Gaussian Quantum Information

Christian Weedbrook

Center for Quantum Information and Quantum Control, Department of Electrical and Computer Engineering and Department of Physics, University of Toronto, Toronto, M5S 3G4, Canada and
Research Laboratory of Electronics, Massachusetts Institute of Technology, Cambridge MA 02139, USA

Stefano Pirandola

Department of Computer Science, University of York, Deramore Lane, York YO10 5GH, United Kingdom

Raúl García-Patrón

Research Laboratory of Electronics, Massachusetts Institute of Technology, Cambridge MA 02139, USA and Max-Planck-Institut für Quantenoptik, Hans-Kopfermann-Strasse 1, Garching, D-85748, Germany

Nicolas J. Cerf

Quantum Information and Communication, Ecole Polytechnique, Université Libre de Bruxelles, 1050 Brussels, Belgium and
Research Laboratory of Electronics, Massachusetts Institute of Technology, Cambridge MA 02139, USA

Timothy C. Ralph

Centre for Quantum Computation and Communication Technology, Department of Physics, University of Queensland, Brisbane, Queensland 4072, Australia

Jeffrey H. Shapiro

Research Laboratory of Electronics, Massachusetts Institute of Technology, Cambridge MA 02139, USA

Seth Lloyd

Research Laboratory of Electronics, Massachusetts Institute of Technology, Cambridge MA 02139, USA and Department of Mechanical Engineering, Massachusetts Institute of Technology, Cambridge MA 02139, USA

(Dated: November 27, 2024)

The science of quantum information has arisen over the last two decades centered on the manipulation of individual quanta of information, known as quantum bits or qubits. Quantum computers, quantum cryptography and quantum teleportation are among the most celebrated ideas that have emerged from this new field. It was realized later on that using continuous-variable quantum information carriers, instead of qubits, constitutes an extremely powerful alternative approach to quantum information processing. This review focuses on continuous-variable quantum information processes that rely on any combination of Gaussian states, Gaussian operations, and Gaussian measurements. Interestingly, such a restriction to the Gaussian realm comes with various benefits, since on the theoretical side, simple analytical tools are available and, on the experimental side, optical components effecting Gaussian processes are readily available in the laboratory. Yet, Gaussian quantum information processing opens the way to a wide variety of tasks and applications, including quantum communication, quantum cryptography, quantum computation, quantum teleportation, and quantum state and channel discrimination. This review reports on the state of the art in this field, ranging from the basic theoretical tools and landmark experimental realizations to the most recent successful developments.

Contents

I. INTRODUCTION

Quantum mechanics is the branch of physics that studies how the universe behaves at its smallest and most fundamental level. Quantum computers and quantum communication systems transform and transmit information using systems such as atoms and photons whose behavior is intrinsically quantum mechanical. As the size of components of computers and the number of photons used to transmit information has pressed downwards to the quantum regime, the study of quantum information processing has potential practical relevance. Moreover, the strange and counterintuitive features of quantum mechanics translate into novel methods for information processing that have no classical analogue. Over the past two decades, a detailed theory of quantum information processing has developed, and prototype quantum computers and quantum communication systems have been constructed and tested experimentally. Simple quantum algorithms have been performed, and a wide variety of quantum communication protocols have been demonstrated, including quantum teleportation and quantum cryptography.

Quantum information comes in two forms, *discrete* and *continuous*. The best-known example of discrete quantum information is the quantum bit or 'qubit', a quantum system with two distinguishable states. Examples of quantum systems that can be used to register a qubit are spin $1/2$ particles such as electrons and many nuclear spins, the two lowest energy states of semiconductor quantum dots or quantized superconducting circuits, and the two polarization states of a single photon. The best-known example of continuous quantum information (Andersen *et al.*, 2010; Braunstein and Pati, 2003; Braunstein and van Loock, 2005; Cerf *et al.*, 2007) is the quantized harmonic oscillator, which can be described by continuous variables such as position and momentum (an alternative description is the discrete but infinite-dimensional representation in terms of energy states). Examples of continuous-variable quantum systems include quantized modes of bosonic systems such as the different degrees of freedom of the electromagnetic field, vibrational modes of solids, atomic ensembles, nuclear spins in a quantum dot, Josephson junctions, and Bose-Einstein condensates. Because they supply the quantum description of the propagating electromagnetic field, continuous-variable quantum systems are particularly relevant for quantum communication and quantum-limited techniques for sensing, detection and imaging. Similarly, atomic or solid-state based encoding of continuous-variable systems can be used to perform quantum computation. Bosonic systems are not only useful in the physical modeling of qubit-based quantum computation, e.g., the quantized vibrational modes of ions embody the medium of communication between qubits in ion-trap quantum computers, but also allows for new approaches to quantum computa-

tion.

A. Gaussian quantum information processing

This review reports on the state of the art of quantum information processing using continuous variables. The primary tools for analyzing continuous-variable quantum information processing are Gaussian states and Gaussian transformations. Gaussian states are continuous-variable states that have a representation in terms of Gaussian functions, and Gaussian transformations are those that take Gaussian states to Gaussian states. In addition to offering an easy description in terms of Gaussian functions, Gaussian states and transformations are of great practical relevance. The ground state and thermal states of bosonic systems are Gaussian, as are states created from such states by linear amplification and loss. Frequently, nonlinear operations can be approximated to a high degree of accuracy by Gaussian transformations. For example, squeezing is a process that decreases the variance of one continuous variable (position or electric field, for example) while increasing the variance of the conjugate variable (momentum or magnetic field). Linear squeezing is Gaussian, and nonlinear squeezing can typically be approximated to first order by a linear, Gaussian process. Moreover, any transformation of a continuous-variable state can be built up by Gaussian processes together with a repeated application of a single nonlinear process such as photodetection.

In reviewing the basic facts of Gaussian quantum information processing (Braunstein and Pati, 2003; Braunstein and van Loock, 2005; Eisert and Plenio, 2003; Ferraro *et al.*, 2005) and in reporting recent developments, we have attempted to present results in a way that is accessible to two communities. Members of the quantum optics and atomic physics communities are very familiar with the basic aspects of Gaussian quantum states and transformations, but may be less acquainted with the application of Gaussian techniques to quantum computation, quantum cryptography, and quantum communication. Members of the quantum information community are familiar with quantum information processing techniques such as quantum teleportation, quantum algorithms, and quantum error correction, but may have less experience in the continuous-variable versions of these protocols, which exhibit a range of features that do not arise in their discrete versions.

The review is self-contained in the sense that study of the introductory material should suffice to follow the detailed derivations of more advanced methods of Gaussian quantum information processing presented in the body of the paper. Finally, the review supplies a comprehensive set of references both to the foundations of the field of Gaussian quantum information processing, and to recent developments.

B. Outline of review

The large subject matter and page length limit means that this review will take a mostly theoretical approach to Gaussian quantum information. In particular, we focus on *optical* Gaussian protocols as they are the natural choice of medium for a lot of the protocols presented in this review. However, we do make mention of Gaussian atomic ensemble protocols (Hammerer *et al.*, 2010) due to the close correspondence between continuous variables for light and atomic ensembles. Furthermore, experiments (both optical and atomic) will be mentioned and cited where appropriate. We also note that fermionic Gaussian states have also been studied in the literature (e.g., see (Bravyi, 2005; Di Vincenzo and Terhal, 2005; Eisert *et al.*, 2010)) but are outside the scope of this review. We limit our discussion of entanglement, quantum teleportation, quantum cloning, and quantum dense coding as these have all been discussed in detail previously, e.g., see Braunstein and van Loock (2005). On the other hand, we give a detailed account of bosonic quantum channels, continuous-variable quantum cryptography and quantum computation.

We begin in Sec. II by introducing the fundamental theoretical concepts of Gaussian quantum information. This includes Gaussian states and their phase-space representations and symplectic structure, along with Gaussian unitaries, which are the simplest quantum operations transforming Gaussian states into Gaussian states. We then give examples of both Gaussian states and Gaussian unitaries. Multimode Gaussian states are discussed next using powerful techniques based on the manipulation of the second-order statistical moments. The quantum entanglement of bipartite Gaussian states is presented with the various measures associated with it. We end this section by introducing the basic models of measurement, such as homodyne detection, heterodyne detection and direct detection.

In Sec. III we begin to go more deeply into Gaussian quantum information processing via the process of distinguishing between Gaussian states. We present general bounds and measures of distinguishability, and discuss specific models for discriminating between optical coherent states. In Sec. IV we introduce basic Gaussian quantum information processing protocols including quantum teleportation and quantum cloning.

In Sec. V we review bosonic communication channels which is one of the fundamental areas of research in quantum information. Bosonic channels include communication by electromagnetic waves (e.g., radio waves, microwaves, and visible light), with Gaussian quantum channels being the most important example. These channels represent the standard model of noise in many quantum information protocols as well as being a good approximation to current optical telecommunication schemes. We begin by first reviewing the general formalisms and chief properties of bosonic channels, and specifically, those of Gaussian channels. This naturally leads to the study of the important class of one-mode Gaussian channels. The established notions of Gaussian channel capacity, both the classical and quantum versions, are presented next. Next up is entanglement-assisted classical capacity with quantum dense coding being a well-known example. This is followed by the concepts of entanglement distribution over noisy Gaussian channels and secret-key capacities. Finally, we end with the discrimination of quantum channels and the protocols of quantum illumination and quantum reading.

The state of the art in the burgeoning field of continuous-

variable quantum cryptography is presented in Sec. VI. We begin by introducing how a generic quantum cryptographic scheme works followed by examples of the most commonly studied protocols. We then consider aspects of their security including what it means to be secure along with the main types of eavesdropping attacks. We continue with the practical situation of finite-size keys and the optimality and full characterization of collective Gaussian attacks before deriving the secret-key rates for the aforementioned protocols. We conclude with a discussion on the future avenues of research in continuous-variable quantum cryptography.

In Sec. VII we review the most recent of the continuous-variable quantum information protocols, namely, quantum computation using continuous-variable cluster states. We begin by listing the most commonly used continuous-variable gates and by discussing the Lloyd-Braunstein criterion which provides the necessary and sufficient conditions for gates to form a universal set. The basic idea of one-way quantum computation using continuous variables is discussed next with teleportation providing an elegant way of understanding how computations can be achieved using only measurements. A common and convenient way of describing cluster states, via graph states and the nullifier formalism, is presented. Next, we consider the practical situations of Gaussian computational errors along with the various optical implementations of Gaussian cluster states. This leads into a discussion on how to incorporate universal quantum computation and quantum error correction into the framework of continuous-variable cluster state quantum computation. We end by introducing two quantum computational algorithms and provide directions for future research. In Sec. VIII, we offer perspectives and concluding remarks.

C. Further readings

For additional readings, perhaps the first place to start for an overview of continuous-variable quantum information is the well-known review article by Braunstein and van Loock (2005). Furthermore, there is also the recent review by Andersen *et al.* (2010) as well as two edited books on the subject by Braunstein and Pati (2003) and Cerf *et al.* (2007). On Gaussian quantum information specifically there is the review article by Wang *et al.* (2007) and the lecture notes of Ferraro *et al.* (2005). For a quantum optics (Bachor and Ralph, 2004; Gerry and Knight, 2005; Leonhardt, 2010) approach to quantum information see the textbooks by Walls and Milburn (2008), Kok and Lovett (2010) and Furusawa and van Loock (2011) (who provide a joint theoretical and experimental point of view). Whilst, the current state of the art of continuous variables using atomic ensembles can be found in the review article of Hammerer *et al.* (2010). For a detailed treatment of Gaussian systems see the textbook by Holevo (2011). An overview of Gaussian entanglement is presented in the review of Eisert and Plenio (2003). For an elementary introduction to Gaussian quantum channels, see Eisert and Wolf (2007), and for continuous-variable quantum cryptography, see the reviews of Scarani *et al.* (2009) and Cerf and Grangier (2007). Cluster state quantum computation using continuous variables is treated in the books of Kok and Lovett (2010) and Furusawa and van Loock (2011).

D. Comment on notation

Throughout this review, the variance of the vacuum noise is normalized to 1. Such a normalization is commonly and conveniently thought of as setting Planck's constant $\hbar$ to a particular value, in our case $\hbar = 2$. Currently, in continuous-variable quantum information there is no general consensus about the value of the variance of the vacuum, with common choices being either $1/4$ ($\hbar = 1/2$), $1/2$ ($\hbar = 1$) or 1. This is important to point out to the reader who, when referring to the many references in this review, should be aware that different papers use different choices of normalization. Another nomenclature issue in the literature is the notation used to define the quadrature operators (and the corresponding eigenvalues). Here we define the 'position' quadrature by $\hat{q}$ and the 'momentum' quadrature by $\hat{p}$. In this review, the logarithm ($\log$) can be taken to be base 2 for bits or ln for nats. $\mathbf{I}$ represents the identity matrix which may be 2×2 (for one mode) or $2N \times 2N$ (for arbitrary N modes). The correct dimensions, if not specified, can be deducted from the context. Since we deal with continuous variables, we can have both discrete and continuous ensembles of states, measurement operators, etcetera. In order to keep the notation as simple as possible, in some parts we consider discrete ensembles. It is understood that the extension to continuous ensembles involves the replacement of sums by integrals. Finally, integrals are taken from $-\infty$ to $+\infty$ unless otherwise stated.

II. ELEMENTS OF GAUSSIAN QUANTUM INFORMATION THEORY

A. Bosonic systems in a nutshell

A quantum system is called a *continuous-variable system* when it has an infinite-dimensional Hilbert space described by observables with continuous eigenspectra. The prototype of a continuous-variable system is represented by N bosonic modes, corresponding to N quantized radiation modes of the electromagnetic field, i.e., N quantum harmonic oscillators. In general, N bosonic modes are associated with a tensor-product Hilbert space $\mathcal{H}^{\otimes N} = \otimes_{k=1}^{N}\mathcal{H}_k$ and corresponding N pairs of bosonic field operators $\{\hat{a}_k, \hat{a}_k^\dagger\}_{k=1}^N$, which are called the annihilation and creation operators, respectively. These operators can be arranged in a vectorial operator $\hat{\mathbf{b}} := (\hat{a}_1, \hat{a}_1^\dagger, \cdots, \hat{a}_N, \hat{a}_N^\dagger)^T$, which must satisfy the bosonic commutation relations

$$[\hat{b}_i, \hat{b}_j] = \Omega_{ij}\ ,\ (i,j = 1, \cdots, 2N) \tag{1}$$

where Ω_{ij} is the generic element of the $2N \times 2N$ matrix

$$\mathbf{\Omega} := \bigoplus_{k=1}^{N} \boldsymbol{\omega} = \begin{pmatrix} \boldsymbol{\omega} & & \\ & \ddots & \\ & & \boldsymbol{\omega} \end{pmatrix} \quad \boldsymbol{\omega} := \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}, \tag{2}$$

known as the symplectic form. The Hilbert space of this system is separable and infinite-dimensional. This is because the single-mode Hilbert space $\mathcal{H}$ is spanned by a countable basis $\{|n\rangle\}_{n=0}^{\infty}$, called the Fock or number state basis, which is composed by the eigenstates of the number operator $\hat{n} := \hat{a}^{\dagger}\hat{a}$, i.e., $\hat{n}\,|n\rangle = n\,|n\rangle$. Over these states the action of the bosonic operators is well-defined, being determined by the bosonic commutation relations. In particular, we have

$$\hat{a}\,|0\rangle = 0, \quad \hat{a}\,|n\rangle = \sqrt{n}\,|n-1\rangle \ \ (\text{for } n \geq 1), \tag{3}$$

and

$$\hat{a}^{\dagger}\,|n\rangle = \sqrt{n+1}\,|n+1\rangle \ \ (\text{for } n \geq 0). \tag{4}$$

Besides the bosonic field operators, the bosonic system may be described by another kind of field operators. These are the quadrature field operators $\{\hat{q}_k, \hat{p}_k\}_{k=1}^{N}$, formally arranged in the vector

$$\hat{\mathbf{x}} := (\hat{q}_1, \hat{p}_1, \ldots, \hat{q}_N, \hat{p}_N)^T. \tag{5}$$

These operators derive from the cartesian decomposition of the bosonic field operators, i.e., $\hat{a}_k := \frac{1}{2}(\hat{q}_k + i\hat{p}_k)$ or equivalently,

$$\hat{q}_k := \hat{a}_k + \hat{a}_k^{\dagger}, \ \hat{p}_k := i(\hat{a}_k^{\dagger} - \hat{a}_k). \tag{6}$$

The quadrature field operators represent dimensionless canonical observables of the system and act like the position and momentum operators of the quantum harmonic oscillator. In fact, they satisfy the canonical commutation relations in natural units ($\hbar = 2$)

$$[\hat{x}_i, \hat{x}_j] = 2i\Omega_{ij}, \tag{7}$$

which are easily derivable from the bosonic commutator relations of Eq. (1). In the following, we will use both kinds of field operators, the bosonic field operators and the quadrature field operators.

Now it is important to note that the quadrature operators are observables with continuous eigenspectra. In fact the two quadrature operators $\hat{q}$ (position) and $\hat{p}$ (momentum) have eigenstates[1]

$$\hat{q}\,|q\rangle = q\,|q\rangle, \ \hat{p}\,|p\rangle = p\,|p\rangle, \tag{8}$$

with continuous eigenvalues $q \in \mathbb{R}$ and $p \in \mathbb{R}$. The two eigensets $\{|q\rangle\}_{q\in\mathbb{R}}$ and $\{|p\rangle\}_{p\in\mathbb{R}}$ identify two bases which are connected by a Fourier transform

$$|q\rangle = \frac{1}{2\sqrt{\pi}} \int dp e^{-iqp/2}\,|p\rangle, \ \ |p\rangle = \frac{1}{2\sqrt{\pi}} \int dq e^{iqp/2}\,|q\rangle. \tag{9}$$

In general, for the N-mode Hilbert space we can write

$$\hat{\mathbf{x}}^T\,|\mathbf{x}\rangle = \mathbf{x}^T\,|\mathbf{x}\rangle, \tag{10}$$

with $\mathbf{x} \in \mathbb{R}^{2N}$ and $|\mathbf{x}\rangle := (|x_1\rangle, \ldots, |x_{2N}\rangle)^T$. Here the quadrature eigenvalues $\mathbf{x}$ can be used as continuous variables to describe the entire bosonic system. This is possible by introducing the notion of phase-space representation.

1. Phase-space representation and Gaussian states

All the physical information about the N-mode bosonic system is contained in its quantum state. This is represented by a density operator $\hat{\rho}$, which is a trace-one positive operator acting on the corresponding Hilbert space, i.e., $\hat{\rho} : \mathcal{H}^{\otimes N} \to \mathcal{H}^{\otimes N}$. We denote by $\mathcal{D}(\mathcal{H}^{\otimes N})$ the space of the density operators, also called the state space. Whenever $\hat{\rho}$ is a projector ($\hat{\rho}^2 = \hat{\rho}$) we say that $\hat{\rho}$ is pure and the state can be represented as $\hat{\rho} = |\varphi\rangle\langle\varphi|$ where $|\varphi\rangle \in \mathcal{H}^{\otimes N}$. Now it is important to note that any density operator has an equivalent representation in terms of a quasi-probability distribution (Wigner function) defined over a real symplectic space (phase space). In fact, let us introduce the Weyl operator

$$D(\boldsymbol{\xi}) := \exp(i\hat{\mathbf{x}}^T\mathbf{\Omega}\boldsymbol{\xi}), \tag{11}$$

where $\boldsymbol{\xi} \in \mathbb{R}^{2N}$. Then, an arbitrary $\hat{\rho}$ is equivalent to a Wigner characteristic function

$$\chi(\boldsymbol{\xi}) = \mathrm{Tr}\left[\hat{\rho}D(\boldsymbol{\xi})\right], \tag{12}$$

and, via Fourier transform, to a Wigner function

$$W(\mathbf{x}) = \int_{\mathbb{R}^{2N}} \frac{d^{2N}\boldsymbol{\xi}}{(2\pi)^{2N}} \exp\left(-i\mathbf{x}^T\mathbf{\Omega}\boldsymbol{\xi}\right)\chi(\boldsymbol{\xi}), \tag{13}$$

which is normalized to one but generally non-positive (quasi-probability distribution). In Eq. (13) the continuous variables $\mathbf{x} \in \mathbb{R}^{2N}$ are the eigenvalues of quadratures operators $\hat{\mathbf{x}}$. These variables span a real symplectic space $\mathcal{K} := (\mathbb{R}^{2N}, \mathbf{\Omega})$ which is called the *phase space*. Thus, an arbitrary quantum state $\hat{\rho}$ of a N-mode bosonic system is equivalent to a Wigner function $W(\mathbf{x})$ defined over a $2N$-dimensional phase space $\mathcal{K}$.

