Palacký University Olomouc
Faculty of Science
Department of Optics

MASTER'S THESIS

Significance of Gaussian Entanglement Measures in Quantum Communication

Author:	**Klára Baksová**
Study programme:	General Physics and Mathematical Physics
Field of study:	General Physics and Mathematical Physics
Form of study:	Full-time
Supervisor:	doc. Mgr. Ladislav Mišta, Ph.D.
Deadline of submitting the thesis:	2 August 2021

Univerzita Palackého v Olomouci
Přírodovědecká fakulta
Katedra optiky

DIPLOMOVÁ PRÁCE

Význam měr gaussovské provázanosti v kvantové komunikaci

Vypracovala:	**Klára Baksová**
Studijní program:	N0533A110004 Obecná fyzika a matematická fyzika
Studijní obor:	Obecná fyzika a matematická fyzika
Forma studia:	Prezenční
Vedoucí práce:	doc. Mgr. Ladislav Mišta, Ph.D.
Termín odevzdání práce:	2. srpen 2021

Declaration

I declare that I have written Master's Thesis "Significance of Gaussian Entanglement Measures in Quantum Communication" on my own under the guidance of doc. Mgr. Ladislav Mišta, Ph.D. by using resources, which are referred to in the list of literature. I agree with the further usage of this document according to the requirements of the Department of Optics.

Declared in Olomouc on August 2, 2021

. . . .

Klára Baksová

Bibliographical identification

Autor's first name and surname	Klára Baksová
Title	Significance of Gaussian Entanglement Measures in Quantum Communication
Type of thesis	Master
Department	Department of Optics
Supervisor	doc. Mgr. Ladislav Mišta, Ph.D.
The year of presentation	2021
Abstract	The Thesis builds on the results of the Bachelor thesis, which supported the presumption of the equivalence of two Gaussian entanglement measures, later proved in [L. Lami, L. Mišta, Jr., and G. Adesso, *arXiv:2010.15729* (2020)]. The first measure is Gaussian intrinsic entanglement, and the second one is Rényi-2 Gaussian entanglement of formation. Unification of these measures provides a unique computable Gaussian entanglement measure equipped with many important properties. Recently, it was shown that for different types of abstract Gaussian cryptographic protocols, the measure constitutes the upper bound on the Gaussian distillable key being an entanglement measure quantifying the secrecy content in a given Gaussian quantum state. In this Thesis, we prove that the measure is an upper bound on the secret key rate for any Gaussian quantum key distribution protocol and verify it for standard continuous-variable protocols. Further, we compare the considered measure with upper bounds on the secret key rate capacity of the channel derived from squashed entanglement and relative entropy of entanglement for pure-loss, thermal-loss, pure-amplifier, thermal-amplifier and additive-noise channel and show that it provides either equal or tighter upper bound than the squashed entanglement, but it always a looser upper bound the one based on the relative entropy of entanglement.
Keywords	quantum entanglement, Gaussian entanglement measures, quantum cryptography, Gaussian quantum channels
Number of pages	40
Number of appendices	0
Language	English

Bibliografická identifikace

Jméno a příjmení autora	Klára Baksová
Název práce	Význam měr gaussovské provázanosti v kvantové komunikaci
Typ práce	Diplomová
Pracoviště	Katedra optiky
Vedoucí práce	doc. Mgr. Ladislav Mišta, Ph.D.
Rok obhajoby práce	2021
Abstrakt	Tato práce navazuje na výsledky Bakalářské práce, které podpořily domněnku o ekvivalenci dvou Gaussovských měr kvantové provázanosti, později dokázanou v [L. Lami, L. Mišta, Jr., and G. Adesso, *arXiv:2010.15729* (2020)]. První mírou je Gaussovská vnitřní kvantová provázanost a druhou je Rényi-2 Gaussovský entanglement formování. Sjednocení těchto měr dává vzniknout unikátní vypočitatelné Gaussovské míře kvantové provázanosti, vybavené mnoha důležitžmi vlastnostmi. Nedávno bylo ukázáno, že pro různé typy abstraktních Gaussovských kryptografických protokolů tvoří míra horní hranici na Gausovský destilovatelný klíč, kde kvantifikuje míru bezpečnosti daného Gaussovského kvantového stavu. V této práci jsme ukázali, že vzniklá míra tvoří horní hranici na rychlost generace tajného klíče pro libovolný Gaussovský kvantový protokol distribuce klíče a provedli ověření na standardních protokolech se spojitými proměnnými. Dále jsme porovnali míru s horními hranicemi na kapacitu kanálu odvozenou ze squashed entanglementu a relativní entropie entanglementu pro čistý ztrátový kanál, termální ztrátový kanál, čistý zesilující kanál, termální zesilující kanál a kanál s přidaným šumem, a ukázali, že daná míra tvoří horní hranici, která je stejná nebo těsnější než horní hranice odvozená ze squashed entanglementu, ale vždy volnější než horní hranice odvozená z relativní entropie entanglementu.
Klíčová slova	kvantová provázanost, gaussovské míry kvantové provázanosti, kvantová kryptografie, gaussovské kvantové kanály
Počet stran	40
Počet příloh	0
Jazyk	anglický

Contents

Introduction

Communication has always been an integral part of human existence. Nevertheless, people have not always wanted to share the information in the message with whoever. Consequently, they have started developing methods hiding the information in the message and making it detectable only for the stated receiver. This can be done by having an encoding key, which is used to encrypt the message into a cipher that is incomprehensible for any eavesdropper but can be decrypted by anyone having the key.
The first attempts are dated thousands of years ago, and they had been using a pen and paper to encrypt the message. Mechanical and electromechanical machines invented in the twentieth century advanced the encryption methods but also the decoding techniques.
Even though the key providing a "perfect secrecy" was introduced by Claude Shannon [1], in practice, the communicating parties always had to trust some messenger or channel to distribute the key.
A breakthrough was brought by quantum mechanics when Bannet and Brassard [2] came up with the techniques of quantum key distribution. There, the eavesdropper always leaves traces that are detectable for the communicating parties. This is caused by the no-cloning theorem [3], which forbids anyone to perfectly copy ensembles of non-orthogonal quantum states.
Additionally, quantum mechanics provides another unique tool that plays a key role in quantum communication. It is quantum entanglement.

Quantum entanglement is a purely quantum phenomenon with no analogy in the classical world. It is made possible by the superposition principle resulting from the linearity of quantum mechanics.
If two quantum systems are entangled, their local properties become uncertain, while the global properties remain well defined. The resulting correlation between the systems is what we call quantum entanglement. With revealing its usage in fundamental quantum information protocols, it has become an interest of broad research.
One of the questions was the quantification of entanglement, which gave rise to the theory of entanglement measures.

The theory of entanglement measures builds on several axioms that every good entanglement measure should satisfy. It should be a non-negative function that is zero on all separable states, and it should not increase under local operations and classical communication (LOCC). Such a function is called an entanglement monotone [4]. Other axioms say that it should reduce to marginal von Neumann entropy on pure states it should be continuous, convex, additive on tensor product and asymptotically continuous function [5]. Above these mathematical properties, entanglement measures should be computable and usable in protocols.
Even though many entanglement measures based on different approaches of entan-

glement quantification were introduced, unfortunately, none of them satisfies all the required features, thus seeking for a good entanglement measure continues.

The aim of our interest will be an entanglement measure called Gaussian intrinsic entanglement (GIE), which is a cryptographically motivated entanglement measure originating from intrinsic entanglement under the restriction to the Gaussian scenario [6].
During its investigation [6, 7, 8], the obtained results coincided with Gaussian convex roof entanglement measure called Gaussian Rényi-2 entanglement of formation (GR2EoF). This gave rise to the question of whether these two measures are equivalent, which was proved in [9] for all Gaussian states with a covariance matrix with block-diagonal position-momentum block form, which includes all two-mode Gaussian states. The unification of these measures formed a unique entanglement measure, which is faithful, monotonic under all Gaussian LOCC, satisfies monogamy inequality [10] and Gaussian Rényi-2 version of Koashi-Winter monogamy relation [11], and it is additive on two-mode symmetric states. Above that, it is computable for many Gaussian states.
However, the operational meaning of this measure was in question.

To answer this question, we investigated GIE in the context of quantum communication a showed that it sets a computable upper bound on the secret key rate for any Gaussian quantum key distribution (CV QKD) protocol. Additionally, we verified this by comparing it with known lower bounds on the secret key rate [12] in standard CV QKD protocols [13, 14, 15].
Above that, we compared GIE with derived upper bounds on the secret key rate capacity of the channel [16] derived from squashed entanglement [17] and relative entropy of entanglement [18]. That showed that GIE also forms a computable upper bound on this quantity for several quantum channels, in more detail, for the pure-loss channel, pure-amplifier channel, thermal-loss channel, thermal-amplifier channel and added-noise channel.
These results set the desired significance of GIE in quantum communication.

Chapter 1

Introduction to Quantum Entanglement and Its Quantification

In the first chapter, we will introduce one of the most interesting phenomenons that can be met exclusively in quantum physics. This phenomenon is quantum entanglement. Here, we will not only describe what quantum entanglement is, but we will also introduce its quantification.

1.1 Quantum Entanglement

Quantum entanglement is a sort of correlation between quantum systems. Let us consider two *isolated* systems A and B, each of which is in some quantum state. According to one of the postulates of quantum mechanics, each of these two states, such as every quantum state of an isolated system, corresponds to a vector ray in a Hilbert space. In Dirac's symbolic, a column vector is denoted by $|\varphi\rangle$, so let us use this symbolic and denote the states of our systems $|\psi\rangle_A$ and $|\phi\rangle_B$.
Firstly, we will show step by step how some two states can be entangled, so the definition of quantum entanglement is clear.

1.1.1 Quantum Superposition

Quantum entanglement is made possible by the superposition principle. This means that quantum state $|\varphi\rangle$ can be in the superposition of two distinct states, e.g. $|0\rangle$ and $|1\rangle$, then it is written as their linear combination

$$|\varphi\rangle = \alpha\,|0\rangle + \beta\,|1\rangle\,, \tag{1.1}$$

where α and β are complex numbers and squares of their absolute values $|\alpha|^2$ and $|\beta|^2$ correspond to the probabilities of finding the system in corresponding states $|0\rangle$ and $|1\rangle$, hence $|\alpha|^2 + |\beta|^2 = 1$.
A good physical example of this phenomenon can be a single photon sent to a beam splitter with some reflectance r and transmittance t, for which applies $|r|^2 + |t|^2 = 1$. Let us denote the the state, in which the photon is transmitted and can be found in the horizontal arm of the beam splitter with probability $|t|^2$, $|\rightarrow\rangle$, and the state, in which the photon is reflected and can be found in the vertical arm with probability $|r|^2$, $|\uparrow\rangle$.

Thus, if we do not perform the measurement in the individual arms, after passing the beams splitter, photon is in a superimposed state of these two states, i.e.

$$|\varphi\rangle_{photon} = t\,|{\rightarrow}\rangle + r\,|{\uparrow}\rangle\,. \tag{1.2}$$

The superposition can be experimentally verified by constructing Mach-Zehnder interferometer and observing interference effects from both arms while a single photon is sent to the input [19].

1.1.2 Examples of an Entangled State

By understanding the quantum superposition, we have good background to understand quantum entanglement as well.

Before we introduce rigorous mathematical and physical definitions in the following sub-chapter, we will set another physical example. Let it be an interaction between a two-level atom with a single-mode electromagnetic field. To make it even simpler, let us work with only a discrete single-photon field.

In such an approximation, if the atom is in an excited state $|e\rangle$ at the beginning, the field is in a vacuum state $|0\rangle$. However, after some time, the atom can transfer into the ground state $|g\rangle$ by spontaneously emitting the photon and the field state becomes $|1\rangle$. Then, the wave-function of the whole system at some time t is a linear combination of these two options

$$|\Phi(t)\rangle = \alpha(t)\,|e\rangle\,|0\rangle + \beta(t)\,|g\rangle\,|1\rangle\,, \tag{1.3}$$

where $\alpha(t)$ is a probability amplitude of finding the atom in the excited state at time t and $\beta(t)$ is a probability amplitude of finding the atom in the ground state with the emitted photon at time t.

Here the atom and field mode are entangled and we say that the state of the system (1.3) is an entangled state. This property allows us to know the information of the field state by measuring the atom state and vice versa.

Such a type of correlation can be generated on many other systems, for instance half-spin particles that are entangled in their spins or pairs of photons that are entangled in their polarization. This is widely used in quantum information theory, where these correlations are used to perform quantum communication.

1.1.3 Definition of Quantum Entanglement

The knowledge of previous sub-chapters can be mathematically defined as follows.

Let $\mathscr{H}_A$ and $\mathscr{H}_B$ be the Hilbert spaces of our systems A and B from the beginning of this chapter and $|\psi\rangle_A$ and $|\phi\rangle_B$ be their states. Thus, if a global state $|\Psi\rangle_{AB}$ cannot be written as a product state of these states, i.e.

$$|\Psi\rangle_{AB} \neq |\psi\rangle_A\,|\phi\rangle_B\,, \tag{1.4}$$

then the state $|\Psi\rangle_{AB}$ is called entangled. Otherwise, it is called separable.

This definition applies for pure states, i.e. states, where the state vector $|\varphi\rangle$ contains the maximal attainable information about the state.

Due to the imperfections of real experimental equipment, we can succeed in preparing our systems in a certain state $|\varphi_j\rangle$ only with some probability p_j. Thus, we say that the prepared state is mixed and describe it with a density matrix

$$\rho = \sum_j p_j \left|\varphi_j\right\rangle \left\langle\varphi_j\right| . \tag{1.5}$$

Hence, in the context of mixed states, a state ρ^{AB} is called entangled if it cannot be written as a mixture of product states, i.e.

$$\rho_{AB} \neq \sum_i p_i \rho_{A_i} \otimes \rho_{B_i}. \tag{1.6}$$

To define entanglement in physical terms, we will use its usage in quantum communication mentioned above.
Let us imagine two parties communicating via a quantum channel. Since every channel is lossy, the transmitted information is depreciated. To increase the amount of shared information the parties can either improve the quality of performed individual local operations or they can use classical communication to coordinate the quantum operations of the opposite party. Nevertheless, local operations and classical communication (LOCC) can create only the states of the form of the right-hand side of Eq. (1.6). Therefore, quantum entanglement can be defined as a sort of quantum correlation that cannot be created by LOCC [5].

