entropy

IMPACT FACTOR 2.0

Indexed in: PubMed

CITESCORE 5.2

Article

Exploring Non-Gaussianity Reduction in Quantum Channels

Micael Andrade Dias and Francisco Marcos de Assis

Special Issue

Continuous Variables for Quantum Key Distribution and Quantum Random Number Generators

Edited by

Dr. Matteo Schiavon, Dr. Marco Avesani and Dr. Cosmo Lupo

MDPI

https://doi.org/10.3390/e27070768

entropy

MDPI

Article

Exploring Non-Gaussianity Reduction in Quantum Channels

Micael Andrade Dias [1,2,*] and Francisco Marcos de Assis [3]

[1] QuIIN—Quantum Industrial Innovation, EMBRAPII CIMATEC Competence Center in Quantum Technologies, SENAI CIMATEC, Av. Orlando Gomes 1845, Salvador 41650-010, BA, Brazil
[2] Department of Electrical and Photonics Engineering, Technical University of Denmark, 2800 Lyngby, Denmark
[3] Department of Electrical Engineering, Federal University of Campina Grande, Campina Grande 58429-900, PB, Brazil; fmarcos@dee.ufcg.edu.br
* Correspondence: mandi@dtu.dk

Abstract

The quantum relative entropy between a quantum state and its Gaussian equivalent is a quantifying function of the system's non-Gaussianity, a useful resource in several applications, such as quantum communication and computation. One of its most fundamental properties is to be monotonically decreasing under Gaussian evolutions. In this paper, we develop the conditions for a non-Gaussian quantum channel to preserve the monotonically decreasing property. We propose a necessary condition to classify between Gaussian and non-Gaussian channels and use it to define a class of quantum channels that decrease the system's non-Gaussianity. We also discuss how this property, combined with a restriction on the states at the channel's input, can be applied to the security analysis of continuous-variable quantum key distribution protocols.

Keywords: quantum resource theory; Gaussian channels; non-Gaussianity

1. Introduction

Quantum resource theory (QRT) stands as a cornerstone in the field of quantum information science, providing a formal framework for understanding and manipulating various quantum resources [1]. From entanglement to coherence, quantum resource theories offer a systematic approach to quantifying and harnessing the unique properties of quantum systems, allowing advancements in quantum communication, computation, and beyond [2,3].

A non-Gaussian (nG) resource theory, for instance, aims to understand which tasks require states and operations to have an nG character and how they can be better used, once the Gaussian sector of quantum states and operations is simpler to manipulate in a laboratory. Central to the study of an nG quantum resource theory (nG-QRT) is the quantum relative entropy (QRE), a powerful tool for quantifying the non-Gaussianity of quantum states [4]. In particular, the QRE plays a pivotal role as a resource quantifying function, offering insights into the distinguishability between a quantum state and its Gaussian equivalent [5,6]. A key property of the quantum relative entropy is its monotonic decrease under Gaussian operations, providing a robust foundation for characterizing nG transformations and their effects on the system's non-Gaussianity.

Although quantum resource theory has found widespread applications across various domains of quantum information science [7–10], its integration into continuous-variable quantum key distribution (CV-QKD) protocols has been relatively limited. In some foundational studies, its developments have been utilized merely to corroborate well-known

check for updates

Academic Editors: Marco Avesani, Matteo Schiavon and Cosmo Lupo

Received: 21 May 2025
Revised: 30 June 2025
Accepted: 7 July 2025
Published: 20 July 2025

Citation: Dias, M.A.; Assis, F.M.d. Exploring Non-Gaussianity Reduction in Quantum Channels. *Entropy* **2025**, 27, 768. https://doi.org/10.3390/e27070768

results from the existing literature, such as the optimality of Gaussian states for entropic quantities, rather than being actively exploited to improve the capabilities and security of CV-QKD schemes [11]. However, one promising avenue for application lies in the security analysis of CV-QKD protocols that utilize nG modulation of coherent states.

In the general setup of a QKD protocol, Alice and Bob (the trusted parties) distribute secret random keys by transmitting quantum states through an untrusted quantum channel. An eavesdropper (also called Eve) has access to the quantum channel and attempts to gain information employing some attack strategy. So, to keep secrecy, Alice and Bob must estimate how much information Eve has had access to during the protocol execution. When assessing this quantity, Alice and Bob must decide which model they will use to describe the quantum channel linking them, either a Gaussian or an nG. When assuming a Gaussian model, they in fact can upper bound Eve's information by reconstructing a covariance matrix using solely the channel transmittance and excess noise parameters. Despite its practical relevance, the Gaussian channel model does not cover the worst-case scenario of Eve's attacks, given that Alice did not prepare her states according to a Gaussian distribution [12].

State-of-the-art security analyses of CV-QKD with nG modulation often involve sophisticated optimization techniques [12–14]. These analyses aim to determine the maximal eavesdropper information by exploring the space of nG quantum channels compatible with the estimated parameters during quantum communication. When nG modulation is used for quantum state transmission, the non-Gaussianity must be taken into account in the security analysis.

In this paper, we investigate the gap between the Gaussian and nG security models of CV-QKD by using tools from nG-QRT. More precisely, we take as starting point one basic property of the QRE measure of non-Gaussianity, its monotone decrease under Gaussian operations, and investigate how it can be extended to nG quantum channels. By presenting the conditions under which an nG quantum channel reduces the system's non-Gaussianity, we discuss how it can be used in security proofs of CV-QKD protocols with nG modulation. We also provide examples of such quantum channels, showing that, for specific mixtures of quantum states at the channel input, the covariance matrix remains unchanged while the system nG is reduced.

The remainder of the paper is structured as follows: Section 2 states the formal definitions and the problem we aim to address. In Section 3, we develop the main results for nG quantum channels, and in Section 4, we explore how it can be used in the security analysis of CV-QKD protocols, with the concluding remarks in Section 5.

Notation

In what follows, we use the standard Dirac notation for quantum mechanics. A and B are quantum systems with the associated Hilbert spaces $\mathcal{H}_A$ and $\mathcal{H}_B$, respectively. $\mathcal{B}(\mathcal{H}_A)$ and $\mathcal{D}(\mathcal{H}_A)$ denote the space of bounded linear operators and the set of density operators in $\mathcal{H}_A$, respectively, with elements represented as $\hat{A} \in \mathcal{B}(\mathcal{H}_A)$ and $\hat{\rho} \in \mathcal{D}(\mathcal{H}_A)$. The subset of $\mathcal{D}(\mathcal{H}_A)$ corresponding to Gaussian states will be denoted by $\mathcal{G}_s(\mathcal{H}_A)$, or simply $\mathcal{G}_s$.