The most relevant quantities that characterize the Wigner representations (χ or W) are the statistical moments of the quantum state. In particular, the first moment is called the displacement vector or, simply, the mean value

$$\bar{\mathbf{x}} := \langle\hat{\mathbf{x}}\rangle = \mathrm{Tr}(\hat{\mathbf{x}}\hat{\rho}), \tag{14}$$

[1] Strictly speaking, $|q\rangle$ and $|p\rangle$ are *improper* eigenstates since they are non-normalizable, thus lying outside the Hilbert space. Correspondingly, q and p are *improper* eigenvalues. In the remainder we take this mathematical subtlety for granted.

and the second moment is called the covariance matrix $\mathbf{V}$, whose arbitrary element is defined by

$$V_{ij} := \tfrac{1}{2}\left\langle \{\Delta\hat{x}_i, \Delta\hat{x}_j\}\right\rangle , \tag{15}$$

where $\Delta\hat{x}_i := \hat{x}_i - \langle\hat{x}_i\rangle$ and $\{,\}$ is the anti-commutator. In particular, the diagonal elements of the covariance matrix provide the variances of the quadrature operators, i.e.,

$$V_{ii} = V(\hat{x}_i), \tag{16}$$

where $V(\hat{x}_i) = \langle(\Delta\hat{x}_i)^2\rangle = \langle\hat{x}_i^2\rangle - \langle\hat{x}_i\rangle^2$. The covariance matrix is a $2N \times 2N$, real and symmetric matrix which must satisfy the uncertainty principle (Simon *et al.*, 1994)

$$\mathbf{V} + i\mathbf{\Omega} \geq 0, \tag{17}$$

directly coming from the commutation relations of Eq. (7), and implying the positive definiteness $\mathbf{V} > 0$. From the diagonal terms in Eq. (17), one can easily derive the usual Heisenberg relation for position and momentum

$$V(\hat{q}_k)V(\hat{p}_k) \geq 1. \tag{18}$$

For a particular class of states the first two moments are sufficient for a complete characterization, i.e., we can write $\hat{\rho} = \hat{\rho}(\bar{\mathbf{x}}, \mathbf{V})$. This is the case of the *Gaussian states* (Holevo, 1975, 2011). By definition, these are bosonic states whose Wigner representation (χ or W) is Gaussian, i.e.,

$$\chi(\boldsymbol{\xi}) = \exp\left[-\frac{1}{2}\boldsymbol{\xi}^T\left(\mathbf{\Omega}\mathbf{V}\mathbf{\Omega}^T\right)\boldsymbol{\xi} - i\left(\mathbf{\Omega}\bar{\mathbf{x}}\right)^T\boldsymbol{\xi}\right], \tag{19}$$

$$W(\mathbf{x}) = \frac{\exp\left[-\frac{1}{2}(\mathbf{x}-\bar{\mathbf{x}})^T\mathbf{V}^{-1}(\mathbf{x}-\bar{\mathbf{x}})\right]}{(2\pi)^N\sqrt{\det\mathbf{V}}}. \tag{20}$$

It is interesting to note that a pure state is Gaussian, if and only if, its Wigner function is non-negative (Hudson, 1974; Mandilara *et al.*, 2009; Soto *et al.*, 1983).

2. Gaussian unitaries

Since Gaussian states are easy to characterize, it turns out that a large class of transformations acting on these states are easy to describe too. In general, a quantum state undergoes a transformation called a quantum operation (Nielsen and Chuang, 2000). This is a linear map $\mathcal{E} : \hat{\rho} \to \mathcal{E}(\hat{\rho})$ which is completely positive and trace-decreasing, i.e., $0 \leq \mathrm{Tr}\left[\mathcal{E}(\hat{\rho})\right] \leq 1$. A quantum operation is then called a quantum channel when it is trace-preserving, i.e., $\mathrm{Tr}\left[\mathcal{E}(\hat{\rho})\right] = 1$. The simplest quantum channels are the ones which are reversible. These are represented by unitary transformations $U^{-1} = U^\dagger$, which transform a state according to the rule $\hat{\rho} \to U\hat{\rho}U^\dagger$ or, simply, $|\varphi\rangle \to U|\varphi\rangle$, if the state is pure.

Now we say that a quantum operation is Gaussian when it transforms Gaussian states into Gaussian states. Clearly, this definition applies to the specific cases of quantum channels and unitary transformations. Thus, Gaussian channels (unitaries) are those channels which preserve the Gaussian character of a quantum state. Gaussian unitaries are generated via $U = \exp(-i\hat{H}/2)$ from Hamiltonians $\hat{H}$ which are second-order polynomials in the field operators. In terms of the annihilation and creation operators $\hat{\mathbf{a}} := (\hat{a}_1, \cdots, \hat{a}_N)^T$ and $\hat{\mathbf{a}}^\dagger := (\hat{a}_1^\dagger, \cdots, \hat{a}_N^\dagger)$ this means that

$$\hat{H} = i(\hat{\mathbf{a}}^\dagger\boldsymbol{\alpha} + \hat{\mathbf{a}}^\dagger\mathbf{F}\hat{\mathbf{a}} + \hat{\mathbf{a}}^\dagger\mathbf{G}\hat{\mathbf{a}}^{\dagger T}) + h.c.\,, \tag{21}$$

where $\boldsymbol{\alpha} \in \mathbb{C}^N$ and $\mathbf{F}, \mathbf{G}$ are $N \times N$ complex matrices and $h.c.$ stands for 'Hermitian conjugate'. In the Heisenberg picture, this kind of unitary corresponds to a linear unitary Bogoliubov transformation

$$\hat{\mathbf{a}} \to U^\dagger\hat{\mathbf{a}}U = \mathbf{A}\hat{\mathbf{a}} + \mathbf{B}\hat{\mathbf{a}}^\dagger + \boldsymbol{\alpha}\,, \tag{22}$$

where the $N \times N$ complex matrices $\mathbf{A}$ and $\mathbf{B}$ satisfy $\mathbf{A}\mathbf{B}^T = \mathbf{B}\mathbf{A}^T$ and $\mathbf{A}\mathbf{A}^\dagger = \mathbf{B}\mathbf{B}^\dagger + \mathbf{I}$ with $\mathbf{I}$ being the identity matrix. In terms of the quadrature operators, a Gaussian unitary is more simply described by an affine map

$$(\mathbf{S}, \mathbf{d}) : \hat{\mathbf{x}} \to \mathbf{S}\hat{\mathbf{x}} + \mathbf{d}, \tag{23}$$

where $\mathbf{d} \in \mathbb{R}^{2N}$ and $\mathbf{S}$ is a $2N \times 2N$ real matrix. This transformation must preserve the commutation relations of Eq. (7), which happens when the matrix $\mathbf{S}$ is *symplectic*, i.e.,

$$\mathbf{S}\mathbf{\Omega}\mathbf{S}^T = \mathbf{\Omega}\,. \tag{24}$$

Clearly the eigenvalues $\mathbf{x}$ of the quadrature operators $\hat{\mathbf{x}}$ must follow the same rule, i.e., $(\mathbf{S}, \mathbf{d}) : \mathbf{x} \to \mathbf{S}\mathbf{x} + \mathbf{d}$. Thus, an arbitrary Gaussian unitary is equivalent to an affine symplectic map $(\mathbf{S}, \mathbf{d})$ acting on the phase space, and can be denoted by $U_{\mathbf{S},\mathbf{d}}$. In particular, we can always write $U_{\mathbf{S},\mathbf{d}} = D(\mathbf{d})U_{\mathbf{S}}$, where the canonical unitary $U_{\mathbf{S}}$ corresponds to a linear symplectic map $\mathbf{x} \to \mathbf{S}\mathbf{x}$, and the Weyl operator $D(\mathbf{d})$ to a phase-space translation $\mathbf{x} \to \mathbf{x} + \mathbf{d}$. Finally, in terms of the statistical moments, $\bar{\mathbf{x}}$ and $\mathbf{V}$, the action of a Gaussian unitary $U_{\mathbf{S},\mathbf{d}}$ is characterized by the following transformations

$$\bar{\mathbf{x}} \to \mathbf{S}\bar{\mathbf{x}} + \mathbf{d}\,,\ \mathbf{V} \longrightarrow \mathbf{S}\mathbf{V}\mathbf{S}^T\,. \tag{25}$$

Thus the action of a Gaussian unitary $U_{\mathbf{S},\mathbf{d}}$ over a Gaussian state $\hat{\rho}(\bar{\mathbf{x}}, \mathbf{V})$ is completely characterized by Eq. (25).

B. Examples of Gaussian states and Gaussian unitaries

Here we introduce some elementary Gaussian states that play a major role in continuous-variable quantum information. We also introduce the simplest and most common Gaussian unitaries and discuss their connection with basic Gaussian states. In these examples we first consider one and then two bosonic modes with the general case (arbitrary N) discussed in Sec. II.C.

1. Vacuum states and thermal states

The most important Gaussian state is the one with zero photons ($\bar{n} = 0$), i.e., the *vacuum state* $|0\rangle$. This is also the

eigenstate with zero eigenvalue of the annihilation operator ($\hat{a}\,|0\rangle = 0$). The covariance matrix of the vacuum is just the identity, which means that position and momentum operators have noise-variances equal to one, i.e., $V(\hat{q}) = V(\hat{p}) = 1$. According to Eq. (18), this is the minimum variance which is reachable symmetrically by position and momentum. It is also known as *vacuum noise* or *quantum shot-noise*.

As we will soon see, every Gaussian state can be decomposed into *thermal states*. From this point of view, a thermal state can be thought of as the most fundamental Gaussian state. By definition, we call thermal a bosonic state which maximizes the von Neumann entropy

$$S := -\mathrm{Tr}(\hat{\rho}\ln\hat{\rho})\,, \tag{26}$$

for fixed energy $\mathrm{Tr}(\hat{\rho}\hat{a}^\dagger\hat{a}) = \bar{n}$, where $\bar{n} \geq 0$ is the mean number of photons in the bosonic mode. Explicitly, its number-state representation is given by

$$\hat{\rho}^{th}(\bar{n}) = \sum_{n=0}^{+\infty} \frac{\bar{n}^n}{(\bar{n}+1)^{n+1}}\,|n\rangle\langle n|\ . \tag{27}$$

One can easily check that its Wigner function is Gaussian, with zero mean and covariance matrix $\mathbf{V} = (2\bar{n}+1)\mathbf{I}$ where $\mathbf{I}$ is the 2×2 identity matrix.

2. Displacement and coherent states

The first Gaussian unitary we introduce is the *displacement operator*, which is just the complex version of the Weyl operator. The displacement operator is generated by a linear Hamiltonian and is defined by

$$D(\alpha) := \exp(\alpha\hat{a}^\dagger - \alpha^*\hat{a})\,, \tag{28}$$

where $\alpha = (q+ip)/2$ is the complex amplitude. In the Heisenberg picture, the annihilation operator is transformed by the linear unitary Bogoliubov transformation $\hat{a} \to \hat{a} + \alpha$, and the quadrature operators $\hat{\mathbf{x}} = (\hat{q},\hat{p})^T$ by the translation $\hat{\mathbf{x}} \to \hat{\mathbf{x}} + \mathbf{d}_\alpha$, where $\mathbf{d}_\alpha = (q,p)^T$. By displacing the vacuum state, we generate coherent states $|\alpha\rangle = D(\alpha)\,|0\rangle$. They have the same covariance matrix of the vacuum ($\mathbf{V} = \mathbf{I}$) but different mean values ($\bar{\mathbf{x}} = \mathbf{d}_\alpha$). Coherent states are the eigenstates of the annihilation operator $\hat{a}\,|\alpha\rangle = \alpha\,|\alpha\rangle$ and can be expanded in number states as

$$|\alpha\rangle = \exp\left(-\tfrac{1}{2}|\alpha|^2\right)\sum_{n=0}^{\infty}\frac{\alpha^n}{\sqrt{n!}}\,|n\rangle\ . \tag{29}$$

Furthermore, they form an overcomplete basis, since they are non-orthogonal. In fact, given two coherent states $|\alpha\rangle$ and $|\beta\rangle$, the modulus squared of their overlap is given by

$$|\langle\beta\,|\alpha\rangle\,|^2 = \exp(-|\beta-\alpha|^2)\,. \tag{30}$$

3. One-mode squeezing and squeezed states

When we pump a nonlinear crystal with a bright laser, some of the pump photons with frequency 2ω are split into pairs of photons with frequency ω. Whenever the matching conditions for a degenerate optical parametric amplifier (OPA) are satisfied (Walls and Milburn, 2008), the outgoing mode is ideally composed of a superposition of even number states ($|2n\rangle$). The interaction Hamiltonian must then contain a $\hat{a}^{\dagger 2}$ term to generate pairs of photons and a term $\hat{a}^2$ to ensure hermiticity. The corresponding Gaussian unitary is the one-mode squeezing operator, which is defined as

$$S(r) := \exp[r(\hat{a}^2 - \hat{a}^{\dagger 2})/2]\,, \tag{31}$$

where $r \in \mathbb{R}$ is called the squeezing parameter. In the Heisenberg picture, the annihilation operator is transformed by the linear unitary Bogoliubov transformation $\hat{a} \to (\cosh r)\hat{a} - (\sinh r)\hat{a}^\dagger$ and the quadrature operators $\hat{\mathbf{x}} = (\hat{q},\hat{p})^T$ by the symplectic map $\hat{\mathbf{x}} \to \mathbf{S}(r)\hat{\mathbf{x}}$, where

$$\mathbf{S}(r) := \begin{pmatrix} e^{-r} & 0 \\ 0 & e^{r} \end{pmatrix}\ . \tag{32}$$

Applying the squeezing operator to the vacuum we generate a *squeezed vacuum state* (Yuen, 1976),

$$|0,r\rangle = \frac{1}{\sqrt{\cosh r}}\sum_{n=0}^{\infty}\frac{\sqrt{(2n)!}}{2^n n!}\tanh r^n\,|2n\rangle\,. \tag{33}$$

Its covariance matrix is given by $\mathbf{V} = \mathbf{S}(r)\mathbf{S}(r)^T = \mathbf{S}(2r)$ which has different quadrature noise-variances, i.e., one variance is squeezed below the quantum shot-noise, whilst the other is anti-squeezed above it.

4. Phase rotation

The phase is a crucial element of the wave behavior of the electromagnetic field with no physical meaning for a single mode on its own. In continuous-variable systems the phase is usually defined with respect to a local oscillator, i.e., a mode-matched classical beam. Applying a phase shift on a given mode is done by increasing the optical path length of the beam compared to the local oscillator. For instance, this can be done by adding a transparent material of a tailored depth and with a higher refractive index than vacuum. The phase rotation operator is generated by the free propagation Hamiltonian $\hat{H} = 2\theta\hat{a}^\dagger\hat{a}$, so that it is defined by $R(\theta) = \exp(-i\theta\hat{a}^\dagger\hat{a})$. In the Heisenberg picture, it corresponds to the simple linear unitary Bogoliubov transformation $\hat{a} \to e^{i\theta}\hat{a}$ for the annihilation operator. Correspondingly, the quadratures are transformed via the symplectic map $\hat{\mathbf{x}} \to \mathbf{R}(\theta)\hat{\mathbf{x}}$, where

$$\mathbf{R}(\theta) := \begin{pmatrix} \cos\theta & \sin\theta \\ -\sin\theta & \cos\theta \end{pmatrix}\ , \tag{34}$$

is a proper rotation with angle θ.

5. General one-mode Gaussian states

Using the singular value decomposition, one can show that any 2×2 symplectic matrix can be decomposed as

$\mathbf{S} = \mathbf{R}(\theta)\mathbf{S}(r)\mathbf{R}(\phi)$. This means that any one-mode Gaussian unitary can be expressed as $D(\mathbf{d})U_{\mathbf{S}}$ where $U_{\mathbf{S}} = R(\theta)S(r)R(\phi)$. By applying this unitary to a thermal state $\hat{\rho}_{th}(\bar{n})$, the result is a Gaussian state with mean $\mathbf{d}$ and covariance matrix

$$\mathbf{V} = (2\bar{n}+1)\mathbf{R}(\theta)\mathbf{S}(2r)\mathbf{R}(\theta)^T \ . \tag{35}$$

This is the most general one-mode Gaussian state. This result can be generalized to arbitrary N bosonic modes as we will see in Sec. II.C. Now, by setting $\bar{n} = 0$ in Eq. (35), we achieve the covariance matrix of the most general one-mode pure Gaussian state. This corresponds to a rotated and displaced squeezed state $|\alpha, \theta, r\rangle = D(\alpha)R(\theta)S(r)\,|0\rangle$.

6. Beam splitter

In the case of two bosonic modes one of the most important Gaussian unitaries is the *beam splitter transformation*, which is the simplest example of an interferometer. This transformation is defined by

$$B(\theta) = \exp[\theta(\hat{a}^\dagger\hat{b} - \hat{a}\hat{b}^\dagger)] \ , \tag{36}$$

where $\hat{a}$ and $\hat{b}$ are the annihilation operators of the two modes, and θ which determines the transmissivity of the beam splitter $\tau = \cos^2\theta \in [0,1]$. The beam splitter is called balanced when $\tau = 1/2$. In the Heisenberg picture, the annihilation operators are transformed via the linear unitary Bogoliubov transformation

$$\begin{pmatrix} \hat{a} \\ \hat{b} \end{pmatrix} \to \begin{pmatrix} \sqrt{1-\tau} & \sqrt{\tau} \\ -\sqrt{\tau} & \sqrt{1-\tau} \end{pmatrix} \begin{pmatrix} \hat{a} \\ \hat{b} \end{pmatrix} \ , \tag{37}$$

and the quadrature operators $\hat{\mathbf{x}} := (\hat{q}_a, \hat{p}_a, \hat{q}_b, \hat{p}_b)^T$ are transformed via the symplectic map

$$\hat{\mathbf{x}} \to \mathbf{B}(\tau)\hat{\mathbf{x}} \ , \ \mathbf{B}(\tau) := \begin{pmatrix} \sqrt{1-\tau}\mathbf{I} & \sqrt{\tau}\mathbf{I} \\ -\sqrt{\tau}\mathbf{I} & \sqrt{1-\tau}\mathbf{I} \end{pmatrix} \ . \tag{38}$$

7. Two-mode squeezing and EPR states

Pumping a nonlinear crystal in the non-degenerate OPA regime, we generate pairs of photons in two different modes, known as the signal and the idler. This process is described by an interaction Hamiltonian which contains the bilinear term $\hat{a}^\dagger\hat{b}^\dagger$. The corresponding Gaussian unitary is known as the *two-mode squeezing operator* and is defined as

$$S_2(r) = \exp\left[r(\hat{a}\hat{b} - \hat{a}^\dagger\hat{b}^\dagger)/2\right] \ , \tag{39}$$

where r quantifies the two-mode squeezing (Braunstein and van Loock, 2005). In the Heisenberg picture, the quadratures $\hat{\mathbf{x}} := (\hat{q}_a, \hat{p}_a, \hat{q}_b, \hat{p}_b)^T$ undergo the symplectic map

$$\hat{\mathbf{x}} \to \mathbf{S_2}(r)\hat{\mathbf{x}} \ , \ \mathbf{S_2}(r) = \begin{pmatrix} \cosh r\,\mathbf{I} & \sinh r\,\mathbf{Z} \\ \sinh r\,\mathbf{Z} & \cosh r\,\mathbf{I} \end{pmatrix} \ , \tag{40}$$

where $\mathbf{I}$ is the identity matrix and $\mathbf{Z} := \mathrm{diag}(1,-1)$. By applying $S_2(r)$ to a couple of vacua, we obtain the *two-mode squeezed vacuum state*, also known as an *Einstein-Podolski-Rosen (EPR) state* $\hat{\rho}^{epr}(r) = |r\rangle\langle r|_{epr}$, where

$$|r\rangle_{epr} = \sqrt{1-\lambda^2}\sum_{n=0}^{\infty}(-\lambda)^n\,|n\rangle_a\,|n\rangle_b \ , \tag{41}$$

where $\lambda = \mathrm{tanh}r \in [0,1]$. This is a Gaussian state with zero mean and covariance matrix

$$\mathbf{V}_{epr} = \begin{pmatrix} \nu\mathbf{I} & \sqrt{\nu^2-1}\mathbf{Z} \\ \sqrt{\nu^2-1}\mathbf{Z} & \nu\mathbf{I} \end{pmatrix} := \mathbf{V}_{epr}(\nu) \ , \tag{42}$$

where $\nu = \mathrm{cosh}2r$ quantifies the noise-variance in the quandratures (afterwards, we also use the notation $|\nu\rangle_{epr}$). Using Eq. (42) one can easily check that

$$V(\hat{q}_-) = V(\hat{p}_+) = e^{-2r} \ , \tag{43}$$

where $\hat{q}_- := (\hat{q}_a - \hat{q}_b)/\sqrt{2}$ and $\hat{p}_+ := (\hat{p}_a + \hat{p}_b)/\sqrt{2}$. Note that for $r = 0$, the EPR state corresponds to two vacua and the previous variances are equal to 1, corresponding to the quantum shot-noise. For every two-mode squeezing $r > 0$, we have $V(\hat{q}_-) = V(\hat{p}_+) < 1$, meaning that the correlations between the quadratures of the two systems beat the quantum shot-noise. These correlations are known as *EPR correlations* and they imply the presence of bipartite entanglement. In the limit of $r \to \infty$ we have an ideal EPR state with perfect correlations: $\hat{q}_a = \hat{q}_b$ and $\hat{p}_a = -\hat{p}_b$. Clearly, EPR correlations can also exist in the symmetric case for $\hat{q}_+$ and $\hat{p}_-$ using the replacement $\mathbf{Z} \to -\mathbf{Z}$ in Eq. (42).