1.2 Entanglement Measures

Having quantum entanglement defined, we want to know how can we quantify it. This can be done by establishing a theory of entanglement measures. It is highly motivated by many other cases alongside quantitative characterization of entanglement. For instance, entanglement measures bound some hardly computable quantities [20], they are an essential tool in proving impossibility [21] and limitations [22] in several quantum information protocols.
In terms of experiment, entanglement measures are used to estimate quality of prepared entangled states [23], entangling gates [24] and establishment of some protocols, such as entanglement distillation [25].

1.2.1 Axioms and Problems of Entanglement Measures

Entanglement measure is a type of mathematical function of certain quantum state parameters, which fulfills conditions associated with properties of entanglement. These conditions constitute eight axioms of entanglement measures. Firstly, entanglement measure should be a non-negative function. Secondly, it should be zero on all separable states. Thirdly, it should not increase under LOCC. A function satisfying these three axioms is so-called entanglement monotone [4]. Further, it should reduce to von Neumann entropy on pure states, it should be continuous, convex, additive on tensor product and asymptotically continuous function [5].
Any good entanglement measure ought to satisfy all these axioms.

Now a natural question arises: 'How can we find such a function?'
Well, there is no unique answer. Since there are many angles, from which we can look

at the entanglement, there have been multiple ideas of entanglement quantification. However, all the introduced entanglement measures so far have their drawbacks.
Firstly, they may not satisfy some of the axioms mentioned above, which can cause their unreasonable behaviour on some classes of states. Secondly, they may not fit into the context of any physical protocol and thus lack any physical meaning. Last but not least, some of the entanglement measures are almost impossible to compute.
Let us introduce some of the known entanglement measures.

1.2.2 Examples of Entanglement Measures

One of the best well known entanglement measures is so-called *logarithmic negativity* [26] defined as

$$E_N(\rho) = \log \|\rho^{\mathrm{T}_A}\|_1, \tag{1.7}$$

where ρ^{T_A} denotes the partial transpose of ρ with respect to party A and the trace norm $\|\rho^{\mathrm{T}_A}\|_1$ is defined as $\|\rho^{\mathrm{T}_A}\|_1 = tr|\rho^{\mathrm{T}_A}|$.
Logarithmic negativity is an easily computable entanglement monotone and it has its operational interpretation as a cost of entanglement under positive partial transpose (PPT) preserving operations [27]. This can be also interpreted as entanglement quantification pursuant to how much a partial transpose of the given state deviates from a physical state. However, a partial transposition itself is not a physical operation, i.e. it cannot be carried out in a laboratory, so this operational interpretation is rather vague. Additionally, it also lacks convexity.

Other well known entanglement measures are *entanglement of distillation* [28] and *entanglement of formation* [29]. These measures have very good operational meaning in the context of entanglement distillation, which is a process using LOCC operations to increase quantum entanglement up to almost maximally entangled states at the cost of reducing the number of states on the output compared to the number of states on the input that are non-maximally entangled. Thereafter, entanglement of distillation defines the number of maximally entangled states per copy, which can be distilled from n identical copies of a given non-maximally entangled state in the asymptotic limit $n \to \infty$. However, such calculation requires optimization over all possible LOCC operations, which makes it almost impossible to compute. Also it vanishes on bound-entangled states [30], i.e. the entangled states from which cannot be distilled a pure state.
On the other hand, entanglement of formation is defined as a number of maximally entangled states needed to prepare copies of particular state [28]. It can be readily seen that it is a dual measure of entanglement of distillation. Moreover, it bounds it from above. Nevertheless, even though entanglement of formation has its operational meaning, it is computable only for qubits [31] and symmetric Gaussian states [32]. Additionally, its additivity is still in doubt.

For the time being, the most promising approach to quantify entanglement is quantification based on a classical cryptographical protocol called secret key agreement (SKA). Very briefly, in this protocol, there are two honest parties, Alice and Bob, having random variables A and B, and an eavesdropper Eve having her random variable E. Alice and Bob communicate via an insecure channel, to which Eve has a full access. Their goal is to generate a secret key, about which Eve has minimal possible information. To do so, variables of Alice and Bob have to be correlated by so-called *secret*

correlations [33, 34].
The motivation to entanglement quantification based on SKA has originated from the analogue between the definition of quantum entanglement and the definition of secret correlations in SKA. Secret correlations are defined as correlations that cannot be established by local operations and public communication (one can see that it is very similar to LOCC) and they can be quantified using so-called *intrinsic information* [35]

$$I(A;B\downarrow E) = \inf_{E\to\tilde{E}}[I(A;B|\tilde{E})], \tag{1.8}$$

where the infimum is taken over all conditional probability distributions $P(\tilde{E}|E)$ defining a new random variable $\tilde{E}$ and

$$I(A;B|\tilde{E}) = H(A|E) - H(A|B,E) \tag{1.9}$$

is conditional mutual information between A and B. Here, $H(X|Y)$ is the conditional Shannon entropy given by $H(X|Y) = H(X,Y) - H(Y)$, where $H(X,Y)$ and $H(Y)$ are joint and marginal Shannon entropies [36].
Now, it is known that relation between secret correlations and quantum entanglement is even mathematically provable and also that we can rigorously pass from SKA to quantum key distribution, which will be described in Chapter 3. Several entanglement measures have been born by using intrinsic information to quantify entanglement.
Undoubtedly, the most significant is *squashed entanglement* [37]

$$E_{sq}\left(\rho_{AB}\right) = \inf\left\{\frac{1}{2}I_{\rho}\left(A;B|E\right):\ \rho_{AB} = \mathrm{Tr}_{E}\rho_{ABE}\right\}, \tag{1.10}$$

where $I_{\rho}\left(A;B|E\right)$ is the *quantum conditional mutual information* of ρ_{ABE} [38]

$$I_{\rho}\left(A;B|E\right) := S(AE) + S(BE) - S(ABE) - S(E) \tag{1.11}$$

and $S(X)$ is the von Neumann entropy of the system. According to this equation, squashed entanglement can be interpreted as an infimum of quantum conditional mutual information $I_{\rho}\left(A;B|E\right)$ of an extension of the investigated quantum state ρ_{AB} with respect to all the extensions ρ_{ABE}.
Squashed entanglement is so important because it is the only known entanglement measure that satisfies all eight required axioms, while it also has an operational meaning in the context of SKA. Unfortunately, it is extremely hard to be evaluated.

Another entanglement measure originating from SKA was introduced by Gisin and Wolf. The speech is about *classical measure of entanglement* [33]

$$\mu\left(\rho_{AB}\right) = \min_{\{|z\rangle\}}\left(\max_{\{|x\rangle\},\{|y\rangle\}}\left(I\left(A;B\downarrow E\right)\right)\right), \tag{1.12}$$

where the infimum is taken over all purifications $\Psi = \sum_z \sqrt{p_z}\phi_z \otimes z$ such that $\rho_{AB} = \mathrm{Tr}_{\mathscr{H}_E}(P_\Psi)$ holds on over all bases $\{|z\rangle\}$ of $\mathscr{H}_E$, the maximum is over all bases $\{|x\rangle\}$ of $\mathscr{H}_A$ and $\{|y\rangle\}$ of $\mathscr{H}_B$, and $P_{XYZ}(x,y,z) := |\langle x,y,z|\Psi\rangle|^2$.
This entanglement measure is faithful, since it is positive iff ρ_{AB} is entangled, and it also reduces to von Neumann entropy on pure states. However, its monotonicity under LOCC has not been proved and its evaluation is very hard for most of the mixed states.

If we change the order of optimization in (1.12), we get another entanglement measure called *intrinsic entanglement* (IE) [6]

$$E_{\downarrow}(\rho_{AB}) = \sup_{\{|A\rangle,|B\rangle\}} \left\{ \inf_{\{|E\rangle,|\Psi\rangle\}} \left[I\left(A;B\downarrow E\right)\right] \right\}, \tag{1.13}$$

where A (Alice) and B (Bob) are two subsystems of entangled state ρ_{AB}, E (Eve) is the purifying subsystem and $|\Psi\rangle$ is a purification of state ρ_{AB}, i.e. $\mathrm{Tr}_E\,|\Psi\rangle\,\langle\Psi| = \rho_{AB}$. It can be readily seen that relation $E_{\downarrow} \leq \mu$ applies according to min-max inequality [39]. Due to the change of the optimization, IE can provide better computability than classical measure of entanglement.

Even though there are several other approaches of entanglement quantification (e.g. geometric measures [40]), we will close this Chapter with two entanglement measures originating from entropic quantities.
The first of them is *relative entropy of entanglement* [41, 42] generated by *quantum relative entropy* [43]. It is defined in terms of relative entropy between an entangled state and its closest separable state, i.e.

$$E_R(\rho) = \min_{\sigma' \in \mathscr{D}} S(\rho||\sigma') = S(\rho||\sigma), \tag{1.14}$$

where $\mathscr{D}$ is the set of separable states, $S(\rho||\sigma) \equiv \mathrm{Tr}(\rho \log \rho - \rho \log \sigma)$ and $\sigma = \sigma(\rho)$ is the closest separable state. It is an entanglement monotone, for pure states it reduces to von Neumann entropy [40, 41] and it is convex. However, its general closed formula has not been found for many states.

Here, let us remark that relative entropy of entanglement possesses some kind of geometric intuition (not in the true sense of the word, since quantum relative entropy is not a true metric, as it is not symmetric and does not satisfy the triangle inequality). One can see that there is no unique view to each entanglement measure. Another example is an entanglement of formation mentioned above, which can be derived by minimization of mean von Neumann entropy of an ensemble realizing a considered density matrix [44], yet it is usually mentioned in the context of entanglement distillation.

The last mentioned will be entanglement quantification using the *Rényi-α entropies* [45] defined as

$$S_\alpha(\rho) = (1-\alpha)^{-1} \ln \mathrm{Tr}\left(\rho^\alpha\right), \tag{1.15}$$

with $\alpha \geq 0$ and $\alpha \neq 1$.
They reduce to von Neumann entropy in the limit $\alpha \to 1$ and they are a good family of quantities for studying correlations in quantum states of composite systems. For a bipartite pure state ρ_{AB} any of the Rényi-α entropies evaluated on reduced density matrix of one of the subsystems is an entanglement monotone, which gives rise to Rényi-α entanglement [46]. Moreover, any such measure can be extended to mixed states via conventional convex roof techniques [47, 48]. Further, in the case of Rényi entropy of order 2 ($\alpha = 2$) it has been proven that originated Rényi-2 measure of entanglement satisfies 'monogamy' inequality [10, 49]. In [50] it has been shown that this entanglement quantification is expedient in the context of Gaussian states and it gave rise to entanglement measure called *Gaussian Rényi-2 entanglement of formation* (GR2EoF), which plays an important role in this Thesis and it will be more discussed in the following chapter.

Chapter 2

Gaussian Intrinsic Entanglement and Gaussian Rényi-2 Entanglement of Formation

The work on this Thesis was inspired by the unification of two ostensibly different Gaussian entanglement measures, which are *Gaussian intrinsic entanglement* (GIE) and *Gaussian Rényi-2 entanglement of formation* (GR2EoF) [9]. This unification transferred one's properties to the other and led to the rise of a unique, monogamous Gaussian entanglement monotone, which is computable for many classes of states. In this chapter, we will start with introducing Gaussian states, then we will separately define both of the measures and we will discuss their properties.
Another important fact is the operational significance of these measures, which is reserved for Chapter 3.

2.1 Gaussian States

Gaussian states are very important states in quantum physics not only because they can be easily prepared in experiments [51] but also because they possess several mathematical advantages. Even though they occur in continuous variable (CV) systems with $\dim \mathscr{H} = \infty$, they are characterized by a finite number of parameters. In more detail, they can be fully described by a vector of first moments and by the covariance matrix (CM) of second moments.
They earned their name due to the Gaussian shape of their Wigner function.

In the case of a general N-mode system with Hilbert space

$$\mathscr{H}_N = \bigotimes_{i=1}^{N} \mathscr{H}_i, \tag{2.1}$$

where $\mathscr{H}_i$ are Hilbert spaces of particular single modes, Gaussian states are described by $2N$ quadrature operators $x_1,p_1,x_2,p_2,\dots x_N,p_N$, where x_i and p_i are canonically conjugated and they fulfill canonical commutation rules

$$[x_i,p_j] = i\delta_{ij}, \quad [x_i,x_j] = [p_i,p_j] = 0, \tag{2.2}$$

where δ_{ij} is the Kronecker symbol.
We will introduce a vector of these operators

$$\mathbf{r} = (x_A,p_A,\dots x_N,p_N)^{\mathrm{T}} \tag{2.3}$$

and rewrite canonical commutation rules as

$$[r_i,r_j] = i\Omega_{Nij}, \tag{2.4}$$

where

$$\Omega_N = \bigoplus_{i=1}^{N} \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix} \tag{2.5}$$

is the so-called symplectic matrix.
Now, we are equipped to introduce above-mentioned $2N \times 1$ vector of first moments d with elements $d_i = \langle r_i \rangle = \mathrm{Tr}(\rho r_i)$ and $2N \times 2N$ CM γ with elements

$$\gamma_{ij} = \langle r_i r_j + r_j r_i \rangle - 2 \langle r_i \rangle \langle r_j \rangle . \tag{2.6}$$

In further work, we will assume $d = 0$, as arbitrary d can be displaced to zero without any impact on the entanglement properties of the state.
Any physical state must satisfy Heisenberg uncertainty principle, which in the terms of CM γ is written as [52]

$$\gamma + i\Omega \geq 0. \tag{2.7}$$

Thus, any real CM $\gamma > 0$ satisfying Eq.(2.7) represents some Gaussian state.

