}\frac{1-\tau}{\tau}\sqrt{(\omega+g)(\omega-g)}\mu, \end{aligned}$$

and

$$\begin{aligned} S_{E|\beta_p B'_p} &= h(\bar{\nu}_+) + h(\bar{\nu}_-) \\ &\overset{\mu\to\infty}{=} \log_2 \frac{e^2}{4}\frac{1-\tau}{\tau}\sqrt{(\omega+g')(\omega-g')}\mu, \end{aligned}$$

Averaging these expressions with the definitions of the total symplectic eigenvalues of Eqs. (B.10) and (B.11),we have the expression

$$S_{E|\beta\beta'} = \frac{S_{E|\beta_q\beta'_q} + S_{E|\beta_q\beta'_q}}{2}, \quad \text{(B.28)}$$

that taking the limit for large μ, become

$$\begin{aligned} S_{E|\beta\beta'} = \frac{1}{2}\log_2 &\left(\frac{e^2}{4}\frac{1-\tau}{\tau}\right)^2 \times \\ &\sqrt{(\omega+g)(\omega-g)(\omega+g')(\omega-g')}\mu^2, \end{aligned}$$

that eventually can be rewritten in the following compact form

$$S_{E|\beta\beta'} = \log_2 \frac{e^2}{4}\frac{1-\tau}{\tau}\sqrt{\nu_-\nu_+}\mu. \quad \text{(B.29)}$$

Key-rate for the switching protocol

Now, using the total von Neumann entropy given in Eq. (6.11), the conditional entropy given in Eq. (B.29) and the expression of the mutual information of Eq. (B.7), we can compute the general key-rate against two-mode Gaussian coherent attacks for the no-switching protocol,

$$\tilde{R} = \log_2 \frac{\sqrt{\nu_- \nu_+}}{(1-\tau)[\tau + (1-\tau)\omega]} - h(\nu_+) - h(\nu_-), \tag{B.30}$$

from which, again, we can recover the standard case of collective attack setting $g = g' = 0$. It is important to underline that there is a non optimal strategy that Bob can apply, consisting in homodyning on different basis within each block c_j. One find a lower key-rate because in this case measuring different quadratures within a block has the effect of de-correlating modes B and B', and consequently any dependency from g, g' is cancelled from the conditional CM. In fact one finds the following doubly degenerate eigenvalues,

$$\bar{\nu}_{1,2} = \sqrt{\frac{(1-\tau)\omega\mu}{\tau}}. \tag{B.31}$$

From Eq. (B.31) and again from Eq. (B.7) and Eq. (B.13), we obtain the following minimum key rate,

$$\bar{R} = \log_2 \frac{\omega}{(1-\tau)[\tau + (1-\tau)\omega]} - h(\nu_+) - h(\nu_-),$$

that is not interesting from a practical point of view, because the parties can always choose to group instances of the protocol with the same quadrature homodyned.

Study of the critical point for the *switching* protocol

We then compute the first derivatives with respect the correlations parameters, g and g', obtaining the following expressions

$$\partial_g \tilde{R} = \frac{\zeta}{2}\left[f(\nu_-) - \frac{2g'}{(\omega + g')\nu_-} - \frac{2\nu_+\nu_-}{(\omega + g')(\omega - g)} f(\nu_+) \right] \tag{B.32}$$

$$\partial_g \tilde{R} = \frac{\zeta'}{2}\left[f(\nu_-) - \frac{2g}{(\omega + g)\nu_-} - \frac{2\nu_+\nu_-}{(\omega + g)(\omega - g')} f(\nu_+) \right]. \tag{B.33}$$

where the function $f(.)$ has been defined in Eq. (B.22), and the symplectic eigenvalues $\nu_\pm$ are given in Eqs. (B.10) and (B.11), ζ and ζ' are defined as follows

$$\zeta := \frac{\nu_-}{2(\omega - g')}, \ \zeta' := \frac{\nu_-}{2(\omega - g)}. \tag{B.34}$$

Note that these derivatives are properly defined within the constraints of Eqs. (4.3,4.4), that identify a sector of g, g' plane for which the conditions $\nu_- > 1$, $\nu_+ > 1$ must hold. In fact, the situation for which one has $\nu_\pm = 1$ can only be obtained in P_0, i.e., if the attack is collective.

Solving, by inspection, the system of equations $\nabla R = 0$ one founds that P_0 is a critical point, and that it is also unique for any $\omega \geq 1$ and g and g' fulfilling Eq. (4.3,4.4).

Positive definiteness of the Hessian matrix

The second order derivatives with respect g, evaluated in P_0 is given by the following expression

$$\partial_g^2 \tilde{R} = -\frac{\omega^2+g^2}{(\omega^2-g^2)^2} + \frac{1}{4}\left[\frac{\kappa_-}{\nu_-^2-1} + \frac{\kappa_+}{\nu_+^2-1}\right] + \frac{1}{4}\left[\frac{\sqrt{\kappa_-}f(\nu_-)}{\omega-g} + \frac{\sqrt{\kappa_+}f(\nu_+)}{\omega+g}\right] \tag{B.35}$$

with the coefficients $\kappa_\pm$ defined as follows

$$\kappa_+ := \frac{\omega+g'}{\omega+g}, \quad \kappa_- := \frac{\omega-g'}{\omega-g}, \tag{B.36}$$

The derivative with respect g', and the mixed terms are given by the expressions

$$\partial_{g'}^2 \tilde{R} = -\frac{\omega^2+g'^2}{(\omega^2-g'^2)^2} + \frac{1}{4}\left[\frac{\kappa_-^{-1}}{(\nu_-^2-1)} + \frac{\kappa_+^{-1}}{(\nu_+^2-1)}\right] + \frac{1}{4}\left[\frac{f(\nu_-)}{\sqrt{\kappa_-}(\omega-g')} + \frac{f(\nu_+)}{\sqrt{\kappa_+}(\omega+g')}\right]$$
$$\partial_{g,g'}^2 \tilde{R} = \partial_{g',g}^2 \tilde{R} = \frac{1}{4}\left[\frac{1}{\nu_-^2-1} + \frac{1}{\nu_+^2-1} - \frac{f(\nu_-)}{\nu_-} - \frac{f(\nu_+)}{\nu_+}\right],$$

that evaluated in P_0, give

$$\partial_g^2 \tilde{R} = \partial_{g'}^2 \tilde{R} = \frac{1}{2}\left(\frac{1}{\omega^2-1} + \omega^{-1} f(\omega)\right) - \frac{1}{\omega^2}, \tag{B.37}$$

$$\partial_{g,g'}^2 \tilde{R} = \partial_{g',g}^2 \tilde{R} = \frac{1}{2}\left(\frac{1}{\omega^2-1} - \omega^{-1} f(\omega)\right). \tag{B.38}$$

We computed the determinant of the Hessian in P_0, obtaining the following expression

$$\begin{aligned}\det H &= \partial_g^2 \tilde{R} \times \partial_{g'}^2 \tilde{R} - \left(\partial_{g,g'}^2 \tilde{R}\right)^2 \\ &= \frac{1}{\omega}\left(\frac{1}{\omega^2-1} - \frac{1}{\omega^2}\right)\left(f(\omega) - \frac{1}{\omega}\right).\end{aligned} \tag{B.39}$$

Now assuming that $\omega > 1$, we have that the following inequalities are verified

$$\begin{aligned} f(\omega) &> \frac{1}{\omega}, \\ \omega^2 - 1 &< \omega^2, \end{aligned} \tag{B.40}$$

thanks to which the condition $\det H > 0$ results verified. We have also checked that that $\det H > 0$ in the limit of $\omega \to 1^+$. Finally we verified that the second order derivative in P_0 is positive. It is easy to make this check starting from Eq. (B.37), and using again the condition of Eq. (B.40), we have the following chain of inequalities

$$\begin{aligned}&\frac{1}{2}\left(\frac{1}{\omega^2-1} + \frac{f(\omega)}{\omega}\right) - \frac{1}{\omega^2} > \frac{1}{2}\frac{1}{\omega^2-1} + \frac{1}{2\omega^2} - \frac{1}{\omega^2} \\ &= \frac{1}{2\omega^2(\omega^2-1)} > 0,\end{aligned}$$

proving that P_0 is indeed an absolute minimum for the key-rate of Eq. (B.30), so that Eq. (4.20) is verified □.

B.5.2 Protocol *squeezed/Hom*

In this protocol Alice sends squeezed states and Bob homodynes, randomly switching between the two quadratures. Alice-Bob mutual information is now given by the following expression for $\mu \gg 1$

$$I_{sque/Hom} = \log_2 \frac{\tau\mu}{(1-\tau)\omega}. \tag{B.41}$$

This is in fact the only change, with respect the switching protocol, one has to consider to obtain the expression of the key-rate. In fact we note that for the squeezed/hom protocol the conditional symplectic spectra are the same of Eqs. (B.26) and Eq. (B.27) depending on quadrature measured. Then, the conditional von Neumann entropy is given by Eq. (B.13) and, using Eq. (B.41), one can obtain the following secret key rates

$$\mathring{R} = \log_2 \frac{\sqrt[4]{(\omega^2-g^2)(\omega^2-g'^2)}}{(1-\tau)^2\omega} - h(\nu_-) - h(\nu_+). \tag{B.42}$$

That is very similar to the rate $\tilde{R}$ of Eq. (B.30), differences occurs in the denominator of Eq. B.42, as here encoding by means of infinitely squeezed quantum states, we do not have contribution from the evolution of the vacuum. Solving the gradient equation $\nabla\mathring{R}$, by inspection, we find again that the origin $P_0 := (g, g') = (0, 0)$ is the only critical point. We computed the Hessian matrix, as described for the previous case and verified that the condition $\det H > 0$ is verified. Then, taking the second order derivative with respect g in P_0, we obtain the following relation

$$\partial_g^2 \mathring{R} = \frac{1}{2\omega^2(\omega^2-1)} + \frac{f(\omega)}{\omega} > 0,$$

that again qualifies P_0 as the absolute minimum.

B.5.3 Protocol Squeezed/Het protocol

In this case, for large μ, Alice-Bob mutual information is given by the following formula

$$I_{sque/Het} = \log_2 \frac{\tau\mu}{1+(1-\tau)\omega}, \tag{B.43}$$

and the conditional symplectic spectrum, depending on which quadrature the final homodyne measurements are performed, is given by the following expressions, when both homodynes are on the $\hat{q}$

$$\begin{aligned}
\bar{\nu}_\pm^q &= \sqrt{\frac{(\omega \pm g)[1+(\omega \pm g')(1-\tau)]}{1-\tau+\omega \pm g}}, \\
\bar{\nu}_1^q &= \sqrt{\frac{1-\tau}{\tau}\mu(1-\tau+\omega+g)}, \\
\bar{\nu}_2^q &= \sqrt{\frac{1-\tau}{\tau}\mu(1-\tau+\omega-g)}.
\end{aligned} \tag{B.44}$$

It is clear that when Bob homodynes measurements are performed in the quadrature $\hat{p}$, then the spectrum can be obtained swapping the role of $g \leftrightarrow g'$ in Eqs. (B.44). Note also that the total symplectic spectrum, $\nu_\pm$, is the same of previous cases. From

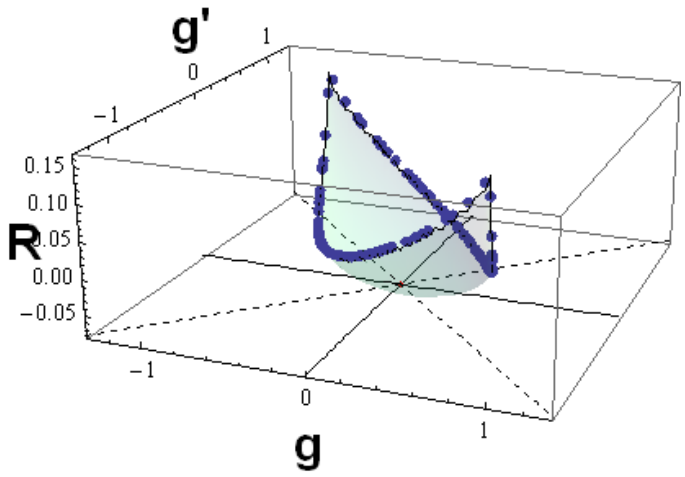

Figure B.1: This plot shows the key-rate of Eq. (B.45), for fixed transmissivity $\tau = 0.2$ and thermal noise $\omega = 1.3$ (SNU). As in previous Fig. 4.3, the red point describe the resulting rate for collective attack ($g = g; = 0$), the blue points describe the key-rate for values values of g, g' verifying the condition $\omega|g + g'| = \omega^2 + gg' - 1$, and the remaining colored region describe all other cases, for which the correlation parameters verify the condition $\omega|g + g'| < \omega^2 + gg' - 1$. One can see that the key-rate under collective attack (red spot) is, strictly, optimal one.

these and previous results of Eq. (B.44), we compute the average von Neumann entropy

$$S_{E|\beta,\beta'} = \frac{S^q_{E|\beta,\beta'} + S^p_{E|\beta,\beta'}}{2},$$

and from this expression, using Eqs. (B.44), (B.43) and (6.11) we obtain the following key rate

$$\breve{R} = \frac{1}{2}\sum_{l=\pm}\left[\sum_{k=p,q} h(\bar{\nu}_l^k) - h(\nu_l)\right] + \log_2 \frac{\sqrt[4]{[(1-\tau+\omega)^2 - g^2][(1-\tau+\omega)^2 - g'^2]}}{(1-\tau)[1+(1-\tau)\omega]}, \quad \text{(B.45)}$$

For which it is easy to check that the origin of the g, g' plane, P_0 minimizes the rate.

Appendix C

Two-way communication against coherent attacks: details of the computations

We here describe in more detail the calculation performed to study the performance of the two-way protocols when Eve perform coherent attacks. The main resource activated by the double use of the channel is the possibility of switching the circuit between a closed (ON) and an open (OFF) circuit at Alice's station (see Fig.C.1).

C.1 Secret-Key Rate and symplectic analysis

The secret-key rate quantifies the gap between Alice-Bob and Eve-Alice(or Bob) correlations. Which of the two parties has to be considered to compute the secret-key rate depends on the reconciliation protocol employed, i.e., on which classical variable (α or β) has to be guessed. The two distinct secret-key rate are given in general by:

$$R^{\blacktriangleright} \coloneqq I(\alpha:\beta) - \chi(\varepsilon:\alpha), \tag{C.1}$$

$$R^{\blacktriangleleft} \coloneqq I(\alpha:\beta) - \chi(\varepsilon:\beta), \tag{C.2}$$

the first describing the secret-key rate in DR, the second the rate in RR. The function $I(\alpha:\beta)$ is the classical mutual information quantifying correlations between Alice's (α), and Bob's (β) variables. It can be computed thanks to the following relation,

$$I(\alpha:\beta) \coloneqq H(\beta) - H(\beta|\alpha), \tag{C.3}$$

where $H(\beta) \coloneqq (1/2)\log V(\beta)$ and $H(\beta|\alpha) \coloneqq (1/2)\log V(\beta|\alpha)$ are the total and conditional Shannon entropy. The function $V(x)$ is the variance of probability distribution $p(x)$ describing x's statistics. On Eve's side we can bound her accessible information by computing the following quantity,

$$\chi(\varepsilon:x) \coloneqq S(\varepsilon) - S(\varepsilon|x), \tag{C.4}$$

defined as the Holevo information, and quantifying the difference between the von Neumann entropy $S(\varepsilon)$ describing the total Eve's, ρ_E, and $S(\varepsilon|x)$ describing the

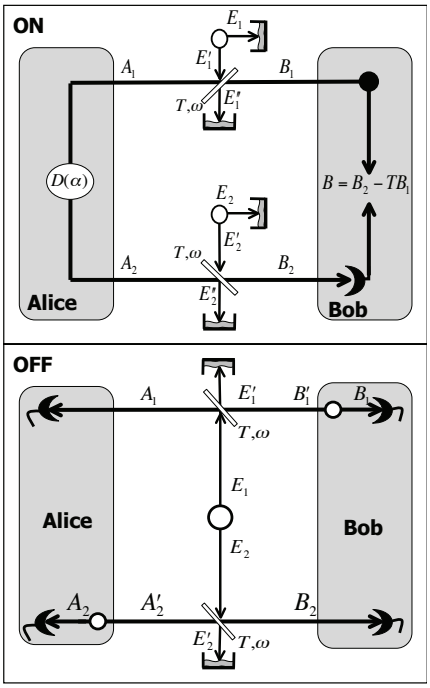

Figure C.1: The top panel shows the two-way scheme in ON configuration, to be used when the channel's tomography detects a collective attacks. The bottom panel illustrates the two-way communication in OFF, configuration to be used in case coherent attacks.

conditional state, $\rho_{E|x}$, where $x = \alpha, \beta$. Solving the two equations $R^{\blacktriangleright} = 0$ and $R^{\blacktriangleleft} = 0$, one finds the corresponding security thresholds.

For Gaussian quantum systems, the relevant statistical properties are encompassed in the CM [11], up to local operations. For an $n-$mode CM, $\mathbf{V}$, its symplectic spectrum provides the entropic properties of the corresponding quantum state, from which we can quantify the von Neumann entropies. The symplectic spectrum and the CM, are connected by the following relation

$$\sqrt{\det \mathbf{V}} = \nu_1 \nu_2 ... \nu_n, \tag{C.5}$$

where eigenvalues $\{\nu_1, \nu_2, ..., \nu_n\}$ are obtained diagonalizing the symplectic form obtained from $\mathbf{V}$ by the following relation

$$\mathbf{M} = i\mathbf{\Omega}\mathbf{V}, \tag{C.6}$$

where $\mathbf{\Omega} = \oplus_1^n \tilde{\omega}_i$, with $\tilde{\omega}_i$ the single-mode symplectic form given by

$$\tilde{\omega}_i = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}. \tag{C.7}$$

From the symplectic spectrum (C.5) one can compute the Holevo information using

$$S(\rho) = \sum_{i=1}^{n} h(\nu_i), \tag{C.8}$$

where $h(x)$ has been defined previously and we recall that in the asymptotic limit it is given by the following formula

$$h(x) \simeq \log_2 \frac{e}{2} x + O(x^{-1}). \tag{C.9}$$

C.2 Protocol *coherent/Het*

In this protocol the parties prepare coherent states and decode by heterodyne detections. To perform the cryptanalysis we followed two different approaches, depending on the configuration: in case ON (see main text), and Eve performing collective attacks, the security for the DR has been studied starting from Eve's Covariance Matrix (CM). For the RR, we complete Eve's CM by including Bob's mode. We then compute the CM resulting from the measurement of Bob's mode on which we apply the measurement to obtain the conditional CM. When the eavesdropper performs coherent attacks, our protocol prescribes to use the data obtained from the circuit set in OFF. In this case the security analysis is performed by means of the Entangled Based (EB) representation, so to be legitimate to get rid of the details of Eve's unitary operation designing the attack.

C.2.1 Case ON.