The EPR state is the most commonly used Gaussian entangled state and has maximally-entangled quadratures, given its average photon number. Besides the use of a non-degenerate parametric amplifier, an alternative way to generate the EPR state is by combining two appropriately rotated squeezed vacuum states (outputs of two degenerate OPAs) on a balanced beam splitter (Braunstein and van Loock, 2005; Furusawa *et al.*, 1998). This passive generation of entanglement from squeezing has been generalized by Wolf *et al.* (2003). When one considers Gaussian atomic processing, the same state can also be created using two atomic (macroscopic) objects as shown by Julsgaard *et al.* (2001). Finally, let us note the important relation between the EPR state and the thermal state. By tracing out one of the two modes of the EPR state, e.g., mode b, we get $\mathrm{Tr}_b[\hat{\rho}^{epr}(r)] = \hat{\rho}_a^{th}(\bar{n})$, where $\bar{n} = \sinh^2 r$. Thus, the surviving mode is described by a thermal state, whose mean photon number is related to the two-mode squeezing. Because of this, we also say that the EPR state is the purification of the thermal state.

C. Symplectic analysis for multimode Gaussian States

In this section we discuss the most powerful approach to studying Gaussian states of multimode bosonic systems. This is based on the analysis and manipulation of the second-order statistical moments, and its central tools are Williamson's theorem and the Euler decomposition.

1. Thermal decomposition of Gaussian states

According to Williamson's theorem, every positive-definite real matrix of even dimension can be put in diagonal form by a symplectic transformation (Williamson, 1936). In particular, this theorem can be applied to covariance matrices. Given an arbitrary N-mode covariance matrix $\mathbf{V}$, there exists a symplectic matrix $\mathbf{S}$ such that

$$\mathbf{V}=\mathbf{S}\mathbf{V}^{\oplus}\mathbf{S}^{T}\ ,\ \mathbf{V}^{\oplus}:=\bigoplus_{k=1}^{N}\nu_{k}\mathbf{I}\ , \tag{44}$$

where the diagonal matrix $\mathbf{V}^{\oplus}$ is called the Williamson form of $\mathbf{V}$, and the N positive quantities ν_k are called the symplectic eigenvalues of $\mathbf{V}$. Here the symplectic spectrum $\{\nu_k\}_{k=1}^{N}$ can be easily computed as the standard eigenspectrum of the matrix $|i\mathbf{\Omega}\mathbf{V}|$, where the modulus must be understood in the operatorial sense. In fact, the matrix $i\mathbf{\Omega}\mathbf{V}$ is Hermitian and is therefore diagonalizable by a unitary transformation. Then, by taking the modulus of its $2N$ real eigenvalues, one gets the N symplectic eigenvalues of $\mathbf{V}$. The symplectic spectrum is very important since it provides powerful ways to express the fundamental properties of the corresponding quantum state. For example, the uncertainty principle of Eq. (17) is equivalent to

$$\mathbf{V}>0,\ \mathbf{V}^{\oplus}\geq\mathbf{I}\ . \tag{45}$$

In other words, a quantum covariance matrix must be positive definite and its symplectic eignevalues must satisfy $\nu_k\geq 1$. Then, the von Neumann entropy $S(\hat{\rho})$ of a Gaussian state $\hat{\rho}$ can be written as (Holevo *et al.*, 1999)

$$S(\hat{\rho})=\sum_{k=1}^{N}g(\nu_{k}), \tag{46}$$

where

$$g(x):=\left(\frac{x+1}{2}\right)\log\left(\frac{x+1}{2}\right)-\left(\frac{x-1}{2}\right)\log\left(\frac{x-1}{2}\right). \tag{47}$$

In the space of density operators, the symplectic decomposition of Eq. (44) corresponds to a thermal decomposition for Gaussian states. In fact, let us consider a zero-mean Gaussian state $\hat{\rho}(\mathbf{0},\mathbf{V})$. Because of Eq. (44), there exists a canonical unitary $U_{\mathbf{S}}$ such that $\hat{\rho}(\mathbf{0},\mathbf{V})=U_{\mathbf{S}}\hat{\rho}(\mathbf{0},\mathbf{V}^{\oplus})U_{\mathbf{S}}^{\dagger}$, where

$$\hat{\rho}(\mathbf{0},\mathbf{V}^{\oplus})=\bigotimes_{k=1}^{N}\hat{\rho}^{th}\left(\tfrac{\nu_{k}-1}{2}\right) \tag{48}$$

is a tensor-product of one-mode thermal states whose photon numbers are provided by the symplectic spectrum $\{\nu_k\}$ of the original state. In general, for an arbitrary Gaussian state $\hat{\rho}(\bar{\mathbf{x}},\mathbf{V})$ we can write the thermal decomposition

$$\hat{\rho}(\bar{\mathbf{x}},\mathbf{V})=D(\bar{\mathbf{x}})U_{\mathbf{S}}\left[\hat{\rho}(\mathbf{0},\mathbf{V}^{\oplus})\right]U_{\mathbf{S}}^{\dagger}D(\bar{\mathbf{x}})^{\dagger}\ . \tag{49}$$

Using the thermal decomposition of Eq. (49) and the fact that thermal states are purified by EPR states, we can derive a very simple formula for the purification of an arbitrary Gaussian state (Holevo and Werner, 2001). In fact, let us denote by A a system of N modes described by a Gaussian state $\hat{\rho}_A(\bar{\mathbf{x}},\mathbf{V})$, and introduce an additional reference system R of N modes. Then, we have $\hat{\rho}_A(\bar{\mathbf{x}},\mathbf{V})=\mathrm{Tr}_R[\hat{\rho}_{AR}(\bar{\mathbf{x}}',\mathbf{V}')]$, where $\hat{\rho}_{AR}$ is a pure Gaussian state for the composite system AR, having mean $\bar{\mathbf{x}}'=(\bar{\mathbf{x}},\mathbf{0})^{T}$ and covariance matrix

$$\mathbf{V}'=\left[\begin{array}{cc}\mathbf{V} & \mathbf{S}\mathbf{C}\\ \mathbf{C}^{T}\mathbf{S}^{T} & \mathbf{V}^{\oplus}\end{array}\right]\ ,\ \mathbf{C}:=\bigoplus_{k=1}^{N}\sqrt{\nu_{k}^{2}-1}\mathbf{Z}\ . \tag{50}$$

2. Euler decomposition of canonical unitaries

The canonical unitary $U_{\mathbf{S}}$ in Eq. (49) can be suitably decomposed using the Euler decomposition (Arvind *et al.*, 1995), alternatively known as the Bloch-Messiah reduction (Braunstein, 2005). First of all, let us distinguish between active and passive canonical unitaries. By definition, a canonical unitary $U_{\mathbf{S}}$ is called passive (active) if it is photon number preserving (non-preserving). A passive $U_{\mathbf{S}}$ corresponds to a symplectic matrix $\mathbf{S}$ which preserves the trace of the covariance matrix, i.e., $\mathrm{Tr}(\mathbf{S}\mathbf{V}\mathbf{S}^{T})=\mathrm{Tr}(\mathbf{V})$ for any $\mathbf{V}$. This happens when the symplectic matrix $\mathbf{S}$ is orthogonal, i.e., $\mathbf{S}^{T}=\mathbf{S}^{-1}$. Passive canonical unitaries describe multiport interferometers, e.g., the beam splitter in the case of two modes. By contrast, active canonical unitaries correspond to symplectic matrices which are not trace-preserving and, therefore, cannot be orthogonal. This is the case of the one-mode squeezing matrix of Eq. (32). Arbitrary symplectic matrices contain both the previous elements. In fact, every symplectic matrix $\mathbf{S}$ can be written as

$$\mathbf{S}=\mathbf{K}\left[\bigoplus_{k=1}^{N}\mathbf{S}(r_{k})\right]\mathbf{L}, \tag{51}$$

where $\mathbf{K},\mathbf{L}$ are symplectic and orthogonal, while $\mathbf{S}(r_1),\cdots,\mathbf{S}(r_N)$ is a set of one-mode squeezing matrices. Direct sums in phase space correspond to tensor products in the state space. As a result, every canonical unitary $U_{\mathbf{S}}$ can be decomposed as

$$U_{\mathbf{S}}=U_{\mathbf{K}}\left[\bigotimes_{k=1}^{N}S(r_{k})\right]U_{\mathbf{L}}\ , \tag{52}$$

i.e., a multiport interferometer ($U_{\mathbf{L}}$), followed by a parallel set of N one-mode squeezers ($\otimes_k S(r_k)$), followed by another passive transformation ($U_{\mathbf{K}}$). Combining the thermal decomposition of Eq. (49) with the Euler decomposition of Eq. (52), we see that an arbitrary multimode Gaussian state $\hat{\rho}(\bar{\mathbf{x}},\mathbf{V})$ can be realized by preparing N thermal states $\hat{\rho}(\mathbf{0},\mathbf{V}^{\oplus})$, applying multimode interferometers and one-mode squeezers according to Eq. (52), and finally displacing them by $\bar{\mathbf{x}}$.

3. Two-mode Gaussian states

Gaussian states of two bosonic modes ($N=2$) represent a remarkable case. They are characterized by simple analytical

formulas and represent the simplest states for studying properties like quantum entanglement. Given a two-mode Gaussian state $\hat{\rho}(\bar{\mathbf{x}}, \mathbf{V})$, let us write its covariance matrix in the block form

$$\mathbf{V} = \begin{pmatrix} \mathbf{A} & \mathbf{C} \\ \mathbf{C}^T & \mathbf{B} \end{pmatrix} , \tag{53}$$

where $\mathbf{A} = \mathbf{A}^T$, $\mathbf{B} = \mathbf{B}^T$ and $\mathbf{C}$ are 2×2 real matrices. Then, the Williamson form is simply $\mathbf{V}^{\oplus} = (\nu_- \mathbf{I}) \oplus (\nu_+ \mathbf{I})$, where symplectic spectrum $\{\nu_-, \nu_+\}$ is provided by

$$\nu_{\pm} = \sqrt{\frac{\Delta \pm \sqrt{\Delta^2 - 4 \det \mathbf{V}}}{2}} , \tag{54}$$

with $\Delta := \det \mathbf{A} + \det \mathbf{B} + 2 \det \mathbf{C}$ and $\det$ is the determinant (Serafini *et al.*, 2004). In this case the uncertainty principle is equivalent to the bona-fide conditions (Pirandola, Serafini, and Lloyd, 2009; Serafini, 2006)

$$\mathbf{V} > 0, \ \det \mathbf{V} \geq 1 \ \text{ and } \ \Delta \leq 1 + \det \mathbf{V}. \tag{55}$$

An important class of two-mode Gaussian states has covariance matrix in the standard form (Duan *et al.*, 2000; Simon, 2000)

$$\mathbf{V} = \begin{pmatrix} a\mathbf{I} & \mathbf{C} \\ \mathbf{C} & b\mathbf{I} \end{pmatrix} , \ \mathbf{C} = \begin{pmatrix} c_1 & 0 \\ 0 & c_2 \end{pmatrix} , \tag{56}$$

where $a, b, c_1, c_2 \in \mathbb{R}$ must satisfy the previous bona-fide conditions. In particular, for $c_1 = -c_2 := c \geq 0$, the symplectic eigenvalues are simply $\nu_{\pm} = [\sqrt{y} \pm (b-a)]/2$, where $y := (a+b)^2 - 4c^2$. In this case, we can also derive the matrix $\mathbf{S}$ realizing the symplectic decomposition $\mathbf{V} = \mathbf{S}\mathbf{V}^{\oplus}\mathbf{S}^T$. This is given by the formula

$$\mathbf{S} = \begin{pmatrix} \omega_+ \mathbf{I} & \omega_- \mathbf{Z} \\ \omega_- \mathbf{Z} & \omega_+ \mathbf{I} \end{pmatrix} , \ \omega_{\pm} := \sqrt{\frac{a+b \pm \sqrt{y}}{2\sqrt{y}}} . \tag{57}$$

D. Entanglement in bipartite Gaussian states

Entanglement is one of the most important properties of quantum mechanics, being central in most quantum information protocols. To begin with let us consider two bosonic systems, A with N modes and B with M modes, having Hilbert spaces $\mathcal{H}_A$ and $\mathcal{H}_B$, respectively. The global bipartite system $A+B$ has a Hilbert space $\mathcal{H} = \mathcal{H}_A \otimes \mathcal{H}_B$. By definition, a quantum state $\hat{\rho} \in \mathcal{D}(\mathcal{H})$ is said to be separable if it can be written as convex combination of product states, i.e.,

$$\hat{\rho} = \sum_i p_i \, \hat{\rho}_i^A \otimes \hat{\rho}_i^B , \ \ \hat{\rho}_i^{A(B)} \in \mathcal{D}(\mathcal{H}_{A(B)}), \tag{58}$$

where $p_i \geq 0$ and $\sum_i p_i = 1$. Note that the index can also be continuous. In such a case, the previous sum becomes an integral and the probabilities are replaced by a probability density function. Physically, Eq. (58) means that a separable state can be prepared via local (quantum) operations and classical communications (LOCCs). By definition, a state is called entangled when it is not separable, i.e., the correlations between A and B are so strong that they cannot be created by any strategy based on LOCCs. In entanglement theory there are two central questions to answer: "Is the state entangled?", and if the answer is yes, then "how much entanglement does it have?". In what follows we review how we can answer those two questions for Gaussian states.

1. Separability

As first shown by Horodecki *et al.* (1996) and Peres (1996), a key-tool for studying separability is the partial transposition, i.e., the transposition with respect to one of the two subsystems, e.g., system B. In fact, if a quantum state $\hat{\rho}$ is separable, then its partial transpose $\hat{\rho}^{T_B}$ is a valid density operator and in particular positive, i.e., $\hat{\rho}^{T_B} \geq 0$. Thus, the positivity of the partial transpose represents a necessary condition for separability. On the other hand, the non-positivity of the partial transpose represents a sufficient condition for entanglement. Note that, in general, the positivity of the partial transpose is not a sufficient condition for separability, since there exist entangled states with positive partial transpose. These states are bound entangled meaning that their entanglement cannot be distilled into maximally entangled states (Horodecki *et al.*, 1998, 2009).

The partial transposition operation corresponds to a local time reversal (Horodecki *et al.*, 1998). For bosonic systems the quadratures $\hat{\mathbf{x}}$ of the bipartite system $A+B$ undergo the transformation $\hat{\mathbf{x}} \to (\mathbf{I}_A \oplus \mathbf{T}_B)\hat{\mathbf{x}}$, where $\mathbf{I}_A$ is the N-mode identity matrix while $\mathbf{T}_B := \oplus_{k=1}^{M} \mathbf{Z}$ (Simon, 2000). Let us consider an arbitrary Gaussian state $\hat{\rho}(\bar{\mathbf{x}}, \mathbf{V})$ of the bipartite system $A+B$, also known as an $N \times M$ bipartite Gaussian state. Under the partial transposition operation, its covariance matrix is transformed via the congruence

$$\mathbf{V} \to (\mathbf{I_A} \oplus \mathbf{T_B})\mathbf{V}(\mathbf{I_A} \oplus \mathbf{T_B}) := \tilde{\mathbf{V}} . \tag{59}$$

where the partially-transposed matrix $\tilde{\mathbf{V}}$ is positive definite. If the state is separable, then $\tilde{\mathbf{V}}$ satisfies the uncertainty principle, i.e., $\tilde{\mathbf{V}} + i\mathbf{\Omega} \geq 0$. Since $\tilde{\mathbf{V}} > 0$, this is equivalent to check the condition $\tilde{\mathbf{V}}^{\oplus} \geq \mathbf{I}$, where $\tilde{\mathbf{V}}^{\oplus}$ is the Williamson form of $\tilde{\mathbf{V}}$. This is also equivalent to check $\tilde{\nu}_- \geq 1$, where $\tilde{\nu}_-$ is the minimum eigenvalue in the symplectic spectrum $\{\tilde{\nu}_k\}$ of $\tilde{\mathbf{V}}$.

The satisfaction (violation) of the condition $\tilde{\nu}_- \geq 1$ corresponds to having the positivity (non-positivity) of the partially transposed Gaussian state. In some restricted situations, this positivity is equivalent to separability. This happens for $1 \times M$ Gaussian states (Werner and Wolf, 2001), and for a particular class of $N \times M$ Gaussian states which are called bisymmetric (Serafini, Adesso, and Illuminati, 2005). In general, the equivalence is not true, as shown already for 2×2 Gaussian states by Werner and Wolf (2001). Finally, note that the partial transposition is not the only way to study separability. In (Duan *et al.*, 2000) the authors constructed an inseparability criterion, generalizing the EPR correlations, which gives a sufficient condition for entanglement (also necessary for 1x1

Gaussian states). Two other useful techniques exist to fully characterize the separability of bipartite Gaussian states. The first uses nonlinear maps as shown by Giedke, Kraus, *et al.* (2001), where the second reduces the separability problem to a semi-definite program (Hyllus and Eisert, 2006).