The subspace of completely positive trace-preserving (CPTP) linear operators from $\mathcal{H}_A$ to $\mathcal{H}_B$ is denoted as $\mathcal{Q}(\mathcal{H}_A \to \mathcal{H}_B)$ with elements $\mathcal{N}_{A\to B}$. All indexes will be dropped when implicit. If $\mathcal{N}$ is a quantum channel, the evolution of a state and the transformations of any of its quantities are represented by $\mathcal{N}(\cdot)$ or $\overset{\mathcal{N}}{\to}$. In particular, we denote by $\mathcal{G}_c(\mathcal{H}_A \to \mathcal{H}_B) \subset \mathcal{Q}(\mathcal{H}_A \to \mathcal{H}_B)$ the subset of all Gaussian quantum channels, or only $\mathcal{G}_c$.

2. Preliminaries and Problem Statement

The question we are proposing is as follows: Can a quantum state have its non-Gaussianity reduced after undergoing an nG evolution? Alternatively, is there any nG channel that makes quantum states "more Gaussian"? By non-Gaussianity of an arbitrary quantum state, the literature often refers to a quantity informing "how much" an nG state fails to pass as a Gaussian state. Operationally, it may be defined as the distance from a Gaussian reference state [4]. Here, we use the QRE as a quantifying function of non-Gaussianity, having in mind that, even though it is not a metric, it satisfies all axioms for a resource quantifying function [1].

Definition 1 ([6]). *Let $\hat{\sigma}$ be an arbitrary quantum state and $\hat{\sigma}^G$ be the Gaussian quantum state with the same mean vector and covariance matrix as $\hat{\sigma}$. The state $\hat{\sigma}^G$ is said to be the Gaussian equivalent to $\hat{\sigma}$. The QRE-based nG measure of $\hat{\sigma}$ is defined as*

$$\delta_{vN}(\hat{\sigma}) = S(\hat{\sigma}||\hat{\sigma}^G). \tag{1}$$

Among the many properties of δ_{vN}, two of them are of special interest:

(i) Non-negativity ($\delta_{vN}(\hat{\sigma}) \geq 0$, with equality if and only if $\hat{\sigma} \in \mathcal{G}_s$);
(ii) Contractivity under Gaussian quantum channels, $\delta_{vN}(\hat{\sigma}) \geq \delta_{vN}(\mathcal{N}(\hat{\sigma}))$ for any $\hat{\sigma} \in \mathcal{D}(\mathcal{H})$ and $\mathcal{N} \in \mathcal{G}_c$.

In an nG-QRT, the QRE-based non-Gaussianity measure is a resource quantifying function and carries some operational meaning in its properties. In such a resource theory, Gaussian states and Gaussian operations are free [11]. Property (ii) implies that no free operation should increase the amount or resource of a quantum state. Then, one way of looking at the questioning about whether an nG quantum channel can reduce the non-Gaussianity of nG states can be rephrased as "can property (ii) be extended to nG quantum channels?". This idea is illustrated in Figure 1, where $\mathcal{N}_1$ is a Gaussian channel and, as such, maps Gaussian states into Gaussian states ($\hat{\rho}$ and $\hat{\rho}'$) and reduces the non-Gaussianity of $\hat{\sigma} \notin \mathcal{G}_s$. For the sake of simplicity, the non-Gaussianity of a quantum state is illustrated as the distance from the set $\mathcal{G}_s$ and should not be taken formally. The question remaining is whether there is any nG channel $\mathcal{N}_2$ still bringing states closer to the Gaussian sector.

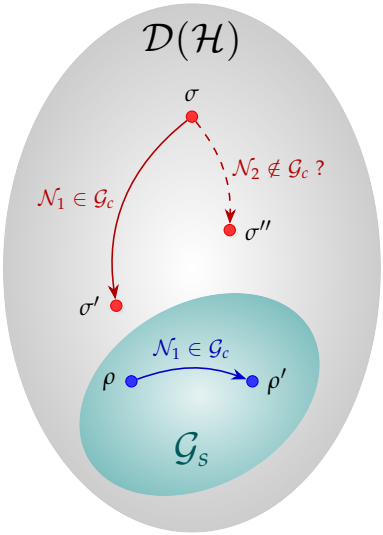


Figure 1. Visual representation of the set of Gaussian states and the action of Gaussian and nG quantum channels relative to reducing the state nG. Every state in $\mathcal{G}_s$ has $\delta_{nG} = 0$, and the action of a Gaussian channel for any state outside $\mathcal{G}_s$ reduces its nG. The same is not necessarily true for nG channels.

Now, consider the following setup: Let $\{X_n\}$ be a sequence of random variables (with corresponding alphabet $\mathcal{X}_n$ and probability mass function $p_{X_n}(x)$) such that it converges in distribution to a complex Gaussian density, that is, $X_n \xrightarrow{D} X_G \sim \mathcal{N}_{\mathbb{C}}(0, \bar{m})$. For this work, we consider X_n to be distributed symmetrically on the complex plane, i.e., $p_{X_n}(x) = p_{X_n}(-x)$ for any $x \in \mathcal{X}_n$. For each X_n, define the ensemble of coherent states $\{|x\rangle, p_{X_n}(x)\}$ and the corresponding mixed state $\hat{\rho}_{X_n} = \sum_{x \in \mathcal{X}_n} p_{X_n}(x)|x\rangle\langle x|$. Such an ensemble can represent what a transmitter (Alice) can send to the receiver (Bob) through a quantum channel $\mathcal{N}_{A\to B}$ in a CV-QKD protocol with discrete modulation (DM), where the modulation format is represented by the random variable X_n.