Total Covariance Matrix

Bob prepares a thermal state modulating coherent states. The global Gaussian modulation of this state is described by the parameter $\mu_B = \mu + 1$, comprehensive of a classical (μ), and the vacuum shot-noise. Alice applies an additional (classical) modulation μ_{ON}, representing her encoding. The resulting thermal state will thus have a final total modulation that reads,

$$\tilde{\mu} = \mu_B + \mu_{ON}. \tag{C.10}$$

Let us consider Eve's outputs modes $\{E_1, E_1'', E_2, E_2''\}$ (see Fig.C.1top).Adopting previous ordering we compute Eve's total CM obtaining

$$\mathbf{V}_E = \begin{pmatrix} \mathbf{A} & \mathbf{C} \\ \mathbf{C}^T & \mathbf{B} \end{pmatrix}, \tag{C.11}$$

where we defined,

$$\mathbf{A} = \begin{pmatrix} \omega\mathbf{I} & \sqrt{\tau(\omega^2-1)}\mathbf{Z} \\ \sqrt{\tau(\omega^2-1)}\mathbf{Z} & \Psi\mathbf{I} \end{pmatrix},$$
$$\mathbf{B} = \begin{pmatrix} \omega\mathbf{I} & \sqrt{\tau(\omega^2-1)}\mathbf{Z} \\ \sqrt{\tau(\omega^2-1)}\mathbf{Z} & \widetilde{\Psi} \end{pmatrix},$$
$$\mathbf{C} = \begin{pmatrix} 0 & \Xi\mathbf{Z} \\ 0 & \Phi\mathbf{Z} \end{pmatrix},$$

with,

$$
\begin{aligned}
\widetilde{\mathbf{\Psi}} &= [\tau\omega + (1-\tau)^2\omega + \tau(1-\tau)\mu_B] + \\
&\quad (1-\tau)\mu_{ON}\Delta(\mu_{ON},\mu_{ON}), \\
\Psi &= \tau(\omega-\mu_B)+\mu_B, \\
\Phi &= (1-\tau)\sqrt{T}(\mu_B-\omega), \\
\Xi &= -(1-\tau)\sqrt{(\omega^2-1)}.
\end{aligned}
\tag{C.12}
$$

where $\Delta(\mu_{ON},\mu_{ON})$ =diag(μ_{ON},μ_{ON}), τ is the transmissivity of the entangling cloners, and ω accounts for the thermal noise injected in the circuit by Eve.
From Eq. (C.11) it is possible to obtain the CM the others protocols simply by redefining Alice's (μ_{ON}) and Bob's modulation (μ_B). Considering the CM of Eq. (C.11), and computing its determinant, taking the asymptotic limit, $\mu_B \sim \mu_{ON} \sim \mu \gg 1$, we get the following determinant,

$$
\det \mathbf{V}_{tot} = (1-\tau)^4\omega^4\mu^4, \tag{C.13}
$$

that we can use to help us in determining the symplectic spectrum that can be computed. In the asymptotic limit one gets,

$$
\{\nu_1,\nu_2,\nu_3\nu_4\} \to \{\omega,\omega,(1-\tau)^2\mu^2\} \tag{C.14}
$$

Conditional CM in Direct Reconciliation

In this case the parties use DR, Bob guesses the encoding performed by Alice, and a simple recipe to account for this operation, starting from eq.(C.11), is *conditioning by collapsing* Alice's classical modulation. For the present protocol, *coherent/Het*, Bob guessing is simulated by setting $\mu_{ON} = 0$, for both quadratures q,p, in the matrix element $\widetilde{\mathbf{\Psi}}$, in Eq. (C.11). This coincides with setting the total modulation $\tilde{\mu} = 1$ after Bob's classical post-processing.
The resulting conditional CM has the following asymptotic determinant,

$$
\text{Det } \mathbf{V}_c^{\blacktriangleright,ON} = (1-\tau^2)^2\omega^2\mu^2, \tag{C.15}
$$

connected, as stated by eq.(C.5), to the symplectic spectrum whose analytical expressions is obtained in the limit of large modulation,

$$
\{\bar{\nu}_1,\bar{\nu}_2,\bar{\nu}_3,\bar{\nu}_4\} \to \{1,1,\omega,(1-\tau^2)\mu\}. \tag{C.16}
$$

Now, using previous Eqs. (C.4,C.8,C.9)and Eqs.(C.14,C.16) we can compute the Holevo function, given by,

$$
\chi(\varepsilon:\alpha) = \log_2 \frac{e}{2}\frac{(1-\tau)}{(1+\tau)}\mu \tag{C.17}
$$

Alice-Bob mutual information

Alice-Bob correlation can be computed by considering the evolution of Bob's mode through the circuit and applying the conditioning to the resulting mode. This last step account for the final measurement scheme applied. For *coherent/Het*, after Eve's processing of the reference coherent state, Alice's encoding and Bob's classical post-processing to subtract the reference state ($B = B_2 - T\beta$) from the received state,

we obtain the following expressions for Alice-Bob mutual information in the large modulation limit ($\mu \gg 1$):

$$I(\alpha:\beta) = \log_2 \frac{\tau\mu}{1+\tau^2+(1-\tau^2)\omega}. \tag{C.18}$$

From Eqs.(C.1,C.17,C.18), we obtain the following secret-key rate in DR for *case ON*

$$R^{\blacktriangleright} = \log_2 \frac{2}{e} \frac{\tau(1+\tau)}{(1-\tau)[1+\tau^2+(1-\tau^2)\omega]} - h(\omega)$$

Conditional Covariance Matrix in Reverse Reconciliation

For the RR, as said previously, we can obtain the conditional CM by: *(i)* completing the total CM of Eq. (C.11) adding Bob's mode B, that will take into account Eve's processing, Alice encoding, and Bob's post-processing and then *(ii)* performing a partial Gaussian measurement [11] on Bob's mode. After this steps we obtain a CM of the same dimensions of that of Eq. (C.11), but now accounting for Eve's guessing on Bob final measurement, and then providing Eve-Bob correlations. Eve's CM of Eq.(C.11), after the inclusion of the Bob's mode, can be written in the canonical form

$$\mathbf{V}^{\blacktriangleleft} = \begin{pmatrix} \mathbf{V}_E & \bar{\mathbf{C}} \\ \bar{\mathbf{C}}^T & \bar{\mathbf{B}} \end{pmatrix},$$

where now

$$\bar{\mathbf{B}} = [\tau^2+\tau\mu+(1-\tau^2)\omega]\mathbf{I},$$
$$\bar{\mathbf{C}} = \sqrt{1-\tau} \begin{pmatrix} \sqrt{\tau(\omega^2-1)}\mathbf{Z} \\ \tau(\omega-1)\mathbf{I} \\ \sqrt{(\omega^2-1)}\mathbf{Z} \\ \sqrt{\tau}[\tau(\omega-1)-\mu]\mathbf{I} \end{pmatrix}.$$

Heterodyning Bob's mode we can compute Eve's conditional CM, defined as follows

$$\mathbf{V}_C^{\blacktriangleleft} = \mathbf{V}_E + \bar{\mathbf{C}}(\bar{\mathbf{B}}+\mathbf{I})^{-1}\bar{\mathbf{C}}^T. \tag{C.19}$$

Performing the symplectic analysis on $\mathbf{V}_C^{\blacktriangleleft}$, in large modulation limit, we can determine the eigenvalue diverging for large modulation obtaining the following spectrum

$$\{\bar{\nu}_1,\bar{\nu}_2,\bar{\nu}_3,\bar{\nu}_4\} \to \{\bar{\nu}_1,\bar{\nu}_2,\bar{\nu}_3,(1-T^2)\mu\},$$

where the others asymptotically constant eigenvalues are defined as follows

$$\bar{\nu}_1\bar{\nu}_2\bar{\nu}_3 = \frac{[1+\tau^3+(1-\tau)(1+\tau^2)\omega]\omega}{\tau(1+\tau)}.$$

These results, together with Eq. (C.14) and Eq. (C.18) provide the expression of the key rate in RR, given in Eq. (7.1) of the main text. This is compared with the corresponding one-way protocol in Fig.7.2.

C.2.2 Case OFF

We study now the security for two-way communication by the *coherent/Het* protocol for *case* OFF, (see Fig.C.1 panel OFF). In this case the security analysis is performed against two-mode coherent attacks, representing the most general attack possible, per use of the protocol, after a symmetrization of the general coherent attack by the *de Finetti* theorem.
We adopted an *Entanglement Based* (EB) representation and computed the security of the equivalent EB circuit, this allows us to get rid of the details of the operations performed by the eavesdropper to perform the coherent attack. Within this representation, the quantum information content of Eve's total (ρ_E) and conditional $(\rho_{E|x})$ state is the same of that of Alice-Bob joint states, ρ_{AB} and $\rho_{AB|x}$ respectively, so that one can write

$$S(\rho_{AB}) = S(\rho_E),$$
$$S(\rho_{AB|x}) = S(\rho_{E|x}),$$

where $x = Alice, Bob$.

The Total Covariance Matrix and the total von Neumann entropy

Bob measuring by heterodyne detection mode B_1, of the EPR pair $\{B_1, B_1'\}$, project a coherent state on mode B_1'. such a state, for Gaussian system, can be described by the following CM,

$$\mathbf{V}_B = \begin{pmatrix} \mu_B \mathbf{I} & \sqrt{\mu_B^2 - 1}\mathbf{Z} \\ \sqrt{\mu_B^2 - 1}\mathbf{Z} & \mu_B \mathbf{I} \end{pmatrix}.$$

The most general state Eve can employ to perform the attack, realized by two entangling cloners mixing the ancillas $\{E_1, E_2\}$ with the signal during the forward and backward stage of the communication (see Fig.C.1), is described by the CM of Eq. (4.2)

$$\mathbf{V}_E = \begin{pmatrix} \omega \mathbf{I} & \mathbf{G} \\ \mathbf{G} & \omega \mathbf{I} \end{pmatrix},$$

where $\mathbf{G}$ =$diag(g, g')$, and g, g' fulfill the *bona fide* conditions given in Eq.(4.3) and (4.4). Computing the CM for Alice-Bob joint state ρ_{AB}, and assuming the modes ordered as follows $\{B_1, A_2, A_1, B_2\}$, one finds the following total CM

$$\mathbf{V}_{AB}^{OFF} = \begin{pmatrix} \widetilde{\mathbf{A}} & \widetilde{\mathbf{C}} \\ \widetilde{\mathbf{C}}^T & \widetilde{\mathbf{B}} \end{pmatrix}, \tag{C.20}$$

where the matrix blocks have been defined as follows

$$\tilde{\mathbf{A}} = \begin{pmatrix} (\mu_B + 1)\mathbf{I} & & \widetilde{\delta}\mathbf{I} \\ & (\mu_A + 1)\mathbf{I} & \\ \widetilde{\delta}\mathbf{I} & & \widetilde{\tau}\mathbf{I} \end{pmatrix},$$
$$\tilde{\mathbf{B}} = [(1 - \tau)\omega + \tau(1 + \mu_A)]\mathbf{I},$$
$$\tilde{\mathbf{C}} = \begin{pmatrix} \mathbf{0} \\ \widetilde{\delta}\mathbf{I} \\ \mathbf{G} \end{pmatrix},$$

with coefficients $\widetilde{\delta}$ and $\widetilde{\tau}$ defined as follows

$$\widetilde{\delta} = \sqrt{\tau[(1+\mu_B)^2 - 1]},$$
$$\widetilde{\tau} = (1-\tau)\omega + T(1+\mu_B).$$

It is easy to compute the analytical expression for the asymptotic symplectic spectrum of CM (C.20), obtaining

$$\{\nu_\pm, \nu_3, \nu_4\} \to \{\sqrt{(\omega \pm g)(\omega \pm g')}, (1-\tau)\mu, (1-\tau)\mu\}, \tag{C.21}$$

From which, using Eqs. (C.8,C.9) one gets the total Eve's von Neumann entropy

$$S^{OFF} = \log_2\left(\frac{e}{2}\right)^2 (1-\tau)^2\mu^2 + h(\nu_-) + h(\nu_+). \tag{C.22}$$

Conditional symplectic spectra and Alice-Bob mutual information

From Eq. (C.20), we compute the conditional CMs for the DR and for the RR respectively. To obtain the conditional CM in DR we collapse Alice and Bob modulation, by setting $\mu_A = \mu_B = 0$, in modes B_1 and A_2.The resulting CM has the following symplectic spectrum

$$\{\bar{\nu}_1, \bar{\nu}_2, \bar{\nu}_+, \bar{\nu}_-\} \to \{1, 1, \sqrt{\lambda_+\lambda'_+}, \sqrt{\lambda_-\lambda'_-}\} \tag{C.23}$$

Where, $\lambda_\pm = \tau + (\omega \pm g)(1-\tau)$ and $\lambda'_\pm = \tau + (\omega \pm g')(1-\tau)$.

The conditional CM corresponding to the RR, is obtained by applying a heterodyne detection on mode B_2 of CM (C.20), followed by a second heterodyne detection on the output matrix with respect mode A_1 (the order of this two measurements can of course be swapped). We end up with a CM, allowing to compute easily the asymptotic symplectic spectrum

$$\bar{\nu}'_\pm \to \frac{\sqrt{[\lambda_\pm + 1 - \tau][\lambda'_\pm + 1 - \tau)]}}{\tau}. \tag{C.24}$$

Alice-Bob Mutual Information and Secret-key rate.

Alice-Bob correlation can be computed easily starting from the coefficient $\widetilde{\tau}$,giving the variance of Bob's mode having experienced Eve's processing by the entangling cloners. The conditional variance can be computed by collapsing Bob's classical modulation, i.e.,by setting $\mu_B = 0$. Assuming $\mu_A = \mu_A = \mu \gg 1$, we obtain

$$I_{AB} = \frac{I_{AB}^{forw} + I_{AB}^{back}}{2} = \log_2 \frac{\tau\mu}{1+\tilde{\Lambda}}, \tag{C.25}$$

where $\tilde{\Lambda} = \tau + (1-\tau)\omega$. We note that the previous expression is not depending from the correlation parameters g, and g'. This can be seen as the consequence of the control the parties have on the random ON/OFF switching of the circuit.

The previous results are used to compute the secret key rate in DR that after some algebra can be written in the following form

$$R^{\blacktriangleright}_{OFF} = \log_2 \frac{\tau}{(1-\tau)(1+\tilde{\Lambda})} + \frac{1}{2}\sum_{k=\pm}[h(\bar{\nu}_k) - h(\nu_k)]. \tag{C.26}$$

It is possible to compute also the rate for the RR, using previous Eq. (C.22) and Eqs. (C.24,C.25).

C.3 Protocol *coherent/Hom*

This protocol is implemented preparing coherent states, and performing homodyne detections at the decoding stage. As said in previous section the total CM is the same for all protocols in ON, so in this and in the next sections we will limit ourselves to provide the steps one should do to obtain the conditional CM from the total one. We provide the cryptanalysis for the ON and OFF cases, in both DR and RR for which we recover the results illustrated in Eqs.(7.5,7.6).

C.3.1 Case ON

Conditional Covariance Matrix: Direct Reconciliation.

The main step to perform to determine the conditional CM in DR for the *coherent/Hom* protocol is in the way we realize the conditioning. We saw that, in general, we can obtain the conditional dynamics by collapsing the classical modulation corresponding to the variable to be guessed. For the present case, and for all those cases where a homodyne detection is involved, the conditioning is performed collapsing to zero the modulation in only one quadrature while the other is defined so to diverge in the asymptotic limit. For instance we are authorized to set

$$\begin{aligned}\bar{\mu}^{q}_{ON} &= 1/\mu \overset{\mu\to\infty}{\to} 0,\\ \bar{\mu}^{p}_{ON} &= \mu,\end{aligned}$$

where the role of the two quadratures is interchangeable. Applying this simple recipe to Eq. (C.11) provides us straightforwardly with the conditional CM for the DR of the remaining protocols coherent/Hom. The same recipe can be used to determine Alice-Bob mutual information from the expression of the final Bob's mode in Eq.(C.12)

$$\tilde{I} = \frac{1}{2}\log_2 \frac{\tau\mu}{\tau^2 + (1-\tau^2)\omega}. \tag{C.27}$$

Note that this expression is similar to that given in Eq.(C.18) for *coherent/Het* protocol. At denominator, it differs for the contribution from the vacuum shot-noise originated, in that case, by final heterodyne measurement. The τ^2 term accounts for the initial vacuum noise of the preparation processed by Eve's entangling cloners. With this in mind one can already foresee which will be the expressions of the mutual informations for the other protocols.

The symplectic analysis for the *coh/Hom* protocol provides the following conditional, asymptotic, symplectic spectrum

$$\{\nu_1^{\blacktriangleright}, \nu_2^{\blacktriangleright}, \nu_3^{\blacktriangleright}\nu_4^{\blacktriangleright}\} \to \{1, \omega, \sqrt{(1-\tau)^2(1-\tau^2)\omega\mu^3}\}, \tag{C.28}$$

and secret-key rate in DR

$$\tilde{R}^{\blacktriangleright}_{ON} = \frac{1}{2}\log_2 \frac{\tau(1+\tau)}{(1-\tau)[\tau^2 + (1-\tau^2)\omega]} - h(\omega).$$

Conditional Covariance Matrix: Reverse Reconciliation.

For the RR , we can compute the evolution of Bob's mode through the channel, obtain the post-processed mode B and from here complete total CM writing it in

the normal form. We then can apply the formula for the partial Gaussian homodyne detection [11] on Bob's mode B

$$\mathbf{V}_C^{\blacktriangleleft} = \mathbf{A} - \mathbf{C}(\mathbf{\Pi}\mathbf{B}\mathbf{\Pi})\mathbf{C}^T,$$

where $\mathbf{\Pi} := diag(1,0)$ when measuring on quadrature $\hat{q}$. The symplectic analysis on CM $\mathbf{V}_C^{\blacktriangleleft}$, gives the conditional symplectic spectrum

$$\begin{aligned}
\nu_1^{\blacktriangleleft} &\to \sqrt{\frac{\omega[1+\tau^2\omega-\tau^3(\omega-1)]}{\tau^2+\omega+\tau^3(\omega-1)}}, \\
\nu_2^{\blacktriangleleft} &\to \omega, \\
\nu_3^{\blacktriangleleft}\nu_4^{\blacktriangleleft} &\to \sqrt{\frac{(1-\tau)^3[\tau^2+\omega+\tau^3(\omega-1)]\mu^3}{\tau}}\}
\end{aligned} \tag{C.29}$$

and rate in RR already given in Eq.(7.5))

$$\tilde{R}_{ON}^{\blacktriangleleft} = \frac{1}{2}\log_2\frac{\tau^2+\omega+\tau^3(\omega-1)}{(1-\tau)[\tau^2+(1-\tau^2)\omega]} + h(\nu_1^{\blacktriangleleft}) - h(\omega). \tag{C.30}$$

C.3.2 Case OFF

For the OFF case we use the EB representation, repeating all the steps of previous protocol and replacing the heterodyne detections by homodyne detections. We compute the conditional symplectic spectra in the asymptotic limit, and from previous relations applying the formula for Gaussian homodyne detection, plus using Eq.(C.1,C.2) we arrive at the following secret key rates:

Direct Reconciliation

$$\begin{aligned}
\tilde{R}_{OFF}^{\blacktriangleright} = \frac{1}{2}\log_2\frac{\tau\sqrt{[1+\tau(\omega-1)]^2-\tau^2g^2}}{(1-\tau)[\tau+(1-\tau)\omega]} - \sum_{k=\pm}\frac{h(\nu_k)}{2} + \\
\frac{1}{2}\sum_{k=\pm}h\left(\sqrt{\frac{(\omega\pm g)[\tau+(1-\tau)(\omega\pm g')]}{1-\tau+\tau(\omega\pm g)}}\right)
\end{aligned} \tag{C.31}$$

Reverse Reconciliation

Performing the same computation for the RR, we find

$$\tilde{R}_{OFF} = \frac{1}{2}\log_2\frac{\sqrt[4]{(\omega^2-g^2)(\omega^2-g'^2)}}{(1-\tau)\tilde{\Lambda}} - \sum_{i=\pm}\frac{h(\nu_i)}{2}$$

where the total symplectic eigenvalues ν_i are those of the total Alice-Bob joint covariance matrix, and are given in Eq.(C.21)

Note that to obtain previous results, we assumed to apply a homodyne detection on $\hat{q}$ quadrature, but it is simple to write the rates and the spectra in case the homodyne detection is performed on the complementary quadrature $\hat{p}$: it suffices to swap the role of $g \to g'$ in previous equations.

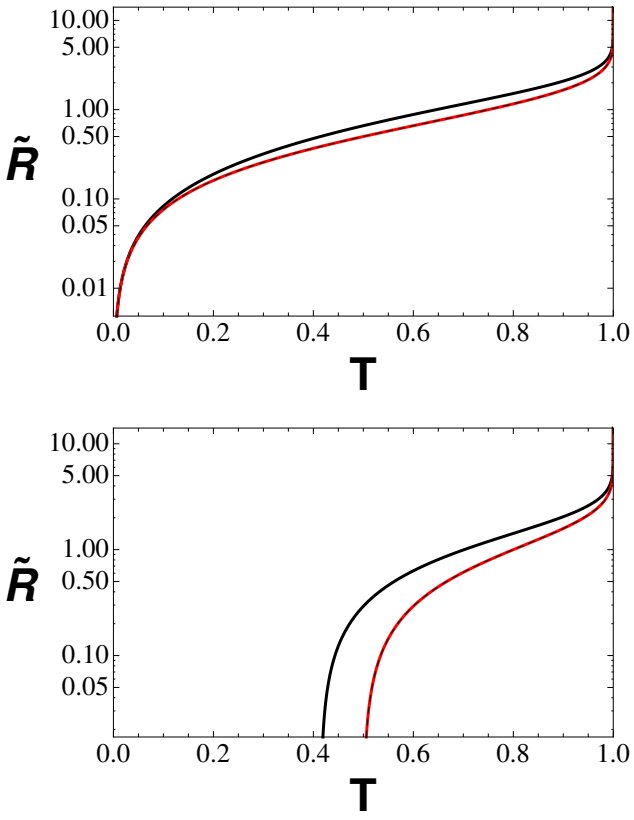

Figure C.2: Plots of the secret-key rate, in both RR (top) and DR (bottom) and in *log*-scale, for the switching protocol as a function of the channel transmissivity τ, for fixed Eve's thermal noise to $\omega = 1$. This represents a reasonable setup that Eve can choose, in order to hide her action as much as possible. One can note that the rate of the two-way (black lines) always strictly exceeds that of the one-way (dashed). Second, the two-way in DR allows the preparation of a secret-key breaking the 3dB ($\tau = 0.5$) limit of the one-way. The red line describes the secret-key rate against coherent attacks, that having $\omega = 1$ in this case coincide with the collective attack.