2. Entanglement measures

In the case of pure $N \times M$ Gaussian states $|\varphi\rangle$, the entanglement is provided by the *entropy of entanglement* $E_V(|\varphi\rangle)$. This is defined as the von Neumann entropy of the reduced states $\hat{\rho}_{A,B} = \mathrm{Tr}_{B,A}(|\varphi\rangle\langle\varphi|)$, i.e., $E_V(|\varphi\rangle) = S(\hat{\rho}_A) = S(\hat{\rho}_B)$ (Bennett, Bernstein, *et al.*, 1996), which can be easily calcuated using Eq. (46). The entropy of entanglement gives the amount of entangled qubits (measured in e-bits) that can be extracted from the state together with the amount of entanglement needed to generate the state, i.e., distillation and generation being reversible for pure states (in the asymptotic limit) (Nielsen and Chuang, 2000). Any bipartite pure Gaussian state can be mapped, using local Gaussian unitaries, into a tensor product of EPR states of covariance matrix $\bigoplus_k \mathbf{V}_{epr}(\nu_k)$ (Botero and Reznik, 2003; Holevo and Werner, 2001). A LOCC mapping a Gaussian pure state to another one exists if and only if $\nu_k \geq \nu'_k$ for all k, where their respective ν_k and ν'_k are in descending order (Giedke *et al.*, 2003).

Unfortunately, for mixed states we do not have a single definition of measure of entanglement (Horodecki *et al.*, 2009). Different candidates exist, each one with its own operational interpretation. Among the most well known is the *entanglement of formation* (Bennett, DiVincenzo, *et al.*, 1996),

$$E_F(\hat{\rho}) = \min_{\{p_k, |\varphi_k\rangle\}} \sum_k p_k E_V(|\varphi_k\rangle) \,, \tag{60}$$

where the minimization is taken over all the possible decompositions $\hat{\rho} = \sum_k p_k |\varphi_k\rangle\langle\varphi_k|$ (the sum becomes an integral for continuous decompositions). In general, this optimization is very difficult to carry out. In continuous variables, we only know the solution for two-mode symmetric Gaussian states (Giedke *et al.*, 2003). These are two-mode Gaussian states whose covariance matrix is symmetric under the permutation of the two modes, i.e., $\mathbf{A} = \mathbf{B}$ in Eq. (53), where $E_F(\hat{\rho})$ is then a function of $\tilde{\nu}_-$. Interestingly the optimal decomposition $\{p_k, |\varphi_k\rangle\}$ leading to this result is obtained from Gaussian states $|\varphi_k\rangle$. This is conjectured to be true for any the Gaussian state, i.e., the Gaussian entanglement of formation $GE_F(\hat{\rho})$, defined by the minimization over Gaussian decompositions satisfies $GE_F(\hat{\rho}) = E_F(\hat{\rho})$ (Wolf *et al.*, 2004).

The distillable entanglement $D(\hat{\rho})$ quantifies the amount of entanglement that can be distilled from a given mixed state $\hat{\rho}$ (Horodecki *et al.*, 2009). It is easy to see that $D(\hat{\rho}) \leq E_F(\hat{\rho})$, otherwise we could generate an infinite amount of entanglement from finite resources, where for pure states we have $D(|\psi\rangle) = E_F(|\psi\rangle) = E_V(|\psi\rangle)$. The entanglement distillation is also hard to calculate, as it needs an optimization over all possible distillation protocols. Little is known about $D(\hat{\rho})$ for Gaussian states, except trivial lower-bounds given by the coherent information (Devetak and Winter, 2004) and its reverse counterpart (García-Patrón *et al.*, 2009). In Giedke, Duan, *et al.* (2001) it was shown that bipartite Gaussian states are distillable if and only if they have a non-positive partial transpose. However, the distillation of mixed Gaussian states into pure Gaussian states is not possible using only Gaussian LOCC operations (Eisert *et al.*, 2002; Fiurà̌sek, 2002a; Giedke and Cirac, 2002), but can be achieved using non-Gaussian operations that map Gaussian states into Gaussian states (Browne *et al.*, 2003), as recently demonstrated by Takahashi *et al.* (2010).

The two previous entanglement measures, i.e., $E_F(\hat{\rho})$ and $D(\hat{\rho})$, are unfortunately very difficult to calculate in full generality. However, a measure easy to compute is the logarithmic negativity (Vidal and Werner, 2002)

$$E_N(\hat{\rho}) = \log ||\hat{\rho}^{T_B}||_1 \tag{61}$$

which quantifies how much the state fails to satisfy the positivity of the partial transpose condition. For Gaussian states it reads

$$E_N(\hat{\rho}) = \sum_k F(\tilde{\nu}^k) \tag{62}$$

where $F(x) = -\log(x)$ for $x < 1$ and $F(x) = 0$ for $x \geq 1$ (Vidal and Werner, 2002). It was shown to be an entanglement monotone (Eisert, 2001; Plenio, 2005) and an upperbound of $D(\hat{\rho})$ (Vidal and Werner, 2002). The logarithmic negativity of $1 \times M$ and $N \times M$ bisymmetric Gaussian states was characterized by Adesso and Illuminati (2007) and Adesso *et al.* (2004), respectively. Finally, we briefly mention that although the separability of a quantum state implies zero entanglement, other types of quantum correlations can exist for separable (non-entangled) mixed states. One measure of such correlations is the quantum discord and has recently been extended to Gaussian states (Adesso and Datta, 2010; Giorda and Paris, 2010).

E. Measuring Gaussian states

A quantum measurement is described by a set of operators $\{E_i\}$ satisfying the completeness relation $\sum_i E_i^\dagger E_i = I$ where I is the identity operator. Given an input state $\hat{\rho}$, the outcome i is found with probability $p_i = \mathrm{Tr}(\hat{\rho} E_i^\dagger E_i)$ and the state is projected onto $\hat{\rho}_i = p_i^{-1} E_i \hat{\rho} E_i^\dagger$. If we are only interested in the outcome of the measurement we can set $\Pi_i := E_i^\dagger E_i$ and describe the measurement as a positive operator-valued measure (POVM). In the case of continuous-variable systems, quantum measurements are often described by continuous outcomes $i \in \mathbb{R}$, so that p_i becomes a probability density. Here we define a measurement as being Gaussian when its application to Gaussian states provides outcomes which are Gaussian-distributed. From a practical point of view, any Gaussian measurement can be accomplished using homodyne detection, linear optics (i.e., active and passive Gaussian unitaries), and Gaussian ancilla modes. A general property of a Gaussian measurement is the following: suppose a Gaussian measurement is made on N modes of an $N + M$

Gaussian state where $N, M \geq 1$; then the classical outcome from the measurement is a Gaussian distribution and the unmeasured M modes are left in a Gaussian state.

1. Homodyne detection

The most common Gaussian measurement in continuous-variable quantum information is homodyne detection, consisting of the measurement of the quadrature $\hat{q}$ (or $\hat{p}$) of a bosonic mode. Its measurement operators are projectors over the quadrature basis $|q\rangle\langle q|$ (or $|p\rangle\langle p|$), i.e., infinitely squeezed states. The corresponding outcome q (or p) has a probability distribution $P(q)$ (or $P(p)$) which is given by the marginal integral of the Wigner function over the conjugate quadrature, i.e.,

$$P(q) = \int W(q,p)dp, \quad P(p) = \int W(q,p)dq. \tag{63}$$

This can be generalized to the situation of partially homodyning a multimode bosonic system by including the integration over both quadratures of the non-measured modes. Experimentally a homodyne measurement is implemented by combining the target quantum mode with a local oscillator into a balanced beam splitter and measuring the intensity of the outgoing modes using two photo-detectors. The subtraction of the signal of both photo-detectors gives a signal proportional to $\hat{q}$ (Braunstein and van Loock, 2005). The $\hat{p}$ quadrature is measured by applying a $\pi/2$ phase shift to the local oscillator. Corrections due to bandwidth effects or limited local oscillator power have also been addressed (Braunstein, 1990; Braunstein and Crouch, 1991). Homodyne detection is also a powerful tool in quantum tomography (Lvovsky and Raymer, 2009). For instance, by using a single homodyne detector, one can experimentally reconstruct the covariance matrix of two-mode Gaussian states (Buono *et al.*, 2010; D'Auria *et al.*, 2009). In tandem to well known homodyne measurements on light, homodyne measurements of the atomic Gaussian spin states via a quantum non-demolition measurement by light have also been developed. For example, the work of Fernholz *et al.* (2008) demonstrated the quantum tomographic reconstruction of a spin squeezed state of the atomic ensemble.

2. Heterodyne detection and Gaussian POVMs

The quantum theory of heterodyne detection was established by Yuen and Shapiro (1980) and is an important example of a Gaussian POVM. Theoretically, heterodyne detection corresponds to a projection onto coherent states, i.e., $E(\alpha) := \pi^{-1/2}|\alpha\rangle\langle\alpha|$. A heterodyne detector combines the measured bosonic mode with a vacuum ancillary mode into a balanced beam splitter and homodynes the quadratures $\hat{q}$ and $\hat{p}$ of the outcome modes. This approach can be generalized to any POVM composed of projectors over pure Gaussian states. As shown by Giedke and Cirac (2002) and Eisert and Plenio (2003), such measurements can be decomposed into a Gaussian unitary applied to the input system and extra ancillary (vacuum) modes followed by homodyne measurements on all the output modes. Finally, a general noisy Gaussian POVM is modeled as before but with part of the output modes traced out.

3. Partial Gaussian measurement

When processing a quantum system we are usually interested in measuring only part of it (for example, subsystem B which contains 1 mode) in order to extract information and continue processing the remaining part (say, subsystem A with N modes). Let us consider a Gaussian state for the global system $A+B$ where the covariance matrix is in block form similar to Eq. (53) (but with $N+1$ modes). Measuring the $\hat{q}$ quadrature of subsystem B transforms the covariance matrix of subsystem A as follows (Eisert *et al.*, 2002; Fiurášek, 2002a)

$$\mathbf{V} = \mathbf{A} - \mathbf{C}(\mathbf{\Pi B \Pi})^{-1}\mathbf{C}^T , \tag{64}$$

where $\mathbf{\Pi} := \mathrm{diag}(1,0)$ and $(\mathbf{\Pi B \Pi})^{-1}$ is a pseudoinverse since $\mathbf{\Pi B \Pi}$ is singular. In particular, we have $(\mathbf{\Pi B \Pi})^{-1} = B_{11}^{-1}\mathbf{\Pi}$, where B_{11} is the top-left element of $\mathbf{B}$. Note that the output covariance matrix does not depend on the specific result of the measurement. This technique can be generalized to model any partial Gaussian measurement, which consists of appending ancillary modes to a system, applying a Gaussian unitary, and processing the output modes as follows: part is homodyned, another part is discarded and the remaining part is the output system. As an example, we can easily derive the effect on a multi-mode subsystem A after we heterodyne a single-mode subsystem B. By heterodyning the last mode, the first N modes are still in a Gaussian state, and the output covariance matrix is given by

$$\mathbf{V} = \mathbf{A} - \mathbf{C}(\mathbf{B} + \mathbf{I})^{-1}\mathbf{C}^T , \tag{65}$$

or, equivalently, $\mathbf{V} = \mathbf{A} - \Theta^{-1}\mathbf{C}(\boldsymbol{\omega}\mathbf{B}\boldsymbol{\omega}^T + \mathbf{I})\mathbf{C}^T$, where $\Theta := \det\mathbf{B} + \mathrm{Tr}\mathbf{B} + 1$, and $\boldsymbol{\omega}$ is defined in Eq. (2).

4. Counting and detecting photons

Finally, there are two measurements, that despite being non-Gaussian, play an important role in certain Gaussian quantum information protocols, e.g., distinguishability of Gaussian states, entanglement distillation and universal quantum computation. The first one is the von Neumann measurement in the number state basis, i.e., $E_n := |n\rangle\langle n|$. The second one is the avalanche photo-diode that discriminates between vacuum $E_0 = |0\rangle\langle 0|$ and one or more photons $E_1 = I - |0\rangle\langle 0|$. Realistic avalanche photo-diode detectors usually have small efficiency, i.e., they detect only a small fraction of the impinging photons. This is modeled theoretically by adding a beam splitter before an ideal avalanche photo-diode detector, with transmissivity given by the efficiency of the detector. Recent technological developments allow experimentalists to approach ideal photon-counting capability for photon numbers of up to five to ten (Lita *et al.*, 2008).

III. DISTINGUISHABILITY OF GAUSSIAN STATES

The laws of quantum information tell us that in general it is impossible to perfectly distinguish between two non-orthogonal quantum states (Fuchs, 2000; Nielsen and Chuang, 2000). This limitation of quantum measurement theory (Helstrom, 1976) is inherent in a number of Gaussian quantum information protocols including quantum cloning and the security of quantum cryptography. Closely related to this is *quantum state discrimination* which is concerned with the distinguishability of quantum states. There are two commonly used distinguishability techniques (Bergou *et al.*, 2004; Chefles, 2000): (1) minimum error state discrimination, and (2) unambiguous state discrimination. In minimum error state discrimination, a number of approaches have been developed which allows one to (imperfectly) distinguish between quantum states provided we allow a certain amount of uncertainty or error in our measurement results. On the other hand, unambiguous state discrimination, is an error-free discrimination process but relies on the fact that sometimes the observer gets an inconclusive result (Chefles and Barnett, 1998b; Enk, 2002). There also exists an intermediate discrimination regime which allows for both errors and inconclusive results (Chefles and Barnett, 1998a; Fiurà̀šek, 2003; Wittmann *et al.*, 2010a). Here we discuss minimum error state discrimination which is more developed than unambiguous state discrimination in the continuous-variable framework particularly in the case of Gaussian states.

This section is structured as follows. In Sec. III.A we begin by introducing some of the basic measures of distinguishability, such as the Helstrom bound, the quantum Chernoff bound and the quantum fidelity. We give their formulation for arbitrary quantum states, providing analytical formulas in the specific case of Gaussian states. Then, in Sec. III.B, we consider the most common Gaussian discrimination protocol: distinguishing optical coherent states with minimum error.

A. Measures of distinguishability

1. Helstrom bound

Let us suppose that a quantum system is described by an unknown quantum state $\hat{\rho}$ which can take two possible forms, $\hat{\rho}_0$ or $\hat{\rho}_1$, with the same probability (more generally, the problem can be formulated for quantum states which are not equiprobable). For discriminating between $\hat{\rho}_0$ and $\hat{\rho}_1$, we can apply an arbitrary quantum measurement to the system. Without loss of generality, we can consider a dichotomic POVM $\{\Pi_0, \Pi_1 := I - \Pi_0\}$ whose outcome $u = 0, 1$ is a logical bit solving the discrimination. This happens up to an error probability

$$p_e = \frac{p(u=0|\hat{\rho}=\hat{\rho}_1) + p(u=1|\hat{\rho}=\hat{\rho}_0)}{2} , \qquad (66)$$

where $p(u|\hat{\rho})$ is the conditional probability of getting the outcome u given the state $\hat{\rho}$. Then we ask: what is the minimum error probability we can achieve by optimizing over the (dichotomic) POVMs? The answer to this question is provided by the Helstrom bound (Helstrom, 1976). Helstrom showed that an optimal POVM is given by $\Pi_1 = P(\gamma_+)$, which is a projector onto the positive part γ_+ of the non-positive operator $\gamma := \hat{\rho}_0 - \hat{\rho}_1$, known as the *Helstrom matrix*. As a result, the minimum error probability is equal to the *Helstrom bound*

$$p_{e,min} = \frac{1}{2}\left[1 - D(\hat{\rho}_0, \hat{\rho}_1)\right] , \qquad (67)$$

where

$$D(\hat{\rho}_0, \hat{\rho}_1) := \frac{1}{2}\mathrm{Tr}\,|\hat{\rho}_0 - \hat{\rho}_1| = \frac{1}{2}\sum |\lambda_j|, \qquad (68)$$

is the *trace distance* between the two quantum states (Nielsen and Chuang, 2000). Here $\sum |\lambda_j|$ is the summation of the absolute values of the eigenvalues of the matrix $\hat{\rho}_0 - \hat{\rho}_1$. In the case of two pure states, i.e., $\hat{\rho}_0 = |\psi_0\rangle\langle\psi_0|$ and $\hat{\rho}_1 = |\psi_1\rangle\langle\psi_1|$, the Helstrom bound takes the simple form

$$p_{e,min} = \frac{1}{2}\left(1 - \sqrt{1 - |\langle\psi_0|\,\psi_1\rangle|^2}\right) . \qquad (69)$$

2. Quantum Chernoff bound

In general, deriving an analytical expression for the trace distance is not easy and, therefore, the Helstrom bound is usually approximated by other distinguishability measures. One of the most recent is the *quantum Chernoff bound* (Audenaert *et al.*, 2007, 2008; Calsamiglia *et al.*, 2008; Nussbaum and Szkola, 2009). This is an upper bound $p_{e,min} \leq p_{QC}$, defined by

$$p_{QC} := \frac{1}{2}\left(\inf_{0\leq s\leq 1} C_s\right) , \; C_s := \mathrm{Tr}\left(\hat{\rho}_0^s \hat{\rho}_1^{1-s}\right) . \qquad (70)$$

Note that the quantum Chernoff bound involves a minimization in s $\in [0, 1]$. In particular, we must use an infimum because of possible discontinuities of C_s at the border $s = 0, 1$. By ignoring the minimization and setting $s = 1/2$, we derive a weaker but easier-to-compute upper bound. This is known as the *quantum Bhattacharyya bound* (Pirandola and Lloyd, 2008)

$$p_B := \frac{1}{2}\mathrm{Tr}\left(\sqrt{\hat{\rho}_0}\sqrt{\hat{\rho}_1}\right) . \qquad (71)$$

a. General formula for multimode Gaussian states

In the case of Gaussian states the quantum Chernoff bound can be computed from the first two statistical moments. A first formula, valid for single-mode Gaussian states, was shown by Calsamiglia *et al.* (2008). Later, Pirandola and Lloyd (2008) provided a general formula for multimode Gaussian states, relating the quantum Chernoff bound to the symplectic spectra (Williamson forms). Here we review this general formula. Since it concerns the term C_s in Eq. (70), it also applies to the quantum Bhattacharyya bound.

First of all it is useful to introduce the two real functions

$$G_s(x) := 2^s\left[(x+1)^s - (x-1)^s\right]^{-1} , \qquad (72)$$

and

$$\Lambda_s(x) := \frac{(x+1)^s + (x-1)^s}{(x+1)^s - (x-1)^s} , \tag{73}$$

which are positive for $x \geq 1$ and $s > 0$. These functions can be computed over a Williamson form $\mathbf{V}^{\oplus}$ via the rule

$$f(\mathbf{V}^{\oplus}) = f\left(\bigoplus_{k=1}^{N} \nu_k \mathbf{I}\right) = \bigoplus_{k=1}^{N} f(\nu_k)\mathbf{I} . \tag{74}$$

Using these functions we can state the following result (Pirandola and Lloyd, 2008). Let us consider two N-mode Gaussian states, $\hat{\rho}_0(\bar{\mathbf{x}}_0, \mathbf{V}_0)$ and $\hat{\rho}_1(\bar{\mathbf{x}}_1, \mathbf{V}_1)$, whose covariance matrices have symplectic decompositions

$$\mathbf{V}_0 = \mathbf{S}_0 \mathbf{V}_0^{\oplus} \mathbf{S}_0^T , \ \mathbf{V}_1 = \mathbf{S}_1 \mathbf{V}_1^{\oplus} \mathbf{S}_1^T . \tag{75}$$

Then, for every $s \in (0,1)$, we can write the Gaussian formula

$$C_s = 2^N \sqrt{\frac{\det \mathbf{\Pi}_s}{\det \mathbf{\Sigma}_s}} \exp\left(-\frac{\mathbf{d}^T \mathbf{\Sigma}_s^{-1} \mathbf{d}}{2}\right) , \tag{76}$$

where $\mathbf{d} := \bar{\mathbf{x}}_0 - \bar{\mathbf{x}}_1$ and

$$\mathbf{\Pi}_s := G_s(\mathbf{V}_0^{\oplus}) G_{1-s}(\mathbf{V}_1^{\oplus}) , \tag{77}$$

$$\mathbf{\Sigma}_s := \mathbf{S}_0 \left[\Lambda_s(\mathbf{V}_0^{\oplus})\right] \mathbf{S}_0^T + \mathbf{S}_1 \left[\Lambda_{1-s}(\mathbf{V}_1^{\oplus})\right] \mathbf{S}_1^T . \tag{78}$$

In the previous formula, the matrix $\mathbf{\Pi}_s$ is diagonal and very easy to compute, depending only on the symplectic spectra. In particular, for pure states ($\mathbf{V}_0^{\oplus} = \mathbf{V}_1^{\oplus} = \mathbf{I}$) we have $\mathbf{\Pi}_s = \mathbf{I}$. By contrast, the computation of $\mathbf{\Sigma}_s$ is not straightforward due to the explicit presence of the two symplectic matrices $\mathbf{S}_0$ and $\mathbf{S}_1$, whose derivation may need non-trivial calculations in the general case (however see II.C.3 for two modes). If the computation of $\mathbf{S}_0$ and $\mathbf{S}_1$ is too difficult, one possibility is to use weaker bounds which depend on the symplectic spectra only, such as the *Minkowski bound* (Pirandola and Lloyd, 2008).