If we want to transform a CM in such a way that Gaussian character of the state remains preserved, we need to use Gaussian unitary operations, which are represented by a real $2N \times 2N$ *symplectic matrix* S satisfying the condition

$$S\Omega_N S^{\mathrm{T}} = \Omega_N. \tag{2.8}$$

Hence, the CM transforms as

$$\gamma' = S\gamma S^{\mathrm{T}}. \tag{2.9}$$

Additionally, according to the Williamson's theorem [53], any N-mode CM γ can be brought by corresponding symplectic transformation S into the *Williamson's normal form*

$$S\gamma S^{\mathrm{T}} = \mathrm{diag}\left(\nu_1,\nu_1,\ldots,\nu_N,\nu_N\right), \tag{2.10}$$

where $\nu_1 \geq \nu_2 \geq \cdots \geq \nu_N$ are the so-called symplectic eigenvalues.

From the previous statements, it has been suggested that for working with Gaussian states it is convenient to use CMs. Above that, we can even simplify our work without loss of any generality by working with the *standard form* of CMs [54], which for a two-mode Gaussian state is

$$\gamma_{AB} = \begin{pmatrix} a & 0 & c_x & 0 \\ 0 & a & 0 & c_p \\ c_x & 0 & b & 0 \\ 0 & c_p & 0 & b \end{pmatrix}, \tag{2.11}$$

where $c_x \geq |c_p| \geq 0$. Any two-mode CM can by brought to the standard form (2.11) by local Gaussian unitary operations.

Two-Mode Squeezed Vacuum

In this Thesis, we will work with entangled Gaussian states. An example of such a state is the two-mode squeezed vacuum state $|\mathrm{TMSV}\rangle$. In the Fock basis [55] the two-mode squeezed vacuum state (TMSV) is written as [12]

$$|\mathrm{TMSV}\rangle = \frac{1}{\sqrt{\cosh r}} \sum_{n=0}^{\infty} (\tanh r)^n |n,n\rangle \,, \tag{2.12}$$

where r is the *squeezing parameter*.
In the terms of CM, the elements of CM in standard form (2.11) for two-mode squeezed vacuum state are $a = b = \frac{1+\Upsilon^2}{1-\Upsilon^2}$ and $c_{x,p} = \frac{2\Upsilon}{1-\Upsilon^2}$ and therefore the CM of TMSV can be written as

$$\gamma_{AB_{\mathrm{TMSV}}} = \begin{pmatrix} \frac{1+\Upsilon^2}{1-\Upsilon^2} & 0 & \frac{2\Upsilon}{1-\Upsilon^2} & 0 \\ 0 & \frac{1+\Upsilon^2}{1-\Upsilon^2} & 0 & \frac{2\Upsilon}{1-\Upsilon^2} \\ \frac{2\Upsilon}{1-\Upsilon^2} & 0 & \frac{1+\Upsilon^2}{1-\Upsilon^2} & 0 \\ 0 & \frac{2\Upsilon}{1-\Upsilon^2} & 0 & \frac{1+\Upsilon^2}{1-\Upsilon^2} \end{pmatrix}, \tag{2.13}$$

where $\Upsilon = \tanh r \in [0,1)$.

In the limit of infinite squeezing, $r \to \infty$ ($\Upsilon \to 1$), we obtain perfect correlation among quadratures x and perfect anti-correlation among quadratures p (2.2), i.e., $x_1 = x_2$ and $p_1 = -p_2$. Such a state is a well known EPR entangled state [56].

The individual modes of TMSV are mixed thermal states and they can be obtained by tracing over the redundant mode, i.e. the states

$$\rho_{A(B)} = \mathrm{Tr}_{B(A)} \left(|\mathrm{TMSV}\rangle \langle \mathrm{TMSV}|\right) = \frac{1}{(\cosh r)^2} \sum_{n=0}^{\infty} (\tanh r)^{2n} |n\rangle \langle n| \tag{2.14}$$

of variance $V = \cosh(2r)$ and an effective average number of photons $\overline{n} = \sinh^2(r)$.

2.2 Gaussian Intrinsic Entanglement

Gaussian intrinsic entanglement (GIE) is a cryptographically motivated Gaussian entanglement measure. It is a special case of IE (1.13) under the restriction to so-called Gaussian scenario, i.e. the cases, in which all states, measurements and channels are Gaussian.
For two-mode state ρ_{AB} with CM γ_{AB} with purifying subsystem E, GIE is defined as [6]

$$E_{\downarrow}^{G}(\rho_{AB}) := \sup_{\Gamma_A,\Gamma_B} \inf_{\Gamma_E} [I\,(A;B|E)], \tag{2.15}$$

where

$$I\,(A;B|E) = \frac{1}{2} \ln \left(\frac{\det \sigma_A \det \sigma_B}{\det \sigma_{AB}} \right). \tag{2.16}$$

Further,

$$\sigma_{AB} = \gamma_{AB|E} + \Gamma_A \oplus \Gamma_B, \tag{2.17}$$

$\sigma_{A,B}$ are local sub-matrices of σ_{AB} and Γ_A (Γ_B) is a single-mode CM of pure-state Gaussian measurement on a mode A (B).
Next,

$$\gamma_{AB|E} = \gamma_{AB} - \gamma_{ABE} \left(\gamma_E + \Gamma_E\right)^{-1} \gamma_{ABE}^{\mathrm{T}} \tag{2.18}$$

is a CM of conditional mutual state $\rho_{AB|E}$ [57]. This state is obtained by a Gaussian measurement with CM Γ_E on purifying subsystem E [8].

GIE possess some of the important properties of entanglement measures. It vanishes on separable states and it does not increase under Gaussian local trace-preserving operations and classical communication [6] . Moreover, its optimum is always reached by homodyne and heterodyne detection, hence it is physically meaningful.

GIE was analytically calculated for two-mode Gaussian states including all symmetric partial minimum uncertainty states, weakly mixed asymmetric squeezed thermal states with partial minimum uncertainty, and weakly mixed symmetric squeezed thermal states [6]. The obtained results showed up to be equal to another Gaussian entanglement measure GR2EoF, which led to a conjecture of equivalence of these two measures. Later, we extended the results of GIE for the class of Gaussian states with minimum negativity for fixed global and local purities (GLEMS) [8] and our results supported the conjecture of the equivalence.

2.3 Gaussian Rényi-2 Entanglement of Formation

Gaussian Rényi-2 Entanglement of Formation (GR2EoF) is Gaussian entanglement measure originating from Rényi-2 entropy, which is a special case of Rényi-α entropies (1.15) with $\alpha = 2$ [9]

$$S_2(\rho) = \frac{1}{2} \ln \det \gamma =: M(\gamma). \tag{2.19}$$

For bipartite pure states, Rényi-α entropies evaluated on the reduced density matrix of one subsystem are an entanglement monotone [4]. Such measures can be universally extended to mixed states via conventional convex roof techniques [47, 48]. Above that, Rényi-2 entropy has been proven to satisfy monogamy inequality [10, 49] for multiqubit states [46, 58]. Finally, in [50] it has been shown that Rényi-2 entropy satisfies the strong subadditivity inequality for arbitrary Gaussian states of quantum harmonic systems, which allows employing Rényi-2 entropy to define valid measures of various correlations in quantum information theory including quantum entanglement.

The convenient properties of Rényi-2 entropy led to defining GR2EoF [50]

$$E_{F,2}^{G}(\gamma_{AB}) := \inf_{\substack{\sigma_{AB} \geq i\Omega_{AB} \\ \sigma_{AB} \mathrm{pure}}} M(\sigma_A), \tag{2.20}$$

where quantum CMs σ are so-called *seeds* of the Gaussian measurements [9] for corresponding modes.

As we already outlined at the beginning of this Chapter, GR2EoF coincide with all the obtained results of GIE [6, 7, 8], which led to the question, whether these entanglement measures are equivalent in general. This has been proven in [9] for all normal CMs with an arbitrary number of modes and notably for all two-mode CMs. Hence, all the

properties of GR2EoF and GIE have been unified. This led to a formation of a unique entanglement measure, which is faithful, it is monotonic under all Gaussian LOCC, it satisfies monogamy inequality [10] and Gaussian Rényi-2 version of Koashi-Winter monogamy relation [11], and it is additive on two-mode symmetric states. Above that, it is computable for many Gaussian states.
A very important property of any entanglement measure is its operational meaning. Luckily, GIE seemed to be a good candidate to provide this feature. In the following chapter, we will show the proof of GIE upper bounding secret key rate in continuous-variable quantum key distribution protocols.

In the rest of the Thesis, we will call the considered entanglement measure GIE but we will mind that some of the following attainments can refer to papers that were originally published in the context of GR2EoF.

Chapter 3

Significance of GIE in Quantum Cryptography

Some entanglement measures have revealed to have an important significance in quantum cryptography. In fact, they can serve as upper bounds on secret key rate [59] and capacity [17, 18]. The question was whether GIE has this meaning as well.

In this chapter, we will show a proof of GIE generating an upper bound on the secret key rate for a generic Gaussian channel in the continuous-variable quantum key distribution [9]. Moreover, we will verify the claim by evaluating GIE for particular CV QKD protocols.

3.1 Secret Key Agreement

Firstly, we will remind the classical secret key agreement outlined in Chapter 1. In this protocol, we have three parties, Alice, Bob and Eve.
Generally, in secret communication, Alice and Bob want to communicate a message and prevent Eve from eavesdropping on it. To do so, they want to share a secret key, so Alice can encode the message into the secret key to turn the message into a cipher, which for Eve is unreadable. Then, Bob can decode the cipher by using the secret key. Nevertheless, Eve can apply decoding algorithms onto the cipher, break it and gain some information about the message from it. Naturally, Alice and Bob want to generate such a cipher that will be unbreakable. This is possible by generating a key of the same length as the length of the message. If the key is truly random, never reused and secure, then the cipher is unbreakable [1]. Arising question is when the key is truly secure. In practice, Alice and Bob always have to rely on some communication channel to distribute the key. The classical key distribution, also known as secret key agreement is described as follows.

Alice and Bob are two honest parties with variables A and B, and they communicate through a public channel. The third party, Eve, is an eavesdropper having a variable E. Eve has full access to a triple of random variable ABE distributed according to a probability distribution P_{ABE} (Fig. 3.1). Alice and Bob have many copies of their variables, and their goal is to use them to generate a secret key in such a way that Eve's information about the key is negligible [60].

To achieve this, Alice and Bob have to apply secret key distillation, error correction

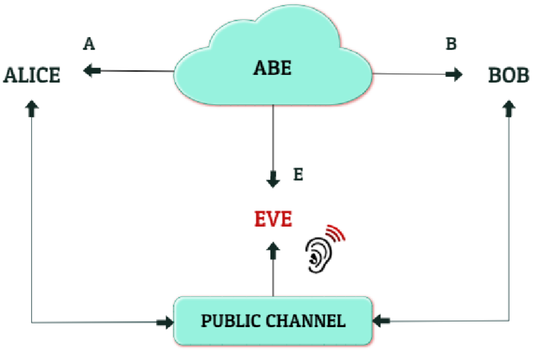

Figure 3.1: Secret key agreement protocol

and privacy amplification [12]. Thereafter, their net gain of the secret key is the secret key rate [12]

$$K(A:B||E) = H(A) - H(A|B) - H(A:E) = H(A:B) - H(A:E), \tag{3.1}$$

where $H(X)$ is a Shannon entropy and $H(X|Y)$ is a conditional entropy [36, 61]. Unfortunately, it is generally almost impossible to compute, however it can be bounded. Usually, when someone wants to compute the secret key rate, they compute its lower bound to know the "worst-case scenario".
On the other hand, one of its upper bounds is already mentioned intrinsic information (3.4) [62, 35]:

$$K(A:B||E) \leq I(A:B\downarrow E). \tag{3.2}$$

It has been shown that the secret key distribution can be perfectly secure using quantum key distribution (QKD) methods [63].
To pass to the quantum protocols, to which we will refer as *continuous variable* (CV) *quantum key distribution* (QKD) protocols [64], we replace the probability distribution P_{ABE} by a quantum state vector $\Psi \in \mathscr{H}_A \otimes \mathscr{H}_B \otimes \mathscr{H}_E$, where $\mathscr{H}_A(\mathscr{H}_B,\mathscr{H}_E)$ is the Hilbert space of Alice's (Bob's, Eve's) system. After all the parties carry out their measurements, they obtain the probability distribution P_{ABE}. It should be add that Eve can carry out *generalized measurements*, i.e. measurements, in which the set $\{|z\rangle\}$ is not in general orthonormal basis but any set generating $\mathscr{H}_E$ and fulfilling the completeness condition $\sum_z |z\rangle\langle z| = \mathbb{1}_{\mathscr{H}_E}$. Henceforth, Alice's and Bob's partial distribution P_{AB} is analogical with the partial state $\rho_{AB} = \mathrm{Tr}_{\mathscr{H}_E}(P_\Psi)$ [65].

3.2 GIE As an Upper Bound on Secret Key Rate in CV QKD

As we now know, intrinsic information upper bounds secret key rate in classical SKA, from which we can rigorously pass to the quantum version of this protocol. Therefore, let us adopt intrinsic information in QKD [66, 67]. There, Alice and Bob share distributed bipartite quantum state ρ_{AB}. They perform measurements $\{\Pi_A\}$ and $\{\Pi_B\}$ over the corresponding subsystems to obtain a probability distribution P_{AB}. Eve may perform many different eavesdropping strategies, each of them carried out by measurements $\{\Pi_E\}$ and giving her a tripartite states ρ_{ABE}. Thus, each strategy extends the probability distribution P_{AB} to

$$P_{ABE} = \mathrm{Tr}\left(\Pi_A \otimes \Pi_B \otimes \Pi_E \rho_{ABE}\right). \tag{3.3}$$

This constitutes a set $\mathscr{P}$ of possible extensions.
Accordingly, the intrinsic information is defined as [66, 67]

$$I(A;B\downarrow E) = \inf_{\mathscr{P}} I(A;B|E), \tag{3.4}$$

where $I(A;B|E)$ is the classical conditional mutual information.

Now, we will show that GIE upper bounds the intrinsic information (3.4). To do so, we want the minimization of the classical conditional mutual information in Eq. (3.4) to be carried over measurements instead of the set $\mathscr{P}$. We can achieve this by rewriting the distributions (3.3) as follows.