Now that we have all the expressions for the secret-key rates, for the various protocols and cases, it is worth noting that the two-way communication not only exceeds the performances of the one-way for what it concerns the security thresholds, but it also beats the one-way performances for what it concerns the rate. In fact, as proved by Fig. C.2 the two-way protocol, here in the coherent/Hom configuration, always provides a secret-key rate strictly larger than that of the corresponding one-way protocol. In this plot we fixed Eve's thermal noise to $\omega = 1$ and plotted the secret-key rate as a function of the channel's transmissivity, in Log-scale.

Appendix D

Canonical forms: calculations

D.1 Non-switching protocol

D.1.1 Canonical form $\mathcal{D}$

We consider the communication channel described by the following canonical form

$$\mathbf{M} = \begin{pmatrix} \sqrt{-\tau}\mathbf{Z} & \sqrt{1-\tau}\mathbf{I} \\ -\sqrt{1-\tau}\mathbf{I} & -\sqrt{-\tau}\mathbf{Z} \end{pmatrix} \tag{D.1}$$

Alice-Bob's joint state, after the evolution described by this channel, is given by the CM (modes' order $\{A, B\}$)

$$\mathbf{V}_{AB}^{\mathcal{D}} = \begin{pmatrix} \mu\mathbf{I} & \sqrt{-\tau}\sqrt{\mu^2-1}\mathbf{I} \\ \sqrt{-\tau}\sqrt{\mu^2-1}\mathbf{I} & [-\tau\mu+(1-\tau)\omega]\mathbf{I} \end{pmatrix}.$$

As usual we compute the mutual information, that is given by the following expression, in the asymptotic limit

$$I_{AB}^{\mathcal{D}} = \log \frac{1-\tau\mu+(1-\tau)\omega}{1-\tau+(1-\tau)\omega} \overset{\mu>>1}{\to} \log_2 \frac{-\tau\mu}{1-\tau+(1-\tau)\omega}.$$

Eve's thermal noise is defined in terms of excess of noise, N, is given by the following formula

$$\omega = \frac{1-\tau-N\tau}{1-\tau},$$

The total Eve's CM is given by

$$\mathbf{V}_{E}^{\mathcal{D}} = \begin{pmatrix} [-\tau\omega+(\mathbf{1}-\tau)\mu]\mathbf{I} & \sqrt{-\tau(\omega^2-1)}\mathbf{I} \\ \sqrt{-\tau(\omega^2-1)}\mathbf{I} & \omega\mathbf{I} \end{pmatrix},$$

whose asymptotic determinant is

$$\det \mathbf{V}_{E}^{\mathcal{D}} = [\tau-(1-\tau)\omega\mu]^2 \overset{\mu>>1}{\to} (1-\tau)^2\omega^2\mu^2.$$

We find the following symplectic spectrum for large μ

$$\nu_1^{\mathcal{D}} = \frac{(1-\tau)(\omega+\mu)+\sqrt{(1-\tau)^2(\omega+\mu)^2-4[-\tau+(1-\tau)\omega\mu]}}{2} \overset{\mu>>1}{\to} (1-\tau)\mu,$$

$$\nu_2^{\mathcal{D}} = \frac{(1-\tau)(\omega+\mu)-\sqrt{(1-\tau)^2(\omega+\mu)^2-4[-\tau+(\tau-1)\omega\mu]}}{2} \overset{\mu>>1}{\to} \omega$$

and the following total von Neumann entropy

$$S_E = h(\nu_1^{\mathcal{D}}) + h(\nu_2^{\mathcal{D}}) \overset{\mu>>1}{\to} h(\omega) + \log_2 \frac{e}{2}(1-\tau)\mu,$$

D.1.2 Direct Reconciliation

Conditioning with respect Alice's state preparation, described by variable α, one obtains the following conditional CM

$$\mathbf{V}^{\mathcal{D}}_{E|\alpha} = \begin{pmatrix} [-\tau\omega+(1-\tau)]\mathbf{I} & -\sqrt{-\tau(\omega^2-1)}\mathbf{I} \\ -\sqrt{-\tau(\omega^2-1)}\mathbf{I} & \omega\mathbf{I} \end{pmatrix}$$

with determinant and conditional spectrum

$$\begin{aligned} &\det \mathbf{V}^{\mathcal{D}}_{E|\alpha} = (\tau+(\tau-1)\omega)^2, \\ &\{\overline{\nu}^{\mathcal{D}}_1, \overline{\nu}^{\mathcal{D}}_2\} \to \{1, -\tau+(1-\tau)\omega\}. \end{aligned}$$

giving the following expression for the conditional von Neumann entropy

$$S^{\mathcal{D}}_{E|\alpha} = h(-\tau+(1-\tau)\omega).$$

The rate is given by

$$\begin{aligned} R^{\blacktriangleright}_{\mathcal{D}}(\mu,\tau,\omega) &= \log_2 \frac{1-\tau\mu+(1-\tau)\omega}{1-\tau+(1-\tau)\omega} + h(-\tau+(1-\tau)\omega) - h(\nu^{\mathcal{D}}_1) + h(\nu^{\mathcal{D}}_2), \\ &\overset{\mu>>1}{\to} h(-\tau+(1-\tau)\omega) - h(\omega) + \log_2 \frac{2}{e}\frac{-\tau}{(1-\tau)[1-\tau+(1-\tau)\omega]}. \end{aligned}$$

D.1.3 Reverse Reconciliation

The conditional covariance matrix is given by the following CM

$$\mathbf{V}^{\mathcal{D}}_{E|\beta} = \begin{pmatrix} \frac{\tau(\omega+\mu)-(1+\omega)\mu}{\tau\mu-(1-\tau)\omega-1}\mathbf{I} & -\frac{\sqrt{-\tau(\omega^2-1)}(\mu-1)}{-1+(\tau-1)\omega+\tau\mu}\mathbf{I} \\ -\frac{\sqrt{-\tau(\omega^2-1)}(\mu-1)}{-1+(\tau-1)\omega+\tau\mu}\mathbf{I} & \frac{\tau(\omega+\mu)-(1+\omega)\mu}{\tau\mu-(1-\tau)\omega-1}\mathbf{I} \end{pmatrix},$$

which provides the following conditional determinant

$$\det \mathbf{V}^{\mathcal{D}}_{E|\beta} = \left(\frac{\tau-\mu(1+\omega)+\tau\omega\mu}{-1+(\tau-1)\omega+\tau\mu}\right)^2 \overset{\mu>>1}{\to} \frac{(1+(1-\tau)\omega)^2}{\tau^2}$$

and symplectic spectrum

$$\{\widetilde{\nu}^{\mathcal{D}}_1, \widetilde{\nu}^{\mathcal{D}}_2\} = \left\{1, \frac{-\tau+\mu(1+\omega)-\tau\omega\mu}{1+(1-\tau)\omega-\tau\mu}\right\} \overset{\mu>>1}{\to} \{1, \frac{1+(1-\tau)\omega}{\tau}\}.$$

The conditional von Neumann entropy and the secret key rate are

$$\begin{aligned} S^{\mathcal{D}}_{E|\beta} &= h(\widetilde{\nu}^{\mathcal{D}}_2) = h\left[\left|\frac{1+(1-\tau)\omega}{\tau}\right|\right], \\ R^{\blacktriangleleft}_{\mathcal{D}}(\mu,\tau,\omega) &= \log \frac{1-\tau\mu+(1-\tau)\omega}{1-\tau+(1-\tau)\omega} + h\left[\widetilde{\nu}^{D}_1\right] - h(\nu^{D}_1) + h(\nu^{D}_2), \\ &\overset{\mu>>1}{\to} h\left[\frac{1+(1-\tau)\omega}{\tau}\right] - h(\omega) + \log_2 \frac{2}{e}\frac{-\tau}{(1-\tau)(1-\tau+(1-\tau)\omega)}. \end{aligned}$$

D.2 Canonical form $\mathcal{A}_2$

This channel is described by the symplectic matrix

$$\mathbf{M}_{\mathcal{A}_2} = \begin{pmatrix} \frac{\mathbf{I}+\mathbf{Z}}{2} & \mathbf{I} \\ I & \frac{\mathbf{Z}-\mathbf{I}}{2} \end{pmatrix} = \begin{pmatrix} 1 & & 1 & \\ & & & 1 \\ 1 & & & \\ & 1 & & -1 \end{pmatrix}. \tag{D.2}$$

We note that this canonical form, does not generate correlation between p-quadratures, so the contribution to the mutual information from this terms will be null. In this protocol Alice and Bob variables generating correlation will be q.

The output joint CM is then given by the following expression

$$\mathbf{V}_{AB}^{\mathcal{A}_2} = \begin{pmatrix} \mu & & \sqrt{\mu^2-1} & \\ & \mu & & \\ \sqrt{\mu^2-1} & & \omega+\mu & \\ & & & \omega \end{pmatrix}. \tag{D.3}$$

From which we compute Alice-Bob's mutual information

$$I_{AB}^{\mathcal{A}_2} = \frac{I_{AB}^q + I_{AB}^p}{2} = \frac{\log_2 \frac{\mu+\omega+1}{\omega+1} + \log_2 \frac{\omega+1}{\omega+1}}{2} = \frac{1}{2}\log_2 \frac{\mu+\omega+1}{\omega+1+1} \overset{\mu>>1}{\to} \frac{1}{2}\log \frac{\mu}{\omega+2} \tag{D.4}$$

The total Eve's CM is

$$\mathbf{V}_{E}^{\mathcal{A}_2} = \begin{pmatrix} \mu & & & \\ & \omega+\mu & & \sqrt{\omega^2-1} \\ & & \omega & \\ & \sqrt{\omega^2-1} & & \omega \end{pmatrix}, \tag{D.5}$$

and the corresponding total symplectic spectrum is given by the following formulas

$$\nu_1^{\mathcal{A}_2} = \sqrt{\frac{\omega^2+\omega\mu+\mu^2-\sqrt{\omega^4+2\omega\mu(\omega^2-2)-\omega^2\mu^2+2\omega\mu^3+\mu^4}}{2}} \overset{\mu>>1}{\to} \omega, \tag{D.6}$$

$$\nu_2^{\mathcal{A}_2} = \sqrt{\frac{\omega^2+\omega\mu+\mu^2+\sqrt{\omega^4+2\omega\mu(\omega^2-2)-\omega^2\mu^2+2\omega\mu^3+\mu^4}}{2}} \overset{\mu>>1}{\to} \mu \tag{D.7}$$

From this, as usual, we obtain the total von Neumann entropy

$$S_E = h(\nu_1^{\mathcal{A}_2}) + h(\nu_2^{\mathcal{A}_2}) \overset{\mu>>1}{\to} h(\omega) + \log_2 \frac{e}{2}\mu,$$

D.2.1 Direct Reconciliation

The conditional CM can easily be computed. It is given by the following matrix

$$\mathbf{V}_{E|\alpha}^{\mathcal{A}_2} = \begin{pmatrix} 1 & & & \\ & \omega+1 & & \sqrt{\omega^2-1} \\ & & \omega & \\ & \sqrt{\omega^2-1} & & \omega \end{pmatrix},$$

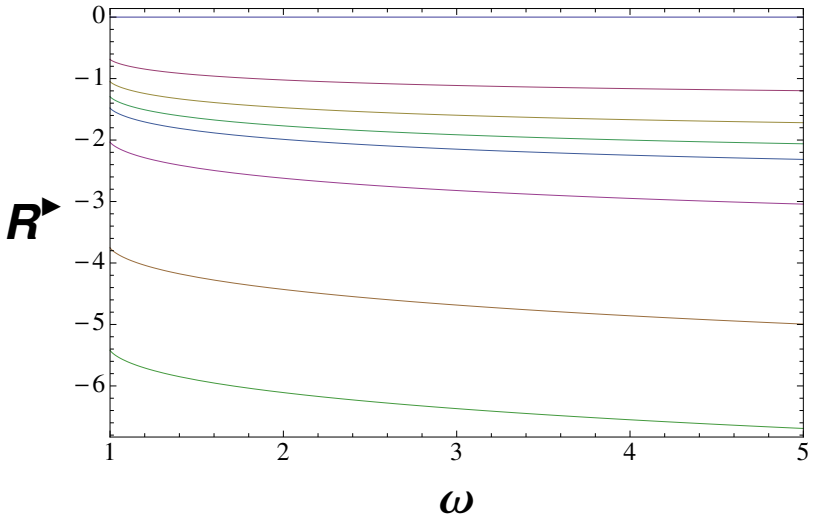

Figure D.1: Canonical form $\mathcal{A}_2$, non-switching, DR. The secret-key rate is always negative. The plots describe the dependency of the secret-key from the classical modulation of the prepared state (μ) and from Eve's thermal noise. $\mu = 1, 2, 3, 4, 5, 10, 100, 10^3$ (from top to bottom).

from which one can compute the following conditional spectrum

$$\{\overline{\nu}_1^{\mathcal{A}_2}, \overline{\nu}_2^{\mathcal{A}_2}\} \rightarrow \{1, \sqrt{\omega(1+\omega)}\},$$

and the conditional von Neumann entropy

$$S_{E|Alice}^{\mathcal{A}_2} = h[\sqrt{\omega(1+\omega)}].$$

The rate is given by

$$\begin{aligned} R_{\mathcal{A}_2}^{\blacktriangleright}(\mu,\omega) &= \frac{1}{2}\log_2\frac{\mu+\omega+1}{\omega+1+1} + h[\sqrt{\omega(1+\omega)}] - h(\nu_1^{A_2}) - h(\nu_2^{A_2}), \\ &\overset{\mu>>1}{\rightarrow} h[\sqrt{\omega(1+\omega)}] - h(\omega) + \log_2\frac{2}{e}\frac{1}{\sqrt{(\omega+2)\mu}}. \end{aligned}$$

note that the asymptotic secret-key rate $R_{\mathcal{A}_2}^{\blacktriangleright}(\mu >> 1, \omega)$ is always negative,as described in Fig. D.1.

D.2.2 Reverse Reconciliation

We can write the conditional CM in the following form

$$\mathbf{V}_{E|\beta}^{A_2} = \begin{pmatrix} \frac{(1+\omega)\mu}{1+\omega+\mu} & & -\frac{\sqrt{\omega^2-1}\mu}{1+\omega+\mu} & \\ & \frac{\omega}{\omega+1}+\mu & & \frac{\omega-1}{\sqrt{\omega^2-1}} \\ -\frac{\sqrt{\omega^2-1}\mu}{1+\omega+\mu} & & \frac{1+\omega+\omega\mu}{1+\omega+\mu} & \\ & \frac{\omega-1}{\sqrt{\omega^2-1}} & & 1 \end{pmatrix},$$

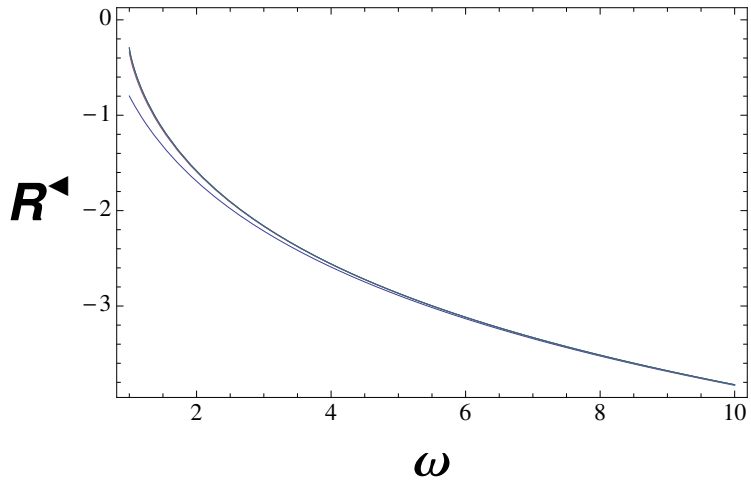

Figure D.2: Canonical form A_2, non-switching protocol in RR. We plotted for several values of the modulation $\mu = 1$ (bottom line) and $\mu = 10, 100, 10^3, 10^6$ (top lines).

from which one can compute the following determinant and conditional spectrum

$$\det \mathbf{V}_{E|\beta}^{A_2} = \frac{\mu(1+\mu+\omega\mu)}{1+\omega+\mu} \overset{\mu>>1}{\to} (1+\omega)\mu,$$
$$\{\widetilde{\nu}_1^{A_2}, \widetilde{\nu}_2^{A_2}\} \to \left\{1, \sqrt{\frac{\mu(1+\mu+\omega\mu)}{1+\omega+\mu}}\right\} \overset{\mu>>1}{\to} \{1, \sqrt{\mu(1+\omega)}\},$$

and asymptotic conditional von Neumann entropy

$$S_{E|Bob}^{A_2} = h\left[\sqrt{\frac{\mu(1+\mu+\omega\mu)}{1+\omega+\mu}}\right] \overset{\mu>>1}{\to} h[\sqrt{\mu(1+\omega)}].$$

The rate is given by

$$R_{A_2}^{\blacktriangleleft}(\mu,\omega) = \frac{1}{2}\log_2\frac{\mu+\omega+1}{\omega+1+1} + h\left[\sqrt{\frac{\mu(1+\mu+\omega\mu)}{1+\omega+\mu}}\right] - h(\nu_1^{A_2}) - h(\nu_2^{A_2}),$$
$$\overset{\mu>>1}{\to} -h(\omega) + \frac{1}{2}\log_2\frac{\omega+1}{\omega+2}.$$

The rate is again always negative (see Fig. D.2).

D.3 Canonical form $\mathcal{B}_1$

We consider the case $\omega = 1$ and we start from the CM describing Alice's initial state, that is given by

$$\mathbf{V}_{AA'} = \begin{pmatrix} \mu\mathbf{I} & \sqrt{\mu^2-1}\mathbf{Z} \\ \sqrt{\mu^2-1}\mathbf{Z} & \mu\mathbf{I} \end{pmatrix}.$$

The symplectic canonical form characterizing the interaction between modes A' and E', is given by the following matrix [11]

$$\mathbf{M}_{B_1} = \begin{pmatrix} \mathbf{I} & \frac{\mathbf{Z}+\mathbf{I}}{2} \\ \frac{I-\mathbf{Z}}{2} & -\mathbf{I} \end{pmatrix}, \tag{D.8}$$

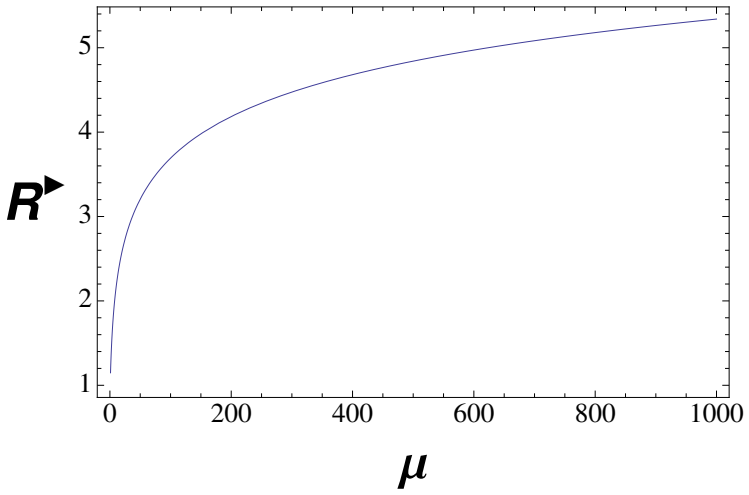

Figure D.3: Plot of the key-rate, for the canonical form B_1, in DR, as a function of Alice's modulation μ.

and after the interaction, the output joint Alice-Bob CM is given by

$$\mathbf{V}_{AB}^{\mathcal{B}_1} = \begin{pmatrix} \mu & & \sqrt{\mu^2-1} & \\ & \mu & & -\sqrt{\mu^2-1} \\ \sqrt{\mu^2-1} & & \mu+1 & \\ & -\sqrt{\mu^2-1} & & \mu \end{pmatrix}. \tag{D.9}$$

From the matrix elements describing Bob's mode, we can compute Alice-Bob's mutual information, that is given by the following expression

$$I_{AB}^{\mathcal{B}_1} = \frac{1}{2}\log_2 \frac{(\mu+1)(\mu+2)}{6} \overset{\mu>>1}{\to} \log \frac{\mu}{\sqrt{6}}. \tag{D.10}$$

D.3.1 Direct Reconciliation

Now we compute the Holevo bound. Eve's input state is described by the following CM

$$\mathbf{V}_{EE'}^{\mathcal{B}_1} = \begin{pmatrix} \mathbf{I} & \\ & \mathbf{I} \end{pmatrix},$$

which gives the following Eve's output CM after the processing

$$\mathbf{V}_{EE''}^{\mathcal{B}_1} = \begin{pmatrix} 1 & & & \\ & \mu+1 & & \\ & & 1 & \\ & & & 1 \end{pmatrix}. \tag{D.11}$$

This gives the following total symplectic spectrum

$$\nu_1^{\mathcal{B}_1} = 1,$$
$$\nu_2^{\mathcal{B}_1} = \sqrt{1+\mu} \overset{\mu>>1}{\to} \sqrt{\mu},$$

and total Eve's von Neumann entropy

$$S_E = \log_2 \frac{e}{2}\sqrt{\mu+1} \overset{\mu>>1}{\to} \log_2 \frac{e}{2}\sqrt{\mu}. \tag{D.12}$$

Finally we compute the conditional spectrum from the conditional CM of Eq. (D.11). We obtain the CM matrix

$$\mathbf{V}^{\mathcal{B}_1}_{EE''|\alpha} = \begin{pmatrix} 1 & & & \\ & 2 & & \\ & & 1 & \\ & & & 1 \end{pmatrix}, \tag{D.13}$$

whose determinant and symplectic spectrum are respectively

$$\det \mathbf{V}^{\mathcal{B}_1}_{EE''|\alpha} = 2,$$
$$\{\overline{\nu}^{B_1}_1, \overline{\nu}^{B_1}_2\} = \{\sqrt{2}, 1\},$$

The conditional von Neumann entropy is then very simply given by

$$S_{EE''|\alpha} = h(\overline{\nu}^{\mathcal{B}_1}_2),$$

where the Shannon binary entropic function $h(.)$ already defined in previous sections. We finally arrive at the following expression for the key-rate, that is given by

$$R^{\blacktriangleright}_{\mathcal{B}_1}(\mu,\tau,\omega) = \log_2 \frac{e}{2}\sqrt{\mu+2} + h(\sqrt{2}),$$

that is plotted in Fig. D.3 as a function of the modulation μ.