3. Quantum fidelity

Further bounds can be constructed using the *quantum fidelity*. In quantum teleportation and quantum cloning, the fidelity F is a commonly used measure to compare the input state to the output state. Given two quantum states, $\hat{\rho}_0$ and $\hat{\rho}_1$, their fidelity is defined by (Jozsa, 1994; Uhlmann, 1976)

$$F(\hat{\rho}_0, \hat{\rho}_1) := \left[\mathrm{Tr}\left(\sqrt{\sqrt{\hat{\rho}_0}\hat{\rho}_1\sqrt{\hat{\rho}_0}}\right)\right]^2 , \tag{79}$$

which ranges from zero (for orthogonal states) to one (for identical states). In the specific case of two single-mode Gaussian states, $\hat{\rho}_0(\bar{x}_0, \mathbf{V}_0)$ and $\hat{\rho}_1(\bar{x}_1, \mathbf{V}_1)$, we have (Holevo, 1975; Nha and Carmichael, 2005; Olivares *et al.*, 2006; Scutaru, 1998)

$$F(\hat{\rho}_0, \hat{\rho}_1) = \frac{2}{\sqrt{\Delta + \delta} - \sqrt{\delta}} \exp\left[-\frac{1}{2}\mathbf{d}^T (\mathbf{V}_0 + \mathbf{V}_1)^{-1} \mathbf{d}\right] , \tag{80}$$

where $\Delta := \det(\mathbf{V}_0 + \mathbf{V}_1)$, $\delta := (\det \mathbf{V}_0 - 1)(\det \mathbf{V}_1 - 1)$ and $\mathbf{d} := \bar{x}_1 - \bar{x}_0$. Using the fidelity, we can define the two fidelity bounds (Fuchs and de Graaf, 1999)

$$F_- := \tfrac{1}{2}\left[1 - \sqrt{1 - F(\hat{\rho}_0, \hat{\rho}_1)}\right] , \ F_+ := \tfrac{1}{2}\sqrt{F(\hat{\rho}_0, \hat{\rho}_1)} , \tag{81}$$

which provide further estimates for the minimum error probability. In particular, they satisfy the chain of inequalities

$$F_- \leq p_{e,min} \leq p_{QC} \leq p_B \leq F_+ . \tag{82}$$

4. Multicopy discrimination

In general, let us assume that we have M copies of the unknown quantum state $\hat{\rho}$, which again can take the two possible forms, $\hat{\rho}_0$ or $\hat{\rho}_1$, with the same probability. In other words, we have the two equiprobable hypotheses

$$H_0 : \hat{\rho}^{\otimes M} = \hat{\rho}_0^{\otimes M} := \overbrace{\hat{\rho}_0 \otimes \cdots \otimes \hat{\rho}_0}^{M} , \tag{83}$$

$$H_1 : \hat{\rho}^{\otimes M} = \hat{\rho}_1^{\otimes M} := \underbrace{\hat{\rho}_1 \otimes \cdots \otimes \hat{\rho}_1}_{M} . \tag{84}$$

The optimal quantum measurement for discriminating the two cases is now a collective measurement involving all the M copies. This is the same dichotomic POVM as before, now projecting on the positive part of the Helstrom matrix $\gamma = \hat{\rho}_0^{\otimes M} - \hat{\rho}_1^{\otimes M}$. Correspondingly, the Helstrom bound for the M-copy state discrimination takes the form

$$p_{e,min}^{(M)} = \frac{1}{2}\left[1 - D\left(\hat{\rho}_0^{\otimes M}, \hat{\rho}_1^{\otimes M}\right)\right] . \tag{85}$$

This quantity is upper bounded by the general M-copy expression of the quantum Chernoff bound, i.e.,

$$p_{e,min}^{(M)} \leq p_{QC}^{(M)} := \frac{1}{2}\left(\inf_{0 \leq s \leq 1} C_s\right)^M . \tag{86}$$

Interestingly, in the limit of many copies ($M \gg 1$), the quantum Chernoff bound is exponentially tight (Audenaert *et al.*, 2007). This means that, for large M, the two quantities $p_{e,min}^{(M)}$ and $p_{QC}^{(M)}$ decay exponentially with the same error-rate exponent, i.e.,

$$p_{e,min}^{(M)} \to \vartheta \exp(-M\kappa) , \ p_{QC}^{(M)} \to \upsilon \exp(-M\kappa) , \tag{87}$$

where $\vartheta \leq \upsilon$ and κ is known as the quantum Chernoff information (Calsamiglia *et al.*, 2008). Note that we can also consider other measures of distinguishability, like the M-copy version of the quantum Bhattacharyya bound

$$p_{QC}^{(M)} \leq p_B^{(M)} := \frac{1}{2}\left[\mathrm{Tr}\left(\sqrt{\hat{\rho}_0}\sqrt{\hat{\rho}_1}\right)\right]^M . \tag{88}$$

However, even though it is easier to compute, it is not exponentially tight in the general case.

B. Distinguishing optical coherent states

The distinguishing of coherent states with minimum error is one of the fundamental tasks in optical communication theory. For example, we can consider a simple theoretical way of modeling current telecommunication systems by considering weak coherent states to send binary information which has been encoded via the amplitude or phase modulation of a laser beam[2]. Such states have small amplitudes and are largely overlapping (i.e., nonorthogonal) and hence the ability to successfully decode this classical information is bounded by the minimum error given the Helstrom bound. Note that starting off with orthogonal states might make more sense, however, if orthogonal states were to be used their orthogonality is typically lost due to real world imperfections such as energy dissipation and excess noise on the optical fibre. By achieving the lowest error possible, the information transfer rate between the sender and receiver can be maximized. We will now illustrate a typical protocol involving the distinguishing of coherent states.

Suppose we have a sender, Alice, and a receiver, Bob. Alice prepares one of two binary coherent states $\hat{\rho}_0$ and $\hat{\rho}_1$ where one may be encoded as a logical "0" and the other a logical "1", respectively. These two states form what is known as the *alphabet* of possible states from which Alice can choose to send and whose contents are also known by Bob. Furthermore, the probabilities of each state being sent, p_0 and p_1, are also known by Bob. Alice can decide to use either an amplitude modulation keyed encoding, or a binary phase-shift keyed encoding, given respectively as,

$$|0\rangle \quad \text{and} \quad |2\,\alpha\rangle\,, \qquad |\alpha\rangle \quad \text{and} \quad |-\alpha\rangle\,. \tag{89}$$

We note that it is possible to transform between the two encoding schemes by using a displacement, e.g., by applying the displacement operator $D(\alpha)$ to each of the two binary phase-shift keyed coherent states we retrieve the amplitude modulation keyed encodings: $D(\alpha)\,|-\alpha\rangle = |0\rangle$ and $D(\alpha)\,|\alpha\rangle = |2\,\alpha\rangle$. Bob's goal is to decide with minimum error, which of the two coherent states he received from Alice (over, for example, a quantum channel with no loss and no noise). Bob's strategy is based on *quantum hypothesis testing* in which he devises two hypotheses: H_0 and H_1. Here H_0 corresponds to the situation where $\hat{\rho}_0$ was sent whilst H_1 corresponds to $\hat{\rho}_1$ being sent. As mentioned earlier, the POVM that optimizes this decision problem is actually a projective or von Neumann measurement, i.e., described by the two operators Π_0 and Π_1, such that $\Pi_i \geq 0$ for $i = 0, 1$ and $\Pi_0 + \Pi_1 = I$. Here the measurement described by the operator Π_0 selects the state $\hat{\rho}_0$ while $\Pi_1 = I - \Pi_0$ selects $\hat{\rho}_1$. The probability of error quantifies the probability in misinterpreting which state was actually received by Bob and is given by

$$p_e = p_0\; p(H_1|\hat{\rho}_0) + p_1\; p(H_0|\hat{\rho}_1), \tag{90}$$

where $p(H_i|\hat{\rho}_j)$ is defined as the conditional probability, i.e., probability that Bob decided it was hypothesis H_i when in fact it was $\hat{\rho}_j$, for $i \neq j$. The conditional probabilities can be written as

$$p(H_1|\hat{\rho}_0) = \mathrm{tr}[\Pi_1\hat{\rho}_0], \quad p(H_0|\hat{\rho}_1) = \mathrm{tr}[\Pi_0\hat{\rho}_1]. \tag{91}$$

Consequently, in the binary phase-shift keyed setting we can write the Helstrom bound as

$$p_e = p_0\,\langle\alpha|\,\Pi_1\,|\alpha\rangle + p_1\,\langle-\alpha|\,\Pi_0\,|-\alpha\rangle\,, \tag{92}$$

and for the amplitude modulation keyed encoding

$$p_e = p_0\,\langle 0|\,\Pi_1\,|0\rangle + p_1\,\langle 2\alpha|\,\Pi_0\,|2\alpha\rangle\,. \tag{93}$$

The optimal type of measurement needed to achieve the Helstrom bound when distinguishing between two coherent states was shown (Helstrom, 1976) to correspond to a Schrodinger cat-state basis (i.e., a superposition of two coherent states (Jeong and Ralph, 2007)): $\Pi_0 = |\psi\rangle\langle\psi|$ with $|\psi\rangle = c_0(\gamma)\,|0\rangle + c_1(\gamma)\,|\gamma\rangle$ where the actual weightings (c_1 and c_2) depend on the displacement γ. After Helstrom introduced his error probability bound in 1968, it was not until 1973, that two different physical models of implementing the receiver were discovered. The first construction, by Kennedy (1973), involved building a receiver based on direct detection (or photon counting) that was *near-optimal*, i.e., an error probability that was larger than the optimal Helstrom bound. However, building on Kennedy's initial proposal, Dolinar (1973) discovered how one could achieve the optimal bound using an adaptive feedback process with photon counting. Over the years other researchers have continued to make further progress in this area (Bondurant, 1993; Geremia, 2004; Olivares and Paris, 2004; Osaki *et al.*, 1996). Recently, Kennedy's original idea was improved upon with a receiver that was much simpler to implement than Dolinar's (although still near-optimal) but produced a smaller error probability than Kennedy's. Such a device is called an optimized displacement receiver (Takeoka and Sasaki, 2008; Wittmann *et al.*, 2008). However, the simplest possible receiver to implement is the conventional homodyne receiver, a common element in optical communication which is also near-optimal outperforming the Kennedy receiver, albeit only for small coherent amplitudes. We will now review each of these receivers in more detail.

1. Kennedy receiver

Kennedy (1973) gave the first practical realization of a receiver with an error probability twice that of the Helstrom bound. The Kennedy receiver distinguishes between the alphabet $|\alpha\rangle$ and $|-\alpha\rangle$ by first displacing each of the coherent

[2] More specifically, fiber communications currently employ in-line optical amplifiers, so the states that are received are bathed in amplified spontaneous emission noise and, moreover, received by direct detection. Future fiber systems – in which bandwidth efficiency is being sought – will go to coherent detection, but they will use much larger than binary signal constellations, i.e., quadrature amplitude modulation. Laser communication from space will use direct detection and M-ary pulse-position modulation rather than binary modulation.

states by α, i.e., $|-\alpha\rangle \rightarrow |0\rangle$ and $|\alpha\rangle \rightarrow |2\alpha\rangle$. Bob then measures the number of incoming photons between the times $t = 0$ and $t = T$ using direct photon counting, represented by the operators

$$\Pi_1 = |0\rangle\langle 0| \quad \text{and} \quad \Pi_2 = I - |0\rangle\langle 0|. \tag{94}$$

If the number of photons detected during this time is zero then $|0\rangle$ is chosen (as the vacuum contains no photons) otherwise it is assumed to have been $|2\alpha\rangle$. Hence, the Kennedy receiver always chooses $|0\rangle$ correctly (ignoring experimental imperfections), where the error in the decision results from the vacuum fluctuations in $|2\alpha\rangle$ (as any coherent state has some finite overlap with the vacuum state). Using Eq. (93), where from now on we use the least classical probability situation of $p_1 = p_2 = 1/2$, the error probability is given by $p_e^k = \frac{1}{2}\langle 2\alpha|\,\Pi_1\,|2\alpha\rangle$ which is equal to

$$p_e^k = \frac{1}{2}\exp(-4|\alpha|^2). \tag{95}$$

where we have used Eq. (30). The above error bound is sometimes known as the *shot-noise error*.

2. Dolinar receiver

Dolinar (1973) built upon the results of Kennedy by constructing a physical scheme that saturates the Helstrom bound. Using Eq. (69) with Eq. (30), the Helstrom bound for two pure coherent states $|\alpha\rangle$ and $|-\alpha\rangle$ is given by

$$p_{e,min} = \frac{1}{2}(1 - \sqrt{1 - \exp(-4|\alpha|^2)}).$$

This is the lowest possible error in distinguishing between two pure coherent states. Dolinar's scheme combined photon counting with real-time quantum feedback. Here the incoming coherent signal is combined on a beam splitter with a local oscillator whose amplitude is causally dependent on the number of photons detected in the signal beam. Such an adaptive process is continually repeated throughout the duration of the signal length where a decision is made based on the parity of the final number of photons detected (Geremia, 2004; Helstrom, 1976; Takeoka *et al.*, 2005). Many years after Dolinar's proposal, other approaches, such as using a highly nonlinear unitary operation (Sasaki and Hirota, 1996) or fast feedforward (Takeoka *et al.*, 2005), have also achieved the Helstrom bound by approximating the required Schrodinger cat state measurement basis (the actual creation of such a basis is experimentally very difficult (Ourjoumtsev *et al.*, 2007)). However, an experimental implementation of Dolinar's original approach was recently demonstrated in a proof-of-principle experiment (Cook *et al.*, 2007).

3. Homodyne receiver

As its name suggests the homodyne receiver uses a homodyne detector to distinguish between the coherent states $|\alpha\rangle$ and $|-\alpha\rangle$. Such a setup is considered the simplest setup possible and unlike the other receivers relies only on Gaussian operations. The POVMs for the homodyne receiver are modeled by the projectors

$$\Pi_1 = \int_0^\infty dx\,|x\rangle\langle x| \quad \text{and} \quad \Pi_2 = I - \Pi_1, \tag{96}$$

where a positive (negative) outcome is obtained identifying $|\alpha\rangle$ ($|-\alpha\rangle$). It was proven by Takeoka and Sasaki (2008) that the simple homodyne detector is optimal among all available Gaussian measurements. In fact, for weak coherent states (amplitudes $|\alpha|^2 < 0.4$), the homodyne receiver is near-optimal and has a lower error probability than the Kennedy receiver. Such a regime corresponds to various quantum communication protocols as well as deep space communication. Using Eq. (92) with the projectors from Eq. (96) and the fact that $|\langle -\alpha|\,x\rangle|^2 = \pi^{-1/2}\exp[-(x + |\alpha|/2)^2]$, the error probability for the homodyne receiver is given by (Olivares and Paris, 2004; Takeoka and Sasaki, 2008)

$$p_e^h = \frac{1}{2}\Big(1 - \mathrm{erf}\Big[|\alpha|/2\Big]\Big), \tag{97}$$

where $\mathrm{erf}[\cdot]$ is the error function. This limit is known as the *homodyne limit*.

4. Optimized displacement receiver

The optimized displacement receiver (Takeoka and Sasaki, 2008) is a modification of the Kennedy receiver where instead of displacing $|\alpha\rangle$ and $|-\alpha\rangle$ by α, both are now displaced by an optimized value β, where $\alpha, \beta \in \mathbb{R}$. This displacement $D(\beta)$ is based on optimizing both terms in the error probability of Eq. (92). When considering the Kennedy receiver, only the $p_1\langle -\alpha|\,\Pi_1\,|-\alpha\rangle$ term is minimized. However, the optimized displacement receiver, is based on optimizing the sum of the two probabilities as a function of the displacement β. The signal states $|\pm\alpha\rangle$ are now displaced by β according to

$$|\pm\alpha\rangle \rightarrow \left|\pm\sqrt{\tau}\alpha + \beta\right\rangle, \tag{98}$$

for a transmission τ in the limit of $\tau \rightarrow 1$. As with the Kennedy receiver photon detection is used to detect the incoming states and is described by the projectors given in Eq. (94). Using Eqs. (92) and (30) but with the coherent states now given by Eq. (98), the error probability can be expressed as

$$p_e^\beta = \frac{1}{2} - \exp[-(\tau|\alpha|^2 + |\beta|^2)]\sinh(2\sqrt{\tau}\alpha\beta). \tag{99}$$

The optimized displacement receiver outperforms both the homodyne receiver and the Kennedy receiver for all values of α. It is interesting to note that such a receiver has applications in quantum cryptography where it has been shown to increase the secret-key rates of certain protocols (Wittmann *et al.*, 2010a,b). Furthermore, by including squeezing with the displacement, an improvement in the performance of the receiver can be achieved (Takeoka and Sasaki, 2008). The optimized

displacement receiver has also been demonstrated experimentally (Tsujino *et al.*, 2011; Wittmann *et al.*, 2008).

To summarize, in terms of performance, the hierarchy for the above mentioned receivers is the following: (1) Dolinar receiver, (2) optimized displacement receiver, (3) Kennedy receiver and (4) homodyne receiver. Again, out of the ones mentioned, the Dolinar receiver is the only one that is optimal. Furthermore, the Kennedy receiver has a lower error probability than the homodyne receiver for most values of amplitude. Finally, we point out that our discussions of binary receivers (photon counters) presumes unity quantum efficiency with no dark noise or thermal noise, and hence paints an ideal theoretical comparison between all of the mentioned receivers.

IV. EXAMPLES OF GAUSSIAN QUANTUM PROTOCOLS

A. Quantum teleportation and variants

Quantum teleportation is one of the most beautiful protocols in quantum information. Originally developed for qubits (Bennett *et al.*, 1993), it was later extended to continuous-variable systems (Braunstein and Kimble, 1998; Ralph and Lam, 1998; Vaidman, 1994), where coherent states are teleported via the EPR correlations shared by two distant parties. It has also been demonstrated experimentally (Bowen *et al.*, 2003; Furusawa *et al.*, 1998; Zhang *et al.*, 2003). Here we review the quantum teleportation protocol for Gaussian states using the formalism of (Chizhov *et al.*, 2002; Fiurášek, 2002b; Pirandola and Mancini, 2006).