Firstly, in Eq. (3.3) states ρ_{ABE} represent all possible extensions of $\rho_{AB} = \mathrm{Tr}_E\left(\rho_{ABE}\right)$. Every extension can be created by an action of a trace preserving completely-positive map $\mathscr{E}_E$ on Eve's part of a purification $|\Psi\rangle_{ABE}$ of the state $\rho_{AB} = \mathrm{Tr}_E\left(|\Psi\rangle_{ABE}\langle\Psi|\right)$, i.e., $\rho_{ABE} = \left(\mathbb{1}_{AB}\otimes\mathscr{E}_E\right)\left(|\Psi\rangle_{ABE}\langle\Psi|\right)$. Thus we can rewrite Eq.(3.3) as

$$P_{ABE} = \mathrm{Tr}\left[\Pi_A \otimes \Pi_B \otimes \Pi_E \mathscr{E}_E\left(|\Psi\rangle_{ABE}\langle\Psi|\right)\right]. \tag{3.5}$$

Secondly, we want to get rid of the map $\mathscr{E}_E$ in (3.5). Here, we will use the fact, that to every map $\mathscr{E}$, there exists a dual map $\mathscr{E}^*$ defined by the relation $\mathrm{Tr}[A\mathscr{E}(B)] = \mathrm{Tr}[\mathscr{E}^*(A)B]$ and thus $\mathrm{Tr}[\Pi_E\mathscr{E}\left(|\Psi\rangle_{ABE}\langle\Psi|\right)] = \mathrm{Tr}[\mathscr{E}^*_E(\Pi_E)\,|\Psi\rangle_{ABE}\langle\Psi|]$.
Due to the unitality (i.e. a property preserving the completeness relation) of the dual map $\mathscr{E}^*$, its acting on the measurement Π_E generates new measurements on subsystem E $\Pi^*_E := \mathscr{E}^*_E(\Pi_E)$. Finally, we can rewrite Eq. (3.5) as

$$P_{ABE} = \mathrm{Tr}\left(\Pi_A \otimes \Pi_B \otimes \Pi^*_E\,|\Psi\rangle_{ABE}\langle\Psi|\right). \tag{3.6}$$

It should be added that the measurements $\{\Pi_A\}$ and $\{\Pi_B\}$, and an arbitrary fixed purification $|\Psi\rangle_{ABE}$ in the previous equations are Gaussian.

Finally, we can prove that GIE upper bounds intrinsic information by the following sequence of equations and inequalities:

$$\begin{aligned} I(A;B\downarrow E) &= \inf_{\{\Pi^*_E\}} I(A;B|E) \\ &\leq \inf_{\Gamma_E} I_M(A:B|E)_{\gamma_{ABE}+\Gamma_E\oplus\Gamma_B\oplus\Gamma_E} \\ &\leq \sup_{\Gamma_A,\Gamma_B}\inf_{\Gamma_E} I_M\left(A:B|E\right)_{\gamma_{ABE}+\Gamma_A\oplus\Gamma_B\oplus\Gamma_E} = E^G_\downarrow(\gamma_{AB}). \end{aligned} \tag{3.7}$$

The first equality follows from employing the representation of the distribution P_{ABE} (3.6) and the minimization over measurements $\{\Pi^*_E\}$ is carried over all measurements on subsystem E, since the set of all measurements can be mapped onto itself by the

special case of $\mathscr{E}_E$ (resp. its dual map $\mathscr{E}_E^*$), which is an identity map.
The following inequality follows from the restriction to Gaussian measurements, which reduces the set, over which the minimization is carried, so the infimum must be always equal or greater. Further, the restriction reduces the conditional mutual information to the log-determinant form (2.16).
The second inequality follows from maximization the the infimum over the set of all Gaussian measurements on subsystems A and B. The resulting expression is nothing else but the definition of GIE (2.15).

Here we showed that GIE upper bounds intrinsic information and thus also secret key rate in any Gaussian CV QKD protocol, which gives it a significant meaning in these protocols.
In the following section, we will introduce specific CV QKD protocols with their lower bounds on the secret key rate published in [12], so we can compare them to the GIE results for these protocols in the last section of this chapter and thus verify the claim introduced here for specific examples.

3.3 Particular CV QKD Protocols and Their Secret Key Rates

So far, we have discussed CV QKD in rather mathematical terms to introduce the quantities related to these protocols. Now, let us move to a less abstract explanation and show some specific CV QKD protocols. To do so, we will simply outline the principle of protocols, in which entanglement is not needed [12], to understand the idea of a generation of the secret key between Alice and Bob.

Squeezed States Protocol

In this protocol, Alice can either prepare a x-squeezed vacuum state and encode a random Gaussian-distributed variable a into the x-displacement applied to the squeezed vacuum state ($d : (0{,}0) \rightarrow (a{,}0)$), or prepare a p-squeezed vacuum state and encode the variable a into the p-displacement ($d : (0{,}0) \rightarrow (0{,}a)$). This is shown in Fig. 3.2.

She randomly chooses between squeezing and displacing in x and p and sends these states to Bob.
Bob does not know, which states he receives, so he randomly chooses to measure either x or p. Bob's measurement is carried out by balanced homodyne detection.
After Bob has measured all the pulses, Alice announces whether she displaced x or p in each round. Bob keeps only the cases, in which they have agreed on the same quadrature.
Now, they share a string of random variables a.
To find out, whether their communication was eavesdropped by a third party, they apply a reconciliation protocol [68]. This is done via classical communication, in which they publish a part of their secret key. The reconciliation can be *direct* (the classical communication is done in the same direction as the quantum communication) or *reverse* (the classical communication is done in the opposite direction as the quantum communication). Based on the amount of found errors, they decide whether the com-

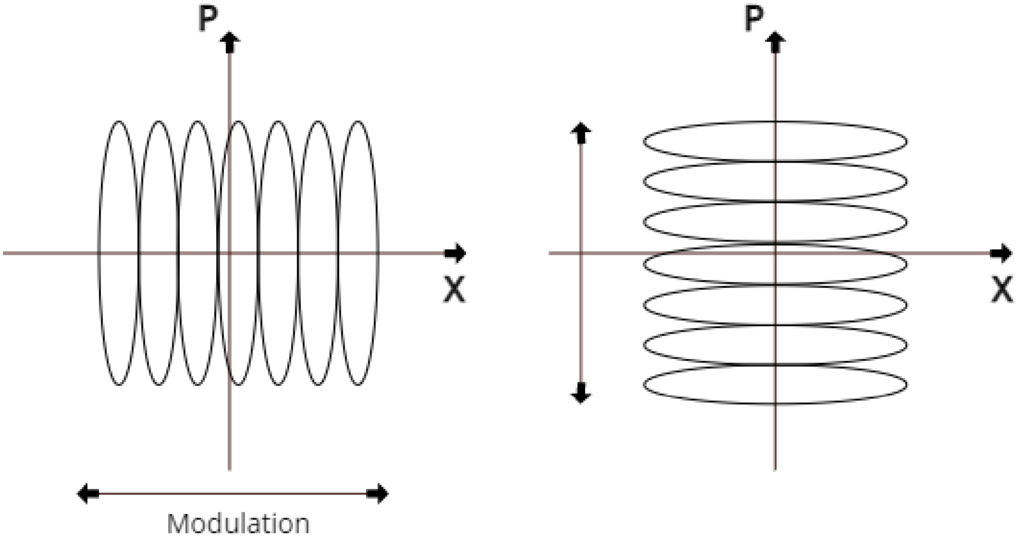

Figure 3.2: x-squeezed states displaced along x and p-squeezed states displaced along p.

munication was secure.

Coherent States Protocol

In coherent states protocol, Alice encodes a random bi-variate Gaussian-distributed variable (a_x,a_p) into the (x,p)-displacement applied to the vacuum. She sends the generated coherent state centred in $d = (a_x,a_p)$ to Bob (Fig. 3.3).
Bob randomly chooses to measure either x or p.

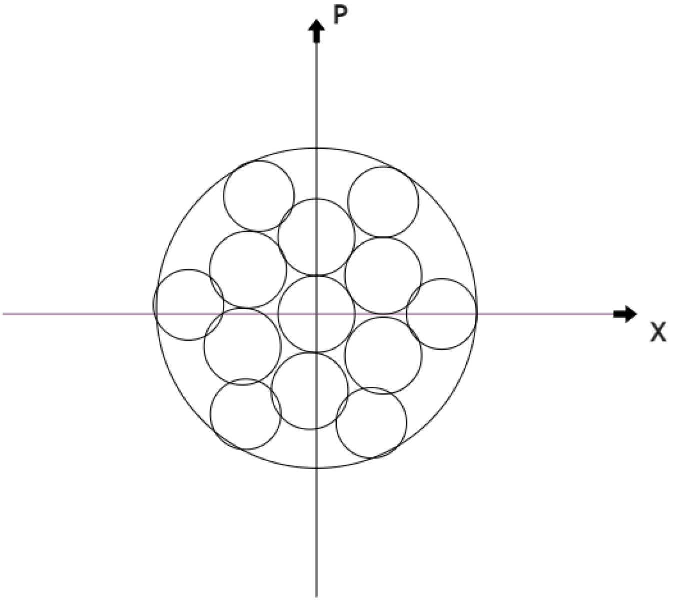

Figure 3.3: Alice's generated coherent states with random mean value (a_x,a_p).

After measuring all the pulses, Bob discloses, whether he measured x or p and Alice keeps only a_x or a_p in accordance with the Bob's measurement. Finally, they apply the reconciliation protocol.

Entanglement Based Protocols

The previous protocols are strictly equivalent to entanglement-based scheme, in which Alice generates an entangled EPR state and sends the mode B to Bob through a quantum channel. Then, she carries out a measurement on her mode A in order to project Bob's mode B to the respective state.
The case, in which Alice applies homodyne measurement over her mode A corresponds to the squeezes states protocol. On the other hand, if she applies heterodyne measurement, it corresponds to the coherent states protocol.
Moreover, Bob can also choose between homodyne and heterodyne detection (Fig. 3.4).

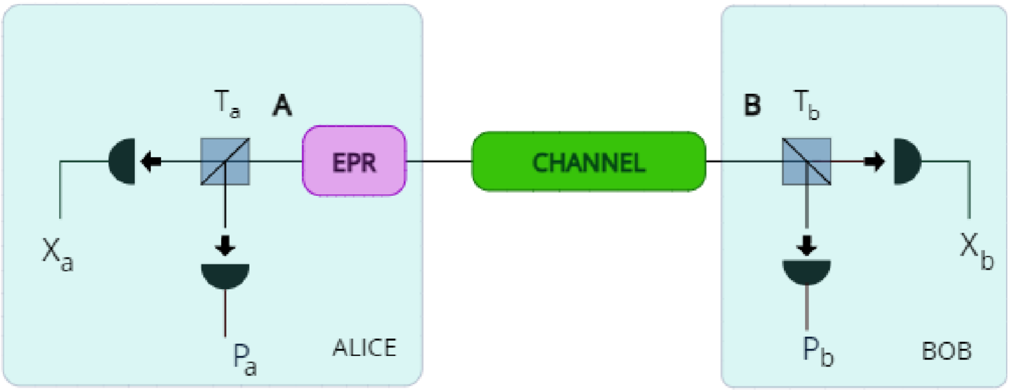

Figure 3.4: Entanglement-based scheme: For beam-splitter transmittance $T_a = 1$ ($T_a = 1/2$) Alice generates squeezed (coherent) states. Transmittance $T_b = 1$ ($T_b = 1/2$) corresponds to homodyne (heterodyne) measurement on Bob's side.

Thus, we have four different CV QKD entanglement-based protocols.

In the following protocols, the EPR state prepared by Alice is the two-mode squeezed vacuum state (2.12) with variance μ and the quantum channel through which the mode B is sent is an insecure phase-insensitive Gaussian channel $\mathscr{C}$ [64] with transmissivity parameter T and added noise ε. This forms a shared two-mode Gaussian state $\rho^{\mu}_{\mathscr{C}}$ with CM $\gamma^{\mu}_{\mathscr{C}}$.
For this state we computed GIE and compared the results with derived lower bounds on the secret key rate for all four protocols published in [12]. There, the bounds were derived in the restriction to one-way reconciliation and individual attacks. In the restriction to the individual attacks, Eve interacts individually with each Alice's pulse and she stores each ancilla in quantum memory [69]. She performs an individual measurement on each ancilla right after Alice and Bob announce, whether they measured quadrature x or p in each round.
We denote the lower bounds of the secret key rate K_{DR} in the case of direct reconciliation and K_{RR} for the reverse reconciliation. As it is usually done for the simplicity, we will refer to these bounds as to secret key rates in the rest of this chapter, even though we will mind that they only bound the actual secret key rate (3.2) from below.