D.3.2 Reverse Reconciliation

We consider the CM composed by the output modes $\{B, E, E''\}$, and apply an heterodyne measurement on mode B. We obtain the following conditional CM

$$\mathbf{V}^{\mathcal{B}_1}_{EE''|\beta} = \begin{pmatrix} \frac{1+\mu}{2+\mu} & & & \\ & 2-\frac{1}{1+\mu} & & \\ & & 1 & \\ & & & 1 \end{pmatrix}.$$

We write the determinant of this matrix

$$\det \mathbf{V}^{\mathcal{B}_1}_{EE''|\beta} = 2 - \frac{3}{2+\mu},$$

that help us in to identify the symplectic spectrum and obtain the conditional von Neumann entropy. This is given by the following expressions

$$\widetilde{\nu}^{\mathcal{B}_1}_1 = 1,$$
$$\widetilde{\nu}^{\mathcal{B}_1}_2 = \sqrt{2 - \frac{3}{2+\mu}}.$$
$$S^{\mathcal{B}_1}_{EE''|\beta} = h(\widetilde{\nu}^{\mathcal{B}_1}_2).$$

From previous equation, used with Eq. (D.10) and (D.12), we have the following key-rate

$$R^{\blacktriangleleft,B_1,Het-Hom}_{B_1}(\mu) = \frac{1}{2}\log_2 \frac{(\mu+1)(\mu+2)}{6} + h\left(\sqrt{2-\frac{3}{2+\mu}}\right) - h(\sqrt{\mu+1}),$$

that describes the reverse reconciliation plotted in Fig. D.4

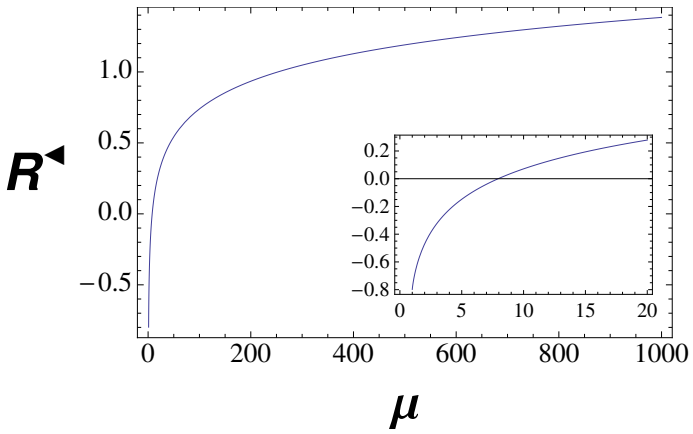

Figure D.4: Rate of the canonical form $\mathcal{B}_1$, for the non-switching protocol in RR. We see that a positive key-rate starts to be achievable increasing the modulation μ.

D.4 Switching protocol

D.4.1 $\mathcal{C}$(amp) canonical form

We rapidly describe here the steps and some detail of the computation. This case has been discussed also in the main text. Alice-Bob mutual information is given by the following expression

$$I_{AB}^{\mathcal{C},switch} = \frac{1}{2}\log_2 \frac{\tau\mu + (\tau-1)\omega}{\tau + (\tau-1)\omega}.$$

We note that the excess noise has been calculated in eq.(5.13) and if compared to the previous non-switching case, the only thing changing here is the conditioning. So one can focus on computing the conditional von Neumann entropies for both DR and RR. We briefly illustrate this calculations in the next sections.

Direct Reconciliation

We compute the CCM, by setting $\mu = 1$, in one quadrature, of the following CM build from Eve's outputs modes $\{E, E''\}$

$$\mathbf{V}_{EE''|\alpha}^{\mathcal{C},switch} = \begin{pmatrix} \tau\omega+(\tau-1) & & \sqrt{\tau(\omega^2-1)} & \\ & [\tau\omega+(\tau-1)\mu] & & -\sqrt{\tau(\omega^2-1)} \\ \sqrt{\tau(\omega^2-1)} & & \omega & \\ & -\sqrt{\tau(\omega^2-1)} & & \omega \end{pmatrix}.$$

From here we can compute the determinant and the conditional symplectic spectrum, obtaining respectively

$$\det \mathbf{V}_{EE''|\alpha}^{\mathcal{C},switch} = [\tau + (\tau-1)\omega][\tau + (\tau-1)\omega\mu] \overset{\mu>>1}{\to} (\tau-1)\omega[\tau + (\tau-1)\omega]\mu,$$

$$\{\overline{\nu}_1^{\mathcal{C},switch}, \overline{\nu}_2^{\mathcal{C},switch}\} = \left\{ \sqrt{\frac{\Delta - \sqrt{\Delta^2 - 4\det V_{E|Alice}^C}}{2}}, \sqrt{\frac{\Delta - \sqrt{\Delta^2 - 4\det V_{E|Alice}^C}}{2}} \right\},$$

where $\Delta = \det\mathbf{A} + \det\mathbf{B} - 2\det\mathbf{C}$ is in this case given by the following relation

$$\Delta = (\tau\omega + \tau - 1)(\tau\omega + (\tau-1)\mu) + \omega^2 - 2\tau(\omega^2 - 1),$$

and where the matrices $\mathbf{A}, \mathbf{B}, \mathbf{C}$ define the usual blocks form of a general CM $\mathbf{V}^{\mathcal{C}}_{EE''|\alpha}$

$$\mathbf{V} = \begin{pmatrix} \mathbf{A} & \mathbf{C} \\ \mathbf{C}^T & \mathbf{B} \end{pmatrix}.$$

The asymptotic spectrum is given taking the limit of large μ, and it is easy to verify that we obtain

$$\{\overline{\nu}_1^{\mathcal{C},switch}, \overline{\nu}_2^{\mathcal{C},switch}\} \overset{\mu>>1}{\to} \left\{\sqrt{\frac{\omega[\tau + (\tau-1)\omega]}{\tau - 1 + \tau\omega}}, \sqrt{(\tau-1)(\tau - 1 + \tau\omega)\mu}\right\}.$$

From these expression we can compute the conditional von Neumann entropy that is given by

$$S^{\mathcal{C},switch}_{EE''|\alpha} = h(\overline{\nu}_1^{\mathcal{C},switch}) + \frac{1}{2}\log_2\left(\frac{e}{2}\right)^2 (\tau-1)(\tau - 1 + \tau\omega)\mu, \tag{D.14}$$

and the key rate, that using previous equation can be written as follows

$$R^{\blacktriangleright,switch}_{\mathcal{C}}(\mu,\tau,\omega) = h(\overline{\nu}_1^{\mathcal{C},switch}) - h(\omega) + \log_2\frac{\tau(\tau - 1 + \tau\omega)}{(\tau-1)[\tau + (\tau-1)\omega]} \tag{D.15}$$

Reverse Reconciliation

The conditional CM, determinant and spectrum are now given by the following expressions

$$\mathbf{V}^{\mathcal{C},switch}_{EE''|\beta} = \begin{pmatrix} \frac{\omega\mu}{(\tau-1)\omega+\tau\mu} & & \frac{\sqrt{\tau(\omega^2-1)}\mu}{\tau\mu+(\tau-1)\omega} & \\ & \tau(\omega+\mu) - \mu & & -\sqrt{\tau(\omega^2-1)} \\ \frac{\sqrt{\tau(\omega^2-1)}\mu}{\tau\mu+(\tau-1)\omega} & & \frac{\tau+\tau\omega\mu-1}{(\tau-1)\omega+\tau\mu} & \\ & -\sqrt{\tau(\omega^2-1)} & & \omega \end{pmatrix},$$

$$\det\mathbf{V}^{\mathcal{C},switch}_{EE''|\beta} = \frac{\mu[\tau + (\tau-1)\omega\mu]}{(\tau-1)\omega + \tau\mu} \overset{\mu>>1}{\to} \frac{(\tau-1)\omega\mu}{\tau},$$

$$\{\widetilde{\nu}_1^{\mathcal{C},switch}, \widetilde{\nu}_2^{\mathcal{C},switch}\} = \left\{1, \sqrt{\frac{\mu[\tau + (\tau-1)\omega\mu]}{(\tau-1)\omega + \tau\mu}}\right\} \overset{\mu>>1}{\to} \left\{1, \sqrt{\frac{(\tau-1)\omega\mu}{\tau}}\right\}.$$

The conditional von Neumann entropy is

$$S^{\mathcal{C},switch}_{E|Bob} = h(\widetilde{\nu}_2^{\mathcal{C}}) \overset{\mu>>1}{\to} \log_2\frac{e}{2}\sqrt{\frac{(\tau-1)\omega\mu}{\tau}},$$

and the security rate

$$\begin{aligned} R^{\blacktriangleleft,switch}_{\mathcal{C}}(\mu,\tau,\omega) &= \log_2\frac{\tau\mu + (\tau-1)\omega}{\tau + (\tau-1)\omega} + h(\widetilde{\nu}_1^C) + h(\widetilde{\nu}_2^C) - h(\nu_1^C) - h(\nu_2^C), \\ &\overset{\mu>>1}{\to} -h(\omega) + \frac{1}{2}\log_2\frac{\omega}{(\tau-1)(\tau + (\tau-1)\omega)}. \end{aligned}$$

The security regions of these both these rates in DR and RR are summarized in Fig. 5.7 (dashed lines)

D.4.2 $\mathcal{D}$ canonical form

Alice-Bob mutual information is given by the expression

$$I_{AB}^{\mathcal{D},switch} = \log_2 \frac{(1-\tau)\omega - \tau\mu}{(1-\tau)\omega - \tau} \overset{\mu>>1}{\to} \log_2 \frac{-\tau\mu}{(1-\tau)\omega - \tau}, \tag{D.16}$$

as already described in the main text. Eve's total CM,, is easy to be computed and is given by the matrix

$$\mathbf{V}_E^{\mathcal{D},switch} = \begin{pmatrix} [(1-\tau)\mu - \tau\omega]\mathbf{I} & -\sqrt{-\tau(\omega^2-1)}\mathbf{I} \\ -\sqrt{-\tau(\omega^2-1)}\mathbf{I} & \omega\mathbf{I} \end{pmatrix},$$

giving the following spectrum, that asymptotically ($\mu >> 1$) gives

$$\nu_1^{\mathcal{D},switch} = \frac{(1-\tau)(\omega+\mu) + \sqrt{(1-\tau)^2(\mu+\omega)^2 - 4[\omega\mu(1-\tau)-\tau]}}{2} \overset{\mu>>1}{\to} (1-\tau)\mu,$$
$$\nu_2^{\mathcal{D},switch} = \frac{(1-\tau)(\omega+\mu) - \sqrt{(1-\tau)^2(\mu+\omega)^2 - 4[\omega\mu(1-\tau)-\tau]}}{2} \overset{\mu>>1}{\to} \omega,$$

The total von Neumann entropy is then

$$S_E^{\mathcal{D}} = h(\omega) + \log_2 \frac{e}{2}(1-\tau)\mu,$$

Direct Reconciliation

Conditioning with respect Alice's state preparation, we get the following CCM

$$V_{E|Alice}^{\mathcal{D}} = \begin{pmatrix} (1-\tau)-\tau\omega & & -\sqrt{-\tau(\omega^2-1)} & \\ & [(1-\tau)\mu - \tau\omega]\,\mu & & -\sqrt{-\tau(\omega^2-1)} \\ -\sqrt{-\tau(\omega^2-1)} & & \omega & \\ & -\sqrt{-\tau(\omega^2-1)} & & \omega \end{pmatrix}$$

with determinant and conditional spectrum given by

$$\det \mathbf{V}_{E|Alice}^{\mathcal{D},switch} = [\tau - (1-\tau)\omega][\tau - (1-\tau)\omega\mu] \overset{\mu>>1}{\to} (1-\tau)[(1-\tau)\omega - \tau]\omega\mu$$
$$\{\overline{\nu}_1^{\mathcal{D}}, \overline{\nu}_2^{\mathcal{D}}\} \overset{\mu>>1}{\to} \left\{ \sqrt{\frac{\omega[(1-\tau)\omega-\tau]}{1-\tau(\omega+1)}}, \sqrt{(1-\tau)[1-\tau(\omega+1)]\mu} \right\}.$$

From previous equation we can compute the conditional von Neumann entropy

$$S_{E|Alice}^{\mathcal{D},switch} = h(\overline{\nu}_1^{\mathcal{D}}) + h(\overline{\nu}_2^{\mathcal{D}})$$
$$\overset{\mu>>1}{\to} h\left(\sqrt{\frac{\omega[(1-\tau)\omega-\tau]}{1-\tau(\omega+1)}} \right) + \frac{1}{2}\log_2 \left(\frac{e}{2}\right)^2 (1-\tau)[1-\tau(\omega+1)]\mu$$

The rate is given by

$$R_{\mathcal{D},switch}^{\blacktriangleright} \overset{\mu>>1}{\to} h\left(\sqrt{\frac{\omega[(1-\tau)\omega-\tau]}{1-\tau(\omega+1)}} \right) - h(\omega) + \frac{1}{2}\log_2 \frac{-\tau(1-\tau(\omega+1))}{(1-\tau)((1-\tau)\omega-\tau)}$$

As we have seen in the main text this communication channel is always insecure.

Reverse Reconciliation

We give now some more detail of the computation for the reverse reconciliation. We need the CCM, that is given by the following matrix

$$\mathbf{V}_{E|\beta}^{\mathcal{D},switch} = \begin{pmatrix} -\frac{(1-2\tau)^2\omega\mu}{\tau\mu-(1-\tau)\omega} & & \frac{(1-2\tau)\sqrt{-\tau(\omega^2-1)\mu}}{\tau\mu-(1-\tau)\omega} & \\ & \mu-\tau(\omega+\mu) & & -\sqrt{-\tau(\omega^2-1)} \\ \frac{(1-2\tau)\sqrt{-\tau(\omega^2-1)\mu}}{\tau\mu-(1-\tau)\omega} & & \frac{(1-2\tau)^2\omega\mu}{\tau\mu-(1-\tau)\omega} & \\ & -\sqrt{-\tau(\omega^2-1)} & & \omega \end{pmatrix},$$

This has the following determinant

$$\det \mathbf{V}_{E|\beta}^{\mathcal{D},switch} = \frac{(1-2\tau)^2(\tau-(1-\tau)\omega\mu)\mu}{\tau\mu-(1-\tau)\omega} \overset{\mu>>1}{\to} -\frac{(1-2\tau)^2(1-\tau)\omega\mu}{\tau}$$

from which we can extract the symplectic spectrum

$$\{\widetilde{\nu}_1^{\mathcal{D}},\widetilde{\nu}_2^{\mathcal{D}}\}_{switch} = \left\{1,(1-2\tau)\sqrt{\frac{(\tau-(1-\tau)\omega\mu)\mu}{\tau\mu-(1-\tau)\omega}}\right\} \overset{\mu>>1}{\to} \left\{1,(1-2\tau)\sqrt{\frac{(1-\tau)\omega\mu}{-\tau}}\right\}.$$

The conditional von Neumann entropy and the secret key rate are

$$S_{E|\beta}^{\mathcal{D},switch} \overset{\mu>>1}{\to} (1-2\tau)\sqrt{\frac{(1-\tau)\omega\mu}{-\tau}},$$
$$R_{\mathcal{D}}^{\blacktriangleleft,switch}(\mu,\tau,\omega) \overset{\mu>>1}{\to} \frac{1}{2}\log_2\frac{(1-2\tau)^2\omega}{(1-\tau)[(1-\tau)\omega-\tau]} - h(\omega)$$

D.4.3 $\mathcal{A}_2$ canonical form

The symplectic form corresponding to this canonical form is given by eq.(D.2), and Alice-Bob state are described by the following CM

$$\mathbf{V}_{AB}^{\mathcal{A}_2} = \begin{pmatrix} \mu & & \sqrt{\mu^2-1} & \\ & \mu & & \\ \sqrt{\mu^2-1} & & \omega+\mu & \\ & & & \omega \end{pmatrix},$$

from which we can compute the following Alice-Bob mutual information

$$I_{AB}^{\mathcal{A}_2,switch} = \frac{1}{2}\log_2\frac{\mu}{\omega+1} \tag{D.17}$$

Now, Eve's CM is the same as in Eq. (D.5) and then symplectic eigenvalues of Eqs. (D.6,D.7). The total von Neumann entropy is of course the same for all protocols

$$S_E^{\mathcal{A}_2,switch} = h(\nu_1^{A_2}) + h(\nu_2^{A_2}) \overset{\mu>>1}{\to} h(\omega) + \log_2\frac{e}{2}\mu,$$

Direct Reconciliation

The CCM changes depending on the measurements, i.e., the conditioning. There are two conditioning, depending on the quadrature measured by Bob, $\hat{q}$ or $\hat{p}$

$$\mathbf{V}_{E|\alpha}^{\mathcal{A}_2,switch(\hat{q})} = \begin{pmatrix} 1 & & \\ & \omega+\mu & \sqrt{\omega^2-1} \\ & \omega & \\ & \sqrt{\omega^2-1} & \omega \end{pmatrix}$$

$$\mathbf{V}_{E|\alpha}^{\mathcal{A}_2,switch(\hat{p})} = \begin{pmatrix} \mu & & \\ & \omega+1 & \sqrt{\omega^2-1} \\ & \omega & \\ & \sqrt{\omega^2-1} & \omega \end{pmatrix}$$

The first gives the following determinant and conditional spectrum

$$\begin{aligned} \det \mathbf{V}_{E|Alice}^{\mathcal{A}_2,switch(\hat{q})} &= \omega(1+\omega\mu), \\ \overline{\nu}_1^{\mathcal{A}_2,switch(\hat{q})} &= \sqrt{\frac{\omega+\omega^2+\mu-\sqrt{\omega[\omega(1+\omega)^2-4]-2\omega\mu(\omega-1)+\mu^2}}{2}}, \\ \overline{\nu}_2^{\mathcal{A}_2,switch(\hat{q})} &= \sqrt{\frac{\omega+\omega^2+\mu+\sqrt{\omega[\omega(1+\omega)^2-4]-2\omega\mu(\omega-1)+\mu^2}}{2}}. \end{aligned}$$

while from phase measurements ($\mathbf{V}_{E|\alpha}^{\mathcal{A}_2,switch(\hat{p})}$) we have

$$\begin{aligned} \det \mathbf{V}_{E|\alpha}^{\mathcal{A}_2,switch(\hat{p})} &= \omega(1+\omega)\mu, \\ \overline{\nu}_1^{\mathcal{A}_2,switch(\hat{p})} &= \sqrt{\frac{\omega+\omega(\omega+\mu)-\sqrt{\omega^4+2\omega\mu(\omega-2)(\omega+1)+(1+\omega)^2\mu^2}}{2}}, \\ \overline{\nu}_2^{\mathcal{A}_2,switch(\hat{p})} &= \sqrt{\frac{\omega+\omega(\omega+\mu)+\sqrt{\omega^4+2\omega\mu(\omega-2)(\omega+1)+(1+\omega)^2\mu^2}}{2}}. \end{aligned}$$

From here, taking the average of the two possible von Neumann entropies form the basis measured, we arrive at the final expression for the conditional von Neumann entropy

$$\begin{aligned} S_{E|\alpha}^{\mathcal{A}_2,switch(\hat{q})} &= h[\overline{\nu}_1^{\mathcal{A}_2,switch(\hat{q})}] + h[\overline{\nu}_2^{\mathcal{A}_2,switch(\hat{q})}] \\ S_{E|\alpha}^{\mathcal{A}_2,switch(\hat{p})} &= h[\overline{\nu}_1^{\mathcal{A}_2,switch(\hat{p})}] + h[\overline{\nu}_2^{\mathcal{A}_2,switch(\hat{p})}] \\ S_{E|\alpha}^{\mathcal{A}_2,switch} &= \frac{S_{E|\alpha}^{\mathcal{A}_2,\mathcal{A}_2,switch(\hat{q})} + S_{E|\alpha}^{\mathcal{A}_2,switch(\hat{p})}}{2}. \end{aligned}$$

The secret-key rate is given by

$$\begin{aligned} R_{\mathcal{A}_2}^{\blacktriangleright,switch}(\mu,\omega) &= I_{AB}^{\mathcal{A}_2,switch} + S_{E|\alpha}^{\mathcal{A}_2,switch} - S_E^{\mathcal{A}_2,switch}, \\ &\overset{\mu>>1}{\to} \frac{h(\sqrt{\omega})}{2} - \frac{h(\omega)}{2} + \frac{1}{4}\log_2\frac{1}{\omega+1}, \end{aligned} \tag{D.18}$$

that provide a key-rate that is always negative.