Two parties, say Alice and Bob, possess two modes, a and b, prepared in a zero-mean Gaussian state $\hat{\rho}(\mathbf{0},\mathbf{V})$ whose covariance matrix $\mathbf{V}$ can be written in the $(\mathbf{A},\mathbf{B},\mathbf{C})$-block form of Eq. (53). This state can be seen as a virtual channel that Alice can exploit to transfer an input state to Bob. In principle the input state can be completely arbitrary. In practical applications she will typically pick her state from some previously agreed alphabet. Consider the case in which she wishes to transfer a Gaussian state $\hat{\rho}_{in}(\bar{\mathbf{x}}_{in},\mathbf{V}_{in})$, with fixed covariance matrix $\mathbf{V}_{in}$ but unknown mean $\bar{\mathbf{x}}_{in}$ (chosen from a Gaussian distribution), from her input mode in to Bob. To accomplish this task, Alice must destroy her state $\hat{\rho}_{in}$ by combining modes in and a in a joint Gaussian measurement, known as a *Bell measurement*, where Alice mixes in and a in a balanced beam splitter and homodynes the output modes, $-$ and $+$ by measuring $\hat{q}_-$ and $\hat{p}_+$, respectively. The outcome of the measurement $\gamma := (q_- + ip_+)/2$ is then communicated to Bob via a standard telecom line. Once he receives this information, Bob can reconstruct Alice's input state by applying a displacement $D(\gamma)$ on his mode b, which outputs a Gaussian state $\hat{\rho}_{out} \simeq \rho_{in}$. The performance of the protocol is expressed by the teleportation fidelity F. This is the fidelity between the input and the output states averaged over all the outcomes of the Bell measurement. Assuming pure Gaussian states as input, one has (Fiurášek, 2002b)

$$F = \frac{2}{\sqrt{\det \mathbf{\Gamma}}},\ \mathbf{\Gamma} := 2\mathbf{V}_{in}+\mathbf{Z}\mathbf{A}\mathbf{Z}+\mathbf{B}-\mathbf{Z}\mathbf{C}-\mathbf{C}^T\mathbf{Z}^T. \quad (100)$$

where again $\mathbf{Z} := \mathrm{diag}(1,-1)$. This formula can be generalized to virtual channels $\hat{\rho}(\bar{\mathbf{x}},\mathbf{V})$ with arbitrary mean $\bar{\mathbf{x}} = (\bar{q}_a,\bar{p}_a,\bar{q}_b,\bar{p}_b)^T$. This is possible if Bob performs the modified displacement $D(\gamma+\tilde{\gamma})$, where $\tilde{\gamma} := [(\bar{q}_b-\bar{q}_a)-i(\bar{p}_b+\bar{p}_a)]/2\sqrt{2}$ (Pirandola and Mancini, 2006).

In order to be truly quantum, the teleportation must have a fidelity above a classical threshold F_{class}. This value corresponds to the classical protocol where Alice measures her states, communicates the results to Bob who, in turn, reconstructs the states from the classical information. In general, a necessary condition for having $F > F_{class}$ is the presence of entanglement in the virtual channel. For bosonic systems, this is usually assured by the presence of EPR correlations. For instance, let us consider the case where the input states are coherent states chosen from a broad Gaussian distribution and the virtual channel is an EPR state $\hat{\rho}^{epr}(r)$. In this case, the teleportation fidelity is simply given by (Adesso and Illuminati, 2005; Furusawa *et al.*, 1998; Mari and Vitali, 2008)

$$F = (1+\tilde{\nu}_-)^{-1},\ \ \tilde{\nu}_- = \exp(-2\,|r|)\,. \quad (101)$$

Here the presence of EPR correlations ($r > 0$) guarantees the presence of entanglement ($\tilde{\nu}_- < 1$) and, correspondingly, one has $F > 1/2$, i.e., the fidelity beats the classical threshold for coherent states (Braunstein, Fuchs *et al.*, 2001; Hammerer *et al.*, 2005). A more stringent threshold for teleportation is to require that the quantum correlations between the input field and the teleported field are retained (Ralph and Lam, 1998). In turn this implies that the teleported field is the best copy of the input allowed by the no-cloning bound (Grosshans and Grangier, 2001). At unity gain this requires that $\tilde{\nu}_- < 1/2$ and corresponds to a coherent state fidelity $F > 2/3$ as was first demonstrated by Takei *et al.* (2005).

In continuous variables, the protocol of quantum teleportation has been extended in several ways, including number-phase teleportation (Milburn and Braunstein, 1999), all-optical teleportation (Ralph, 1999b), quantum teleportation networks (van Loock and Braunstein, 2000), teleportation of single photon states (Ide *et al.*, 2001; Ralph, 2001), quantum telecloning (van Loock and Braunstein, 2001), quantum gate teleportation (Bartlett and Munro, 2003), assisted quantum teleportation (Pirandola *et al.*, 2005), quantum teleportation games (Pirandola, 2005), and teleportation channels (Wolf *et al.*, 2007). One of the most important variants of the protocol is the teleportation of entanglement also known as *entanglement swapping* (Jia *et al.*, 2004; Takei *et al.*, 2005; van Loock and Braunstein, 1999). Here Alice and Bob possess two entangled states, $\hat{\rho}_{aa'}$ and $\hat{\rho}_{bb'}$, respectively. Alice keeps mode a and sends mode a' to a Bell measurement, while Bob keeps mode b and sends b'. Once a' and b' are measured and the outcome communicated, Alice and Bob will share an output state $\hat{\rho}_{ab}$, where a and b are entangled. For simplicity, let us suppose that Alice's and Bob's initial states are EPR states, i.e., $\hat{\rho}_{aa'} = \hat{\rho}_{bb'} = \hat{\rho}^{epr}(r)$. Using the input-output relations given in Pirandola *et al.* (2006), one can easily check that the output Gaussian state $\hat{\rho}_{ab}$ has logarithmic negativity $E_N(\hat{\rho}_{ab}) = \ln\cosh(2r)$, corresponding to entanglement for

every $r > 0$. By generalizing to two-mode entanglement, polarization entanglement can be swapped and shown to still violate a Bell inequality for $r > 0$ (Polkinghorne and Ralph, 1999).

Teleportation and entanglement swapping are protocols which may involve bosonic systems of different nature. For example, in Sherson *et al.* (2006) a quantum state was teleported from an optical mode onto a macroscopic object consisting of an atomic ensemble of about 10^{12} Caesium atoms. Theoretically, this kind of result can also be realized by using radiation pressure. In fact, by impinging a strong monochromatic laser beam onto a highly reflecting mirror, it is possible to generate a scattering process where an optical mode becomes entangled with an acoustic (massive) mode excited over the surface of the mirror. Exploiting this hybrid entanglement, the teleportation from an optical to an acoustic mode is possible in principle (Mancini *et al.*, 2003; Pirandola *et al.*, 2003), as well as the generation of entanglement between two acoustic modes by means of entanglement swapping (Pirandola *et al.*, 2006).

B. Quantum cloning

Following the seminal works of Wootters and Zurek (1982) and Dieks (1982), it is well known that a quantum transformation that outputs two perfect copies of an arbitrary input state $|\psi\rangle$ is precluded by the laws of quantum mechanics. This is the content of the celebrated *quantum no-cloning theorem*. More precisely, perfect cloning is possible, if and only if, the input state is drawn from a set of orthogonal states. Then, a simple von Neumann measurement enables the perfect discrimination of the states (see Sec. III), which in turn enables the preparation of exact copies of the measured state. In contrast, if the input state is drawn from a set of non-orthogonal states, perfect cloning is impossible. A notable example of this are coherent states which cannot be perfectly distinguished nor cloned as a result of Eq. (30). Interestingly, although perfect cloning is forbidden, one can devise approximate *cloning machines*, which produce imperfect copies of the original state. The concept of a cloning machine was introduced by Bužek and Hillery (1996), where the cloning machine produced two identical and optimal clones of an arbitrary single qubit. Their work launched a whole new field of investigation (Cerf and Fiurášek, 2006; Scarani *et al.*, 2005). Cloning machines are intimately related to quantum cryptography (see Sec. VI) as they usually constitute the optimal attack against a given protocol, so that finding the best cloning machine is crucial to address the security of a quantum cryptographic protocol (Cerf and Grangier, 2007).

The extension of quantum cloning to continuous-variable systems was first carried out by Cerf *et al.* (2000) and Lindblad (2000), where a Gaussian cloning machine was shown to produce two noisy copies of an arbitrary coherent state (where the figure of merit here is the single-clone excess noise variance). The input mode, described by the quadratures $(\hat{q}_{in}, \hat{p}_{in})$, is transformed into two noisy clones $(\hat{q}_{1(2)}, \hat{p}_{1(2)})$ according to

$$\hat{q}_{1(2)} = \hat{q}_{in} + \hat{N}_{q1(2)}, \quad \hat{p}_{1(2)} = \hat{p}_{in} + \hat{N}_{p1(2)}, \tag{102}$$

where $\hat{N}_{q1(2)}$ and $\hat{N}_{p1(2)}$ stand for the added noise operators on the output mode 1 (2). We may impose $\langle \hat{N}_{q1(2)} \rangle = \langle \hat{N}_{p1(2)} \rangle = 0$, so that the mean values of the output quadratures coincide with those of the original state. It is the variance of the added noise operators which translates the cloning imperfection: a generalized uncertainty relation for the added noise operators can be derived (Cerf, 2003; Cerf *et al.*, 2000),

$$\Delta \hat{N}_{q1} \Delta \hat{N}_{p2} \geq 1, \quad \Delta \hat{N}_{p1} \Delta \hat{N}_{q2} \geq 1, \tag{103}$$

which is saturated (i.e., lower bounded) by this cloning machine. The above inequalities clearly imply that it is impossible to have two clones with simultaneously vanishing noise in the two canonically conjugate quadratures. This can be straightforwardly linked to the impossibility of simultaneously measuring perfectly the two canonically conjugate quadratures of the input mode: if we measure $\hat{q}$ on the first clone and $\hat{p}$ on the second clone, the cloning machine actually produces the exact amount of noise that is necessary to prevent this procedure from beating the optimal (heterodyne) measurement (Lindblad, 2000).

The Gaussian cloning machine was first derived in the quantum circuit language (Cerf *et al.*, 2000), which may, for example, be useful for the cloning of light states onto atomic ensembles (Fiurášek *et al.*, 2004). However, an optical version was later developed by Braunstein, Cerf *et al.* (2001) and Fiurášek (2001), which is better suited for our purposes here. The cloning machine can be realized with a linear phase-insensitive amplifier of intensity gain two, followed by a balanced beam splitter. The two clones are then found in the two output ports of the beam splitter, while an anti-clone is found in the idler output of the amplifier. The anti-clone is defined as an imperfect version of the phase-conjugate $|\alpha^*\rangle$ of the input state $|\alpha\rangle$, where $\alpha = (q + ip)/2$ and $\alpha^* = (q - ip)/2$. The symplectic transformation on the quadrature operators $\hat{\mathbf{x}} = (\hat{q}_1, \hat{p}_1, \hat{q}_2, \hat{p}_2, \hat{q}_3, \hat{p}_3)^T$ of the three input modes reads

$$\hat{\mathbf{x}} \to \mathbf{C}\hat{\mathbf{x}}, \qquad \mathbf{C} = (\mathbf{B} \oplus \mathbf{I})(\mathbf{I} \oplus \mathbf{S}_2) \tag{104}$$

where $\mathbf{B}$ is the symplectic map of a beam splitter with transmittance $\tau = 1/2$ as defined in Eq. (38), $\mathbf{S}_2$ is the symplectic map of a two-mode squeezer with intensity gain $\cosh^2 r = 2$ as defined in Eq. (40), and $\mathbf{I}$ is a 2×2 identity matrix. The input mode of the cloner is the signal mode of the amplifier (mode 2), while the idler mode of the amplifier (mode 3) and the second input mode of the beam splitter (mode 1) are both prepared in the vacuum state. At the output, modes 1 and 2 carry the two clones, while mode 3 carries the anti-clone. By reordering the three $\hat{q}$ quadratures before the three $\hat{p}$ quadratures, we can express the cloning symplectic map as

$$\mathbf{C} = \begin{pmatrix} 2^{-1/2} & 1 & 2^{-1/2} \\ -2^{-1/2} & 1 & 2^{-1/2} \\ 0 & 1 & 2^{1/2} \end{pmatrix} \oplus \begin{pmatrix} 2^{-1/2} & 1 & -2^{-1/2} \\ -2^{-1/2} & 1 & -2^{-1/2} \\ 0 & -1 & 2^{1/2} \end{pmatrix} \tag{105}$$

The second columns of the $\hat{q}$ and $\hat{p}$ blocks immediately imply that the two clones are centered on the input state $(\hat{q}_2, \hat{p}_2)$, while the anti-clone is centered on the phase conjugate of the input state $(\hat{q}_2, -\hat{p}_2)$. We can also check that the covariance matrix of the output modes can be expressed as

$$\mathbf{V}_1 = \mathbf{V}_2 = \mathbf{V}_{in} + \mathbf{I}, \qquad \mathbf{V}_3 = \mathbf{Z}\mathbf{V}_{in}\mathbf{Z} + 2\mathbf{I} \tag{106}$$

where $\mathbf{V}_{in}$ is the covariance matrix of the input mode (mode 2) and again $\mathbf{Z} = \mathrm{diag}(1, -1)$. Thus, the two clones suffer exactly one unit of additional shot-noise, while the anti-clone suffers two shot-noise units. This can be expressed in terms of the cloning fidelities of Eq. (80). The fidelity of each of the clones is given by $F = 2/3$, regardless of which coherent state is cloned. The anti-clone is noisier, and characterized by a fidelity of $F = 1/2$. Note that this latter fidelity is precisely that of an optimal joint measurement of the two conjugate quadratures (Arthurs and Kelly, Jr., 1965), so that optimal (imperfect) phase conjugation can be classically achieved by heterodyning the state and preparing its phase-conjugate (Cerf and Iblisdir, 2001b).

A variant of this optical cloner was demonstrated experimentally by Andersen *et al.* (2005), where the amplifier was replaced by a feed forward optical scheme which only requires linear optical components and homodyne detection (Lam *et al.*, 1997). A fraction of the signal beam is tapped off and measured using heterodyne detection. The outcomes of this measurement are then used to apply an appropriate displacement to the remaining part of the signal beam. This setup demonstrates near optimal quantum noise limited performances, and can also be adapted to produce a phase-conjugate output (Josse *et al.*, 2006). This 1-to-2 Gaussian cloner can be straightforwardly extended to a more general setting, where M identical clones are produced from N identical replica of an unknown coherent state with a fidelity $F = MN/(MN + M - N)$ (Cerf and Iblisdir, 2000). More generally, one can add N' replica of the phase-conjugate state at the input and produce $M' = M + N' - N$ anti-clones (Cerf and Iblisdir, 2001a). In this more elaborate scheme, the signal mode carries all inputs and clones, while the idler mode carries all phase-conjugate inputs and anti-clones. Interestingly, for a fixed total number of inputs $N+N'$ the clones have a higher fidelity if $N' > 0$, a property which holds regardless of M and even survives at the limit of a measurement $M \to \infty$. So the cloning or measurement performances are enhanced by phase-conjugate inputs. For example, the precision of measuring the quadratures of two phase-conjugate states $|\alpha\rangle\,|\alpha^*\rangle$ is as high as that achieved when measuring four identical states $|\alpha\rangle^{\otimes 4}$ though half of the mean energy is needed, as experimentally demonstrated by Niset *et al.* (2007). Furthermore, the cloning of phase-conjugate coherent states was suggested by Chen and Zhang (2007) and also suggested, as well as demonstrated, by Sabuncu *et al.* (2007) using the linear cloner of Andersen *et al.* (2005).

Gaussian cloners have also been theoretically devised in an asymmetric setting, where the clones have different fidelities (Fiurášek, 2001). The way to achieve asymmetry is to use an additional beam splitter that deflects a fraction of the input beam before entering the signal mode of the amplifier. This deflected beam bypasses the amplifier and feeds the vacuum input port of the beam splitter that yields the two clones. By tuning the transmittance of the beam splitters, one can generate the entire family of cloners saturating Eq. (103). This idea can also be generalized to define the optimal asymmetric cloner producing M different clones (Fiurášek and Cerf, 2007). Other research into Gaussian quantum cloning includes, the relationship of the no-cloning limit to the quality of continuous-variable teleportation (Grosshans and Grangier, 2001), the optimal cloning of coherent states with a finite distribution (Cochrane *et al.*, 2004), the cloning of squeezed and thermal states (Olivares *et al.*, 2006), and the cloning of both entangled Gaussian states and Gaussian entanglement (Weedbrook *et al.*, 2008). Finally, it is worth noting that all the Gaussian cloners discussed above are optimal if the added noise variance is taken as the figure of merit. The Gaussian transformation of Eq. (105) produces clones with the minimum noise variance, namely one unit of shot-noise. Surprisingly, if the single-clone fidelity is chosen instead as the figure of merit, the optimal cloner is a non-Gaussian cloner which slightly outperforms the Gaussian cloner (its fidelity is 2.4 % higher) for the cloning of Gaussian (coherent) states (Cerf *et al.*, 2005).

V. BOSONIC GAUSSIAN CHANNELS

A central topic in quantum information theory is the study of bosonic channels, or more properly, linear bosonic channels (Demoen *et al.*, 1977; Lindblad, 2000). In particular, Gaussian channels represent the standard model of noise in many quantum communication protocols (Eisert and Wolf, 2007; Holevo *et al.*, 1999; Holevo and Werner, 2001). They describe all those communication processes where the interaction between the bosonic system carrying the information and the external decohering environment is governed by a linear and/or bilinear Hamiltonian. In the simplest scenario, Gaussian channels are memoryless, meaning that different bosonic systems are affected independently and identically. This is the case of the one-mode Gaussian channels, where each mode sent through the channel is perturbed in this way (Holevo, 2007; Holevo and Werner, 2001).

This section is structured as follows. In Sec. V.A, we give a general introduction to bosonic channels and, particularly, Gaussian channels, together with their main properties. Then, in Sec. V.B, we discuss the specific case of one-mode Gaussian channels and their recent full classification. In Secs. V.C and V.D we discuss the standard notions of classical and quantum capacity, respectively, with quantum dense coding and entanglement-assisted classical capacity revealed in Sec. V.E. Entanglement distribution and secret key capacities are discussed in Sec. V.F. Finally, in Sec. V.G, we consider the problem of Gaussian channel discrimination and its potential applications.

A. General formalism

Let us consider a multimode bosonic system, with arbitrary N modes, whose quantum state is described by an arbitrary density operator $\hat{\rho} \in \mathcal{D}(\mathcal{H}^{\otimes N})$. Then, an N-mode bosonic channel is a linear map $\mathcal{E} : \hat{\rho} \rightarrow \mathcal{E}(\hat{\rho}) \in \mathcal{D}(\mathcal{H}^{\otimes N})$, which must be completely positive and trace-preserving (CPT) (Nielsen and Chuang, 2000). There are several equivalent ways to represent this map, one of the most useful being the Stinespring dilation (Stinespring, 1955). As depicted in Fig. 1, a multimode bosonic channel can be represented by a unitary interaction U between the input state $\hat{\rho}$ and a pure state $|\Phi\rangle_E$ of ancillary N_E modes associated with the environment. Then the output of the channel is given by tracing out the environment after interaction, i.e.,

$$\mathcal{E}(\hat{\rho}) = \mathrm{Tr}_E \left[U \left(\hat{\rho} \otimes |\Phi\rangle \langle\Phi|_E \right) U^{\dagger} \right] . \tag{107}$$

An important property of the Stinespring dilation is its uniqueness up to partial isometries (Paulsen, 2002). As a result, one can always choose $|\Phi\rangle_E = |0\rangle_E$, where $|0\rangle_E$ is a multimode vacuum state.

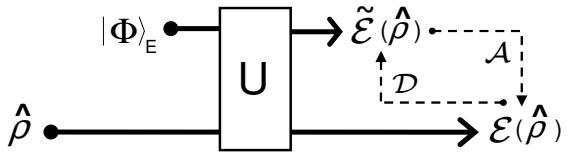


FIG. 1 Stinespring dilation of a bosonic channel $\mathcal{E}$. The input state $\hat{\rho}$ interacts unitarily with a pure state $|\Phi\rangle_E$ of the environment, which can be chosen to be the vacuum. Note that, besides the output $\mathcal{E}(\hat{\rho})$, there is a complementary output $\tilde{\mathcal{E}}(\hat{\rho})$ for the environment. In some cases, the two outputs are connected by CPT maps (see text).