By considering a mixture of coherent states that is induced by a random variable taken from a sequence that converges to a Gaussian distribution, one can prove the following statements [15]:

$$\lim_{n\to\infty} \delta_{vN}(\hat{\rho}_{X_n}) = 0 \tag{2}$$

$$\lim_{n\to\infty} \inf_{\mathcal{N}_{A\to B}} \{\delta_{vN}(\mathcal{N}_{A\to B}(\hat{\rho}_{X_n}))\} = 0, \tag{3}$$

where the infimum must be computed for all quantum channels $\mathcal{N}_{A\to B}$ compatible with the statistics observed at the output up to the second moment (We point out that in [15], the main problem was the analysis of the role of non-Gaussianity in security proofs of continuous-variable quantum key distribution protocols using discrete modulation of coherent states. That is why it is relevant to restrict the quantum channels to the ones matching the first and second statistical moments at the reception when defining the infimum in Equation (3)). It is important to note that the quantum channel that minimizes the QRE-nG function in Equation (3) does not need to be Gaussian. Consider an arbitrary $\mathcal{N} \in \mathcal{G}_c$ and let $\mathcal{N}^* \in \mathcal{Q}$ be the quantum channel for which the infimum in Equation (3) is achieved for some n. Then, using the monotonicity of δ_{vN}, the following inequality holds:

$$\delta_{vN}(\hat{\rho}_{X_n}) \geq \delta_{vN}(\mathcal{N}(\hat{\rho}_{X_n})) \geq \delta_{vN}(\mathcal{N}^*(\hat{\rho}_{X_n})), \tag{4}$$

and by adding the convergence $X_n \xrightarrow{D} X_G \sim \mathcal{N}_{\mathbb{C}}(0, \bar{m})$, one has that

$$\lim_{n\to\infty} \delta_{vN}(\mathcal{N}^*(\hat{\rho}_{X_n})) \leq \lim_{n\to\infty} \delta_{vN}(\hat{\rho}_{X_n}) = 0. \tag{5}$$

Besides the guarantee of small non-Gaussianity before and after the quantum channel for sufficiently large n whenever $X_n \to X_G$, there is no constraint for $\mathcal{N}^*$ to be Gaussian. The question of extending property (ii) of δ_{vN} gains operational importance in understanding which conditions a quantum channel has to satisfy for one to be able to compute the minimal output non-Gaussianity, given the input state and the data statistics up to the second moment. As will be discussed in the following sections, this minimal non-Gaussianity quantity can be directly linked to the problem of accessing the security of CV-QKD protocols with discrete (nG) modulation.

3. Quantum Relative Entropy Monotonicity Under Non-Gaussian Quantum Channels

In this section, we will develop the conditions under which an nG quantum channel maintains the monotonic property of the QRE non-Gaussianity and provide numerical results for a class of mixtures of quantum states that are of practical interest for CV-QKD protocols. The first step is to prove the following lemma:

Lemma 1. *Let $\mathcal{N}$ be a quantum channel, let $\hat{\rho}$ be an arbitrary quantum state, and define*

$$\Delta(\mathcal{N},\hat{\rho}) = \mathrm{tr}\Big[\mathcal{N}(\hat{\rho})(\log\mathcal{N}(\hat{\rho})^G - \log\mathcal{N}(\hat{\rho}^G))\Big]. \tag{6}$$

If $\mathcal{N} \in \mathcal{G}_c$ then $\Delta(\mathcal{N},\hat{\rho}) = 0$ for any quantum state $\hat{\rho}$.

Proof. If $\mathcal{N}$ is a Gaussian channel and $\mathbf{\Gamma}$ is the covariance matrix of an arbitrary quantum state $\hat{\rho}$, then $\mathbf{\Gamma}(\hat{\rho}) = \mathbf{\Gamma}(\hat{\rho}^G)$ and $\mathbf{\Gamma} \overset{\mathcal{N}}{\to} \mathbf{\Gamma}'$. This means that $\mathbf{\Gamma}(\mathcal{N}(\hat{\rho})^G) = \mathbf{\Gamma}(\mathcal{N}(\hat{\rho}^G)) = \mathbf{\Gamma}'$. Since the first moment will follow in the same way, $\mathcal{N}(\hat{\rho}^G) = \mathcal{N}(\hat{\rho})^G$ for any $\hat{\rho} \in \mathcal{D}(\mathcal{H})$, and then $\Delta(\mathcal{N},\hat{\rho}) = 0$ for arbitrary $\hat{\rho}$. □

This result gives a sufficient condition to classify a quantum channel concerning its non-Gaussianity: if it is verified that $\Delta(\mathcal{N},\hat{\rho}) \neq 0$ for some quantum state $\hat{\rho}$, then $\mathcal{N}$ is nG. Now, define the set of quantum channels for which $\Delta \geq 0$, $\mathcal{F} = \{\mathcal{N} \in \mathcal{Q} : \Delta(\mathcal{N},\hat{\rho}) \geq 0 \,\forall\, \hat{\rho} \in \mathcal{D}(\mathcal{H})\}$. Then, $\mathcal{G}_c \subset \mathcal{F}$ and this allows us to propose the following statement:

Theorem 1. *If $\mathcal{N} \in \mathcal{F}$, then $\delta_{vN}(\mathcal{N}(\hat{\rho})) \leq \delta_{vN}(\hat{\rho})$ for any $\hat{\rho} \in \mathcal{D}(\mathcal{H})$.*

Proof. Let $\hat{\rho}$ and $\mathcal{N}$ be as in the setup. From quantum relative entropy contractivity under quantum channels, one gets

$$\begin{aligned}
\delta_{vN}(\hat{\rho}) &\overset{(a)}{=} S(\hat{\rho}||\hat{\rho}^G) && (7)\\
&\overset{(b)}{\geq} S(\mathcal{N}(\hat{\rho})||\mathcal{N}(\hat{\rho}^G)) && (8)\\
&\overset{(c)}{=} \mathrm{tr}\Big[\mathcal{N}(\hat{\rho})(\log\mathcal{N}(\hat{\rho}) - \log\mathcal{N}(\hat{\rho}^G))\Big] + \mathrm{tr}\Big[(\mathcal{N}(\hat{\rho}) - \mathcal{N}(\hat{\rho})^G)\log\mathcal{N}(\hat{\rho})^G\Big] && (9)\\
&\overset{(d)}{=} S(\mathcal{N}(\hat{\rho})^G) - S(\mathcal{N}(\hat{\rho})) + \Delta(\mathcal{N},\hat{\rho}) && (10)\\
&\overset{(e)}{=} S(\mathcal{N}(\hat{\rho})||\mathcal{N}(\hat{\rho})^G) + \Delta(\mathcal{N},\hat{\rho}) && (11)\\
&\overset{(f)}{\geq} \delta_{vN}(\mathcal{N}(\hat{\rho})), && (12)
\end{aligned}$$

where (a) comes from the definition of δ_{vN}, (b) from the monotonicity of quantum relative entropy [16], (c) uses the fact that $\mathrm{tr}\big[(\hat{\sigma} - \hat{\sigma}^G)\log(\hat{\sigma}^G)\big] = 0$ for arbitrary $\hat{\sigma}$ [17], (d) applies the definition in Lemma 1, (e) follows from Definition 1, and (f) holds because $\mathcal{N}$ and $\hat{\rho}$ were chosen such that $\Delta(\mathcal{N},\hat{\rho}) \geq 0$. □

Theorem 1 provides an interpretation to the quantity $\Delta(\mathcal{N},\hat{\rho})$, with its non-negativity being a necessary condition for a channel to reduce the non-Gaussianity character of a quantum state. In other words, the δ_{vN} non-increasing property was extended to nG quantum channels satisfying the conditions of Theorem 1.