Reverse Reconciliation

We have the following conditional CMs

$$\mathbf{V}_{E|\beta}^{\mathcal{A}_2,switch(\hat{q})} = \begin{pmatrix} \frac{\omega\mu}{\omega+\mu} & & -\frac{\sqrt{\omega^2-1}\mu}{\omega+\mu} & \\ & \omega+\mu & & \sqrt{\omega^2-1} \\ -\frac{\sqrt{\omega^2-1}\mu}{\omega+\mu} & & \frac{1+\omega\mu}{\omega+\mu} & \\ & \sqrt{\omega^2-1} & & \omega \end{pmatrix},$$

$$\mathbf{V}_{E|\beta}^{\mathcal{A}_2,switch(\hat{p})} = \begin{pmatrix} \mu & & & \\ & \mu & & \\ & & \omega & \\ & & & \frac{1}{\omega} \end{pmatrix},$$

with determinant and conditional spectrum given by the following expressions

$$\det \mathbf{V}_{E|\beta}^{\mathcal{A}_2,switch(\hat{q})} = \frac{\mu(1+\omega\mu)}{\omega+\mu} \overset{\mu>>1}{\to} \omega\mu,$$

$$\{\widetilde{\nu}_1^{\mathcal{A}_2,switch(\hat{q})}, \widetilde{\nu}_2^{\mathcal{A}_2,switch(\hat{q})}\} \to \left\{1, \sqrt{\frac{\mu(1+\omega\mu)}{\omega+\mu}}\right\} \overset{\mu>>1}{\to} \{1, \sqrt{\mu\omega}\}.$$

From these we have the conditional von Neumann entropy for measurements on $\hat{q}$

$$S_{E|\beta}^{\mathcal{A}_2,switch(\hat{q})} = h\left[\sqrt{\frac{\mu(1+\omega\mu)}{\omega+\mu}}\right] \overset{\mu>>1}{\to} h[\sqrt{\mu\omega}],$$

and for measurements on $\hat{p}$ we have the following spectrum

$$\det V_{E|\beta}^{\mathcal{A}_2,switch(\hat{p})} = \mu^2,$$

$$\{\widetilde{\nu}_1^{\mathcal{A}_2,switch(\hat{p})}, \widetilde{\nu}_2^{\mathcal{A}_2,switch(\hat{p})}\} = \{1, \mu\},$$

providing the von Neumann entropy conditioned to the measurement performed by Bob

$$S_{E|\beta}^{\mathcal{A}_2,switch(\hat{p})} = h(\mu).$$

We can then compute the average von Neumann entropy, considering a switching between the two possible bases measured

$$S_{E|\beta}^{\mathcal{A}_2,switch} = \frac{S_{E|\beta}^{\mathcal{A}_2,switch(\hat{q})} + S_{E|\beta}^{\mathcal{A}_2,switch(\hat{p})}}{2},$$

from which one arrives at the following formula for the secret-key rate in reverse reconciliation

$$R_{A_2}^{\blacktriangleleft}(\mu,\omega) = \frac{1}{2}\log_2\frac{\mu}{\omega+1} + S_{E|\beta}^{\mathcal{A}_2,switch} - S_E^{\mathcal{A}_2,switch}. \tag{D.19}$$

The previous key-rates and that one for the DR, given by Eq. (D.18), are represented in Fig. D.5. One can see that in DR the parties cannot prepare a secret key (left panel), while for the RR (right panel), increasing the modulation μ, it appears to be possible to prepare a secret-key also for increasing thermal noise ω.

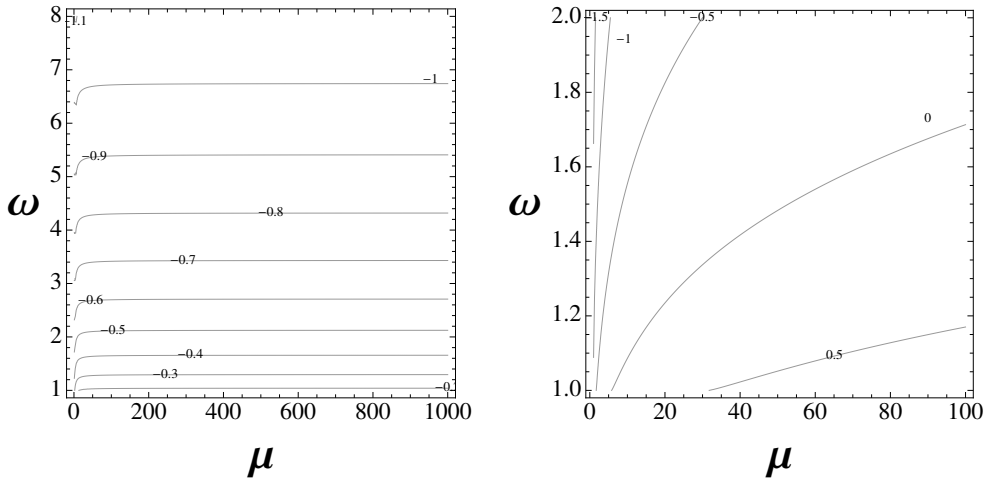

Figure D.5: This figure describes the thresholds for the one-way switching protocol with the canonical forms $\mathcal{A}_2$. The left panel describes the behavior of the DR key rate of Eq. (D.18). Teh right panel gives the RR thresholds as from the key-rate of Eq. (D.19)

D.4.4 $\mathcal{B}_1$ canonical form

Let us consider Alice's, Bob's and Eve's modes ordered as $\{A, B, E, E''\}$. The total Alice-Bob-Eve joint state is described by a CM that, after the evolution through the quantum channel described by the canonical form $\mathcal{B}_1$, is given by an 8×8 matrix that we can write as

$$\mathbf{V}_{\mathcal{B}_1}^{switch} = \begin{pmatrix} \mathbf{V}_{AB} & \mathbf{C} \\ \mathbf{C}^T & \mathbf{V}_{EE''}^{\mathcal{B}_1} \end{pmatrix}, \tag{D.20}$$

where

$$\mathbf{V}_{AB}^{\mathcal{B}_1,switch} = \begin{pmatrix} \mu & & \sqrt{\mu^2-1} & \\ & \mu & & -\sqrt{\mu^2-1} \\ \sqrt{\mu^2-1} & & \mu+1 & \\ & -\sqrt{\mu^2-1} & & \mu \end{pmatrix}, \tag{D.21}$$

$$\mathbf{C} = \begin{pmatrix} & -\sqrt{\mu^2-1} & \\ 1 & & \\ & \mu & \end{pmatrix}$$

and the block describing Eve's output is given by the following matrix

$$\mathbf{V}_{EE''}^{\mathcal{B}_1,switch} = \begin{pmatrix} 1 & & & \\ & 1+\mu & & \\ & & 1 & \\ & & & 1 \end{pmatrix}. \tag{D.22}$$

From Eq. (D.21) we can compute Alice-Bob's mutual information considering the average between final measurements performed on the two possible basis. We have

$$I_{AB}^{switch} = \frac{1}{4}\log_2 \frac{\mu(\mu+1)}{2} \overset{\mu>>1}{\to} \frac{1}{2}\log_2 \frac{\mu}{\sqrt{2}}. \tag{D.23}$$

Direct Reconciliation

To proceed with the analysis we can choose to use both the Alice-Bob CM or that relative to Eve. Let us consider $\mathbf{V}_{AB}^{\mathcal{B}_1,switch}$ of Eq. (D.21). It is easy to verify that this provides the following total symplectic spectrum

$$\begin{aligned}\nu_1^{\mathcal{B}_1} &= 1,\\ \nu_2^{\mathcal{B}_1} &= \sqrt{1+\mu} \overset{\mu>>1}{\to} \sqrt{\mu},\end{aligned}$$

from which we can obtain the total von Neumann entropy

$$S_E = \log_2 \frac{e}{2}\sqrt{\mu+1} \overset{\mu>>1}{\to} \log_2 \frac{e}{2}\sqrt{\mu}.$$

To compute the conditional CM, starting from Eq. (D.21) we can apply an heterodyne detection on Alice mode A, and obtain the following conditional symplectic eigenvalue

$$\overline{\nu}_1^{\mathcal{B}_1,switch} = \sqrt{2},$$

from which it is straightforward to obtain the conditional von Neumann entropy

$$S_{E|\alpha}^{\mathcal{B}_1,switch} = h(\overline{\nu}_1^{\mathcal{B}_1,switch}),$$

The security rate (always >0)

$$R_{\mathcal{B}_1}^{\blacktriangleright} = \frac{1}{2}\log_2 \frac{\mu(\mu+1)}{2} + h\left(\overline{\nu}_1^{\mathcal{B}_1,switch}\right) - h(\sqrt{\mu+1}). \tag{D.24}$$

This rate is always positive, and is plotted in right panel of Fig. D.6.

Reverse Reconciliation

The conditional CM, determinant and spectrum are now

$$\begin{aligned}\mathbf{V}_{E|Bob}^{\mathcal{B}_1(\hat{q})} &= \begin{pmatrix} \frac{\mu}{1+\mu} & & & \\ & 1+\mu & & \\ & & 1 & \\ & & & 1 \end{pmatrix},\\ \det \mathbf{V}_{E|Bob}^{\mathcal{B}_1(q)} &= \mu,\\ \widetilde{\nu}_1^{B_1(q)} &= 1,\\ \widetilde{\nu}_2^{B_1(q)} &= \sqrt{\mu}.\end{aligned}$$

The conditional von Neumann entropy is

$$S_{E|Bob}^{B_1(q)} = h(\sqrt{\mu}),$$

and the security rate (not always positive)

$$R_{B_1}^{\blacktriangleleft}(\mu,\omega) = R_{B_1}^{\blacktriangleright}(\mu,\omega) = \frac{1}{2}\log \frac{\mu(\mu+1)}{2} + h(\sqrt{\mu}) - h(\sqrt{1+\mu}), \tag{D.25}$$

has a threshold given in fig.D.6

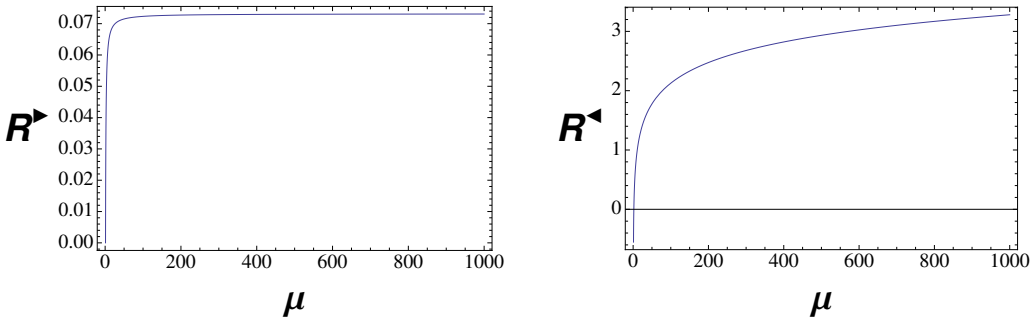

Figure D.6: The left panel of this figure represent the positive key-rate, in direct reconciliation, described by Eq. (D.24). The right panel describe the RR key-rate of Eq. (D.25), for the canonical form $\mathcal{B}_1$. Both are plotted as function of the modulation μ. In the asymptotic limit both key rate are positive.

D.5 $Hom - Het$ protocol

We provide now the details of the computation for the first of the two protocols based on squeezed state. We assume that Alice prepare send squeezed states through the quantum channel and Bob performs the decoding by heterodyne detection.

D.5.1 $\mathcal{C}(amp)$ canonical form

We start with the $\mathcal{C}(amp)$ canonical form, and we choose to study this canonical form using Eve's CM. We will provide only the main results.

Mutual Information

$$I_{AB}^{\mathcal{C},Hom-Het} = \frac{1}{2}\log\frac{(\tau-1)\omega+\tau\mu+1}{1+(\tau-1)\omega} \overset{\mu>>1}{\to} \frac{1}{2}\log\frac{\tau\mu}{1+(\tau-1)\omega},$$

The excess noise has been already defined in eq.(5.13).

Direct Reconciliation

Eve's total symplectic spectrum is given by the Eq. (5.15) and (5.16) from which we can compute the total von Neumann entropy of Eq. (5.17). We then compute the conditional CM, completing Eve's CM with Alice mode A and applying a homodyne detection on this mode. After some algebra we obtain the following CM

$$\mathbf{V}_E^{\mathcal{C},Hom-Het} = \begin{pmatrix} \frac{\tau-1+\tau\omega\mu}{\mu} & & \sqrt{\tau(\omega^2-1)} & \\ & (\tau-1)+\tau\omega & & -\sqrt{\tau(\omega^2-1)} \\ \sqrt{\tau(\omega^2-1)} & & \omega & \\ & -\sqrt{\tau(\omega^2-1)} & & \omega \end{pmatrix},$$

that has two symplectic eigenvalues that can be written as follows

$$\{\overline{\nu}_1^{\mathcal{C}},\overline{\nu}_2^{\mathcal{C}}\}_{Het-Hom} = \left\{1,\sqrt{\frac{[(\tau-1)\omega+\tau\mu][\tau+(\tau-1)\omega\mu]}{\mu}}\right\} \overset{\mu>>1}{\to} \{1,\sqrt{(\tau-1)\tau\omega\mu}\}, \tag{D.26}$$

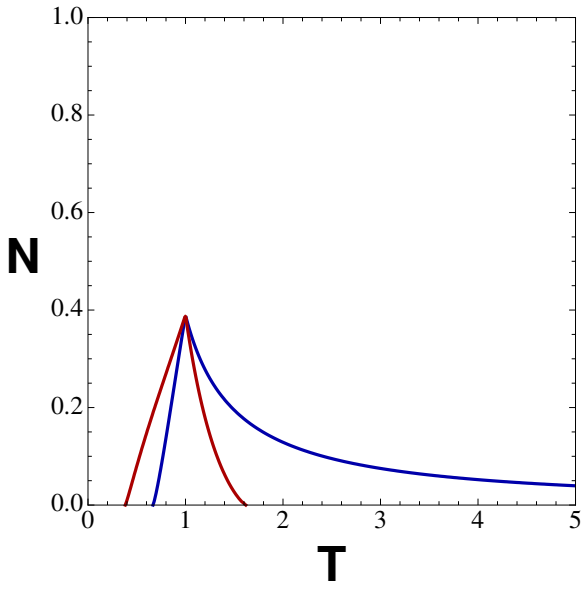

Figure D.7: Security thresholds of the Canonical form C(amp), compared with the C(loss) form, for the $Hom-Het$ protocol in DR (blue) and RR (red).

The conditional von Neumann entropy is then

$$S_{E|\alpha}^{\mathcal{C},Het-Hom} = h(\overline{\nu}_2^{\mathcal{C}}) = h\left(\sqrt{\frac{[(\tau-1)\omega+\tau\mu][\tau+(\tau-1)\omega\mu]}{\mu}}\right) \overset{\mu>>1}{\to} \log\frac{e}{2}\sqrt{(\tau-1)\tau\omega\mu}, \tag{D.27}$$

And the security rate is given by

$$R_{\mathcal{C}}^{\blacktriangleright,Hom-Het}(\mu,\tau,\omega) = \log\frac{\tau\mu+(\tau-1)\omega+1}{1+(\tau-1)\omega} + h\left(\sqrt{\frac{[(\tau-1)\omega+\tau\mu][\tau+(\tau-1)\omega\mu]}{\mu}}\right) \tag{D.28}$$

$$- h(\nu_1^C) - h(\nu_2^C),$$

$$\overset{\mu>>1}{\to} -h(\omega) + \frac{1}{2}\log\frac{\tau^2\omega}{(\tau-1)[1+(\tau-1)\omega]} \tag{D.29}$$

Reverse Reconciliation

The conditional CM, determinant and spectrum are now

$$\mathbf{V}_{E|\beta}^{\mathcal{C},Hom-Het} = \begin{pmatrix} \frac{\omega\mu}{(\tau-1)\omega+\tau\mu} & & \frac{\mu\sqrt{\tau(\omega^2-1)}}{\tau\mu+(\tau-1)\omega} & \\ & (\tau-1)\mu+\tau\omega & & -\sqrt{\tau(\omega^2-1)} \\ \frac{\mu\sqrt{\tau(\omega^2-1)}}{\tau\mu+(\tau-1)\omega} & & \frac{\tau\omega\mu+\tau-1}{\tau\mu+(\tau-1)\omega} & \\ & -\sqrt{\tau(\omega^2-1)} & & \omega \end{pmatrix},$$

$$\det \mathbf{V}_{E|\beta}^{\mathcal{C},Hom-Het} = \frac{\mu(\tau+(\tau-1)\omega\mu}{(\tau-1)\omega+\tau\mu} \overset{\mu>>1}{\to} \frac{(\tau-1)\omega\mu}{\tau},$$

$$\widetilde{\nu}_1^{\mathcal{C},Hom-Het} = 1,$$

$$\widetilde{\nu}_2^{\mathcal{C},Hom-Het} = \sqrt{\frac{\mu(\tau+(\tau-1)\omega\mu}{(\tau-1)\omega+\tau\mu}} \overset{\mu>>1}{\to} \sqrt{\frac{(\tau-1)\omega\mu}{\tau}}.$$

The conditional von Neumann entropy is

$$S_{E|\beta}^{\mathcal{C},Hom-Het} = h(\widetilde{\nu}_2^{\mathcal{C},Hom-Het}) = h\left(\sqrt{\frac{(\tau-1)\omega\mu}{\tau}}\right),$$

and the security rate

$$R_{\mathcal{C}}^{\blacktriangleleft,Hom-Het}(\mu,\tau,\omega) = \log\frac{1+\tau\mu+(\tau-1)\omega}{1+\tau+(\tau-1)\omega} + h(\frac{1+\omega(\tau-1)}{\tau}) - h(\nu_1^C) + h(\nu_2^C),$$
$$\overset{\mu>>1}{\to} -h(\omega) + \frac{1}{2}\log\frac{\omega}{(\tau-1)[1+(\tau-1)\omega]}$$

Fig.(D.7) shows a summary of the behavior of the security thresholds.