Note that, in the physical representation provided by the Stinespring dilation, the environment has an output too. In fact, we can consider the *complementary* bosonic channel $\tilde{\mathcal{E}} : \hat{\rho} \rightarrow \tilde{\mathcal{E}}(\hat{\rho})$ which is defined by tracing out the system after interaction. For particular kinds of bosonic channels, the two outputs $\mathcal{E}(\hat{\rho})$ and $\tilde{\mathcal{E}}(\hat{\rho})$ are connected by CPT maps. This happens when the channel is *degradable* or *anti-degradable*. By definition, we say that a bosonic channel $\mathcal{E}$ is *degradable* if there exists a CPT map $\mathcal{D}$ such that $\mathcal{D} \circ \mathcal{E} = \tilde{\mathcal{E}}$ (Devetak and Shor, 2005). This means that the environmental output $\tilde{\mathcal{E}}(\hat{\rho})$ can be achieved from the system output $\mathcal{E}(\hat{\rho})$ by applying another bosonic channel $\mathcal{D}$. By contrast, a bosonic channel $\mathcal{E}$ is called *anti-degradable* when there is a CPT map $\mathcal{A}$ such that $\mathcal{A} \circ \tilde{\mathcal{E}} = \mathcal{E}$ (Caruso and Giovannetti, 2006) (see Fig. 1).

The most important bosonic channels are the Gaussian channels, defined as those bosonic channels transforming Gaussian states into Gaussian states. An arbitrary N-mode Gaussian channel can be represented by a Gaussian dilation. This means that the interaction unitary U in Eq. (107) is Gaussian and the environmental state $|\Phi\rangle_E$ is pure Gaussian (or, equivalently, the vacuum). Furthermore, we can choose an environment composed of $N_E \leq 2N$ modes (Caruso *et al.*, 2008, 2011). The action of a N-mode Gaussian channel over an arbitrary Gaussian state $\hat{\rho}(\bar{\mathbf{x}}, \mathbf{V})$ can be easily expressed in terms of the first and second statistical moments. In fact, we have (Holevo and Werner, 2001)

$$\bar{\mathbf{x}} \rightarrow \mathbf{T}\bar{\mathbf{x}} + \mathbf{d} \, , \;\; \mathbf{V} \rightarrow \mathbf{T}\mathbf{V}\mathbf{T}^T + \mathbf{N} \, , \tag{108}$$

where $\mathbf{d} \in \mathbb{R}^{2N}$ is a displacement vector, while $\mathbf{T}$ and $\mathbf{N} = \mathbf{N}^T$ are $2N \times 2N$ real matrices, which must satisfy the complete positivity condition

$$\mathbf{N} + i\boldsymbol{\Omega} - i\mathbf{T}\boldsymbol{\Omega}\mathbf{T}^T \geq 0 \, , \tag{109}$$

where $\boldsymbol{\Omega}$ is defined in Eq. (2). Note that, for $\mathbf{N} = \mathbf{0}$ and $\mathbf{T} := \mathbf{S}$ symplectic, the channel corresponds to a Gaussian unitary $U_{\mathbf{S},\mathbf{d}}$ (see Sec. II.A.2).

B. One-mode Gaussian channels

The study of one-mode Gaussian channels plays a central role in quantum information theory, representing one of the standard models to describe the noisy evolution of one-mode bosonic states. Furthermore, these channels represent the manifest effect of the most important eavesdropping strategy in continuous-variable quantum cryptography, known as collective Gaussian attacks, which will be fully discussed in Sec. VI.B.4. One of the central results in the theory of one-mode Gaussian channels is the Holevo's canonical classification. This result was originally derived by Holevo (2007) and then exploited by several authors to study the degradability and security properties of these channels (Caruso *et al.*, 2006; Pirandola, Braunstein, and Lloyd, 2008; Pirandola, García-Patrón, *et al.*, 2009).

An arbitrary one-mode Gaussian channel $\mathcal{G}$ is fully characterized by the transformations of Eq. (108), where now $\mathbf{d} \in \mathbb{R}^2$ and $\mathbf{T}, \mathbf{N}$ are 2×2 real matrices, satisfying

$$\mathbf{N} = \mathbf{N}^T \geq 0, \;\; \det \mathbf{N} \geq (\det \mathbf{T} - 1)^2 \, . \tag{110}$$

The latter conditions can be derived by specifying Eq. (109) to one mode ($N = 1$). According to Holevo (2007), the mathematical structure of a one-mode Gaussian channel $\mathcal{G} = \mathcal{G}(\mathbf{d}, \mathbf{T}, \mathbf{N})$ can be greatly simplified. As depicted in Fig. 2(a), every $\mathcal{G}$ can be decomposed as

$$\mathcal{G}(\hat{\rho}) = W \left[\mathcal{C}(U\hat{\rho}U^{\dagger}) \right] W^{\dagger} \, , \tag{111}$$

where U and W are Gaussian unitaries, while the map $\mathcal{C}$, which is called the *canonical form*, is a simplified Gaussian channel $\mathcal{C} = \mathcal{C}(\mathbf{d}_c, \mathbf{T}_c, \mathbf{N}_c)$ with $\mathbf{d}_c = \mathbf{0}$ and $\mathbf{T}_c, \mathbf{N}_c$ diagonal. The explicit expressions of $\mathbf{T}_c$ and $\mathbf{N}_c$ depend on three quantities which are preserved by the action of the Gaussian unitaries. These invariants are the generalized *transmissivity* $\tau := \det \mathbf{T}$ (ranging from $-\infty$ to $+\infty$), the *rank* of the channel $r := \min[\mathrm{rank}(\mathbf{T}), \mathrm{rank}(\mathbf{N})]$ (with possible values $r = 0, 1, 2$) and the *thermal number* $\bar{n}$, which is a non-negative number defined by

$$\bar{n} := \begin{cases} (\det \mathbf{N})^{1/2} \, , & \text{for } \tau = 1 \, , \\ \dfrac{(\det \mathbf{N})^{1/2}}{2\,|1-\tau|} - \dfrac{1}{2} \, , & \text{for } \tau \neq 1 \, . \end{cases} \tag{112}$$

These three invariants $\{\tau, r, \bar{n}\}$ fully characterize the two matrices $\mathbf{T}_c$ and $\mathbf{N}_c$, thus identifying a unique canonical form $\mathcal{C} = \mathcal{C}(\tau, r, \bar{n})$. In particular, the first two invariants $\{\tau, r\}$ determine the *class* of the form. The full classification is shown in table I.

τ	r	Class	Form	$\mathbf{T}_c$	$\mathbf{N}_c$
0	0	A_1	$\mathcal{C}(0,0,\bar{n})$	$\mathbf{0}$	$(2\bar{n}+1)\mathbf{I}$
0	1	A_2	$\mathcal{C}(0,1,\bar{n})$	$\frac{\mathbf{I}+\mathbf{Z}}{2}$	$(2\bar{n}+1)\mathbf{I}$
1	1	B_1	$\mathcal{C}(1,1,0)$	$\frac{\mathbf{I}+\mathbf{Z}}{2}$	$\frac{\mathbf{I}-\mathbf{Z}}{2}$
1	2	B_2	$\mathcal{C}(1,2,\bar{n})$	$\mathbf{I}$	$\bar{n}\mathbf{I}$
1	0	$B_2(Id)$	$\mathcal{C}(1,0,0)$	$\mathbf{I}$	$\mathbf{0}$
$(0,1)$	2	$C(Loss)$	$\mathcal{C}(\tau,2,\bar{n})$	$\sqrt{\tau}\mathbf{I}$	$(1-\tau)(2\bar{n}+1)\mathbf{I}$
>1	2	$C(Amp)$	$\mathcal{C}(\tau,2,\bar{n})$	$\sqrt{\tau}\mathbf{I}$	$(\tau-1)(2\bar{n}+1)\mathbf{I}$
<0	2	D	$\mathcal{C}(\tau,2,\bar{n})$	$\sqrt{-\tau}\mathbf{Z}$	$(1-\tau)(2\bar{n}+1)\mathbf{I}$

(113)

TABLE I The values of $\{\tau, r\}$ in the first two columns specify a canonical class A_1, A_2, B_1, B_2, C or D (third column). Within each class, the possible canonical forms are expressed in the fourth column, where also the invariant $\bar{n}$ must be considered. The corresponding expressions of $\mathbf{T}_c$ and $\mathbf{N}_c$ are shown in the last two columns, where $\mathbf{Z} := \mathrm{diag}(1,-1)$, $\mathbf{I} := \mathrm{diag}(1,1)$ and $\mathbf{0}$ is the zero matrix.

Let us discuss the various classes. Class A_1 is composed by forms which are completely depolarizing channels, i.e., replacing input states with thermal states. Classes A_2 and B_1 are special and involve canonical forms transforming the quadratures asymmetrically. Class B_2 describes the classical-noise channels, transforming the quadratures as $\hat{\mathbf{x}} \to \hat{\mathbf{x}} + \boldsymbol{\xi}$ where $\boldsymbol{\xi}$ is Gaussian noise with classical covariance matrix $\bar{n}\mathbf{I}$. This class collapses to the identity channel for $\bar{n} = 0$. Class C describes canonical forms with transmissivities $0 < \tau \neq 1$. This class is further divided in two subclasses: C(Loss) for $0 < \tau < 1$, and C(Amp) for $\tau > 1$. Canonical forms in C(Loss) are known as *lossy channels*, also denoted by $\mathcal{L}(\tau, \bar{n}) := \mathcal{C}(0 < \tau < 1, 2, \bar{n})$. These are the most important ones, representing the basic model to describe communication lines such as optical fibers. In a lossy channel, the input signals are attenuated and combined with thermal noise, i.e., we have $\hat{\mathbf{x}} \to \sqrt{\tau}\hat{\mathbf{x}} + \sqrt{1-\tau}\hat{\mathbf{x}}_{th}$, where $\hat{\mathbf{x}}_{th}$ are in a thermal state with $\bar{n}$ photons. Canonical forms in C(Amp) are known as *amplifying channels*, denoted by $\mathcal{A}(\tau, \bar{n}) := \mathcal{C}(\tau > 1, 2, \bar{n})$. They describe optical processes, such as phase-insensitive amplifiers, where the input signals are amplified with the addition of thermal noise, i.e., $\hat{\mathbf{x}} \to \sqrt{\tau}\hat{\mathbf{x}} + \sqrt{\tau - 1}\hat{\mathbf{x}}_{th}$. Finally, class D is associated with negative transmissivities. Its forms can be seen as complementary outputs of the amplifying channels.

We can easily construct the Stinespring dilation of all the canonical forms (Pirandola, Braunstein, and Lloyd, 2008). As depicted in Fig. 2(b), an arbitrary form $\mathcal{C}(\tau, r, \bar{n})$ can be dilated to a three-mode canonical unitary $U_{\mathbf{L}}$ corresponding to a 6×6 symplectic matrix $\mathbf{L}$. This unitary transforms the input state $\hat{\sigma}$ (mode A) together with an environmental EPR state $|\nu\rangle$ (modes E and e) of suitable noise-variance ν [see Eq. (42)]. In particular, the symplectic matrix is determined by the class, i.e., $\mathbf{L} = \mathbf{L}(\tau, r)$, while the EPR state is determined by the thermal number, i.e., $\nu = 2\bar{n} + 1$. Let us analyze $\mathbf{L}(\tau, r)$ for the various classes, starting from B_2. For null rank, class B_2 collapses to the identity and we simply have $\mathbf{L}(1,0) = \mathbf{I}$. However, for full rank the symplectic matrix $\mathbf{L}(1,2)$ does not have a simple expression (Holevo, 2007). If we exclude the class B_2, the symplectic matrix $\mathbf{L}$ can always be decomposed as $\mathbf{L}(\tau, r) = \mathbf{M}(\tau, r) \oplus \mathbf{I}_e$, where $\mathbf{M}$ describes a two-mode canonical unitary acting on modes A and E, while $\mathbf{I}_e$ is just the identity on mode e. As depicted in Fig. 2(c), this means that only one mode E of the EPR state $|\nu\rangle$ is actually combined with the input mode A. Clearly by tracing out the unused EPR mode e, we get a thermal state with $\bar{n}$ photons on mode E, as depicted in Fig. 2(d). Thus the canonical forms $\mathcal{C}(\tau, r, \bar{n})$ of all the classes but B_2 admit a physical representation where a single-mode thermal state $\hat{\rho}(\bar{n})$ interacts with the input state via a two-mode symplectic transformation $\mathbf{M}(\tau, r)$. Despite being simpler than the Stinespring dilation, this unitary dilation involves a mixed environmental state and, therefore, it is not unique up to partial isometries. The explicit expressions of $\mathbf{M}(\tau, r)$ are relatively easy (Caruso *et al.*, 2006). For classes A_1, A_2 and B_1, we

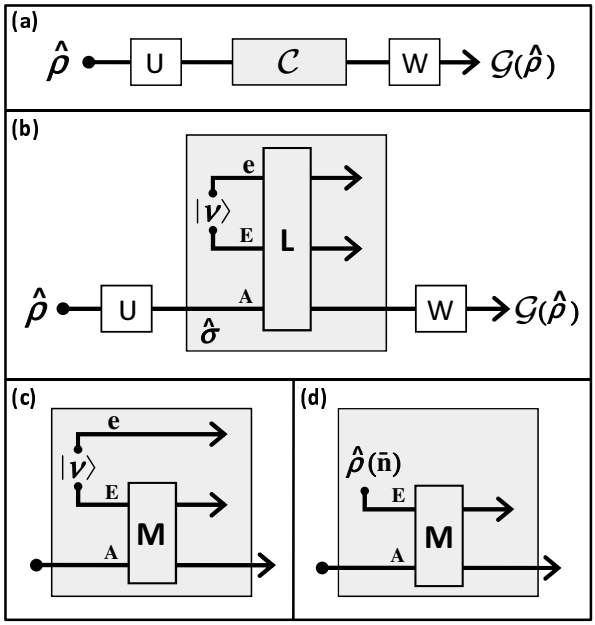


FIG. 2 (a) A generic one-mode Gaussian channel $\mathcal{G}$ can be represented by a canonical form $\mathcal{C}$ up to input and output Gaussian unitaries U and W. (b) An arbitrary canonical form $\mathcal{C} = \mathcal{C}(\tau, r, \bar{n})$ can be dilated to a three-mode canonical unitary $U_{\mathbf{L}}$ which is described by a class-dependent symplectic transformation $\mathbf{L} = \mathbf{L}(\tau, r)$. This unitary evolves the input state $\hat{\sigma}$ together with an EPR state $|\nu\rangle$ with noise-variance $\nu = 2\bar{n} + 1$ and belonging to the environment. (c) Apart from class B_2, all the other classes can be dilated using $\mathbf{L}(\tau, r) = \mathbf{M}(\tau, r) \oplus \mathbf{I}_e$. This means that only one mode E of the EPR state $|\nu\rangle$ is combined with the input mode A. (d) Tracing out mode e, we get a thermal state $\hat{\rho}(\bar{n})$ on mode E. Thus the canonical forms of all the classes but B_2 can be represented by a single-mode thermal state interacting with the input state via a two-mode symplectic transformation $\mathbf{M}$.

have

$$\mathbf{M}(0,0)=\begin{pmatrix}\mathbf{0} & \mathbf{I}\\ \mathbf{I} & \mathbf{0}\end{pmatrix}\ ,\ \mathbf{M}(0,1)=\begin{pmatrix}\frac{\mathbf{I}+\mathbf{Z}}{2} & \mathbf{I}\\ \mathbf{I} & \frac{\mathbf{Z}-\mathbf{I}}{2}\end{pmatrix}\ , \quad (114)$$

$$\mathbf{M}(1,1)=\begin{pmatrix}\mathbf{I} & \frac{\mathbf{I}+\mathbf{Z}}{2}\\ \frac{\mathbf{I}-\mathbf{Z}}{2} & -\mathbf{I}\end{pmatrix}\ . \quad (115)$$

Then, for classes $C(\text{Loss})$, $C(\text{Amp})$ and D, we have

$$\mathbf{M}(0<\tau<1,2)=\begin{pmatrix}\sqrt{\tau}\mathbf{I} & \sqrt{1-\tau}\mathbf{I}\\ -\sqrt{1-\tau}\mathbf{I} & \sqrt{\tau}\mathbf{I}\end{pmatrix}\ , \quad (116)$$

$$\mathbf{M}(\tau>1,2)=\begin{pmatrix}\sqrt{\tau}\mathbf{I} & \sqrt{\tau-1}\mathbf{Z}\\ \sqrt{\tau-1}\mathbf{Z} & \sqrt{\tau}\mathbf{I}\end{pmatrix}\ , \quad (117)$$

$$\mathbf{M}(\tau<0,2)=\begin{pmatrix}\sqrt{-\tau}\mathbf{Z} & \sqrt{1-\tau}\mathbf{I}\\ -\sqrt{1-\tau}\mathbf{I} & -\sqrt{-\tau}\mathbf{Z}\end{pmatrix}\ . \quad (118)$$

Here it is important to note that Eq. (116) is just the beam splitter matrix (cf. Eq. (38)). This means that the Stinespring dilation of a lossy channel $\mathcal{L}(\tau,\bar{n})$ is an entangling cloner (Grosshans, van Assche, *et al.*, 2003), i.e., a beam splitter with transmissivity τ which combines the input mode with one mode of an environmental EPR state $|\nu\rangle$. Clearly, this implies the well-known physical representation for the lossy channel where a beam splitter of transmissivity τ mixes the input state with a single-mode thermal state $\hat{\rho}(\bar{n})$. A particular case of lossy channel is the pure-loss channel $\mathcal{L}(\tau,0)$ which is given by setting $\bar{n}=0$. In this case the Stinespring dilation is just a beam splitter mixing the input with the vacuum.

Finally, let us review the degradability properties of the one-mode Gaussian channels. Since these properties are invariant by unitary equivalence, we have that a degradable (antidegradable) channel $\mathcal{G}$ corresponds to a degradable (antidegradable) form $\mathcal{C}$. All the forms $\mathcal{C}(\tau,r,\bar{n})$ with transmissivity $\tau\leq 1/2$ are antidegradable (Caruso and Giovannetti, 2006). This includes all the forms of classes A_1, A_2, D and part of the forms of class C, i.e., lossy channels $\mathcal{L}(\tau,\bar{n})$ with $\tau\leq 1/2$. By unitary equivalence, this means that one-mode Gaussian channels with transmissivity $\tau\leq 1/2$ are all antidegradable. For $\tau\geq 1/2$ the degradability properties are not so straightforward. However, we know that pure-loss channels $\mathcal{L}(\tau,0)$ with $\tau\geq 1/2$ and ideal amplifying channels $\mathcal{A}(\tau,0)$ are all degradable.

C. Classical capacity of Gaussian channels

Shannon proved that sending information through a noisy channel can be achieved with vanishing error, in the limit of many uses of the channel. He developed an elegant mathematical theory in order to calculate the ultimate limits on data transmission rates achievable over a classical communication channel $\mathcal{N}$, known as the channel capacity (Shannon, 1948). Let us consider two parties, Alice and Bob, which are connected by an arbitrary noisy channel $\mathcal{N}$. At the input, Alice draws letters from a random variable (or alphabet) $A:=\{a,p_a\}$, where the letter a occurs with probability p_a. The information content of this variable is expressed in terms of bits per letter and quantified by the Shannon entropy $H(A)=-\sum_a p_a\log p_a$ (it is understood that when we consider continuous variables, the probabilities are replaced by probability densities and sums by integrals.) By drawing many times, Alice generates a random message $a_1,a_2,\cdots$ which is sent to Bob through the noisy channel. As long as the channel is memoryless, i.e., it does not create correlations between different letters, Bob's output message can be described by drawings from another random variable $B:=\{b,p_b\}$ correlated to the input one $B=\mathcal{N}(A)$. On average, the number of bits per letter which are communicated to Bob is given by the mutual information $I(A:B)=H(B)-H(B|A)$, where $H(B|A)$ is Shannon entropy of B conditioned on the knowledge of A (Cover and Thomas, 2006). Now, the channel capacity $C(\mathcal{N})$, expressed in bits per channel use, is given by maximizing the mutual information over all of Alice's possible inputs

$$C(\mathcal{N})=\max_A I(A:B)\ . \quad (119)$$

It is important to note that many communication channels, such as wired and wireless telephone channels and satellite links are currently modeled as classical Gaussian channels. Here the input variable A generates a continuous signal a with variance P which is transformed to a continuous output $b=\tau a+\xi$, where τ is the transmissivity of the channel, and ξ is drawn from a Gaussian noise-variable of variance V. Shannon's theory gives the capacity $C(\mathcal{N})=\frac{1}{2}\log\left(1+\tau PV^{-1}\right)$ (Cover and Thomas, 2006). We remark that this result predicts an infinite communication rate through a noiseless channel ($V=0$). This counterintuitive result is due to the lack of limitation to the measurement accuracy in classical physics. This is no longer true when we consider the actual quantum nature of the physical systems. In fact, if we encode classical information in the temporal modes (pulses) of the quantized electromagnetic field, then the capacity of the identity channel is no longer infinite but depends on the input energy. As shown by Yuen and Ozawa (1993), the capacity of the identity channel $\mathcal{I}$ is given by $C(\mathcal{I})=g(2\bar{m}+1)$, where $g(\cdot)$ is given in Eq. (47) and $\bar{m}$ is the mean number of photons per pulse. Thus, a quantum mechanical treatment of the problem gives a finite solution for finite energy, showing that quantum mechanics is mandatory in understanding the ultimate limits of communication.