3.3.1 Squeezed States and Homodyne Detection

The protocol with squeezed states and homodyne detection [15] can be equivalently replaced by entanglement-based protocol, where Alice and Bob share EPR state and they both apply homodyne measurements over their modes A and B (Fig. 3.5). The secret key rates K were derived in the restriction to individual attacks and one-way reconciliation in [71, 12]. For the direct reconciliation, the secret key rate K_{DR} reads as

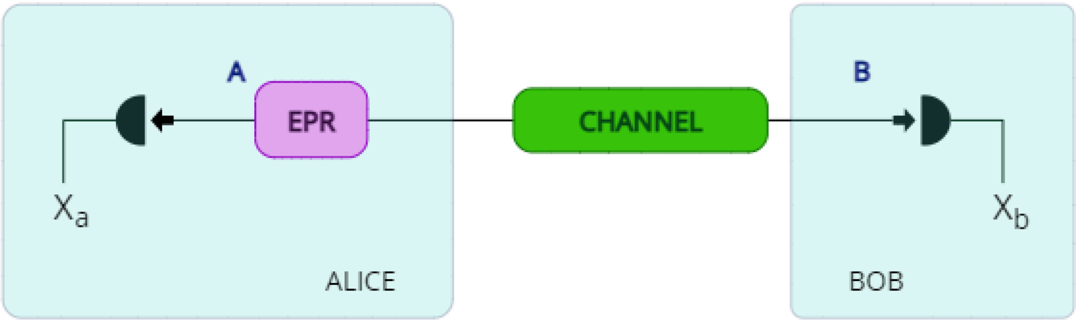

Figure 3.5: Entanglement based scheme of the protocol based on Alice sending squeezed states and Bob applying homodyne detection.

$$K_{DR} = \log\left[\frac{V+\chi}{V\chi+1}\right] \tag{3.8}$$

with $\chi = \frac{1-T}{T} + \varepsilon$, where T is the transmissivity parameter of the channel and ε is the excess noise. Further, V is the variance of a thermal state and log is a base 2 logarithm. In the case of reverse reconciliation, the secret key rate K_{RR} is

$$K_{RR} = \log\left[\frac{1}{T\left(\chi+1/V\right)}\right]. \tag{3.9}$$

Considering infinite squeezing $r \to \infty$ ($V = \cosh(2r) \to \infty$), the previous equations reduce to

$$K_{DR} = \log\left[\frac{V + \frac{1-T}{T} + \varepsilon}{V\left(\frac{1-T}{T} + \varepsilon\right) + 1}\right] \xrightarrow[r\to\infty]{} \log\left[\frac{T}{1+T\left(\varepsilon-1\right)}\right] \tag{3.10}$$

and

$$K_{RR} = \log\left[\frac{1}{T\left(\frac{1-T}{T} + \varepsilon + \frac{1}{V}\right)}\right] \xrightarrow[r\to\infty]{} \log\left[\frac{1}{1+T\left(\varepsilon-1\right)}\right]. \tag{3.11}$$

For the cases without any excess noise ($\varepsilon = 0$), the equations (3.10) and (3.11) simplify to

$$K_{DR} \overset{\varepsilon=0}{=} \log\left(\frac{T}{1-T}\right) \tag{3.12}$$

and

$$K_{RR} \overset{\varepsilon=0}{=} \log\left(\frac{1}{1-T}\right). \tag{3.13}$$

Since the transmittance is always $T \leq 1$, it can be readily seen that $K_{RR} \geq K_{DR}$ always applies for this protocol.

3.3.2 Coherent States and Homodyne Detection

The protocol, in which Alice prepares coherent states and Bob performs homodyne measurement [13] is equivalent to the entanglement-based protocol, in which the heterodyne measurement is carried out over Alice's mode A and Bob applies homodyne measurement over his mode B (Fig. 3.6).

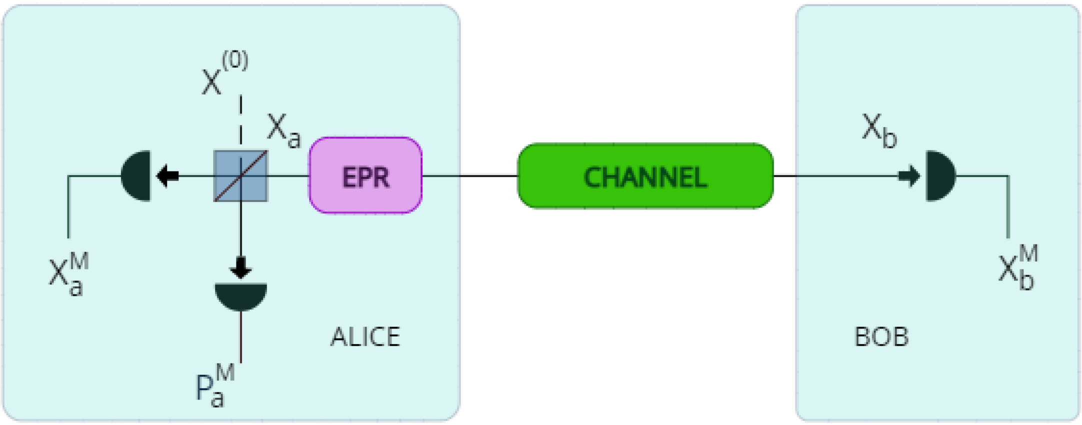

Figure 3.6: Entanglement based scheme of the protocol based on Alice sending coherent states and Bob applying homodyne detection.

The secret key rates for direct reconciliation and reverse reconciliation read as [12]

$$K_{DR} = \frac{1}{2}\log\left[\frac{V+\chi}{V\chi+1}\right] \tag{3.14}$$

and

$$K_{RR} = \frac{1}{2}\log\left[\frac{1}{T^2\left(\chi+1/V\right)\left(\chi+1\right)}\right]. \tag{3.15}$$

Applying the infinite squeezing $r \to \infty$ as in the previous protocol, we get

$$K_{DR} = \frac{1}{2}\log\left[\frac{T}{1+T\left(\varepsilon-1\right)}\right] \tag{3.16}$$

and

$$K_{RR} = \frac{1}{2}\log\left\{\frac{1}{\left[1+T\left(\varepsilon-1\right)\right]\left(1+\varepsilon T\right)}\right\}. \tag{3.17}$$

For zero noise $\varepsilon = 0$, the secret key rates simplify to

$$K_{DR} \overset{\varepsilon=0}{=} \frac{1}{2}\log\left(\frac{T}{1-T}\right) \tag{3.18}$$

and

$$K_{RR} \overset{\varepsilon=0}{=} \frac{1}{2}\log\left(\frac{1}{1-T}\right). \tag{3.19}$$

One can see that in the absence of the excess noise ε, $K_{RR} \geq K_{DR}$ applies again. Moreover, it can be readily seen that by comparing the equations (3.18) and (3.19) with secret key rates (3.12) and (3.13) in the previous protocol with homodyne detection on both modes, one finds that in the absence of excess noise, the secret key rates for the individual reconciliations are smaller for the protocol with heterodyne detection on the Alice's side and homodyne detection on the Bob's side. Specifically speaking, they are half.

3.3.3 Squeezed States and Heterodyne Detection

This protocol is equivalent to an entanglement-based protocol, in which Alice carries out an homodyne measurement over mode A and Bob applies heterodyne measurements over mode B (Fig. 3.7).
Then, the secret key rates are [12]

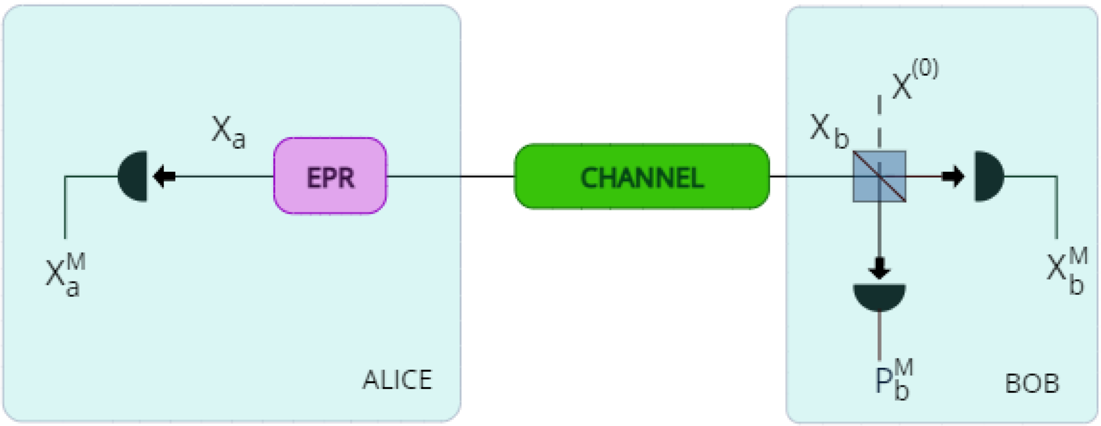

Figure 3.7: Entanglement based scheme of the protocol based on Alice sending squeezed states and Bob applying heterodyne detection.

$$K_{DR} = \frac{1}{2}\log\left\{\frac{(V+\chi)[T(V+\chi)+1]}{(V\chi+1)[T(V\chi+1)+V]}\right\} \tag{3.20}$$

and

$$K_{RR} = \frac{1}{2}\log\left[\frac{1}{T(\chi+1/V)}\right]. \tag{3.21}$$

In the restriction to infinite squeezing, one gets

$$K_{DR} = \frac{1}{2}\log\left\{\frac{T^2}{[1+T(\varepsilon-1)][2+T(\varepsilon-1)]}\right\} \tag{3.22}$$

and

$$K_{RR} = \frac{1}{2}\log\left[\frac{1}{1+T(\varepsilon-1)}\right]. \tag{3.23}$$

Once again, we will also show the results for $\varepsilon = 0$, which are

$$K_{DR} \overset{\varepsilon=0}{=} \frac{1}{2}\log\left[\frac{T^2}{(1-T)(2-T)}\right] \tag{3.24}$$

and

$$K_{RR} \overset{\varepsilon=0}{=} \frac{1}{2}\log\left(\frac{1}{1-T}\right). \tag{3.25}$$

Comparing the equations (3.24) and (3.25), after some simple algebra, one can find that $K_{RR} \geq K_{DR}$ in the absence of the excess noise.

Further, K_{DR} is always larger in comparison to the result in the previous protocol (coherent states and homodyne detection), whilst the results of K_{RR} are in the absnce of noise equal.
Finally, comparing the results with the first protocol (squeezed states and homodyne detection), both secret key rates are larger than the results that we obtained in this section.

3.3.4 Coherent States and Heterodyne Detection

The last protocol is the protocol based on coherent states and heterodyne detection [14], which is equivalent to the protocol with shared entangled EPR state, where both modes A and B are measured by heterodyne detection (Fig. 3.8). The secret key rates for this protocol are [12]

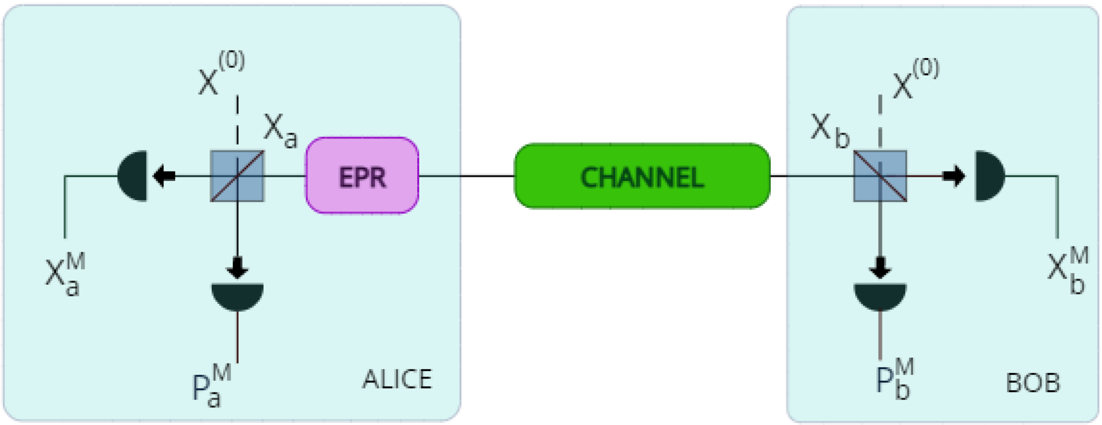

Figure 3.8: Entanglement based scheme of the protocol based on Alice sending coherent states and Bob applying heterodyne detection.

$$K_{DR} = \log\left\{\frac{(\chi+1)[T(V+\chi)+1]}{(V\chi+1)[T(\chi+1)+1]}\right\} \tag{3.26}$$

and

$$K_{RR} = \log\left\{\frac{T(V\chi+1)+V}{T(V\chi+1)[T(\chi+1)+1]}\right\}. \tag{3.27}$$

Using the same method as in all the previous protocols, we obtain for $r \to \infty$

$$K_{DR} = \log\left\{\frac{T(1+\varepsilon T)}{[1+T(\varepsilon-1)](2+\varepsilon T)}\right\} \tag{3.28}$$

and

$$K_{RR} = \log\left\{\frac{2+T(\varepsilon-1)}{[1+T(\varepsilon-1)](2+\varepsilon T)}\right\}. \tag{3.29}$$

Finally, in the absence of the excess noise, the secret key rates reduce to

$$K_{DR} \overset{\varepsilon=0}{=} \log\left[\frac{T}{2(1-T)}\right] \tag{3.30}$$

and

$$K_{RR} \overset{\varepsilon=0}{=} \log\left[1+\frac{T}{2(1-T)}\right]. \tag{3.31}$$

It is clear that for $\varepsilon = 0$ the inequality $K_{RR} \geq K_{DR}$ applies once again and so we can conclude that it does in all the considered protocols.

3.4 Gaussian Channels

As we already outlined, in the previous protocols, Alice and Bob share two-mode Gaussian state $\rho^{\mu}_{\mathscr{C}}$ with CM $\gamma^{\mu}_{\mathscr{C}}$, which is established by sending one of the modes of the two-mode squeezed vacuum state (2.12) with variance μ prepared by Alice through an insecure phase-insensitive Gaussian channel $\mathscr{C}$. In this section, we will denote the transmittance of the channel $\mathscr{C}$ by τ and the added noise by ν.

In general, quantum channels are completely positive (CP) trace-preserving maps, which is a class of irreversible operations transforming N-mode CM as

$$\gamma_{out} = X\gamma_{in}X^{\mathrm{T}} + Y, \tag{3.32}$$

where X and Y are $2N \times 2N$ matrices and Y is symmetric [72].
Further, they satisfy the positivity condition

$$Y + i\Omega - iX\Omega X^{\mathrm{T}} \geq 0. \tag{3.33}$$

The vector of first moments d transforms as

$$d_{out} = Xd_{in}. \tag{3.34}$$

Pure-Loss Channel

For the pure loss channel $\mathcal{L}_p$ with transmittance τ, the matrices in Eq. (3.32) are defined as $X = \sqrt{\tau}\mathbb{1}$ and $Y = (1-\tau)\mathbb{1}$. Such a channel can be constructed by a beam splitter with transmittance τ.