However, the specification of $\mathcal{F}$ may have been too broad by demanding $\Delta(\mathcal{N},\hat{\rho})$ to be non-negative for all quantum states in the system, and we cannot affirm whether $\mathcal{F} \setminus \mathcal{G} = \{\varnothing\}$ or not. A relaxation in this condition can be achieved by considering only a specific set of quantum states, which we chose to be the states relevant to DM-CVQKD protocols, and can help describe a set of QRE-nG non-increasing quantum channels.

Let $\mathcal{S}_{\bar{n}} = \{\hat{\sigma} \in \mathcal{D}(\mathcal{H}) : \hat{\sigma} = \sum_{x\in\mathcal{X}_n} p(x)\hat{\rho}^{th}(x,\bar{n})\}$ with X_n being a discrete symmetric random variable and $\hat{\rho}^{th}(x,\bar{n})$ be the displaced thermal state with $\bar{n}$ average photons and the first moment $\bar{x} = 2\cdot(\mathrm{Re}\{x\},\mathrm{Im}\{x\})^T$. Constellations of coherent states are represented by the set $\mathcal{S}_0$, and any state in $\mathcal{S}_{\bar{n}}$ has a diagonal covariance matrix for any value of $\bar{n}$, which means that its equivalent Gaussian quantum state is a thermal

state with the appropriate mean photon number. Then, we can define a relaxed set $\mathcal{F}_{\bar{n}} = \{\mathcal{N} \in \mathcal{Q} : \Delta(\mathcal{N}, \hat{\rho}) \geq 0 \, \forall \, \hat{\rho} \in \mathcal{S}_{\bar{n}}\}$ such that the QRE-nG of any quantum state in $\mathcal{S}_{\bar{n}}$ is non-increasing under the action of any channel in $\mathcal{F}_{\bar{n}}$. Also, we have $\mathcal{G}_c \subset \mathcal{F} \subset \mathcal{F}_{\bar{n}}$ for any $\bar{n}$. The states in $\mathcal{S}_{\bar{n}}$ are relevant for the QKD setup because they represent the mixed states output by a noisy modulation device with modulation noise $\bar{n}$. We can affirm the following proposition:

Proposition 1. $\mathcal{F}_0 \setminus \mathcal{G} \neq \{\varnothing\}$.

Proof. Take the phase diffusion process described in Appendix A and represent it by $\mathcal{N}_\kappa$, which is the model of a non-Gaussian evolution of a quantum system. It is known that the QRE-nG of coherent states under phase diffusion increases with the diffusion parameter κ. In Appendix A, it is shown that for any $\hat{\rho} \in \mathcal{S}_0$, $\bar{\boldsymbol{x}}(\hat{\rho}) = \bar{\boldsymbol{x}}(\mathcal{N}_\kappa(\hat{\rho})) = 0$ and $\boldsymbol{\Gamma}(\hat{\rho}) = \boldsymbol{\Gamma}(\mathcal{N}_\kappa(\hat{\rho}))$, which implies that $\hat{\rho}^G = \mathcal{N}_\kappa(\hat{\rho})^G$. That is, the phase diffusion process does not modify the first and second statistical moments of appropriate mixtures of coherent states. In addition, it does not affect thermal states, meaning that $\mathcal{N}_\kappa(\hat{\rho}^G) = \hat{\rho}^G$. We conclude that $\mathcal{N}_\kappa(\hat{\rho}^G) = \mathcal{N}_\kappa(\hat{\rho})^G$, which results in $\Delta(\mathcal{N}_\kappa, \hat{\rho}) = 0$ for any state in $\mathcal{S}_0$ and then $\mathcal{N}_\kappa \in \mathcal{F}_0 \setminus \mathcal{G} \neq \{\varnothing\}$. □

We conjecture that Proposition 1 can be extended to other values of $\bar{n}$ different from zero, although we have not yet worked out the proof. A graphical representation of the action of the phase diffusion channel is given in Figure 2a. The states in $\mathcal{S}_0$ are convex mixtures of Gaussian states which, by linearity of the quantum channel, are mapped to a convex mixture of nG states $\hat{\rho}' = \mathcal{N}_\kappa(\hat{\rho})$. Since the phase diffusion process does not modify the covariance matrix of the states in $\mathcal{S}_0$, both $\hat{\rho}$ and $\hat{\rho}'$ have the same covariance matrix and the same Gaussian equivalent state, represented by $\hat{\sigma}$ in Figure 2a. The consequence of Proposition 1 is that $\hat{\rho}'$ is closer to $\hat{\sigma}$ than $\hat{\rho}$ in the sense of QRE.

To illustrate how an nG channel can reduce the non-Gaussianity of an ensemble of coherent states, consider QAM-like (Quadrature Amplitude Modulation) constellations of coherent states, where each quadrature follows a Gauss–Hermite distribution. Such constellations are known to converge exponentially to the capacity of the additive white Gaussian noise (AWGN) channel in classical communication scenarios [18].

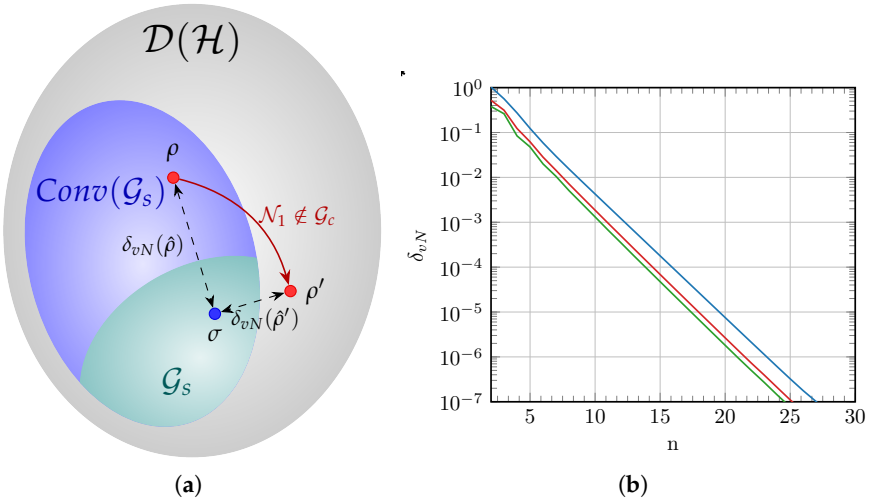
The Gauss–Hermite constellation is constructed by taking the n-th Hermite polynomial, defined via the derivatives of the standard Gaussian probability density function $p_X(x)$:

$$H_n(x) = \frac{(-1)^n}{p_X(x)} \frac{\mathrm{d}^n p_X(x)}{\mathrm{d}x^n}. \tag{13}$$