D.5.2 $\mathcal{D}$ canonical form

Mutual Information

$$I_{AB}^{\mathcal{D},Hom-Het} = \frac{1}{2}\log\frac{(1-\tau)\omega-\tau\mu+1}{(1-\tau)\omega+1} \overset{\mu>>1}{\to} \frac{1}{2}\log\frac{-\tau\mu}{(1-\tau)\omega+1}.$$

The excess noise is given by the same relation of eq.(5.30)

Direct Reconciliation

Conditioning with respect Alice's state preparation, we get the following conditional CM

$$\mathbf{V}_{E|\alpha}^{\mathcal{D},Hom-Het} = \begin{pmatrix} -\frac{\tau-1+\tau\omega\mu}{\mu} & & -\sqrt{-\tau(\omega^2-1)} & \\ & \mu(1-\tau)-\tau\omega & & -\sqrt{-\tau(\omega^2-1)} \\ -\sqrt{-\tau(\omega^2-1)} & & \omega & \\ & -\sqrt{-\tau(\omega^2-1)} & & \omega \end{pmatrix}.$$

Note that this CM is the same as that for the case $C(amp)$. The only change is in the sign of the parameter τ and the conditional spectrum is

$$\{\overline{\nu}_1^{\mathcal{D}},\overline{\nu}_2^{\mathcal{D}}\}_{Hom-Het} \to \left\{1, \frac{[(1-\tau)\omega-\tau\mu][(1-\tau)\omega\mu-\tau]}{\mu}\right\} \overset{\mu>>1}{\to} \{1, \sqrt{(\tau-1)\tau\omega\mu}\}.$$

giving the following conditional von Neumann entropy

$$S_{E|\alpha}^{\mathcal{D},Hom-Het} = h(\overline{\nu}_1^{\mathcal{D}}) + h(\overline{\nu}_2^{\mathcal{D}}) \overset{\mu>>1}{\to} \log \frac{e}{2}\sqrt{(\tau-1)\tau\omega\mu}.$$

τhe rate is given by

$$R_{\mathcal{D}}^{\blacktriangleright,Hom-Het}(\mu,\tau,\omega) = \frac{1}{2}\log\frac{(1-\tau)\omega-\tau\mu+1}{(1-\tau)\omega+1} + h(\overline{\nu}_1^{\mathcal{D}}) + h(\overline{\nu}_2^{\mathcal{D}}) - h(\nu_1^{\mathcal{D}}) - h(\nu_2^{\mathcal{D}}),$$
$$\overset{\mu>>1}{\to} -h(\omega) + \frac{1}{2}\log\frac{\tau^2\omega}{(1-\tau)[1+(1-\tau)\omega]},$$

That is the same of eq.(D.28) but now with negative values of the parameter τ, and with the excess noise given by eq.(5.30) The protocol is always insecure.

Reverse Reconciliation

For the reverse reconciliation we proceed as in previous sections and compute the conditional CM, that is given by the following mathematical expression

$$\mathbf{V}_{E|\beta}^{\mathcal{D},Hom-Het} = \begin{pmatrix} \frac{\omega\mu}{\omega-\tau(\omega+\mu)} & & \frac{\mu\sqrt{-\tau(\omega^2-1)}}{\omega-\tau(\omega+\mu)} & \\ & \mu-\tau(\omega+\mu) & & -\sqrt{-\tau(\omega^2-1)} \\ \frac{\mu\sqrt{-\tau(\omega^2-1)}}{\omega-\tau(\omega+\mu)} & & \frac{1-\tau(1+\omega\mu)}{\omega-\tau(\omega+\mu)} & \\ & -\sqrt{-\tau(\omega^2-1)} & & \omega \end{pmatrix}.$$

This has symplectic spectrum

$$\{\widetilde{\nu}_1^{\mathcal{D}},\widetilde{\nu}_2^{\mathcal{D}}\}_{Hom-Het} = \left\{\sqrt{\frac{\mu[(1-\tau)\omega\mu-\tau]}{\omega-\tau(\omega+\mu)}},1\right\} \overset{\mu>>1}{\to} \left\{\sqrt{\frac{(\tau-1)\omega\mu}{\tau}},1\right\},$$

and conditional von Neumann entropy and the secret key rate

$$S_{E|Bob}^{\mathcal{D},Hom-Het} = h(\widetilde{\nu}_1^{\mathcal{D},Hom-Het}) \overset{\mu>>1}{\to} \log\frac{e}{2}\sqrt{\frac{(\tau-1)\omega\mu}{\tau}},$$
$$R_{\mathcal{D}}^{\blacktriangleleft,Hom-Het}(\mu,\tau,\omega) = \frac{1}{2}\log\frac{(1-\tau)\omega-\tau\mu+1}{(1-\tau)\omega+1} + h(\widetilde{\nu}_1^{\mathcal{D},Hom-Het}) - h(\nu_1^{\mathcal{D}}) - h(\nu_2^{\mathcal{D}}),$$
$$\overset{\mu>>1}{\to} -h(\omega) + \log\frac{\omega}{(1-\tau)[1+(1-\tau)\omega]}$$

Plotting the key-rates in both DR and RR we find that they are always negative. Again the canonical form $\mathcal{D}$ behaves as a denial-of-service channel.

D.6 Hom^2 protocol

In this protocol Alice prepares squeezed states and Bob performs homodyne measurements on the incoming signals.

D.6.1 $\mathcal{C}$(amp) canonical form

The joint Alice-Bob state is described by eq.(D.9) from which we compute Alice-Bob's mutual information,

$$I_{AB}^{HOM^2} = \frac{1}{2}\log\frac{\tau\mu+(\tau-1)\omega}{(\tau-1)\omega} \overset{\mu>>1}{\to} \frac{1}{2}\log\frac{\tau\mu}{(\tau-1)\omega}. \tag{D.30}$$

From previous equation we can calculate the expression of the excess noise (note that this expression holds also for the case of finite μ)

$$\omega = \frac{\tau-1+N\tau}{\tau-1}$$

The properties of the total CM are given by eqs(D.9-5.13) .We arrive to the following expression for the total von Neumann entropy

$$S_E^{C(amp),Hom^2} = h(\nu_1^C)+h(\nu_2^C) \overset{\mu>>1}{\to} h(\omega)+\log\frac{e}{2}(\tau-1)\mu$$

D.6.2 Direct Reconciliation

The CCM describing Eve's outputs is given by

$$\mathbf{V}_{E|A}^{C(amp),Hom^2} = \begin{pmatrix} \frac{\tau-1+\tau\mu}{\mu} & & \sqrt{\tau(\omega^2-1)}\mathbf{Z} \\ & (\tau-1)\mu+\tau\omega & \\ \sqrt{\tau(\omega^2-1)}\mathbf{Z} & & \omega\mathbf{I} \end{pmatrix}. \tag{D.31}$$

The determinant is

$$\det\mathbf{V}_{E|A}^{C(amp),Hom^2} = \frac{[\tau+(\tau-1)\omega\mu][(\tau-1)\omega+\tau\mu]}{\mu} \overset{\mu>>1}{\to} (\tau-1)\tau\omega\mu, \tag{D.32}$$

The total symplectic eigenvalues (exact and asymptotic expressions) are given by

$$\overline{\nu}_{1|A}^{C(amp),Hom^2} = 1 \overset{\mu>>1}{\to} 1, \tag{D.33}$$

$$\overline{\nu}_{2|A}^{C(amp),Hom^2} = \sqrt{\frac{[\tau+(\tau-1)\omega\mu][(\tau-1)\omega+\tau\mu]}{\mu}} \overset{\mu>>1}{\to} \sqrt{(\tau-1)\tau\omega\mu}. \tag{D.34}$$

These provide the following total Eve's von Neumann entropies

$$S_{E|A}^{C(amp),Hom^2} = h\left(\sqrt{\frac{[\tau+(\tau-1)\omega\mu][(\tau-1)\omega+\tau\mu]}{\mu}}\right) \overset{\mu>>1}{\to} \log\frac{e}{2}\sqrt{(\tau-1)\tau\omega\mu}. \tag{D.35}$$

The security rate is then

$$R_{C(amp)}^{\blacktriangleright,Hom^2}(\mu,\tau,\omega) = \frac{1}{2}\log\frac{\tau\mu+(\tau-1)\omega}{(\tau-1)\omega} + h\left(\sqrt{\frac{[\tau+(\tau-1)\omega\mu][(\tau-1)\omega+\tau\mu]}{\mu}}\right) - h(\nu_1^C)+h(\nu_2^C), \tag{D.36}$$

$$\overset{\mu>>1}{\to} -h(\omega)+\frac{1}{2}\log\frac{\tau^2}{(\tau-1)^2} \tag{D.37}$$

Reverse Reconciliation

The conditional CM, determinant and spectrum are now

$$\mathbf{V}_{E|Bob}^{C(amp)} = \begin{pmatrix} \frac{\omega\mu}{(\tau-1)\omega+\tau\mu} & & \frac{\sqrt{\tau(\omega^2-1)}\mu}{(\tau-1)\omega+\tau\mu} & \\ & (\tau-1)\mu+\tau\omega & & \sqrt{\tau(\omega^2-1)} \\ \frac{\sqrt{\tau(\omega^2-1)}\mu}{(\tau-1)\omega+\tau\mu} & & \frac{\tau-1\tau\omega\mu}{(\tau-1)\omega+\tau\mu} & \\ & \sqrt{\tau(\omega^2-1)} & & \omega \end{pmatrix},$$

$$\det \mathbf{V}_{E|Bob}^{C(amp)} = \frac{[\tau+(t-1)\omega\mu]\mu}{(\tau-1)\omega+\tau\mu} \overset{\mu>>1}{\to} \frac{\omega\mu(\tau-1)}{\tau},$$

$$\widetilde{\nu}_1^{C(amp)} = 1,$$

$$\widetilde{\nu}_2^{C(amp)} = \sqrt{\frac{[\tau+(t-1)\omega\mu]\mu}{(\tau-1)\omega+\tau\mu}} \overset{\mu>>1}{\to} \sqrt{\frac{\omega\mu(\tau-1)}{\tau}}.$$

The conditional von Neumann entropy is,

$$S_{E|Bob}^{C(amp)} = h(\widetilde{\nu}_2^{C(amp)}) = h\left(\sqrt{\frac{[\tau+(t-1)\omega\mu]\mu}{(\tau-1)\omega+\tau\mu}}\right) \overset{\mu>>1}{\to} \log\frac{e}{2}\sqrt{\frac{\omega\mu(\tau-1)}{\tau}},$$

and the security rate

$$R_{C(amp)}^{\blacktriangleleft}(\mu,\tau,\omega) = \frac{1}{2}\log\frac{\tau\mu+(\tau-1)\omega}{(\tau-1)\omega} + h\left(\sqrt{\frac{[\tau+(t-1)\omega\mu]\mu}{(\tau-1)\omega+\tau\mu}}\right) - h(\nu_1^C) + h(\nu_2^C),$$

$$\overset{\mu>>1}{\to} -h(\omega) + \frac{1}{2}\log\frac{1}{(\tau-1)^2}$$

In Fig.(D.8) summarizes the behavior of the security thresholds for the Hom^2 protocol, for an attack performed by an amplifier described by the canonical form $\mathcal{C}(amp)$,

D.6.3 D canonical form

After the processing of $\mathcal{D}$ channel Alice and Bob's joint state CM is given by the following expression

$$\mathbf{V}_{AB}^{\mathcal{D}} = \begin{pmatrix} \mu\mathbf{I} & \sqrt{-\tau}\sqrt{\mu^2-1}\mathbf{I} \\ \sqrt{-\tau}\sqrt{\mu^2-1}\mathbf{I} & [-\tau\mu+(1-\tau)\omega]\mathbf{I} \end{pmatrix}.$$

The mutual information is the following

$$I_{AB}^{\mathcal{D}} = \frac{1}{2}\log\frac{-\tau\mu+(1-\tau)\omega}{(1-\tau)\omega} \overset{\mu>>1}{\to} \frac{1}{2}\log\frac{-\tau\mu}{(1-\tau)\omega}.$$

The relation between Eve's thermal noise and channel's excess noise N, obtained from previous expression, is given by

$$\omega = \frac{1-\tau-N\tau}{1-\tau}$$

The total Eve's CM, determinant and spectrum are the same of previous cases, giving the following total von Neumann entropy

$$S_E = h(\nu_1^C) + h(\nu_2^C) \overset{\mu>>1}{\to} h(\omega) + \log\frac{e}{2}(1-\tau)\mu,$$

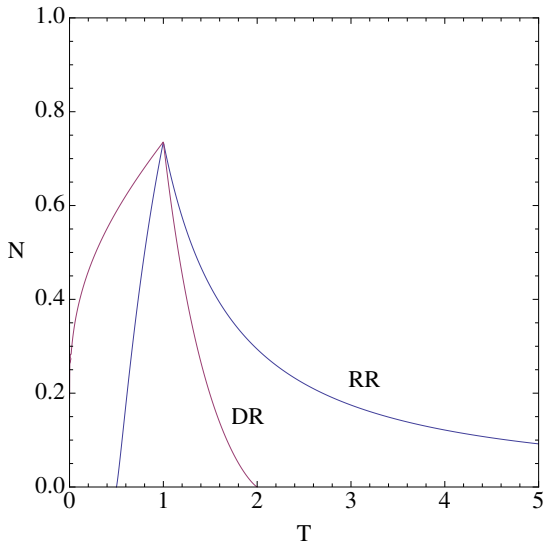

Figure D.8: Protocol Hom^2 with canonical form $\mathcal{C}$(amp): DR (*blue*) and RR (*red*).

Direct Reconciliation

Conditioning with respect Alice's state preparation, we get the following CCM

$$\mathbf{V}_{E|Alice}^{\mathcal{D},Hom^2} = \begin{pmatrix} \frac{1-\tau-\tau\omega\mu}{\mu} & & -\sqrt{-\tau(\omega^2-1)}\mathbf{I} \\ & \mu-\tau(\omega+\mu) & \\ -\sqrt{-\tau(\omega^2-1)}\mathbf{I} & & \omega\mathbf{I} \end{pmatrix}$$

with determinant and conditional spectrum

$$\det \mathbf{V}_{E|Alice}^{\mathcal{D},Hom^2} = \frac{[(\tau-1)\omega+t\mu][-\tau-(1-\tau)\omega]}{\mu} \overset{\mu>>1}{\to} (\tau-1)\tau\omega\mu,$$
$$\{\overline{\nu}_1^{\mathcal{D},Hom^2}, \overline{\nu}_2^{\mathcal{D},Hom^2}\} \to \{1, \sqrt{(\tau-1)\tau\omega\mu}\}.$$

giving the following expression for the conditional von Neumann entropy

$$S_{E|Alice}^{\mathcal{D},Hom^2} = h\left(\sqrt{(\tau-1)\tau\omega\mu}\right) \overset{\mu>>1}{\to} \log\frac{e}{2}(\tau-1)\tau\omega\mu.$$

The rate is given by

$$R_D^{\blacktriangleright,Hom^2}(\mu,\tau,\omega) = \frac{1}{2}\log\frac{-\tau\mu+(1-\tau)\omega}{(1-\tau)\omega} + h\left(\sqrt{(\tau-1)\tau\omega\mu}\right) - h(\nu_1^D) + h(\nu_2^D),$$
$$\overset{\mu>>1}{\to} -h(\omega) + \frac{1}{2}\log\frac{\tau^2}{(1-\tau)^2}$$

The protocol is always insecure,

Reverse Reconciliation

the CCM is,

$$\mathbf{V}_{E|Bob}^{\mathcal{D},Hom^2} = \begin{pmatrix} \frac{\omega\mu}{\omega(1-\tau)-\tau\mu} & & -\frac{\sqrt{-\tau(\omega^2-1)}\mu}{(\tau-1)\omega+\tau\mu} & \\ & \mu(1-\tau)-\tau\omega & & -\sqrt{-\tau(\omega^2-1)} \\ -\frac{\sqrt{-\tau(\omega^2-1)}\mu}{(\tau-1)\omega+\tau\mu} & & \frac{-1+\tau+\tau\omega\mu}{(\tau-1)\omega+\tau\mu} & \\ & -\sqrt{-\tau(\omega^2-1)} & & Gw \end{pmatrix},$$

which provides the following conditional determinant,

$$\det \mathbf{V}_{E|Bob}^{\mathcal{D},Hom^2} = \frac{\mu[\tau+(\tau-1)\omega\mu]}{(\tau-1)\omega+\tau\mu} \overset{\mu>>1}{\to} \frac{(\tau-1)\omega\mu}{\tau}$$

and symplectic spectrum,

$$\{\widetilde{\nu}_1^{\mathcal{D},Hom^2}, \widetilde{\nu}_2^{\mathcal{D},Hom^2}\} = \left\{1, \sqrt{\frac{\mu[\tau+(\tau-1)\omega\mu]}{(\tau-1)\omega+\tau\mu}}\right\} \overset{\mu>>1}{\to} \{1, \sqrt{\frac{(\tau-1)\omega\mu}{\tau}}\}.$$

The conditional von Neumann entropy and the secret key rate are,

$$S_{E|Bob}^{\mathcal{D},Hom^2} = h\left(\sqrt{\frac{\mu[\tau+(\tau-1)\omega\mu]}{(\tau-1)\omega+\tau\mu}}\right) \overset{\mu>>1}{\to} h\left(\sqrt{\frac{(\tau-1)\omega\mu}{\tau}}\right),$$

$$R_{\mathcal{D}}^{\blacktriangleleft,Hom^2}(\mu,\tau,\omega) = \frac{1}{2}\log\frac{-\tau\mu+(1-\tau)\omega}{(1-\tau)\omega} + h\left(\sqrt{\frac{\mu[\tau+(\tau-1)\omega\mu]}{(\tau-1)\omega+\tau\mu}}\right) - h(\nu_1^D) + h(\nu_2^D),$$

$$\overset{\mu>>1}{\to} -h(\omega) + \frac{1}{2}\log\frac{1}{(1-\tau)^2}$$

The protocol is always insecure.

D.7 Summary: asymptotic thresholds for $\mathcal{C}(loss), \mathcal{C}(amp)$, and $\mathcal{D}$.

In all protocols for the relevant cases, represented by the canonical forms $\mathcal{C}(loss), \mathcal{C}(amp)$, and $\mathcal{D}$. In the following lines we rewrite the expressions of the asymptotic thresholds in a compact form and, as we have already assumed throughout this dissertation, with symbol $\blacktriangleright$ we indicate the direct reconciliation, while $\blacktriangleleft$, denotes reverse reconciliation.

D.7.1 Non-switching protocol

We can compress the previous secret key rates' expressions for $\mathcal{C}(amp), \mathcal{C}(loss), \mathcal{D}$ in the following forms

$$R_{\mathcal{C}\&\mathcal{D}}^{\blacktriangleright} = \begin{cases} h\left[\omega|1-\tau|+\tau\right] - h(\omega) + \log\frac{2}{e}\frac{\tau}{|1-\tau|[1+\tau+|1-\tau|\omega]}, \tau > 0 \\ h\left[\omega(1+\tau)+\tau\right] - h(\omega) + \log\frac{2}{e}\frac{\tau}{(1+\tau)[1+\tau+(1+\tau)\omega]}, \tau < 0 \end{cases}$$

$$R_{\mathcal{C}\&\mathcal{D}}^{\blacktriangleleft} = \begin{cases} h\left[\left|\frac{\omega(1-\tau)+1}{\tau}\right|\right] - h(\omega) + \log\frac{2}{e}\frac{\tau}{(1-\tau)[1+\tau+(1-\tau)\omega]}, \tau > 0 \\ h\left[\left|\frac{\omega(1+\tau)+1}{\tau}\right|\right] - h(\omega) + \log\frac{2}{e}\frac{\tau}{(1+\tau)[1+\tau+(1+\tau)\omega]}, \tau < 0 \end{cases}$$

D.7.2 Switching protocol

$$R_{\mathcal{C}\&\mathcal{D}}^{\blacktriangleright,switch} = \begin{cases} h\left(\sqrt{\frac{\omega[\tau+(|1-\tau|)\omega]}{|1-\tau|+\tau\omega}}\right) - h(\omega) + \log\frac{\tau(|1-\tau|+\tau\omega)}{|1-\tau|[\tau+(|1-\tau|)\omega]}, \tau > 0 \\ h\left(\sqrt{\frac{\omega[(1+\tau)\omega+\tau]}{1+\tau(\omega+1)}}\right) - h(\omega) + \frac{1}{2}\log\frac{\tau(1+\tau(\omega+1))}{(1+\tau)((1+\tau)\omega+\tau)}, \tau < 0 \end{cases}$$

$$R_{\mathcal{C}\&\mathcal{D}}^{\blacktriangleleft,switch} = \begin{cases} -h(\omega) + \frac{1}{2}\log\frac{\omega}{|1-\tau|(\tau+|1-\tau|\omega)}, \tau > 0 \\ -h(\omega) + \frac{1}{2}\log\frac{(1+2\tau)^2\omega}{(1+\tau)[(1+\tau)\omega+\tau]}, \tau < 0 \end{cases}$$

D.7.3 $Hom-Het$ protocol

$$R^{\blacktriangleright,Hom-Het}_{\mathcal{C}\&\mathcal{D}} = \begin{cases} -h(\omega) + \frac{1}{2}\log\frac{\tau^2\omega}{|1-\tau|[1+|1-\tau|\omega]}, \tau > 0 \\ -h(\omega) + \frac{1}{2}\log\frac{\tau^2\omega}{(1-\tau)[1+(1-\tau)\omega]}, \tau < 0 \end{cases}$$
$$R^{\blacktriangleleft,Hom-Het}_{\mathcal{C}\&\mathcal{D}} = \begin{cases} -h(\omega) + \frac{1}{2}\log\frac{\omega}{|1-\tau|[1+|1-\tau|\omega]}, \tau > 0 \\ -h(\omega) + \frac{1}{2}\log\frac{\omega}{(1-\tau)[1+(1-\tau)\omega]}, \tau < 0 \end{cases}$$

D.7.4 Hom^2 protocol

$$R^{Hom^2,\blacktriangleright}_{\mathcal{C}\&\mathcal{D}} = \begin{cases} -h(\omega) + \frac{1}{2}\log\frac{\tau^2}{|1-\tau|^2}, \tau > 0 \\ -h(\omega) + \frac{1}{2}\log\frac{\tau^2}{(1-\tau)^2}, \tau < 0 \end{cases}$$
$$R^{Hom^2,\blacktriangleright}_{\mathcal{C}\&\mathcal{D}} = \begin{cases} -h(\omega) + \frac{1}{2}\log\frac{1}{|1-\tau|^2}, \tau > 0 \\ -h(\omega) + \frac{1}{2}\log\frac{1}{(1-\tau)^2}, \tau < 0 \end{cases}$$

D.8 Summary: $\mathcal{A}_2$ and $\mathcal{B}_1$ protocols

In this summary we provide a summary of the key-rate computed for all possible implementation of the one-way communication, for the remaining classes $\mathcal{A}_2$ and $\mathcal{B}_1$. In particular here one can find the asymptotic analytical expressions of the key-rate computed for the protocol based on squeezed state preparation that, for brevity have not been included in this Appendix.