Thermal-Loss Channel

In the addition to the transmittance τ, the thermal-loss channel $\mathcal{L}$ is also defined by the added thermal noise ν. Hence, the CP map is defined by $X = \sqrt{\tau}\mathbb{1}$ and $Y = \nu\mathbb{1}$, with $\nu = (1-\tau)(2\overline{n}+1)$, where $\overline{n}$ is the mean number of the photons in the environment. It can be constructed by mixing the input signal with a thermal state of variance $V = \frac{\nu}{1-\tau}$ at the beam splitter with transmittance τ.

Thermal-Amplifier Channel

In the case of thermal-amplifier channel $\mathcal{A}$, we consider $\tau > 1$, so we call it an amplification parameter. Thus, it is defined by $X = \sqrt{\tau}$ and $Y = \nu\mathbb{1}$, with $\nu = (\tau-1)(2\overline{n}+$ $+\,1)$.
If there is no added thermal noise, i.e., $\overline{n} = 0$, the channel is called Pure-Amplifier Channel $\mathcal{A}_p$.

We can summarize these attainments and rewrite the Eq. (3.32) in the terms of parameters τ and ν. Hence, a two-mode Gaussian state with CM γ sent through such a single-mode Gaussian channel $\mathscr{C}$ transforms as

$$\gamma_{in} \xrightarrow{\mathscr{C}} \gamma_{out} = \left(\mathbb{1} \oplus \sqrt{\tau}\mathbb{1}\right)\gamma_{in}\left(\mathbb{1} \oplus \sqrt{\tau}\mathbb{1}\right)^{\mathrm{T}} + (0 \oplus \nu\mathbb{1}), \tag{3.35}$$

where $\nu = |1-\tau|(2\overline{n}+1)$ with $0 < \tau < 1$ for lossy channels and $\tau > 1$ for amplifying channels.

3.5 GIE as an Upper Bound on Secret Key Rate in Particular CV QKD Protocols

Now, we want to know formulas of GIE for the states $\rho^{\mu}_{\mathscr{C}}$ in the cases of particular channels.
If $\nu \geq 1+|\tau|$, the channel is an entanglement breaking channel, entanglement vanishes and thus $E^{G}_{\downarrow} = 0$.
Otherwise, GIE of the state $\rho^{\mu}_{\mathscr{C}}$ with CM $\gamma^{\mu}_{\mathscr{C}}$ is [50]

$$E^{G}_{\downarrow}(\gamma^{\mu}_{\mathscr{C}}) = \ln[\cosh(2r_0)], \tag{3.36}$$

where r_0 represents the minimum two-mode squeezing [73] needed for establishing $\rho^{\mu}_{\mathscr{C}}$. When a single mode of TMSV is sent by a channel $\mathscr{C}$, r_0 is given by

$$\begin{aligned} r_0 =& \frac{1}{4}\ln\frac{1}{2\left[\nu - 2\sqrt{\tau}\sinh(2r) + (1+\tau)\cosh(2r)\right]^2} \\ &\times \{3 + [2\nu - (1-\tau)^2]\cosh(4r) + \tau(3\tau+2) + 4\nu(1+\tau)\cosh(2r) \\ &- 4\sqrt{\nu^2 - (1-\tau)^2}\sinh(2r)[\nu\cosh(2r) + 1 + \tau]\}. \end{aligned} \tag{3.37}$$

In the case of the infinite squeezing $r \to \infty$ ($\Upsilon = \tanh r \to 1$ in (2.13)), we refer to the state of a Gaussian channel as the so-called *Choi state* $\rho_{\mathscr{C}} := \lim_{\mu\to\infty}\rho^{\mu}_{\mathscr{C}}$. In this limit we have

$$\begin{aligned} \tau \neq 1 \implies r_0^{\text{Choi}} &= \frac{1}{4}\ln\frac{2\nu\left[\nu - \sqrt{\nu^2-(1-\tau)^2}\right] - (1-\tau)^2}{(1-\sqrt{\tau})^4}, \\ \tau = 1 \implies r_0^{\text{Choi}} &= \frac{1}{4}\ln\frac{4}{\nu^2}. \end{aligned} \tag{3.38}$$

Hence, substituting the fist equation of (3.38) into the Eq. (3.36), GIE for a Choi state of thermal-loss (thermal-amplifier channel) is

$$E^{G}_{\downarrow}(\gamma_{\mathcal{L},\mathcal{A}}) = \ln\left[\frac{(2\overline{n}+1)(\tau+1) - 4\sqrt{\tau\overline{n}(\overline{n}+1)}}{|\tau-1|}\right]. \tag{3.39}$$

For pure-loss channel and pure-amplifier channel with $\overline{n} = 0$ it reduces to

$$E^{G}_{\downarrow}(\gamma_{\mathcal{L}_p,\mathcal{A}_p}) = \ln\left(\frac{\tau+1}{|\tau-1|}\right). \tag{3.40}$$

Now, we want to compare GIE to the secret key rates derived in the Section 3. To do so, we will translate the formula of GIE (3.39) into the corresponding variables, i.e., $\tau \longleftrightarrow T$ and $\nu = (1-\tau)(2\overline{n}+1) \longleftrightarrow T\chi$. For the thermal-loss channel with $0 < T < 1$ the Eq. (3.39) reads in these variables as

$$E^{G}_{\downarrow}(\gamma_{\mathcal{L}}) = \ln\left\{\frac{\left(1+\frac{T\varepsilon}{1-T}\right)(T+1) - 2\sqrt{T\left[\left(1+\frac{T\varepsilon}{1-T}\right)^2 - 1\right]}}{1-T}\right\}. \tag{3.41}$$

Using straightforward algebra, which we supported by verification in mathematical software, we can conclude that formula (3.41) is larger than secret key rates for both types of reconciliation in all four CV QKD protocols in Section 3 up to the irrelevant choice of the logarithm base, as expected.

This verifies the proof (3.7) on particular four CV QKD protocols against individual attacks from Section 3 with thermal-loss channel in the limit of infinite squeezing.

Chapter 4

GIE as an Upper Bound on Channel Capacity

Besides upper bounding the secret key rate, another cryptographical significance of GIE has been found. In the case of the pure-loss channel $\mathcal{L}_p$ and the pure-amplifier channel $\mathcal{A}_p$, the formula (3.40) is equal to the secret key rate capacity of the channel derived from squashed entanglement (1.10) [17]. This motivates the investigation, whether it is an upper bound on the capacity of other channels and also the question, whether it can be claimed in general. Unfortunately, the general proof requires monotonicity under LOCC, whilst GIE provides this only in the restriction to Gaussian local operations, so the general method cannot be applied [16].
Hence, in the first section, we will introduce the secret key rate capacity of the channel and in the second section, we will compare GIE with already known bounds on it.

4.1 Channel Capacity

To define the secret key capacity of the channel, we will borrow the notation from [16].
Here, the definition applies to the adaptive protocol for quantum or private communication over an arbitrary quantum channel $\mathscr{C}$. Alice and Bob have local registers **a** and **b**, each with a countable number of systems. They apply and adaptive LOCC Λ_0 to their registers and, which prepares and initial state $\rho^0_{\mathbf{ab}}$.
In the first round, Alice picks a system a_1 from her register **a** and sends it through the channel $\mathscr{C}$. Bob receives the output system b_1 and includes it into his register, which changes his register $b_1\mathbf{b} \to \mathbf{b}$. Then they apply another adaptive LOCC Λ_1 onto their registers, which generates the state $\rho^1_{\mathbf{ab}}$.
They can apply this procedure for n rounds, resulting in n uses of the channel $\mathscr{C}$ and a sequence of adaptive LOCCs $\mathcal{P}\{\lambda_0,...,\Lambda_n\}$. The sequence $\mathcal{P}$ characterizes the protocol and provides the output state $\rho^n_{\mathbf{ab}}$. The output state is epsilon-close to some ideal target state ϕ^n, with nR_n bits, where R_n represents the number of bits per channel use, i.e., $\|\rho^n_{\mathbf{ab}} - \phi_n\| \leq \varepsilon$ in the trace norm.
Hence, the generic two-way capacity is defined as

$$\mathcal{C}(\mathscr{C}) := \sup_{\mathcal{P}} \lim_{n} R_n, \tag{4.1}$$

which defines the capacity as the highest R_n at which a shared key can be reliably and securely generated using the channel many times in conjunction with unlimited two-way classical communication over an authenticated public channel [17].

Now, if the target state ϕ_n is maximally-entangled state, capacity $\mathcal{C}$ (4.1) is the two-way entanglement-distribution capacity D_2. Further, with two-way classical communication, the D_2 is equal to the quantum capacity Q_2.
In the case of ϕ_n being a private state [74], then $\mathcal{C}$ is the secret key capacity K, which is also equal to the capacity of protocol with private transmission of classical bits, i. e. so called two-way private capacity P_2.
To summarize this, we can say that inequality

$$Q_2 = D_2 \leq K = P_2 \tag{4.2}$$

applies for the the particular types of capacity.

It has been shown the the capacity P_2 (and therefore all the other capacities in (4.2)) can be bounded from above using some known entanglement measures.
In the following section, we will focus on the upper bounds derived from squashed entanglement (1.10) [17] and the best known upper bounds derived from relative entropy of entanglement (1.14) [18] and compare them with GIE.

4.2 Comparison of GIE with Known Upper Bounds on Channel Capacity

As mentioned above, the formula of GIE (3.40) for the pure-loss channel $\mathcal{L}_p$ and the pure-amplifier channel $\mathcal{A}_p$ coincides with the upper bound on the secret key rate capacity derived from squashed entanglement [17] up to the irrelevant choice of the base of the logarithm, which we will choose to be natural.
We will continue the investigation for thermal-loss channel $\mathcal{L}$ (thermal-amplifier channel $\mathcal{A}$), which is for the Choi state defined by Eq. (3.39), whereas the upper bound derived from squashed entanglement reads as [70]

$$E_{sq_{\mathcal{L}}}(\tau,\overline{n}) = \ln\left[\frac{(1-\tau)\overline{n}+1+\tau}{(1-\tau)\overline{n}+1-\tau}\right]. \tag{4.3}$$

To compare the Eq. (3.39) and Eq. (4.3), we will use the noise parametrized in accordance with the thermal noise (2.14) $\overline{n} = \sinh^2(r)$ and rewrite the equations in terms of $x = \tanh(r)$, which corresponds to substituting

$$\overline{n} = \frac{x^2}{1-x^2}, \quad \overline{n}+1 = \frac{1}{1-x^2}, \quad 2\overline{n}+1 = \frac{1+x^2}{1-x^2}, \tag{4.4}$$

and $z = \sqrt{\tau}$. In terms of variables x and z, the thermal-loss channel $\mathcal{L}$ corresponds to the cases with $0 < z < 1$ and $x < z$, and the thermal-amplifier channel corresponds to the cases with $z > 1$ and $x < \frac{1}{2}$.
Using these substitutions one gets the formula (3.39) in the form of

$$E^G_{\downarrow}(\gamma_{\mathcal{L},\mathcal{A}}) = \ln\left[\frac{(1+x^2)(1+z^2)-4xz}{(1-x^2)|1-z^2|}\right] \tag{4.5}$$

and the formula (4.3) in the form of

$$E_{sq_{\mathcal{L}}}(z,x) = \ln\left(\frac{1+z^2-2x^2z^2}{1-z^2}\right). \tag{4.6}$$

Let us define the difference

$$\Delta_{\mathcal{L}}(z,x) := E_{sq_{\mathcal{L}}}(z,x) - E_{\downarrow}^{G}(\gamma_{\mathcal{L}}), \tag{4.7}$$

which is obviously expressed as

$$\Delta_{\mathcal{L}}(x,z) = \ln\left[\frac{(1-x^2)(1+z^2-2x^2z^2)}{(1+x^2)(1+z^2)-4xz}\right]. \tag{4.8}$$

One can readily see that the case with $x = 0$ corresponds to the pure-loss channel $\mathcal{L}_p$ and $\Delta_{\mathcal{L}}(z,0) = \ln(1) = 0$ as expected. As $0 < x < z < 1$ holds for the thermal-loss channel, it is correct to claim that

$$z < \frac{1}{x} \quad \wedge \quad z > \frac{x}{1-x^2} \tag{4.9}$$

holds as well.
If we subtract the denominator from the numerator in the fraction (4.8), i. e.,

$$\begin{aligned}&(1-x^2)(1+z^2-2x^2z^2) - [(1+x^2)(1+z^2)-4xz] \\ &\qquad = 2x^2(2-x^2)\left(\frac{1}{x}-z\right)\left(z-\frac{z}{2-x^2}\right) > 0,\end{aligned} \tag{4.10}$$

we will get a strictly positive result, which means that the argument of the logarithm in (4.8) is strictly larger than one and thus the difference $\Delta_{\mathcal{L}}(z,x)$ is strictly positive. Finally, getting back into the variables τ and $\overline{n}$ this results in the inequality

$$E_{sq_{\mathcal{L}}}(\tau,\overline{n}) \geq E_{\downarrow}^{G}(\gamma_{\mathcal{L}}). \tag{4.11}$$

We can apply the same principle onto the thermal-amplifier channel with $z > 1$ and $x < \frac{1}{z}$, since inequalities (4.9) hold again and thus

$$E_{sq_{\mathcal{A}}}(\tau,\overline{n}) \geq E_{\downarrow}^{G}(\gamma_{\mathcal{A}}). \tag{4.12}$$

Therefore, we can conclude that GIE is always equal or greater than the upper bound on the secret key rate capacity derived from squashed entanglement.