This polynomial has n distinct real roots, denoted by the set $\mathcal{X}_n$, which determine the constellation points. Each root $x_{i,n}$ is associated with a weight (interpreted as a probability) given by the following:

$$w_{i,n} = \frac{(n-1)!}{n H_{n-1}^2(x_{i,n})}. \tag{14}$$

Examples of these constellations are shown in Figure 3. The top row displays the roots and associated weights of $H_n(x)$ for $n = 2, 4, 6, 8$, representing one-dimensional constellations along a single quadrature. As n increases, the point distribution increasingly resembles a Gaussian profile. The bottom row shows the resulting QAM-like two-dimensional constellations formed by taking the Cartesian product of two independent one-dimensional Gauss–Hermite constellations, corresponding to statistically independent quadratures.



(**a**) (**b**)

Figure 2. (**a**) Visual representation of the action of an nG quantum channel on an nG quantum state according to Proposition 1. The set $Conv(\mathcal{G}_s)$ is the convex hull of $\mathcal{G}_s$. (**b**) Values of the QRE-nG for the GH-QAM constellation with m points per quadrature under a phase diffusion process with fixed modulation variance $\bar{m} = 2.5$ and increasing constellation size. The upper line (blue) corresponds to the constellation nG before the channel and in the constellation under the process with parameters $\kappa = 0.15$ and $\kappa = \infty$, respectively.

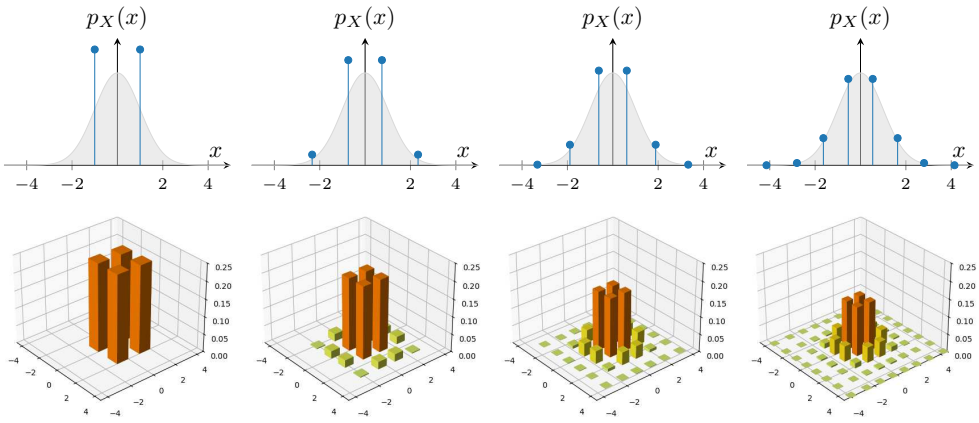


Figure 3. Constellations resulting from the Hermite polynomials of Equation (13) with $n \in \{2, 4, 6, 8\}$. On top, the roots and weights of $H_n(x)$ form the probability distribution $p_X(x)$. At the bottom, the corresponding QAM-like constellations obtained by the Cartesian product are shown.

Figure 2b shows the numerical results for the computation of the QRE-based non-Gaussianity of QAM-like constellations, with each axis following a Gauss–Hermite distribution and undergoing a phase diffusion process. The upper blue line corresponds to the QRE-nG measure for the constellations before the phase diffusion process takes place. The lines below represent the calculated $\delta_{vN}(\mathcal{N}_\kappa(\hat{\rho}_{X_n}))$ for $\kappa = 0.15$ (red line) and $\kappa = \infty$ (green line), the latter having the effect of total decoherence in the mixture of coherent states, which destroys the off-diagonal elements in the density matrix. The occasional observed fluctuations near the left end of the plot (low values of n) for the red and green lines can be attributed to the action of the non-Gaussian process, which can map the ensemble of input states to output states with a slightly varying non-Gaussianity reducing rate when the constellation size is still small. After approximately seven states per quadrature, the output-state non-Gaussianity transitions to a clear exponential decay as expected.

As expected, since the Gauss–Hermite distribution converges exponentially to a Gaussian shape, the QRE-based non-Gaussianity also decreases exponentially as the constellation grows. Concerning the action of $\mathcal{N}_\kappa$, two points can be highlighted: First, the bigger the

diffusion parameter κ gets, the lower the constellation non-Gaussianity after the channel is, which is related to the counterintuitive fact that $\mathcal{N}_\kappa$ maps to a convex mixture of nG states that is more Gaussian than the mixed state before it. The second is that the effect of undergoing the nG evolution becomes less significant (in the sense of reducing the state non-Gaussianity) as the mixture becomes more Gaussian-like. For example, if we compute the input–output non-Gaussianity difference $\delta_{vN}(\hat{\rho}_{X_n}) - \delta_{vN}(\mathcal{N}_\kappa(\hat{\rho}_{X_n}))$, with $\kappa = 0.15$, one has that it is $\approx 2.4 \times 10^{-3}$ for $n = 10$ and goes to $\approx 4.8 \times 10^{-6}$ for $n = 20$. This is somehow expected because thermal states commute with the Krauss operators representing the phase diffusion evolution, meaning that as $\hat{\rho}_{X_n}$ becomes "more Gaussian", $\mathcal{N}_\kappa$ has less effect on it.

4. Discussion: Application to QKD Protocols

The basic operation of a QKD protocol can be divided into four main stages: (i) quantum state preparation, transmission, and detection; (ii) classical parameter estimation; (iii) information reconciliation; and (iv) privacy amplification. A QKD protocol that applies discrete modulation—i.e., uses a constellation of symbols—to the quadratures of continuous-variable quantum systems, such as coherent states, is referred to as a DM-CVQKD protocol. The coherent states are prepared with amplitudes drawn from a random variable, transmitted and detected by either a single- or a double-homodyne receiver. The resulting shared sequences—the input data used to modulate the coherent states and the detection outcomes—are called the raw key and should be used to distill a secret random sequence given that they present enough correlation, which is evaluated by the parameter estimation stage under a specific security model. After that, error correction is performed by some information reconciliation protocol, and the eavesdropper information is removed by privacy amplification.