D.8.1 Non-switching protocol

$$R^{\blacktriangleright}_{\mathcal{A}_2} = \frac{1}{2}\log_2\frac{\mu+\omega+1}{\omega+1+1} + h[\sqrt{\omega(1+\omega)}] - h(\nu_1^{\mathcal{A}_2}) - h(\nu_2^{\mathcal{A}_2}),$$
$$R^{\blacktriangleright}_{\mathcal{B}_1} = \log_2\frac{e}{2}\sqrt{\mu+2} + h(\sqrt{2}),$$
$$R^{\blacktriangleleft}_{\mathcal{A}_2} = \frac{1}{2}\log_2\frac{\mu+\omega+1}{\omega+1+1} + h\left[\sqrt{\frac{\mu(1+\mu+\omega\mu)}{1+\omega+\mu}}\right] - h(\nu_1^{\mathcal{A}_2}) - h(\nu_2^{\mathcal{A}_2}),$$
$$R^{\blacktriangleleft}_{\mathcal{B}_1} = \frac{1}{2}\log_2\frac{(\mu+1)(\mu+2)}{6} + h\left(\sqrt{2-\frac{3}{2+\mu}}\right) - h(\sqrt{\mu+1}),$$

D.8.2 Switching protocol

$$R^{\blacktriangleright}_{\mathcal{A}_2} = \frac{1}{2}\log_2\frac{\mu}{\omega+1} + S^{\mathcal{A}_2,switch}_{E|\alpha} - S^{\mathcal{A}_2,switch}_{E},$$
$$R^{\blacktriangleright}_{\mathcal{B}_1} = \frac{1}{2}\log_2\frac{\mu(\mu+1)}{2} + h\left(\sqrt{1+\frac{1}{\mu}}\right) - h(\sqrt{\mu+1}),$$
$$R^{\blacktriangleleft}_{\mathcal{A}_2} = \frac{1}{2}\log_2\frac{\mu}{\omega+1} + S^{\mathcal{A}_2,switch}_{E|\beta} - S^{\mathcal{A}_2,switch}_{E},$$
$$R^{\blacktriangleleft}_{\mathcal{B}_1} = \frac{1}{2}\log_2\frac{\mu(\mu+1)}{2} + h(\sqrt{\mu}) - h(\sqrt{1+\mu}).$$

D.8.3 $Hom-Het$ protocol

$$R^{\blacktriangleright}_{\mathcal{A}_2} = \log_2 \frac{2}{e}\sqrt{\frac{\omega+\mu}{\mu^2\omega}},\ \text{(asymptotically always } < 0)$$

$$R^{\blacktriangleright}_{\mathcal{B}_1} = \frac{1}{4}\log_2 \frac{\mu^2(\mu+1)}{2\mu+1} + \frac{h(\sqrt{1+\frac{1}{\mu}})}{2} - \frac{h(\sqrt{1+\mu})}{2},\ \text{(asymptotically always } > 0)$$

$$R^{\blacktriangleleft}_{\mathcal{A}_2} = \frac{1}{2}\log_2 \frac{\omega+\mu}{\mu} - h(\omega),\ \text{(asymptotically always } < 0)$$

$$R^{\blacktriangleleft}_{\mathcal{B}_1} = \frac{1}{4}\log_2 \frac{\mu^2(\mu+1)}{2\mu+1} + h(\sqrt{\mu}) - h(\sqrt{1+\mu})\ \text{(asymptotically always } > 0).$$

D.8.4 Hom^2 protocol

$$R^{\blacktriangleright}_{\mathcal{A}_2} = \frac{1}{4}\log_2 \frac{\mu+\omega}{\omega} + h(\omega) - h(\nu_1^{\mathcal{A}_2,Hom^2}) - h(\nu_2^{\mathcal{A}_2,Hom^2}),\ \text{always } < 0$$

$$R^{\blacktriangleright}_{\mathcal{B}_1} = \text{ always } > 0,$$

$$R^{\blacktriangleleft}_{\mathcal{A}_2} = \frac{1}{2}\log_2 \frac{\mu+\omega+1}{\omega+1+1} + \frac{1}{2}\left[h\left[\sqrt{\frac{\mu(1+\omega\mu)}{\omega+\mu}}\right] + h(\mu)\right] - h(\nu_1^{\mathcal{A}_2}) - h(\nu_2^{\mathcal{A}_2}),\ \text{always } < 0$$

$$R^{\blacktriangleleft}_{\mathcal{B}_1} = \text{ always } > 0,$$

where $\nu_{1,2}^{\mathcal{A}_2,Hom^2}$ are the symplectic eigenvalues of the total CM whose mathematical expression is

$$\nu_{1,2}^{\mathcal{A}_2,Hom^2} = \sqrt{\frac{\omega^2+\mu^2+\omega\mu \pm \sqrt{\omega^4+2\omega(\omega^2-2)\mu-\omega^2\mu^2+2\omega\mu^3+\mu^4}}{2}}.$$

For the canonical form $\mathcal{B}_1$ we have a divergent expression of Alice-Bob mutual information, for $\mu \to \infty$, so we have that the protocol is always asymptotically secure.

Appendix E

Symmetric MDI quantum cryptography: experimental imperfections

In this appendix we analyze the role of experimental imperfections computing the key-rates and the security thresholds in the presence of Bell detectors with non-ideal quantum efficiencies. We also study finite-size effects connected with finite Gaussian modulations [11], and the role played by the non-ideal efficiency of the classical reconciliation codes [13]. We show that, also in the presence of realistic experimental limitations, the optimal eavesdropping is given by the two-mode coherent "negative-EPR attack".

E.1 Post-relay covariance matrix for non-ideal Bell detectors

We generalize Eq.(9.5) to include detectors' efficiencies by placing two beam splitters with transmissivities η and η', as illustrated in Fig. E.1. To preserve the purity of the global (Alice-Bob-Eve) state, the non-detected signals are sent to Eve's quantum memory (this is the assumption to make in the worst-case scenario, since the relay is untrusted and Eve can control the loss of the detectors).

We follow the general approach given in Ref. [71]. We write the total CM in the block form

$$\mathbf{V} = \begin{pmatrix} \mathbf{V}_{ab} & \mathbf{C} \\ \mathbf{C}^T & \mathbf{B} \end{pmatrix}, \tag{E.1}$$

where the block

$$\mathbf{B} = \begin{pmatrix} \mathbf{B}_1 & \mathbf{D} \\ \mathbf{D}^T & \mathbf{B}_2 \end{pmatrix}, \tag{E.2}$$

describes the modes sent to the relay, A' and B'. These are processed by the balanced beam splitter and then measured. In our case it is easy to verify [71] that the blocks $\mathbf{B}_1$,$\mathbf{B}_2$ and $\mathbf{D}$ take the following expressions

$$\mathbf{B}_1 = \mathbf{B}_2 = [\tau\mu + (1-\tau)\omega]\mathbf{I}, \tag{E.3}$$

$$\mathbf{D}=(1-\tau)\mathbf{G}, \tag{E.4}$$

where $\mathbf{I}$ =diag$(1,1)$ and $\mathbf{G}$ =diag(g,g').

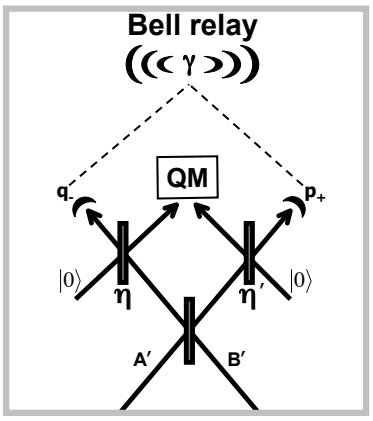

Figure E.1: Untrusted relay with inefficient detectors. Two additional beam splitters, with transmissivities (η, η') are placed in front of the ideal detectors. One output from each beam splitter is sent to the detectors for measurements. The other outputs are sent to Eve's quantum memory.

In Eq. (E.1) the sub-matrix $\mathbf{V}_{ab}$ describes the joint quantum state of remote modes a and b, while the block $\mathbf{C} = (\mathbf{C}_1 \mathbf{C}_2)$ is a rectangular matrix accounting for the correlations between the remote modes and the transmitted ones, i.e., A' and B'. In particular, we compute

$$\mathbf{C}_1 = \begin{pmatrix} \sqrt{\tau(\mu^2-1)}\mathbf{Z} \\ \mathbf{0} \end{pmatrix}, \ \mathbf{C}_2 = \begin{pmatrix} \mathbf{0} \\ \sqrt{\tau(\mu^2-1)}\mathbf{Z} \end{pmatrix}. \tag{E.5}$$

Applying Eq. (74) from Ref. [71] to Eq. (E.1), we obtain Alice and Bob's CM conditioned to the relay Bell measurement. This is given by

$$\mathbf{V}_{ab|\gamma} = \mathbf{V}_{ab} - \frac{1}{2\det\gamma(\eta,\eta')} \sum_{i,j=1,2} \mathbf{C}_i \left(\mathbf{X}_i^T \gamma(\eta,\eta') \mathbf{X}_j\right) \mathbf{C}_j^T, \tag{E.6}$$

where

$$\mathbf{X}_1 = \begin{pmatrix} & 1 \\ 1 & \end{pmatrix}, \ \mathbf{X}_2 = \begin{pmatrix} & 1 \\ -1 & \end{pmatrix}. \tag{E.7}$$

Here the quantum efficiencies of the detectors, simulated by the beam splitter transmissivities η and η', are contained in the symmetric matrix

$$\gamma(\eta,\eta') = \begin{pmatrix} \gamma_1(\eta) & \gamma_3 \\ \gamma_3 & \gamma_2(\eta') \end{pmatrix}. \tag{E.8}$$

In the case of a Bell detection the matrix $\gamma(\eta,\eta')$ can explicitly be computed, according to Eqs. (54-59) of Ref. [71]. In particular, its entries take the form

$$\begin{aligned} \gamma_1(\eta) &= \gamma_1 + \frac{1-\eta}{\eta}, \\ \gamma_2(\eta') &= \gamma_2 + \frac{1-\eta'}{\eta'}, \\ \gamma_3 &= 0 \end{aligned} \tag{E.9}$$

where $\gamma_1 = \tau\mu + (1-\tau)(\omega - g)$ and $\gamma_2 = \tau\mu + (1-\tau)(\omega + g')$ are easily obtained from Eq. (E.3) and (E.4), using the formulas of Ref. [71].

After simple algebra we derive the post-relay covariance matrix inclusive of the quantum efficiencies

$$\mathbf{V}_{ab|\gamma} = \begin{pmatrix} \mu\mathbf{I} & \mathbf{0} \\ \mathbf{0} & \mu\mathbf{I} \end{pmatrix} - \frac{\tau(\mu^2-1)}{2} \times \begin{pmatrix} \frac{1}{\gamma_1(\eta)} & & -\frac{1}{\gamma_1(\eta)} & \\ & \frac{1}{\gamma_2(\eta')} & & \frac{1}{\gamma_2(\eta')} \\ -\frac{1}{\gamma_1(\eta)} & & \frac{1}{\gamma_1(\eta)} & \\ & \frac{1}{\gamma_2(\eta')} & & \frac{1}{\gamma_2(\eta')} \end{pmatrix}$$

This can be rewritten in the form

$$\mathbf{V}_{ab|\gamma} = \begin{pmatrix} \mu\mathbf{I} & \mathbf{0} \\ \mathbf{0} & \mu\mathbf{I} \end{pmatrix} - \frac{\tau(\mu^2-1)}{2} \times \begin{pmatrix} \frac{1}{\tau\mu+\lambda(\eta)} & & -\frac{1}{\tau\mu+\lambda(\eta)} & \\ & \frac{1}{\tau\mu+\lambda'(\eta')} & & \frac{1}{\tau\mu+\lambda'(\eta')} \\ -\frac{1}{\tau\mu+\lambda(\eta)} & & \frac{1}{\tau\mu+\lambda(\eta)} & \\ & \frac{1}{\tau\mu+\lambda'(\eta')} & & \frac{1}{\tau\mu+\lambda'(\eta')} \end{pmatrix} \tag{E.10}$$

where

$$\begin{cases} \lambda(\eta) = (\omega - g)(1-\tau) + \frac{1-\eta}{\eta} \ , \\ \lambda'(\eta') = (\omega + g')(1-\tau) + \frac{1-\eta'}{\eta'} \ . \end{cases} \tag{E.11}$$

Note that Eq. (E.10) could have been computed directly from Eq. (9.5) by applying the transformations [1]

$$\lambda \to \lambda(\eta), \ \lambda' \to \lambda'(\eta'). \tag{E.12}$$

E.1.1 Asymptotic generalized key-rate

From the previous CM we can write the sub-matrix describing Bob's mode

$$\mathbf{V}_{b|\gamma} = \begin{pmatrix} \mu - \frac{\tau(\mu^2-1)}{2[\tau\mu+\lambda(\eta)]} & \\ & \frac{\tau(\mu^2-1)}{2[\tau\mu+\lambda'(\eta')]} \end{pmatrix}. \tag{E.13}$$

Then, by applying Eq. (9.10) to the generalized CM of Eq. (E.10), we derive the doubly-conditional CM of Bob, conditioned to both relay's and Alice's detections, i.e.,

$$\mathbf{V}_{b|\gamma\alpha}(\eta,\eta') = \begin{pmatrix} \mu - \frac{\tau(\mu^2-1)}{[\tau(\mu+1)+2\lambda(\eta)]} & \\ & \mu - \frac{\tau(\mu^2-1)}{[\tau(\mu+1)+2\lambda'(\eta')]} \end{pmatrix}. \tag{E.14}$$

We can now derive the symplectic spectra of the CMs of Eq. (E.10) and (E.14). We find simple analytical expressions in the limit of large modulation. For $\mathbf{V}_{ab|\gamma}$ we have the symplectic eigenvalues $\nu_1(\eta)$ and $\nu_2(\eta')$, while for $\mathbf{V}_{b|\gamma\alpha}$ we have $\nu(\eta,\eta')$.

[1] Note that, in the presence of a pure-loss attack ($\omega = 1$ and $g = g' = 0$), the non-unit quantum efficiencies of the detectors can be included in the loss of the channels. For simplicity, for $\eta = \eta'$ we can write

$$\frac{\tau}{\tau\mu + \lambda(\eta)} = \frac{\tau\eta}{\tau\eta\mu + 1 - \tau\eta}$$

which is equivalent to consider $\tau\eta$ in the CM of Eq. (9.5).

These eigenvalues can be obtained by applying the transformations of Eq. (E.12) to the Eqs. (9.7) and (9.12).

Using these spectra, we can compute the corresponding total and conditional von Neumann entropies and therefore the Holevo bound. In the limit of large modulation, Eve's Holevo information becomes

$$I_{E|\gamma}(\eta,\eta') = \log_2 \frac{e^2\sqrt{\lambda(\eta)\lambda'(\eta')}\mu}{4\tau} - h\left[\frac{\sqrt{[\tau+2\lambda(\eta)][\tau+2\lambda'(\eta')]}}{\tau}\right], \tag{E.15}$$

which extends Eq. (9.13) to arbitrary efficiencies η and η'.

Similarly, we can extend the formula for Alice and Bob's mutual information, which here becomes

$$I_{AB|\gamma}\left(\eta,\eta'\right) = \log_2 \frac{\tau\mu}{4\sqrt{[\tau+\lambda(\eta)][\tau+\lambda'(\eta')]}}, \tag{E.16}$$

for large modulation. Combining the previous results, we derive the asymptotic key-rate in the presence of detector inefficiencies

$$R_{sym} = \log_2\left[\frac{\tau^2}{e^2\sqrt{\lambda(\eta)\lambda'(\eta')[\tau+\lambda(\eta)][\tau+\lambda'(\eta')]}}\right] + h\left[\frac{\sqrt{[\tau+2\lambda(\eta)][\tau+2\lambda'(\eta')]}}{\tau}\right], \tag{E.17}$$

which clearly extends the formula given in Eq. (9.15).

E.1.2 Role of the imperfections on key-rate, security thresholds and achievable distances

In this section we study in detail the combined role of the various experimental limitations and imperfections, confirming the main findings presented in the main body of this paper. We compute the key-rate and the security thresholds considering not only the realistic quantum efficiency of the detectors, but also the use of a finite Gaussian modulation and the non-ideal reconciliation efficiency provided by realistic codes for error correction and privacy amplification.

Secret key rate

In order to extract a secret key, the honest parties must process their correlated data in stages of perform error correction and privacy amplification. This data processing is today implemented with a limited efficiency $\beta \leq 1$, for instance $\beta \simeq 0.95 \div 0.97$ [13, 45]. To include this limitation, we have to multiply Alice and Bob's mutual information by β, and consider the realistic key-rate [11]

$$R(\beta,\mu,\tau,\omega,g,g',\eta,\eta') = \beta I_{AB|\gamma} - I_{E|\gamma}, \tag{E.18}$$

where $I_{AB|\gamma}$ and $I_{E|\gamma}$ are now computed considering finite modulation μ besides non-ideal detector efficiencies η and η' (clearly these quantities must tend to Eqs. (E.15) and (E.16) in the limit of large modulation).

In general, the mutual information can be computed from the formula $I_{AB|\gamma} = \frac{1}{2}\log_2 \Sigma$, where Σ is defined in Ref. [17]. Eve's Holevo information can be computed using the formula of the von Neumann entropy $S = \Sigma_x h(x)$, with $h(x)$ defined in Eq. (5.18) and applied to the numerical symplectic eigenvalues of the CMs given in

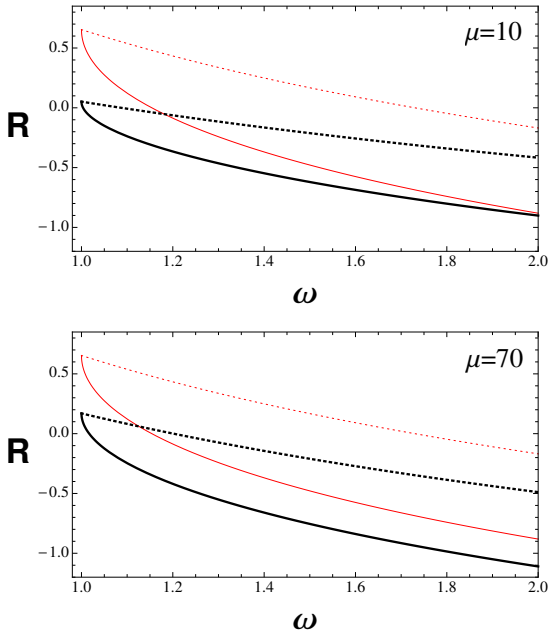

Figure E.2: The key-rate R (bits) is plotted versus thermal noise ω for $\mu = 10$ (SNU) (top-panel) and $\mu = 70$ (bottom-panel). Other parameters are $\tau = 0.9$, $\beta = 0.95$ and $\eta = \eta' = 0.98$. We compare two eavesdropping strategies: The collective one-mode entangling cloner attack $g' = g = 0$ (dotted black line) and the two-mode "negative EPR" attack $g = -g' = -\sqrt{\omega^2 - 1}$ (continuous black line). We see that the key-rate of the two-mode attack is always lower than that of the one-mode attack. For comparison, we have also plotted the performances in the case of ideal reconciliation ($\beta = 1$), ideal detectors ($\eta = \eta' = 1$) and large modulation ($\mu \gg 1$). These ideal performances are represented by the red curves, dotted for the one-mode attack and continuous for the two-mode attack.