Next, we will compare GIE with the upper bounds based on the relative entropy of entanglement (1.14), which is the best known upper bound on the secret key rate capacity of the channel.
For the thermal-loss channel it is defined as [18]

$$E_{R_{\mathcal{L}}}(\tau,\overline{n}) = \begin{cases} -\ln\left[(1-\tau)\tau^{\overline{n}}\right] - h(\overline{n}) & \text{for} \quad \overline{n} < \frac{\tau}{1-\tau}, \\ 0 & \text{otherwise} \end{cases} \tag{4.13}$$

with $h(\overline{n}) = (\overline{n}+1)\ln(\overline{n}+1) - \overline{n}\ln\overline{n}$, and for the thermal-amplifier channel as

$$E_{R_{\mathcal{A}}}(\tau,\overline{n}) = \begin{cases} \ln\left(\frac{\tau^{\overline{n}+1}}{\tau-1}\right) - h(\overline{n}) & \text{for} \quad \overline{n} < \frac{1}{\tau-1}, \\ 0 & \text{otherwise.} \end{cases} \tag{4.14}$$

Substituting (4.4) and $\sqrt{\tau} = z$ into equations (4.13) and (4.14) we get

$$E_{R_{\mathcal{L}}}(z,x) = \begin{cases} -\ln\left[(1-z^2)z^{\left(\frac{2x^2}{1-x^2}\right)}\right] - h(x) & \text{for} \quad x < z, \\ 0 & \text{otherwise} \end{cases} \tag{4.15}$$

and

$$E_{R_{\mathcal{A}}}(z,x) = \begin{cases} \ln\left[\frac{z^{\left(\frac{2}{1-x^2}\right)}}{z^2-1}\right] - h(x) & \text{for} \quad x < \frac{1}{z}, \\ 0 & \text{otherwise} \end{cases} \tag{4.16}$$

with $h(x) = \frac{1}{1-x^2}\ln\frac{1}{1-x^2} - \frac{x^2}{1-x^2}\ln\frac{x^2}{1-x^2}$. Now, we want to compare GIE with the bounds (4.15) and (4.16).To do so, we will analyze the difference

$$\Xi_{\mathcal{L},\mathcal{A}}(z,x) := E_{\downarrow}^{G}(\gamma_{\mathcal{L},\mathcal{A}}) - E_{R_{\mathcal{L},\mathcal{A}}}(z,x), \tag{4.17}$$

which for the thermal-loss channel $\mathcal{L}$ reads as

$$\Xi_{\mathcal{L}}(z,x) = \ln\left[\frac{(1+x^2)(1+z^2)-4xz}{1-x^2}\right] + \frac{2x^2}{1-x^2}\ln z + h(x). \tag{4.18}$$

The difference $\Xi_{\mathcal{L}}(z,x)$ (4.17) is positive if it is bounded by zero from below. we can verify this by finding its minimum on the set characterized by the conditions for the thermal-loss channel, i.e., $0 < z < 1$ and $0 < x < z$. Since the set is an *open* triangle it may not have any minimum and thus we will investigate a larger *closed* set by including the boundaries of the considered triangle as well.

Firstly, we will try to find the stationary points in the z-direction, which correspond to the points fulfilling $\partial\Xi_{\mathcal{L}}/\partial z = 0$, i.e.,

$$\frac{\partial\Xi_{\mathcal{L}}}{\partial z} = \frac{2(1+x^2)(x-z)^2}{z(1-x^2)\left[(1+x^2)(1+z^2)-4xz\right]} = 0. \tag{4.19}$$

One can find that Eq. (4.19) has no solution for $0 < z < 1$ and $0 < x < z$ and therefore the difference (4.17) has no extreme in the interior of the triangle.

Thus, let us consider an open boundary line segment $x = 0$ and $0 < z < 1$. Here the Eq. (4.18) reduces to

$$\Xi_{\mathcal{L}}(z,0) = \ln\bigl(1+z^2\bigr), \tag{4.20}$$

which is obviously a monotonically increasing function with no extreme on the interval $0 < z < 1$.

Taking another open boundary line segment $z = 1$ and $0 < x < 1$, the difference (4.18) reduces to

$$\Xi_{\mathcal{L}}(1,x) = \ln\left[2\left(\frac{1-x}{1+x}\right)\right] + h(x). \tag{4.21}$$

Now, if we derive the Eq. (4.21) with respect to x, we will get

$$\frac{\mathrm{d}\Xi_{\mathcal{L}}}{\mathrm{d}x}(1,x) = \frac{2(x^2 - x\ln x^2 - 1)}{(1-x^2)^2} < 0, \tag{4.22}$$

where the inequality results from substituting $x = \sqrt{\frac{\bar{n}}{\bar{n}+1}}$ and use the *logarithmic-geometric mean inequality*:

$$\frac{b-a}{\ln b - \ln a} > \sqrt{ab} \quad \text{if} \quad 0 < a < b. \tag{4.23}$$

The function (4.22) is monotonically decreasing and therefore there is no extreme on the considered line segment.

The remaining open boundary line segment is the one defined with $x = z$ and $0 < z < 1$, for which the difference is $\Xi_{\mathcal{L}}(z,z) = 0$ and any point of the segment can be an extreme.

For the vertices of the triangle, one gets $\Xi_{\mathcal{L}}(0,0) = 0$ and $\Xi_{\mathcal{L}}(1,0) = \ln 2$.
Let us analyze the last vertex (1,1). Firstly, to see the behaviour of the function (4.17), we will analyze the line segments

$$z = q + (1-q)t, \quad x = t, \quad t \in [0,1] \tag{4.24}$$

starting at the point $(q,0)$ on the z-axis, $q \in [0,1]$, and end at the point (1,1), under the limit $t \to 1$. This is given by

$$L := \lim_{t\to 1} \Xi_{\mathcal{L}}[q + (1-q)t,t] = q + \ln\left[\frac{1}{2}(2 - 2q + q^2)\right]. \tag{4.25}$$

Therefore, $L \in [0,1 - \ln 2$, which implies that the least limit of the function (4.17) at the point (1,1) is zero.
Summarizing the previous claims, we can conclude that on the considered closed triangle always applies $\Xi_{\mathcal{L}}(z,x) \geq 0$ and the equality holds only on the segment with $x = 0$ and $0 < z < 1$. Further, the strict inequality $\Xi_{\mathcal{L}}(z,x) > 0$ holds on the original open triangle together with the line segment $x = 0, 0 < z < 1$, which corresponds to the pure-loss channel $\mathcal{L}_p$. For entanglement breaking channels quantities GIE (3.39) and relative entropy of entanglement (4.13) naturally vanish. Consequently, one finds that for thermal-loss channel, GIE is never less than the upper bound on the channel capacity derived from relative entropy of entanglement, i.e.,

$$E^G_{\downarrow}(\gamma_{\mathcal{L}}) \geq E_{R_{\mathcal{L}}}(\tau,\overline{n}). \tag{4.26}$$

Moving to the thermal-amplifier channel $\mathcal{A}$, Eq. (4.17) gives

$$\Xi_{\mathcal{A}}(z,x) = \ln\left[\frac{(1+x^2)(1+z^2) - 4xz}{(1-x^2)}\right] - \frac{2}{1-x^2}\ln z + h(x) \tag{4.27}$$

and the open set is characterized by the conditions for $\mathcal{A}$, i.e., $z > 1$ and $x < \frac{1}{z}$, on which we want to proof the function (4.27) to be lower bounded by zero.
Once again, we will work with a larger set, which is defined by the same inequalities but not strict, to include the boundary lines as well.
Firstly, the derivative of (4.27) with the respect to z is

$$\frac{\partial \Xi_{\mathcal{A}}}{\partial z} = \frac{2(1+x^2)(xz-1)^2}{z(1-x^2)[(1+x^2)(1+z^2) - 4xz]}, \tag{4.28}$$

which set equal to zero no solution due to the inequality $xz < 1$.
Considering the first boundary segment $x = 0$ and $z < 1$, the difference (4.27) reduces to

$$\Xi_{\mathcal{A}}(z,0) = \ln\left(1 + \frac{1}{z^2}\right), \tag{4.29}$$

which is obviously monotonically decreasing function and thus it does not have any extreme for $z < 1$.
As the second boundary segment, we will take the one defined with $z = 1$ and $0 < x < 1$ and which gives the same result as in the case of the thermal-loss channel, i.e.,

$$\Xi_{\mathcal{A}}(1,x) = \Xi_{\mathcal{L}}(1,x), \tag{4.30}$$

so we can immediately say that there is not any extreme either.
Taking the last boundary segment $x = \frac{1}{z}$ and $z > 1$ gives the difference equal to zero

$$\Xi_{\mathcal{A}}\left(z,\frac{1}{z}\right) = 0 \tag{4.31}$$

and any point of the curve can be an extreme.
Finally, we will investigate the vertices of the set. The first one gives $\Xi\_\mathcal{A}(1,0) = \ln 2$. In the infinitely distant vertex of the z-axis we get

$$\lim_{z\to+\infty} \Xi_{\mathcal{A}}(z,0) = 0, \quad \lim_{z\to+\infty} \Xi_{\mathcal{A}}\left(z,\frac{1}{z}\right) = 0, \tag{4.32}$$

so one can see that the function (4.27) vanishes there.
The last vertex is the point (1,1). To analyze it, we calculate the limits of the function along the segments of the lines starting in the point $(q,0)$ on the z-axis, $q \in [1,2]$, and ending at the point (1,1),

$$L' := \lim_{t\to1} \Xi_{\mathcal{A}}[q+(1-q)t,t] = 2 - q + \ln\left[\frac{1}{2}(2-2q+q^2)\right]. \tag{4.33}$$

Here we can see that for $q \in [1,2]$ one gets $L' \in [1-\ln 2,0]$ and thus the least limit of the function at the point (1,1) is equal to zero, which we wanted to proof.
In conclusion, we can see that for the thermal-amplifier channel we get $\Xi_{\mathcal{A}}(z,x) \geq 0$, where the equality holds only for $x = \frac{1}{z}$ and $z \geq 1$. This implies that the strict inequality $\Xi_{\mathcal{A}}(z,x) > 0$ holds on the original open set and the segment $x = 0$, $z > 1$ corresponding to the pure-amplifier channel $\mathcal{A}_p$. For entanglement-breaking channels the investigated quantities always vanish.
Therefore, we can conclude that for the thermal-amplifier channel GIE (3.39) is never less than the bound based on the relative entropy of entanglement (4.14), i.e.,

$$E_{\downarrow}^{G}(\gamma_{\mathcal{A}}) \geq E_{R_{\mathcal{A}}}(\tau,\overline{n}). \tag{4.34}$$

Here showed that the upper bound on the secret key rate capacity of the channel based on the relative entropy of entanglement is always larger than GIE of the Choi state of the channel for all four investigated channels $(\mathcal{L},\mathcal{A},\mathcal{L}_p,\mathcal{A}_p)$.

Finally, we will investigate the upper bounds for another type of a channel, which is so-called *additive-noise Gaussian channel* characterized by the variance of the added noise $\xi \geq 0$ and the channel is entanglement breaking if $\xi \geq 1$.
If $\xi < 1$, GIE of a Choi state of the channel is defined by Eq. (3.36) [50] with $r_0 = -\ln\sqrt{\xi}$ [73], while it vanishes otherwise, i.e.,

$$E_{\downarrow}^{G}(\gamma_{\text{add}}) = \begin{cases} \ln\left(\frac{1+\xi^2}{2\xi}\right) & \text{for} \quad \xi < 1, \\ 0 & \text{otherwise.} \end{cases} \tag{4.35}$$

The bound derived from the relative entropy of entanglement reads as [18]

$$E_{R_{\text{add}}} = \begin{cases} \xi - 1 - \ln\xi & \text{for} \quad \xi < 1, \\ 0 & \text{otherwise.} \end{cases} \tag{4.36}$$

After substituting into the difference

$$\Xi_{\text{add}}(\xi) := E_{\downarrow}^{G}(\gamma_{\text{add}}) - E_{R_{\text{add}}}(\xi) \tag{4.37}$$

from the equations (4.35) and (4.36) we get

$$\Xi_{\text{add}}(\xi) = \begin{cases} (1-\xi)\left[1 - \frac{1+\xi}{\sqrt{2(1+\xi^2)}}\right] & \text{for} \quad \xi < 1, \\ 0 & \text{otherwise.} \end{cases} \tag{4.38}$$

It is readily seen that $1-\xi > 0$ and $\xi + 1 < \sqrt{2(1+\xi^2)}$ and thus the difference (4.38) is strictly positive for $\xi < 1$. Considering also the entanglement-breaking channels, we can conclude that the inequality

$$E_{\downarrow}^{G}(\gamma_{\text{add}}) \geq E_{R_{\text{add}}}(\xi) \tag{4.39}$$

holds for the additive-noise Gaussian channel as well.

Finally, we compare the bound based on GIE (4.35), the bound based on relative entropy of entanglement (4.36) and the one derived from squashed entanglement [70]

$$E_{sq_{\text{add}}}(\xi) = \begin{cases} \ln\left(\frac{2+\xi}{\xi}\right) & \text{for} \quad \xi < 1, \\ 0 & \text{otherwise} \end{cases} \tag{4.40}$$

in Fig(4.1).

Based on all the results of this section, we can conclude that the GIE of a Choi state upper bounds the secret key rate capacity of the channel for all the investigated channels in this section and moreover, it always lies between the best known upper bound based on relative entropy of entanglement [18] and the one derived from squashed entanglement [17, 70].

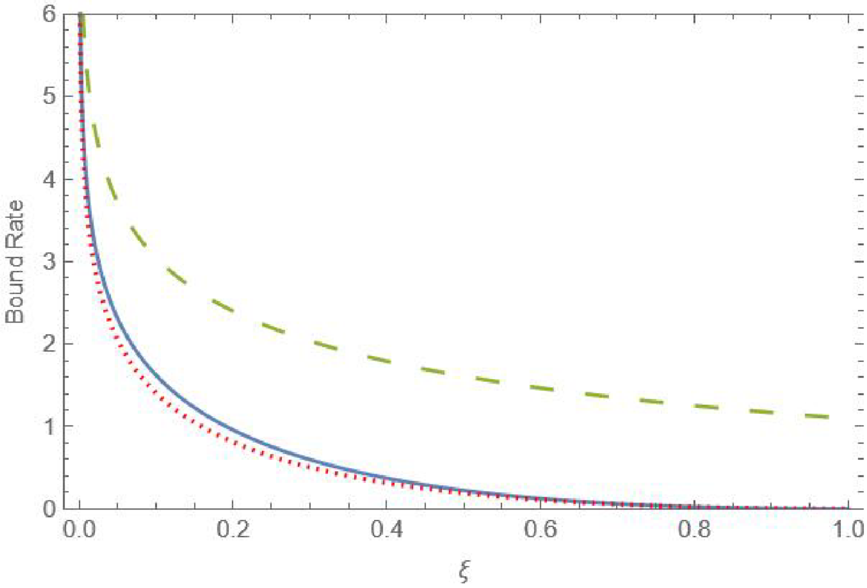

Figure 4.1: The upper bounds on the capacity of additive-noise Gaussian channel based on GIE (blue line), relative entropy of entanglement (red dotted line) and squashed entanglement (green dashed line).