Finding the worst-case eavesdropping strategy is a crucial step towards proving the security of a QKD protocol. For the class of Gaussian-modulated protocols with continuous variables, such as the GG02, the no-switching, and the unidimensional protocols [19–21], the optimality of Gaussian attacks is a pivotal result simplifying the security analysis: if the protocol is based on a Gaussian modulation of coherent states (this means that Alice will transmit coherent states whose amplitudes are drawn from a circular Gaussian distribution, or equivalently, the amplitude on each quadrature is drawn from independent and equally distributed Gaussian random variables), the best Eve can do is to perform the "entangling cloner attack", which is equivalent to a Gaussian quantum channel with transmittance τ and excess noise ξ [22–25]. The consequence is that Alice and Bob can safely assume the Gaussian channel model in the security analysis.

The problem completely changes when Alice applies a discrete modulation. In this case, it is not guaranteed that Gaussian attacks are optimal, and the security analysis must include nG quantum channels compatible with the parameters observed in the classical data for computing the eavesdropper's information [12]. This means that Alice and Bob must estimate the channel parameters τ and ξ using their classical data and compute the eavesdropper information for the *worst-case scenario*, considering any type of quantum channel resulting in the estimated parameters. This reduces to the known Devetak–Winter formula for the secret key rate in the asymptotic scenario:

$$K = \beta I(A;B) - \sup_{\mathcal{N} \in \mathcal{Q}} \chi(B;E), \tag{15}$$

where β is the efficiency of information reconciliation, $I(A;B)$ is the classical mutual information of Alice and Bob's raw keys, and $\chi(E,B)$ is the eavesdropper's accessible information during quantum communication considering reverse reconciliation. In this type of reconciliation, error correction is performed by taking as reference the receiver's

sequence so that Alice has to modify her sequence towards Bob's one, differently from a classical communication task. This maneuver allows the protocol to be able to establish secret keys beyond the 3 dB loss limit.

In Section 3, it was shown that the phase diffusion process preserves the monotone property of the QRE-nG when restricted to an appropriate set of quantum states. Additionally, it does not modify the covariance matrix of the input state. Both statements can be used in the analysis of DM-CVQKD protocols by proposing the following arrangement to decompose the quantum channels considered in the security analysis. Denote by $\mathcal{T}$ the set of quantum channels that preserve the first and second moments of any quantum state in $\mathcal{S}_{\bar{0}}$. Without loss of generality, assume that Alice and Bob are linked by $\mathcal{N} = \mathcal{N}_2 \circ \mathcal{N}_1$, as depicted in Figure 4, where $\mathcal{N}_1 \in \mathcal{T}$ and $\mathcal{N}_2 \in \mathcal{G}_s$ is a thermal-loss channel with transmittance τ and excess noise ξ.

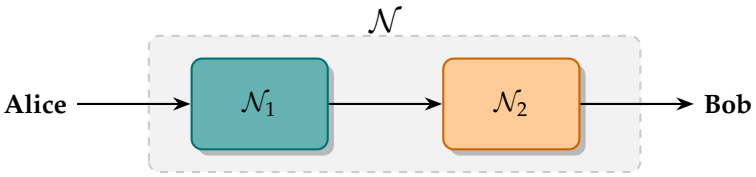


Figure 4. Representation of the proposed quantum channel decomposition. The channel $\mathcal{N}$ connecting Alice and Bob is split into a thermal-loss part $\mathcal{N}_1$ and a non-Gaussian evolution N_2. Alice and Bob reconstruct the covariance matrix by estimating the parameters yielded by $\mathcal{N}_1$. Any security analysis that goes beyond considering Gaussian channels should then quantify the effect of $\mathcal{N}_2$ during quantum communication.

The idea here is to decompose the quantum channel into two parts, the Gaussian $\mathcal{N}_2$ yielding physical parameters in a practical deployment of a QKD protocol, raising the observed parameters τ and ξ, and $\mathcal{N}_1$, which does not modify the covariance matrix (and then does not affect the parameter estimation) but is responsible for non-Gaussian interactions giving more information to the eavesdropper. Such decomposition may allow more accurate lower bounds to the secret key rate by performing a more efficient computation of the eavesdropper's information in security analysis.

Take as an example the security analysis of [12]. Its main objective was to analytically deduce a correction factor for the covariance matrix describing the bipartite state on a DM-CVQKD protocol. When restricting the problem to a linear Gaussian channel, the corrected off-diagonal therm $Z(\tau, \xi)$ of Γ is

$$Z(\tau, \xi) = 2\sqrt{T}\,\mathrm{tr}\left(\hat{\rho}^{1/2}\hat{a}\hat{\rho}^{1/2}a^{\dagger}\right) - \sqrt{2T\xi w}, \tag{16}$$

with $\hat{a}$ and $\hat{a}^{\dagger}$ being the field annihilation and creation operators, respectively; $w := \sum_k p_k(\langle\alpha_k|\hat{a}_{\rho}^{\dagger}\hat{a}_{\rho}|\alpha_k\rangle - |\langle\alpha_k|\hat{a}_{\rho}|\alpha_k\rangle|^2)$ and $\hat{a}_{\rho} = \hat{\rho}^{1/2}\hat{a}\hat{\rho}^{-1/2}a^{\dagger}$. Such a correction factor works as a penalty for describing an nG state with just its second moment. One could extend the analysis by relating its results for arbitrary channels to the minimization of the output-state QRE non-Gaussianity measure, which is also related to a penalty due to nG modulation [15], subject to the empirical constraints estimated on a practical protocol: channel parameters and the expected covariance. This yields a rigorous lower bound on the protocol by estimating the effects of the channel's non-Gaussianity, without the need for knowing upfront which nG quantum channel connects Alice and Bob. The resulting operational framework fits naturally into DM-CVQKD protocols where these quantities are already monitored, enabling practical application of our theoretical results and facilitating tighter security bounds when non-Gaussianity is empirically small.

5. Conclusions

We explored the conditions under which a non-Gaussian quantum channel reduces the amount of non-Gaussianity of a quantum channel using the quantum relative entropy as a quantifying function. We proposed the functional $\Delta(\mathcal{N}, \hat{\rho})$ that can be used to classify the channel $\mathcal{N}$ as Gaussian or non-Gaussian. Based on $\Delta(\mathcal{N}, \hat{\rho})$, we developed a condition under which a non-Gaussian channel reduces the non-Gaussianity of its input states. This result extends the monotone decreasing property of the quantum relative entropy-based non-Gaussianity measure to outside the Gaussian sector of quantum operations.

The characterization of non-Gaussian channels that reduce the non-Gaussianity of input states was used to establish a link between the security analysis of CVQKD protocols and the class of non-Gaussianity-reducing quantum channels. A decomposition of the general channels considered in the security analysis of CVQKD was proposed, with operational implications. It is still an open problem how this decomposition can improve the secret key rate bounds computed with today's security analysis framework. In addition, it may be possible that this decomposition can be used to improve parameter estimation procedures.