Eqs. (E.10) and (E.14). In Fig. E.2, we plot the key-rate of Eq. (E.18) as a function of the thermal noise ω for two values of the Gaussian modulation $\mu = 10$ (top) and $\mu = 70$ (bottom) vacuum shot noise unit (SNU), and choosing $\tau = 0.9$, $\eta = \eta' = 0.98$ and $\beta = 0.95$. We see that the key-rate of a negative EPR attack is clearly lower than that of a collective one-mode attack. This behavior is generic by varying the previous parameters.

Security thresholds and achievable distances

Here we study the impact of the experimental limitations on the security thresholds, comparing the two-mode optimal attack with one-mode collective attack. The security threshold is obtained by solving the equation

$$R(\beta, \mu, \tau, \omega, g, g', \eta, \eta') = 0. \tag{E.19}$$

In this equation, we fix the values of the Gaussian modulation ($\mu = 10$ or 70), the reconciliation efficiency ($\beta = 0.95$), and the quantum efficiencies $\eta = \eta' = 0.98$. Then, for each attack, we can write the security threshold as $\omega = \omega(\tau)$. The comparison is provided in Fig. E.3, where we see that the threshold of the optimal two-mode attack is always lower than the threshold of the one-mode collective attack.

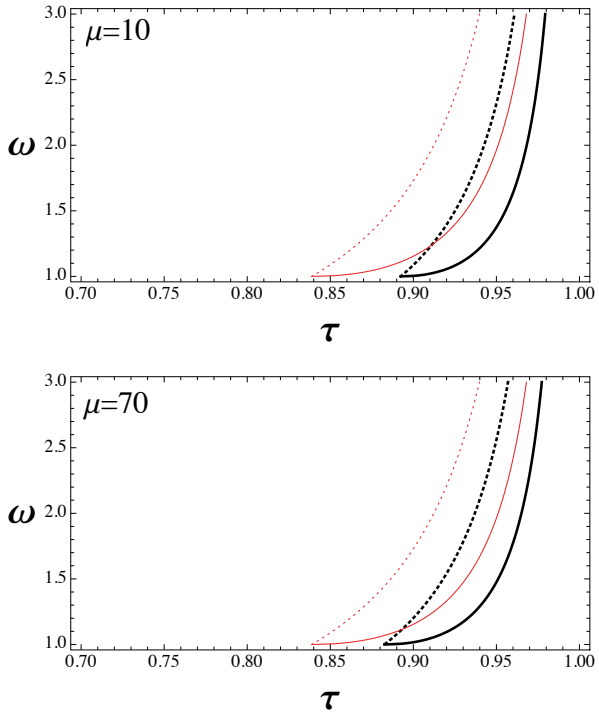

Figure E.3: We plot the security threshold $\omega = \omega(\tau)$ for $\mu = 10$ (top panel) and $\mu = 70$ (bottom panel). Other parameters are $\beta = 0.95$ and $\eta = \eta' = 0.98$. We compare the two-mode negative EPR attack (continuous black lines) and the one-mode entangling cloner attack (dotted black lines). Red curves refer to the ideal case $\beta = \eta = \eta' = 1$ and $\mu \gg 1$.

The previous analysis can be performed by expressing the transmissivity in term of distances. In fact, we may consider $\tau = 10^{-\frac{0.2}{10}d}$, where d is the distance in km, assuming the standard loss rate in fibre of 0.2dB/Km. The achievable distances are shown in Fig. E.4. We see that moving from the ideal conditions (red curves, with $\beta = \eta = \eta' = 1$ and $\mu \gg 1$) the performances deteriorate. All others curves are obtained for realistic reconciliation efficiencies $\beta = 0.95$, and detectors efficiencies $\eta = \eta' = 0.98$. The top panel compares the ideal thresholds with the case $\mu = 70$ (black), while in the bottom panel we show the degradation of the performances while increasing the modulation from $\mu = 70$ (black) to $\mu = 1000$ (green).

It is interesting to note the effect of the reconciliation efficiency on the optimal modulation variance. For values of $\beta < 1$, the optimal modulation is not infinite. In fact, for the realistic value considered here, $\beta = 0.95$, we have a range of finite modulations $30 \lesssim \mu \lesssim 70$, for which the performances are improved.

Discussion

Here we summarize some important aspects emerged from this further analysis. First, we have shown that positive key-rates are still achievable over the range of metropolitan distances in the presence of various experimental limitations. Second, the negative-EPR attack, already identified to be the optimal attack in the ideal case (see main text) continues to be the most powerful eavesdropping strategy also

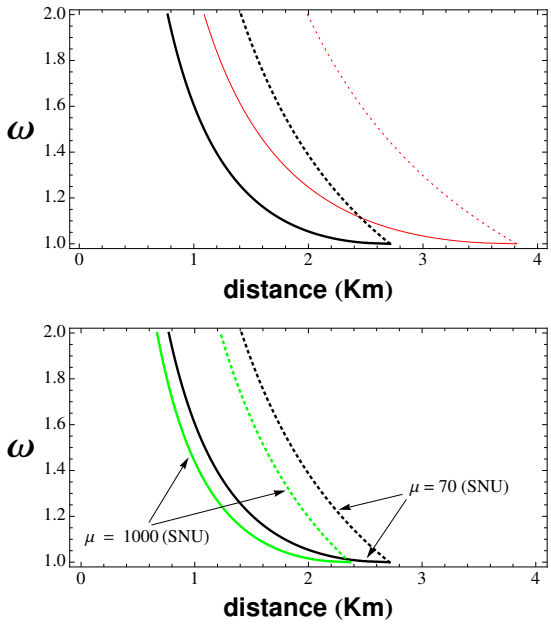

Figure E.4: This figure shows the security thresholds as $\omega = \omega(d)$, where d is the distance in km, assuming the loss rate of 0.2 dB/Km. As in previous figures we compare the two-mode negative EPR attack (solid lines) with the one-mode entangling-cloner attack (dotted lines). In the top panel, the red curves refer to the ideal conditions $\beta = \eta = \eta' = 1$ and $\mu \gg 1$. The black curves refer to the non ideal case $\beta = 0.95$, $\eta = \eta' = 0.98$ and $\mu = 70$ (SNU). The bottom panel shows the degradation of the performance as we increase the modulation from $\mu = 70$ (black curves) to $\mu = 1000$ (green curves), for $\beta = 0.95$, $\eta = \eta' = 0.98$.

considering realistic experimental conditions, i.e., finite modulation, non-ideal reconciliation and non-ideal detectors. Third, the degradation of the performances of the protocol does not come from the finite modulation (e.g., we checked that values as low as $\mu = 10$ are still acceptable) but mainly from the quantum efficiencies of the detectors, η and η', and the reconciliation efficiency β of the classical codes.

Bibliography

[1] John D. Jackson, Classical Electrodynamics, Wiley & Sons, New York, 1975.

[2] Michael Nielsen and Isaac Chuang, Quantum Computation and Quantum Information, Cambridge University Press, 2000.

[3] Valerio Scarani, Helle Bechmann-Pasquinucci, Nicolas J. Cerf, Miloslav Dušek, Norbert Lütkenhaus, and Momtchil Peev, Rev. Mod. Phys. **81**, 1301, 2009.

[4] Claude Shannon, Bell System Technical Journal **28** (4), 656–715 1949.

[5] Bruce Schneier, Applied Cryptography, John Wiley & Sons, New York, 1996.

[6] William K. Wootters, Wojciech H. .Zurek, Nature **299**, 802–803, 1982.

[7] Nicolas Gisin, Grégoire Ribordy, Wolfgang Tittel, and Hugo Zbinden, Rev. Mod. Phys. **74**, 145 2002.

[8] Samuel L.Braunstein and Peter van Lock, Rev. Mod. Phys. 77, 513–577, 2005.

[9] Samuel L.Braunstein and Seth. Lloyd, Phys.Rev.Lett. **82**, 1784-1787, 1999.

[10] Samuel L. Braunstein and H.J. Kimble, Phys. Rev. Lett, **80**, 4, 869, 1998.

[11] Christian Weedbrook, Stefano Pirandola, Raul Garcia-Patron, Nicolas J. Cerf, Timothy C. Ralph, Jeffrey H. Shapiro, and Seth Lloyd, Rev. Mod. Phys., **84**, 621, 2012.

[12] Frédéric Grosshans, Gilles Van Assche, Jérôme Wenger, Rosa Brouri, Nicolas J. Cerf and Philippe Grangier, Nature **421**, 238–241, 2003.

[13] Paul Jouguet, Sébastien Kunz-Jacques, Anthony Leverrier, Phys. Rev. A **84, 6**, 062317, 2011.

[14] P. Jouguet Sébastien Kunz-Jacques, Anthony Leverrier, Philippe Grangier, Eleni Diamanti., Nature Photonics **7**, 378–381, 2013.

[15] R. Ursin, F. Tiefenbacher, T. Schmitt-Manderbach, H. Weier, T. Scheidl, M. Lindenthal, B. Blauensteiner, T. Jennewein, J. Perdigues, P. Trojek, B. Ömer, M. Fürst, M. Meyenburg, J. Rarity, Z. Sodnik, C. Barbieri, H. Weinfurter and A. Zeilinger, Nature Physics **3**, 481-486, 2007.

[16] Masahiro Takeoka, Saikat Guha and Mark M. Wilde, Nat. Comm. **5**, 5235, 2014.

[17] Stefano Pirandola, Carlo Ottaviani Gaetana Spedalieri, Christian Weedbrook, Samuel L. Braunstein, Seth Lloyd, Tobias Gehring, Christian S. Jacobsen and Ulrik L. Andersen, Nature Photonics **9**, 397-402, 2015.

[18] Carlo Ottaviani, Gaetana Spedalieri, Samuel L. Braunstein, Stefano Pirandola, Phys. Rev. A, **91**, 022320, 2015.

[19] Renato Renner, Nature Physics **3**, 645 - 649, 2007.

[20] Renato Renner, Juan Ignacio Cirac, Phys. Rev. Lett. **102**, 110504, 2009.

[21] Alexande S.Holevo, Problems of Information Transmission **9**, 177–183, 1973.

[22] Timothy Ralph, Phys.Rev. A, **61**, 010302 1999.

[23] Mark Hillery, Phys.Rev. A, **61**, 022309 2000.

[24] M.D. Reid, Phys. Rev. A **62**, 062308, 2000.

[25] Nicolas J. Cerf, M. Levy, and G. van Assche, Phys. Rev. A **63**,052311, 2001.

[26] Daniel Gottesman and John Preskill, Phys. Rev. A **63**, 022309, 2001.

[27] Frédéric Grosshans and Philippe Grangier, Phys. Rev. Lett. **88**, 057902, 2002.

[28] Frédéric Grosshans, Nicolas J. Cerf , Jérôme Wenger, Rosa Tualle-Brouri and Philippe Grangier, Quantum Information & Computation, **3**(7), 535-552, 2003.

[29] Christian Weedbrook, Andrew M. Lance, Warwick P. Bowen, Thomas Symul, Timothy C. Ralph, and Ping Koy Lam, Phys. Rev. Lett., **93** (17), 170504 ,2004.

[30] Michael M Wolf, Geza Giedke, J Ignacio Cirac, Phys. Rev. Lett. **96** (8), 080502, 2006.

[31] Miguel Navascués, Frédéric Grosshans and Antonio Acín, Phys. Rev. Lett. **97**, 190502 (2006).

[32] Raul Garcia-Patron et al., Phys. Rev. Lett. **97**, 190503, 2006.

[33] Jens Eisert, S.Scheel and Martin B. Plenio, Phys. Rev. Lett. **89**, 137903, 2002.

[34] Jaromir Fiurăsek, Phys. Rev. Lett. **89**, 137904, 2002.

[35] Kim Boström and Timo Felbinger, Physical Review Letters **89** (18), 187902, .

[36] Stefano Piradola, Stefano Mancini, Samuel L. Braunstein, Seth Lloyd, Nature Physics, **4**, 726-730, 2008.

[37] Kim Boström and Timo Felbinger, Phys. Lett. A **372**, 3953, 2008.

[38] Filippo Caruso, Vittorio Giovannetti, New Journal of Physics, **8**, 310, 2006.

[39] S. Pirandola, S.Lloyd and S.L. Braunstein, Physical review letters **96** (8), 080502 2008.

[40] Stefano Pirandola, New Journal of Physics, **15**, 113046, 2013.

[41] Christian Weedbrook, Carlo Ottaviani and Stefano Pirandola, Phys. Rev. A **89**, 012309, 2014.

[42] C. Eichler, D. Bozyigit, C. Lang, L. Steffen, J. Fink, A. Wallraff, Phys. Rev. Lett. **106**, 220503, 2011.

[43] C. Eichler, D. Bozyigit, A. Wallraff, Phys. Rev. A **86**, 032106, 2012.

[44] Anthony Leverrier, Raul García-Patrón, Renato Renner, and Nicolas J. Cerf, Phys. Rev. Lett. **110**, 030502, 2013.

[45] Paul Jouguet, Sebastien Kunz-Jacques, Eleni Diamanti, and Anthony Leverrier, Phys. Rev. A **86**, 032309, 2012.

[46] Jaromir Fiuràšek and Nicolas J. Cerf, Phys. Rev. A **86**, 060302(R), 2012.

[47] Remi Blandino, Anthony. Leverrier, Marco Barbieri, Jean Etesse, Philippe Grangier, and Rosa Tualle-Brouri, Phys. Rev. A **86**, 012327, 2012.

[48] Nathan Walk, Timothy C. Ralph, Thomas Symul, Ping Koy Lam, Phys. Rev. A. **87**, 020303, 2013.

[49] Radim Filip, Phys. Rev. A **77**, 022310, 2008.

[50] Vladislav C. Usenko and Radim Filip, Phys. Rev. A **81**, 022318, 2010.

[51] Christian Weedbrook, Stefano Pirandola, Seth Lloyd, and Timothy C. Ralph, Phys. Rev. Lett. **105**, 110501, 2010.

[52] Christian Weedbrook, Stefano Pirandola, and Timothy C. Ralph, Phys. Rev. A **86**, 022318, 2012.

[53] M. Sun, X. Peng, Y. Shen, and H. Guo, Int. J. Quantum Inform. **10**, 1250059, 2012.

[54] Y. -C. Zhang, Z. Li, C. Weedbrook, S. Yu, W. Gu, M. Sun, X. Peng, H. Guo, arXiv:1307.7590, 2013.

[55] Jeffrey H. Shapiro, Phys. Rev. A **80**, 022320, 2009.

[56] Z. Zhang, M. Tengner, T. Zhong, F. N. C. Wong, and J. H. Shapiro, Phys. Rev. Lett. **111**, 010501, 2013.

[57] Seth Lloyd, Science **321**, 1463, 2008.

[58] Si-Hui Tan, Baris I. Erkmen, Vittorio Giovannetti, Saikat Guha, Seth Lloyd, Lorenzo Maccone, Stefano Pirandola, and Jeffrey H. Shapiro, Phys. Rev. Lett. **101**, 253601, 2008.

[59] M. Wang and W. Pan, Phys. Lett. A **374**, 2434, 2010.

[60] Renato Renner, Nicolas Gisin, and Barbara Kraus, Phys. Rev. A **72**, 012332, 2005.

[61] Miguel Navascués and Antonio Acín, Phys. Rev. Lett. **94**, 020505, 2005.

[62] Raul García-Patrón and Nicolas J. Cerf, Phys. Rev. Lett. **102**, 130501, 2009.

[63] Stefano Pirandola, Raul García-Patrón, Samuel L. Braunstein, and Seth. Lloyd, Phys. Rev. Lett. **102**, 050503, 2009.

[64] C. Weedbrook, A. M. Lance, W. P. Bowen, T. Symul, T. C. Ralph, P. K. Lam, Phys. Rev. Lett. **93**, 170504, 2004.

[65] S. Pirandola, S. L. Braunstein, and S. Lloyd, Phys. Rev. Lett. **101**, 200504, 2008.

[66] Peter Kok and B. Lovett, *Introduction to optical quantum information processing*, Cambridge University Press, Cambridge, 2010

[67] Carlo Ottaviani and Stefano Pirandola, in preparation.

[68] In DR one of the parties guesses the *encoding* of the other, while in RR it is the *decoding* to be guessed. In the two-way protocol, the encoding is Alice's random displacement a, while the decoding is Bob's post-processed variable b.

[69] Claude. E. Shannon, Bell Syst. Tech. J. **27**, 623-656 (1948).

[70] Aexander S. Holevo, M. Sohma, and Osamu Hirota, Phys. Rev. A **59**, 1820-1828 (1999).

[71] Gaetana Spedalieri, Carlo Ottaviani, and Stefano Pirandola, Open Syst. Inf. Dyn. **20**, 1350011 (2013).

[72] Christopher C. Gerry and Peter L. Knight, *Introductory Quantum Optics*, Cambridge University Press, Cambridge, 2005.

[73] Data on the transmission of infrared radiation in the atmosphere is obtained from http://www.gemini.edu/?q=node/10789.

[74] Samuel L. Braunstein, Stefano Pirandola, Phys. Rev. Lett., **108**, 130502, 2012.

[75] Lo, H.-K., Curty, M. & Qi, B. Measurement-device-independent quantum key distribution. Phys. Rev. Lett. 108, 130503, 2012.

[76] Artur Ekert, Phys. Rev. Lett., **67**, 661, 1991.

[77] D. Mayers and A. Yao, in proceedings of the 39th Annual Symposium on Foundations of Computer Science, Palo Alto, CA, 1998.

[78] J. Barrett, L. Hardy and A. Kent, Phys. Rev. Lett., **95**, 010503, 2005.

[79] Antonio Acin, Nicolas Brunner, Nicolas Gisin, Serge Massar, Stefano Pironio and Valerio Scarani, Phy. Rev. Lett., **98**, 230501, 2007.

[80] Luis Masanes, Stefano Pironio and Antonio Acin, Nat. Comm., **2**, 238, 2011.

[81] J. Barret, R. Colbeck and A. Kent, Phys. Rev. Lett. **110**, 010503, 2013.

[82] Roger Colbeck, Physics **7**, 99, 2014.

[83] Umesh VAzirani and Thomas Vidick, Phys. Rev. Lett. **113**, 0140501, 2014.

[84] Z. Li, Y-C. Zhang, F. Xu, X. Peng, and H. Guo, Phys. Rev. A 89, 052301, 2014.

[85] X-C. Ma, S-H. Sun, M-S. Jiang, M. Gui, and L-M. Liang, Phys. Rev. A 89, 042335, 2014.

[86] Mark M. Wilde, From Classical to Quantum Shannon Theory, Cambridge University Press, Cambridge, 2013.

[87] Geza Giedke and Juan Ignacio Cirac, Phys. Rev. A, **66**, 032316, 2002.

[88] A. Rubenok, J. A. Slater, P. Chan, I. Lucio-Martinez, and W. Tittel, Phys. Rev. Lett. **111**, 130501, 2013.

[89] T. Ferreira da Silva, D. Vitoreti, G. B. Xavier, G. C. do Amaral, G. P. Temporão, and J. P. von der Weid, Phys. Rev. A **88**, 052303 (2013).

[90] Yan-Lin Tang, Hua-Lei Yin, Si-Jing Chen, Yang Liu, Wei-Jun Zhang, Xiao Jiang, Lu Zhang, Jian Wang, Li-Xing You, Jian-Yu Guan, Dong-Xu Yang, Zhen Wang, Hao Liang, Zhen Zhang, Nan Zhou, Xiongfeng Ma, Teng-Yun Chen, Qiang Zhang, and Jian-Wei Pan, Phys. Rev. Lett. **113**, 190501, 2014.

[91] Carlo Ottaviani and Stefano Pirandola, Gaussian continuous variable quantum cryptography needs half de Finetty theorem. (In preparation).

[92] Carlo Ottaviani and Stefano Pirandola, Two-way Gaussian quantum cryptography against two-mode coherent attacks. (in preparation).

[93] Carlo Ottaviani and Stefano Pirandola, Finite-size effects on point-to-point QKD (unpublished).

[94] Vladyslav C Usenko and Radim Filip, New J. Phys. **13** 113007, 2011.

[95] David J.C. MacKay, "Information Theory, Inference, and Learning Algorithms", Cambridge University Press, 2003.

[96] Marco Tomamichel, Charles C. Wen Lim, Nicolas Gisin, Renato Renner, Nature Communications, **3**, 634, 2012.

[97] Anthony Leverrier, Phy. Rev. Lett. **114**, 070501, (2015).

[98] Marcos Curty, Feihu Xu, Wei Cui, Charles Ci Wen Lim, Kiyoshi Tamaki and Hoi-Kwong Lo, Nature Communications, **5,** 3732, 2014.