Conclusion

After the unification of GIE with GR2EoF, its gained computability allowed and motivated further research of this measure.
The Thesis aimed to show its significance in quantum communication. In Section 3.2 we showed the general proof of GIE upper bounding the secret key rate in CV QKD, followed by its verification for standard CV QKD protocols in Section 3.5.
Further, for the investigated quantum channels, we compared GIE with upper bounds on the secret key rate capacity of the channel in Section 4.2 and showed that it always lies above the best known upper bound derived from relative entropy of entanglement but it is always lower than or equal to the upper bound derived from squashed entanglement.
All these calculations were made in the restriction to a Choi state of the channel. Its investigation for the non-asymptotic regimes remains for further research.

Bibliography

[1] C. E. Shannon, "Communication theory of secrecy systems," in The Bell System Technical Journal **28**, pp. 656-715, 1949.

[2] C. Bennett and G. Brassard. Proceeding of the ieee international conference on computers, systems and signal processing, bangalore, india. IEEE, New York, p. 175, 1984.

[3] W. K. Wootters and W. H. Zurek. A single quantum cannot be cloned. Nature **299**, 802, 1982.

[4] G. Vidal, Entanglement monotones, J. Mod. Opt. **47**, 355, 2000.

[5] Martin B. Plenio and Shashank Virmani, An introduction to entanglement measures. Quant. Inf. Comput. **7**, 51, 2007.

[6] L. Mišta, Jr. and R. Tatham, Gaussian Intrinsic Entanglement, Phys. Rev. Lett. **117**, 240505, 2016.

[7] L. Mišta and R. Tatham, Gaussian intrinsic entanglement: An entanglement quantifier based on secret correlations, Phys. Rev. A **91**, 062331, 2015.

[8] L. Mišta Jr. and Klára Baksová, Gaussian intrinsic entanglement for states with partial minimum uncertainty, Phys. Rev. A **97**, 012305, 2018.

[9] L. Lami, L. Mišta, Jr., and G. Adesso, Fundamental limitations to key distillation from Gaussian states with Gaussian operations, *arXiv:2010.15729*, 2020.

[10] V. Coffman, J. Kundu, and W. K. Wootters, Distributed entanglement, Phys. Rev. A **61**, 052306, 2006.

[11] M. Koashi and A. Winter, Monogamy of quantum entanglement and other correlations, Phys. Rev. A **69**, 022309, 2004.

[12] R. García-Patrón. *Quantum information with optical continuous variables: from Bell tests to key distribution.* PhD thesis, Université libre de Bruxelles, 2007.

[13] F. Grosshans and P. Grangier. Continuous variable quantum cryptography using coherent states. Phys. Rev. Lett. **88**, 057902, 2002.

[14] C. Weedbrook, A. M. Lance, W. P. Bowen, T. Symul, T. C. Ralph, and P. K. Lam. Quantum cryptography without switching. Phys. Rev. Lett. **93**, 170504, 2004.

[15] N. J. Cerf, M. Levy, and G. Van Assche. Quantum distribution of Gaussian keys using squeezed states. Phys. Rev. A **63**, 052311, 2001.

[16] S. Pirandola, S. L. Braunstein, R. Laurenza, C. Ottaviani, T. P. W. Cope, G. Spedalieri, and L. Banchi., Theory of channel simulation and bounds for private communication, Quantum Sci. Technol. **3** 035009, 2018.

[17] M.Takeoka, S. Guha, and M. M. Wilde, Fundamental rate-loss tradeoff for optical quantum key distribution, Nat. Commun. **5**, 5235, 2014.

[18] S. Pirandola, R. Laurenza, C. Ottaviani, and L. Banchi, Fundamental limits of repeaterless quantum communications, Nat. Commun. **8**, 15043, 2017.

[19] A. Aspect and P. Grangier, Wave-particle duality for single photons, Hyperfine Interactions **37**, 3 (1987).

[20] E. M. Rains, A semidefinite program for distillable entanglement, IEEE Trans. Inf. Theory **47**, 2921 (2001).

[21] J. Eisert, S. Scheel, and M. B. Plenio, Distilling Gaussian States with Gaussian Operations is Impossible, Phys. Rev. Lett. **89**, 137903 (2002).

[22] M. Ohliger, K. Kieling, and J. Eisert, Limitations of quantum computing with Gaussian cluster states, Phys. Rev. A **82**, 042336 (2010).

[23] S. P. Walborn, P. H. Souto Ribeiro, L. Davidovich, F. Mintert, and A. Buchleitner, Experimental determination of entanglement with a single measurement, Nature (London) **440**, 1022 (2006).

[24] J. L. O'Brien, G. J. Pryde, A. Gilchrist, D. F. V. James, N. K. Langford, T. C. Ralph, and A. G. White, Quantum Process Tomography of a Controlled-NOT Gate, Phys. Rev. Lett. **93**, 080502 (2004).

[25] T. Yamamoto, M. Koashi, S¸. K. Ozdemir, and N. Imoto, Experimental extraction of an entangled photon pair from two identically decohered pairs, Nature (London) **421**, 343 (2003).

[26] M. B. Plenio, The logarithmic negativity: A full entanglement monotone that is not convex, Phys. Rev. Lett. **95,** 090503 (2005).

[27] K. Audenaert, M. B. Plenio, and J. Eisert, Phys. Rev. Lett. **90,** 027901 (2003).

[28] J. Eirset, Entanglement in quantum information theory, Ph.D. thesis, University of Potsdam, 2001.

[29] C. H. Bennett, G. Brassard, S. Popescu, B. Schumacher, J. A. Smolin, and W. K. Wootters, Purification of Noisy Entanglement and Faithful Teleportation via Noisy Channels, Phys. Rev. Lett. **76**, 722 (1996).

[30] M. Horodecki, P. Horodecki, and R. Horodecki, Mixed-State Entanglement and Distillation: Is there a "Bound" Entanglement in Nature?, Physical Review Letters. **80** 5239 (1998).

[31] W. K. Wootters, Entanglement of Formation of an Arbitrary State of Two Qubits, Phys. Rev. Lett. **80** 2245-2248, 1998.

[32] G. Giedke, M.M. Wolf, O.Krueger, R.F. Werner, J.I. Cirac, Entanglement of formation for symmetric Gaussian states, Phys. Rev. Lett. **91**, 107901, 2003.

[33] N. Gisin and S. Wolf, Linking Classical and Quantum Key Agreement: Is there "Bound Information?", in Proceedings of CRYPTO 2000, Lecture Notes in Computer Science 1880 (Springer, Berlin, 2000) p. 482.

[34] A. Acín and N. Gisin, Quantum Correlations and Secret Bits, Phys. Rev. Lett. **94**, 020501, 2005.

[35] U. M. Maurer and S. Wolf. Unconditionally secure key agreement and the intrinsic conditional information, IEEE Trans. Inf. Theory **45**, 499-519, 1999.

[36] C. E. Shannon, A Mathematical Theory of Communication, Bell Syst. Tech. J. **27**, 379, 1948.

[37] M. Christandl and A. Witner, "Squashed entanglement": An additive entanglement measure, J. Math. Phys. **45**, 829, 2004.

[38] N. J. Cerf and C. Adami, Negative Entropy and Information in Quantum Mechanics, Phys. Rev. Lett. **79**, 5194, 1997.

[39] S. Boyd and L. Vandenberghe, Convex Optimization (Cambridge University Press, Cambridge, 2004).

[40] V. Vedral, M. B. Plenio, M. A. Rippin, and P. L. Knight, Quantifying Entanglement, Phys. Rev. Lett. **78**, 2275, 1997.

[41] V. Vedral and M. B. Plenio, Entanglement measures and purification procedures, Phys. Rev. A **57**, 1619, 1998.

[42] S. Friedland, G. Gour, Closed formula for the relative entropy of entanglement in all dimensions, J. Math. Phys. **52**, 052201, 2011.

[43] V. Vedral, M.B. Plenio, K. Jacobs, and P.L. Knight, Statistical inference, distinguishability of quantum states, and quantum entanglement, Phys. Rev. A **56**, 4452, 1997.

[44] C. H. Bennett, D. P. DiVincenzo, J. A. Smolin, and W. K. Wootters, Mixed-state entanglement and quantum error correction, Phys. Rev. A **54**, 3824, 1996.

[45] A. Rényi, in *Proceedings of the 4th Berkeley Symposium on Mathematics, Statistics and Probability: held at the Statistical Laboratory, University of California, 1960,* editeted by J. Neyman (University of California Press, Berkeley, 1961), p. 547.

[46] J. S. Kim and B. C. Sanders, Monogamy of multi-qubit entanglement using Rényi entropy, J. Phys. A **43**, 445305, 2010.

[47] T. J. Osborne, Convex hulls of varieties and entanglement measures based on the roof construction, Quantum Inf. Comput. **7**, 209, 2007.

[48] R. Horodecki, P. Horodecki, M. Horodecki, and K. Horodecki, Quantum Entanglement, Rev. Mod. Phys. **81**, 865, 2009.

[49] T. J. Osborne and F. Verstraete, General Monogamy Inequality for Bipartite Qubit Entanglement, Phys. Rev. Lett. **96**, 220503, 2006.

[50] G. Adesso, D. Girolami, and A. Serafini, Measuring Gaussian Quantum Information and Correlations Using the Rényi Entropy of Order 2, Phys. Rev. Lett. **109**, 190502, 2012.

[51] Quantum Information with Continuous Variables of Atoms and Light, edited by N. J. Cerf, G. Leuchs, and E. S. Polzik (Imperial College Press, London, 2007).

[52] R. Simon, N. Mukunda, and B. Dutta, Quantum-noise matrix for multimode systems: U(n) invariance, squeezing, and normal forms. Phys. Rev. A **49**, 1567-1583, 1994.

[53] John Williamson. "On the Algebraic Problem Concerning the Normal Forms of Linear Dynamical Systems". In: American Journal of Mathematics **58**, 141– 163, 1936.

[54] R. Simon, Peres-Horodecki Separability Criterion for Continuous Variable Systems, Phys. Rev. Lett. **84**, 2726, 2000.

[55] Fox, Mark. Quantum optics: an introduction, pages 156-159, Oxford, Oxford Univ. Press, 2006.

[56] A. Einstein, B. Podolsky, and N. Rosen. Can quantum-mechanical description of physical reality be considered complete? Phys. Rev. **47**, 777, 1935

[57] G. Giedke and J. I. Cirac, Characterization of Gaussian operations and distillation of Gaussian states, Phys. Rev. A **66**, 032316, 2002.

[58] M. F. Cornelio and M. C. de Oliveira, Strong superadditivity and monogamy of the Rényi measure of entanglement, Phys. Rev. A **81**, 032332, 2010.

[59] M. Christandl, A. Ekert, M. Horodecki, P. Horodecki, J. Oppenheim, and R. Renner, Unifying classical and quantym key distillation. In S.P. Vadhan, editor, *Theory of Cryptography*, pages 456-478, Berlin, Heidelberg, 2007. Springer Berlin Heidelberg.

[60] U. M. Maurer, Secret key agreement by public discussion from common information. IEEE Trans. Inf. Theor. **39**, 733-742, 1993.

[61] I. Csiszar and J. Korner. Broadcast channels with confidential messages. IEEE Transaction on Information Theory, **24** (3), 1978.

[62] R. Ahlswede and I. Csiszar, Common randomness in information theory and cryptography, I. Secret sharing. IEEE Trans. Inf. Theory **39**, 1121-1132, 1993.

[63] C. Bennett and G. Brassard. Proceeding of the ieee international conference on computers, systems and signal processing, bangalore, india. IEEE, New York, p. 175, 1984.

[64] C. Weedbrook, S. Pirandola, R. García-Patrón, N. J. Cerf, T. C. Ralph, J. H. Shapiro, and S. Lloyd, Gaussian quantum information, Rev. Mod. Phys. **84**, 621-669, 2012.

[65] K. Baksová, Gaussian Intrinsic Entanglement, Bachelor's Thesis, page 9. Palacký University, Faculty of Science, Department of Optics, Olomouc, 2019, Supervised by L. Mišta, Jr.

[66] M. Curty, M. Lewenstein, and N. Lütkenhaus, Entalgement as a precondition for secure quantum key distribution, Phys. Rev. Lett. **92**, 217903, 2004.

[67] T. Moroder, M. Curty, and N. Lütkenhaus, Upper bound on the secret key rate distillable from effective quantum correlations with imperfect detectors, Phys. Rev. A **73**, 012311, 2006.

[68] G. van Assche. Quantum Cryptography and Secret-Key Distillation. CUP, Cambridge, 2006.

[69] B. Julsgaard, J. Sherson, J. I. Cirac, J. Fiurášek, and E. S. Polzik. Experimental demonstration of quantum memory for light. Nature **432**, 482, 2004.

[70] M. Takeoka, S. Guha, and M. M. Wilde, The squashed entanglement of a quantum channel, IEEE Trans. Inf. Theory, **60** (8), 4987-4998, 2014.

[71] S. L. Braunstein, N. J. Cerf, S. Iblisdir, P. van Loock, and S. Massar. Optimal cloning of coherent states with linear amplifier and beam splitter. Phys. Rev. Lett. **86**, 4938, 2001.

[72] J. Eisert and M. Plenio. Introduction to the basics of entanglement theory in continuous-variable system. *arXiv:quant-ph/0312071*, 2003.

[73] S. Tserkis, J. Dias, and T. C. Ralph. Simulation of Gaussian channels via teleportation and error correction of Gaussian states. Phys. Rev. A **98**, 052335, 2018.

[74] K. Horodecki, M. Horodecki, P. Horodecki and J. Oppenheim, Secure key from bound entanglement, Phys. Rev. Lett. **94**, 160502, 2005.