Future work can also be concentrated on generalizing Proposition 1 and developing the properties of $\Delta(\mathcal{N}, \hat{\rho})$. In addition, it should be noted that the difference $S(\hat{\rho}||\hat{\rho}^G) - S(\mathcal{N}(\hat{\rho})||\mathcal{N}(\hat{\rho}^G))$ (see the proof of Theorem 1) is related to state recovery maps (Petz recovery maps), which are maps that can recover the state that suffered some physical evolution. Such recovery maps can be extended to quantum systems in infinite dimensions [26] and may have connections with the "production of non-Gaussianity" and with CVQKD security analysis.

Author Contributions: Writing—original draft preparation, M.A.D.; writing—review and editing, M.A.D. and F.M.d.A. All authors have read and agreed to the published version of the manuscript.

Funding: This work has been partially funded by the project QIN-AFCCT-2025-4-16-3 "Analysis and development of distribution matching algorithms for CV-QKD" supported by QuIIN—Quantum Industrial Innovation, EMBRAPII CIMATEC Competence Center in Quantum Technologies, with financial resources from the PPI IoT/Manufatura 4.0 of the MCTI grant number 053/2023, signed with EMBRAPII; the National Council for Scientific and Technological Development (CNPq) under research Grant No. 311680/2022-4; the Coordination of Superior Level Staff Improvement (CAPES/PROEX) under research Grant No. 88887.014949/2024-00; and by EU HORIZON 2023 Marie Skłodowska-Curie Actions Postdoctoral Fellowships under project number 101153602 (COCoVaQ).

Institutional Review Board Statement: Not applicable.

Data Availability Statement: The original contributions presented in this study are included in the article. Further inquiries can be directed to the corresponding author.

Conflicts of Interest: The authors declare no conflicts of interest.

Appendix A. The Phase Diffusion Process

One of the most harmful noisy processes in quantum information is one that provokes decoherence, where quantum states lose their "quantumness"—full decohered states reduce to mixtures of orthogonal states which can be perfectly distinguished. Some open-system processes result in random changes in the relative phase of the states that are in superposition in the main quantum system. Such a relative phase fluctuation results in a loss of coherence and is called phase damping or phase diffusion [27].

The single-mode evolution of the system under such a process can be described by the master equation [11,28]:

$$\frac{\mathrm{d}}{\mathrm{d}t}\hat{\rho} = \Gamma\mathcal{L}[\hat{a}^\dagger\hat{a}]\hat{\rho}, \tag{A1}$$

where $\mathcal{L}[\hat{O}]\hat{\rho} = 2\hat{O}^\dagger\hat{\rho}\hat{O} - \hat{O}^\dagger\hat{O}\hat{\rho} - \hat{\rho}\hat{O}^\dagger\hat{O}$, or as the Hamiltonian of a harmonic oscillator open to an N mode environment [27]:

$$H = \hbar\omega\hat{a}^\dagger\hat{a} + \hbar\sum_{i=1}^{N}\omega_i\hat{a}_i^\dagger\hat{a}_i + \hbar\sum_{i=1}^{N}\chi_i\hat{a}^\dagger\hat{a}(\hat{a}_i + \hat{a}_i^\dagger), \tag{A2}$$

where $\hat{a}$ and $\hat{a}^\dagger$ are the annihilation and creation operators of the main system with frequency ω, and $\hat{a}_i$ and $\hat{a}_i^\dagger$ refer to the ith environment system with frequency ω_i. The quantity χ_i represents a coupling parameter between the main system and the ith environment mode.

This non-Gaussian evolution of a quantum state is an important source of noise in optical communication links. Its Krauss operator set $\{P_k(t)\}$, $0 \le k \le \infty$ has elements

$$P_k(t) = \sum_{n=0}^{\infty} e^{-\frac{1}{2}n^2\lambda^2}\sqrt{\frac{(n^2\lambda^2)^k}{k!}}|n\rangle\langle n| \tag{A3}$$

where $\lambda = t\sqrt{\Lambda}$ and $\Lambda = \sum_i \chi_i^2\sqrt{1 - e^{-n^2\lambda^2}}$.

Regarding the effect of phase diffusion on Gaussian states, the thermal state with average photon number $\bar{n}$, $\hat{\rho}^{th}(\bar{n})$, is invariant under the phase diffusion process state, since both $\bar{n}$ and $P_k(t)$ are diagonal in the same basis. For coherent states, it is well known that they are sensitive to relative phase fluctuations: for a coherent state $|\alpha\rangle$ with arbitrary α, one has

$$\mathcal{N}_\kappa(|\alpha\rangle\langle\alpha|) = e^{-|\alpha|^2}\sum_{m,n=0}^{\infty}\exp\left\{-\kappa^2(n-m)^2\right\} \times \frac{\alpha^n\alpha^{*m}}{\sqrt{n!m!}}|n\rangle\langle m|, \tag{A4}$$

which is a non-Gaussian mixed state with $\kappa = \lambda^2/2$.

In contrast to thermal states, coherent states suffer from decoherence in a phase diffusion evolution, with the off-diagonal elements of the density operator being more affected as the noise parameter κ becomes larger.

Now, consider the mixtures of coherent states as defined in Section 3 by the set $\mathcal{S}_0$. Denote a constellation by the set of complex amplitudes $\{\alpha_i\}$ with associated probabilities $\{p_i\}$. Also, by symmetry, $\sum p_i\alpha_i = 0$, and let $\bar{m} = \sum p_i|\alpha_i|^2$ be the modulation variance. Represent the constellation of coherent state by $\hat{\rho} = \sum_i p_i|\alpha_i\rangle\langle\alpha_i|$, and denote $\hat{\rho}_\kappa = \mathcal{N}_\kappa(\hat{\rho})$. Due to the linearity of the channel, we use (A4) directly and have

$$\hat{\rho}_\kappa = \sum_{m,n=0}^{\infty} e^{-\kappa^2(n-m)^2}\sum_{i=0}^{N} p_i e^{-|\alpha_i|^2}\frac{\alpha_i^n\alpha_i^{*m}}{\sqrt{n!m!}}|n\rangle\langle m|. \tag{A5}$$

Clearly, as each coherent state is transformed into an nG mixed state, the resultant mixture will also be nG, although in contrast to a single coherent state, a symmetric convex mixture has the first and second moments invariant under phase diffusion, that is,

$$\mathrm{tr}(\hat{q}\hat{\rho}_\kappa) = \mathrm{tr}(\hat{p}\hat{\rho}_\kappa) = 0, \tag{A6}$$

and

$$\mathbf{\Gamma} = \begin{pmatrix} 1+2\bar{m} & 0 \\ 0 & 1+2\bar{m} \end{pmatrix} \tag{A7}$$

so that $\mathbf{\Gamma}(\hat{\rho}_\kappa) = \mathbf{\Gamma}(\hat{\rho})$.

References

1. Chitambar, E.; Gour, G. Quantum Resource Theories. *Rev. Mod. Phys.* **2019**, *91*, 025001. [CrossRef]
2. Zhuang, Q.; Shor, P.W.; Shapiro, J.H. Resource Theory of Non-Gaussian Operations. *Phys. Rev. A* **2018**, *97*, 052317. [CrossRef]
3. Takagi, R.; Zhuang, Q. Convex Resource Theory of Non-Gaussianity. *Phys. Rev. A* **2018**, *97*, 062337. [CrossRef]
4. Marian, P.; Marian, T.A. Relative Entropy Is an Exact Measure of Non-Gaussianity. *Phys. Rev. A* **2013**, *88*, 012322. [CrossRef]
5. Genoni, M.G.; Paris, M.G.A.; Banaszek, K. Measure of the Non-Gaussian Character of a Quantum State. *Phys. Rev. A* **2007**, *76*, 042327. [CrossRef]
6. Genoni, M.G.; Paris, M.G.A.; Banaszek, K. Quantifying the Non-Gaussian Character of a Quantum State by Quantum Relative Entropy. *Phys. Rev. A* **2008**, *78*, 060303. [CrossRef]
7. Fiurášek, J. Gaussian Transformations and Distillation of Entangled Gaussian States. *Phys. Rev. Lett.* **2002**, *89*, 137904. [CrossRef]
8. Giedke, G.; Ignacio Cirac, J. Characterization of Gaussian Operations and Distillation of Gaussian States. *Phys. Rev. A* **2002**, *66*, 032316. [CrossRef]
9. Niset, J.; Fiurášek, J.; Cerf, N.J. No-Go Theorem for Gaussian Quantum Error Correction. *Phys. Rev. Lett.* **2009**, *102*, 120501. [CrossRef]
10. Ralph, T.C.; Gilchrist, A.; Milburn, G.J.; Munro, W.J.; Glancy, S. Quantum Computation with Optical Coherent States. *Phys. Rev. A* **2003**, *68*, 042319. [CrossRef]
11. Genoni, M.G.; Paris, M.G.A. Quantifying Non-Gaussianity for Quantum Information. *Phys. Rev. A* **2010**, *82*, 052341. [CrossRef]
12. Denys, A.; Brown, P.; Leverrier, A. Explicit Asymptotic Secret Key Rate of Continuous-Variable Quantum Key Distribution with an Arbitrary Modulation. *Quantum* **2021**, *5*, 540. [CrossRef]
13. Lin, J.; Upadhyaya, T.; Lütkenhaus, N. Asymptotic Security Analysis of Discrete-Modulated Continuous-Variable Quantum Key Distribution. *Phys. Rev. X* **2019**, *9*, 041064. [CrossRef]
14. Liu, W.B.; Li, C.L.; Xie, Y.M.; Weng, C.X.; Gu, J.; Cao, X.Y.; Lu, Y.S.; Li, B.H.; Yin, H.L.; Chen, Z.B. Homodyne Detection Quadrature Phase Shift Keying Continuous-Variable Quantum Key Distribution with High Excess Noise Tolerance. *PRX Quantum* **2021**, *2*, 040334. [CrossRef]
15. Dias, M.A.; Assis, F.M. Converging State Distributions for Discrete Modulated CVQKD Protocols. *arXiv* **2023**, arXiv:2305.06484.
16. Wilde, M.M. *Quantum Information Theory*, 2nd ed.; Cambridge University Press: Cambridge, UK, 2017.
17. Holevo, A.S.; Sohma, M.; Hirota, O. Capacity of Quantum Gaussian Channels. *Phys. Rev. A* **1999**, *59*, 1820–1828. [CrossRef]
18. Wu, Y.; Verdú, S. The Impact of Constellation Cardinality on Gaussian Channel Capacity. In Proceedings of the 2010 48th Annual Allerton Conference on Communication, Control, and Computing (Allerton 2010), Monticello, IL, USA, 29 September–1 October 2010; pp. 620–628. [CrossRef]
19. Grosshans, F.; Grangier, P. Continuous Variable Quantum Cryptography Using Coherent States. *Phys. Rev. Lett.* **2002**, *88*, 57902. [CrossRef]
20. Weedbrook, C.; Lance, A.M.; Bowen, W.P.; Symul, T.; Ralph, T.C.; Lam, P.K. Quantum Cryptography without Switching. *Phys. Rev. Lett.* **2004**, *93*, 170504. [CrossRef]
21. Usenko, V.C.; Grosshans, F. Unidimensional Continuous-Variable Quantum Key Distribution. *Phys. Rev. A* **2015**, *92*, 062337. [CrossRef]
22. Cerf, N.J.; Leuchs, G.; Polzik, E.S. *Quantum Information with Continuous Variables of Atoms and Light*; Imperial College Press (ICP): London, UK, 2007. [CrossRef]
23. Wolf, M.M.; Giedke, G.; Cirac, J.I. Extremality of Gaussian Quantum States. *Phys. Rev. Lett.* **2006**, *96*, 080502. [CrossRef]
24. García-Patrón, R.; Cerf, N.J. Unconditional Optimality of Gaussian Attacks against Continuous-Variable Quantum Key Distribution. *Phys. Rev. Lett.* **2006**, *97*, 190503. [CrossRef] [PubMed]
25. Navascués, M.; Grosshans, F.; Acín, A. Optimality of Gaussian Attacks in Continuous-Variable Quantum Cryptography. *Phys. Rev. Lett.* **2006**, *97*, 190502. [CrossRef] [PubMed]
26. Junge, M.; Renner, R.; Sutter, D.; Wilde, M.M.; Winter, A. Universal Recovery Maps and Approximate Sufficiency of Quantum Relative Entropy. *Ann. Henri Poincaré* **2018**, *19*, 2955–2978. [CrossRef]
27. Liu, Y.x.; Özdemir, S.K.; Miranowicz, A.; Imoto, N. Kraus Representation of a Damped Harmonic Oscillator and Its Application. *Phys. Rev. A* **2004**, *70*, 042308. [CrossRef]
28. Memarzadeh, L.; Mancini, S. Minimum Output Entropy of a Non-Gaussian Quantum Channel. *Phys. Rev. A* **2016**, *94*, 022341. [CrossRef]