Since information is fundamentally encoded in a physical system and quantum mechanics is the most accurate representation of the physical world, it is therefore natural to ask what are the ultimate limits set by quantum mechanics to communication? Since the 1980s several groups started studying quantum encoding and detection over optical channels, modeled as Gaussian quantum channels (Caves and Drummond, 1994; Hall, 1994; Shapiro, 1984; Yuen and Shapiro, 1980). An important milestone was achieved with the Holevo-Schumacher-Westmoreland (HSW) theorem (Holevo, 1998; Schumacher and Westmoreland, 1997), which laid the basis for a quantum generalization of Shannon's communication theory. First of all, let us introduce the notions of quantum ensemble and Holevo bound (Holevo, 1973). An arbitrary random variable $A=\{a,p_a\}$ can be encoded in a quantum

ensemble (or source) $\mathcal{A} = \{\hat{\rho}_a, p_a\}$, where each letter a is associated with a quantum letter-state $\hat{\rho}_a$ occurring with probability p_a. Since quantum states are generally non-orthogonal, a non-trivial question is the following: what is the maximum information that we can extract from $\mathcal{A}$ using a quantum measurement? This quantity is called the accessible information of the ensemble and is less than or equal to the Holevo bound, defined as

$$\chi(\mathcal{A}) = S(\hat{\sigma}_A) - \sum_a p_a S(\hat{\rho}_a) \, , \tag{120}$$

where $S(\cdot)$ is the von Neumann entropy and $\hat{\sigma}_A = \sum_a p_a \hat{\rho}_a$ is the average state of the ensemble (for continuous ensembles, the previous sums become integrals). Now, the key-result of the HSW theorem is that the Holevo bound is asymptotically achievable when we consider a large number of extractions from the source and a collective quantum measurement. In this limit, the Holevo bound $\chi(\mathcal{A})$ provides the accessible information per letter-state.

These results can be directly applied to memoryless quantum channels $\mathcal{M}$. In this case, the letter-states drawn from a source $\mathcal{A} = \{\hat{\rho}_a, p_a\}$ are transformed identically and independently by the channel, i.e., $\hat{\rho}_{a_1} \otimes \hat{\rho}_{a_2} \cdots \to \mathcal{M}(\hat{\rho}_{a_1}) \otimes \mathcal{M}(\hat{\rho}_{a_2}) \cdots$ By performing a collective measurement on the output message-state, Bob can extract an average of $\chi(\mathcal{A}, \mathcal{M})$ bits per channel use, where

$$\chi(\mathcal{A}, \mathcal{M}) = S\left[\mathcal{M}(\hat{\sigma}_A)\right] - \sum_a p_a S[\mathcal{M}(\hat{\rho}_a)] \, . \tag{121}$$

Thus the Holevo bound $\chi(\mathcal{A}, \mathcal{M})$ gives the optimal communication rate which is achievable over the memoryless quantum channel $\mathcal{M}$ for fixed source $\mathcal{A}$. Maximizing this quantity over all the sources $\mathcal{A}$ we obtain the (single-shot) capacity of the channel

$$C^{(1)}(\mathcal{M}) = \max_{\mathcal{A}} \chi(\mathcal{A}, \mathcal{M}) \, . \tag{122}$$

For bosonic systems, where memoryless channels are usually one-mode channels, the quantity of Eq. (122) must be constrained by restricting the maximization over sources with bounded energy $\mathrm{Tr}(\hat{\sigma}_A \hat{n}) \leq \bar{m}$.

Note that we have introduced the notation single-shot in the definition of Eq. (122). This is because we are restricting the problem to single-letter sources which input product states. In general, we can consider multi-letter sources which input states that are (generally) entangled between n uses of the channel $\mathcal{M}^{\otimes n}$. Then, we can define the full capacity of the channel via the regularization

$$C(\mathcal{M}) = \lim_{n \to \infty} \frac{1}{n} C^{(1)}(\mathcal{M}^{\otimes n}) \, . \tag{123}$$

For one-mode bosonic channels, the computation of Eq. (123) involves the maximization over sources which emit n-mode entangled states and satisfying the energy constraint $\mathrm{Tr}(\hat{\sigma}_A \hat{n}^{\otimes n}) \leq n\bar{m}$. Now an important question to ask is if the presence of entanglement can really enhance the rate of classical communication. In other words, do we have $C(\mathcal{M}) > C^{(1)}(\mathcal{M})$? Hastings (2009) proved the existence of channels for which this is the case. However, for one-mode bosonic Gaussian channels this is still an open question.

A first step in this direction has been the computation of the capacity of a pure-loss channel $\mathcal{L}_p := \mathcal{L}(\tau, 0)$. By exploiting the sub-additivity of the von Neumann entropy, Giovannetti *et al.* (2004a) obtained an upper-bound for $C(\mathcal{L}_p)$ coinciding with the lower-bound reported by Holevo *et al.* (1999) and Holevo and Werner (2001). As a result, a pure-loss channel $\mathcal{L}_p$ of transmissivity τ has classical capacity $C(\mathcal{L}_p) = g(\tau\mu + 1 - \tau)$, where $\mu := 2\bar{m} + 1$ and $\bar{m}$ is the mean number of photons per input mode. Interestingly, one can achieve this capacity by sending coherent states modulated with a Gaussian distribution of variance $V = \mu - 1$. At the detection stage, collective measurements might be necessary. However, this is not the case in the regime of many photons, where heterodyne detection is sufficient to achieve the capacity.

The model of pure-loss channel $\mathcal{L}_p$ can be adopted to describe broadband communication lines, such as wave guides, where the losses are independent from the frequency. For a pure-loss channel of this kind which employs a set of frequencies $\omega_k = k\delta\omega$ for integer k, one can derive the capacity $C = \xi\sqrt{\tau P T}$, where τ is the transmissivity, $T = 2\pi/\delta\omega$ is the transmission time, P is the average transmitted power, and ξ is a constant (Giovannetti *et al.*, 2004a, 2003; Yuen and Ozawa, 1993). Another important scenario is free-space optical communication. Here, transmitter and receiver communicate through circular apertures of areas A_t and A_r which are separated by a distance L. Far-field regime corresponds to having a single spatial mode, which happens when $A_t A_r \omega^2 \left(2\pi c L\right)^{-2} := \tau(\omega) \ll 1$, where c is the speed of light and $\tau(\omega)$ is the transmissivity of the optimal spatial mode with frequency ω (Yuen and Shapiro, 1978). We have a broadband far-field regime when we use frequencies up to a critical frequency ω_c, such that $\tau(\omega_c) \ll 1$. In this case, we can compute the capacity

$$C = (\omega_c T / 2\pi y_0) \int_0^{y_0} dx \; g[(e^{1/x} - 1)^{-1}], \tag{124}$$

where y_0 is a parameter which is connected with the energy constraint (Giovannetti *et al.*, 2004a; Guha, 2008; Shapiro *et al.*, 2005). Recently, the computation of this classical capacity has been generalized to the presence of optical refocusing systems between transmitter and receiver (Lupo *et al.*, 2011).

1. Bosonic minimum output entropy conjecture

Despite a huge research effort in recent years, little progress has been achieved in the calculation of the classical capacity of other one-mode Gaussian channels. However, by using Gaussian encodings, we can easily give lower bounds (Lupo *et al.*, 2011). For instance, using a coherent state encoding at the input of a lossy channel $\mathcal{L}(\tau, \bar{n})$, we can compute the following lower bound for the capacity

$$C(\mathcal{L}) \geq g[\tau\mu + (1-\tau)\nu] - g[\tau + (1-\tau)\nu] := \underline{C}(\mathcal{L}), \tag{125}$$

where $\nu := 2\bar{n}+1$, $\mu := 2\bar{m}+1$, and $\bar{m}$ is the mean number of photons per input mode (Holevo *et al.*, 1999). It is believed that this lower-bound is tight, i.e., $C(\mathcal{L}) = \underline{C}(\mathcal{L})$. This conjecture is implied by another conjecture, known as the bosonic minimum output entropy conjecture and stating that the minimum entropy at the output of a lossy channel is realized by a vacuum state at the input, i.e., $S[\mathcal{L}(|0\rangle\langle 0|)] \leq S[\mathcal{L}(\hat{\rho})]$ for every $\hat{\rho}$. It seems extremely reasonable to assume that sending nothing through the channel is the best way of minimizing the noise (entropy) at its output. However, such a simple statement is still today without a proof. Using Lagrangian minimization it has been possible to prove that vacuum is a local minimum of the output entropy (Giovannetti *et al.*, 2004b; Lloyd *et al.*, 2009). In the work of Giovannetti *et al.* (2004b) a simulated annealing optimization suggested that outputs produced by a vacuum input majorize all the other outputs, and therefore have smaller entropy. Other studies showed that the output Rényi entropy of integer orders ≥ 2 is minimized by the vacuum input and is also additive (Giovannetti and Lloyd, 2004; Giovannetti, Lloyd, *et al.*, 2004). Unfortunately, the von Neumann entropy is the Rényi entropy of order 1, which is therefore not covered by these results. By restricting the input states to Gaussian states it was proven that vacuum gives the minimal output entropy (Giovannetti *et al.*, 2004b; Hiroshima, 2006; Serafini, Eisert, and Wolf, 2005); unfortunately this does not preclude the possibility of having non-Gaussian input states performing better. Finally, alternative approaches to the problem were also proposed, such as proving the *entropy photon-number inequality* (Guha, 2008), which is a quantum version of the classical *entropy power inequality* (Cover and Thomas, 2006).

D. Quantum capacity of Gaussian channels

Quantum channels can be used to transfer not just classical information but also quantum information. In the typical quantum communication scenario, Alice aims to transmit quantum states to Bob through a memoryless quantum channel $\mathcal{M}$. The quantum capacity $Q(\mathcal{M})$ of the channel gives the number of qubits per channel use that can be reliably transmitted. As shown by Schumacher and Nielsen (1996), a crucial role in the definition of the quantum capacity is played by the coherent information $J(\mathcal{M},\hat{\rho}_A)$, which is a function of Alice's input $\hat{\rho}_A$ and the channel $\mathcal{M}$. In order to define this quantity, let us introduce a mirror system R and the purification $\Phi_{RA} = |\Phi\rangle\langle\Phi|_{RA}$ of the input state $\hat{\rho}_A = \mathrm{Tr}_R(\Phi_{RA})$, as shown in Fig. 3. Then, the coherent information is defined by

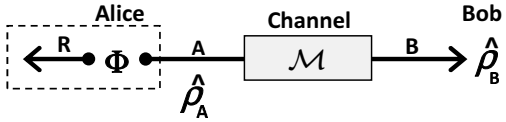


FIG. 3 Alice's input state $\hat{\rho}_A$ is transformed into Bob's output state $\hat{\rho}_B$ by a generic memoryless channel $\mathcal{M}$. The input state $\hat{\rho}_A$ can be purified by introducing an additional mirror system R.

$$J(\mathcal{M},\hat{\rho}_A) = S(\hat{\rho}_B) - S(\hat{\rho}_{RB})\,, \tag{126}$$

where $\hat{\rho}_{RB} := (\mathcal{I}_R \otimes \mathcal{M})(\Phi_{RA})$, $\mathcal{I}_R$ being the identity channel on the mirror system R. The (single-shot) quantum capacity is computed by maximizing over all the input states

$$Q^{(1)}(\mathcal{M}) = \max_{\hat{\rho}_A} J(\mathcal{M},\hat{\rho}_A). \tag{127}$$

Since this quantity is known to be non-additive (Di Vincenzo *et al.*, 1998; Smith and Smolin, 2007; Smith *et al.*, 2011; Smith and Yard, 2008), the correct definition of quantum capacity is given by the regularization (Devetak, 2005; Lloyd, 1997; Shor, 2002)

$$Q(\mathcal{M}) = \lim_{n\to\infty} \frac{1}{n} \max_{\hat{\rho}_{A^n}} J(\mathcal{M}^{\otimes n},\hat{\rho}_{A^n})\,, \tag{128}$$

where the input state $\hat{\rho}_{A^n}$ is generally entangled over n uses of the channel $\mathcal{M}^{\otimes n}$. It is important to note that the coherent information computed over bosonic channels is finite even for infinite input energy. As a result the quantum capacity of bosonic channels is still defined as in Eq. (128) without the need of energy constraints. Another important consideration regards degradable and antidegradable channels. As shown by Devetak and Shor (2005), degradable channels have additive quantum capacity, i.e., $Q(\mathcal{M}) = Q^{(1)}(\mathcal{M})$. By contrast, antidegradable channels have null quantum capacity $Q(\mathcal{M}) = 0$ (Caruso and Giovannetti, 2006).

Let us consider the specific case of one-mode Gaussian channels. In this case a lower bound can be computed by restricting the quantum capacity to a single use of the channel and pure Gaussian states. Thus, for an arbitrary one-mode Gaussian channel $\mathcal{G}$ with transmissivity $\tau \neq 1$, we can write the lower-bound (Holevo and Werner, 2001; Pirandola, García-Patrón, *et al.*, 2009)

$$Q(\mathcal{G}) \geq Q^{(1,g)}(\mathcal{G}) = \max\left\{0, \log\left|\frac{\tau}{1-\tau}\right| - g(\nu)\right\}\,, \tag{129}$$

where $\nu := 2\bar{n}+1$ and $\bar{n}$ is the thermal number of the channel. Clearly this formula applies to all the canonical forms of classes A_1, A_2, C and D. There are remarkable cases where the bound in Eq. (129) is tight. This happens when the one-mode Gaussian channel is degradable. The proof given in (Wolf *et al.*, 2007) combines the additivity for degradable channels $Q(\mathcal{G}) = Q^{(1)}(\mathcal{G})$ with the extremality of Gaussian states $Q^{(1)}(\mathcal{G}) = Q^{(1,g)}(\mathcal{G})$ (Wolf *et al.*, 2006). Important examples of degradable one-mode Gaussian channels are the ideal amplifying channels $\mathcal{A}(\tau,0)$ and the pure-loss channels $\mathcal{L}(\tau,0)$ with transmissivity $\tau \geq 1/2$. Another case, where the previous bound is tight, regards all the one-mode Gaussian channels with transmissivity $\tau \leq 1/2$. These channels are in fact antidegradable and we have $Q(\mathcal{G}) = Q^{(1,g)}(\mathcal{G}) = 0$. Note that we can also compute a lower bound to the quantum capacity for $\tau = 1$ in the case of a canonical form B_2. This is achieved by using continuous-variable stabilizer codes (Harrington and Preskill, 2001).

E. Quantum dense coding and entanglement-assisted classical capacity

The classical capacity of a quantum channel can be increased if Alice and Bob share an entangled state. This effect is known as *quantum dense coding*. The analysis that reaches this conclusion ignores the cost of distributing the entanglement. The rationale for doing this is that the entanglement does not carry any information per se. Originally introduced in the context of qubits (Bennett and Wiesner, 1992), dense coding was later extended to continuous variables (Ban, 1999; Braunstein and Kimble, 1999; Ralph and Huntington, 2002), with a series of experiments in both settings (Li *et al.*, 2002; Mattle *et al.*, 1996; Mizuno *et al.*, 2005; Pereira *et al.*, 2000).

The basic setup in continuous variables considers the distribution of information over an identity channel $\mathcal{I}$ by means of a single bosonic mode. Here Bob possesses an EPR state of variance V. This state can be generated by combining a pair of single-mode squeezed states with orthogonal squeezings into a balanced beam splitter. In particular, the squeezed quadratures must have variance $V_{sq} = V - \sqrt{V^2 - 1}$. Bob sends one mode of the EPR state to Alice, while keeping the other mode. To transmit classical information, Alice modulates both quadratures and sends the mode back to Bob, with mean number of photons equal to $\bar{m}$. To retrieve information, Bob detects both received and kept modes by using a Bell measurement with detector efficiency $\eta \in [0, 1]$. The achievable rate is given by (Ralph and Huntington, 2002)

$$R_{dc}(\mathcal{I}) = \log \left[1 + \frac{\eta(4\bar{m} - V_{sq} - 1/V_{sq} + 2)}{4(\eta V_{sq} + 1 - \eta)} \right]. \quad (130)$$

This rate can exceed the classical capacity of the identity channel $C(\mathcal{I})$ at the same fixed average photon number $\bar{m}$ for a considerable range of values of V_{sq} and η.

The advantages of quantum dense coding can be extended to an arbitrary memoryless channel $\mathcal{M}$. This leads to the notion of entanglement-assisted classical capacity $C_E(\mathcal{M})$, which is defined as the maximum asymptotic rate of reliable bit transmission over a channel $\mathcal{M}$ assuming the help of unlimited pre-shared entanglement. As shown by Bennett *et al.* (2002) this is equal to

$$C_E(\mathcal{M}) = \max_{\hat{\rho}_A} I(\mathcal{M}, \hat{\rho}_A), \quad (131)$$

where $I(\mathcal{M}, \hat{\rho}_A) = S(\hat{\rho}_A) + J(\mathcal{M}, \hat{\rho}_A)$ is the quantum mutual information associated with the channel $\mathcal{M}$ and the input state $\hat{\rho}_A$ (J is the coherent information). For one-mode Gaussian channels, the capacity C_E must be computed under the energy constraint $\mathrm{Tr}(\hat{\rho}_A \hat{n}) \leq \bar{m}$. In particular, for a pure-loss channel $\mathcal{L}_p = \mathcal{L}(\tau, 0)$, we have (Holevo and Werner, 2001)

$$C_E(\mathcal{L}_p) = g(\mu) + g(\tau\mu + 1 - \tau) - g(\lambda_-) - g(\lambda_+), \quad (132)$$

where $\mu = 2\bar{m} + 1$ and $\lambda_\pm = D \pm \bar{m}(1 - \tau)$, with

$$D = \{[1 + \bar{m}(\tau + 1)]^2 - 4\tau\bar{m}(\bar{m} + 1)\}^{1/2}. \quad (133)$$

This capacity is achieved by a Gaussian state. For $\tau \to 1$ we have the identity channel and we get $C_E(\mathcal{I}) = 2g(\mu)$, which is twice its classical capacity $C(\mathcal{I})$.

F. Entanglement distribution and secret-key capacities

Other important tasks that can be achieved in quantum information are the distribution of entanglement and secret keys over quantum noisy channels. Given a memoryless channel $\mathcal{M}$, its entanglement distribution capacity $E(\mathcal{M})$ quantifies the number of entanglement-bits which are distributed per use of the channel. As shown by Barnum *et al.* (2000), this quantity coincides with the quantum capacity, i.e., $E(\mathcal{M}) = Q(\mathcal{M})$. Then, the secret-key capacity $K(\mathcal{M})$ of the channel provides the number of secure bits which are distributed per use of the channel (Devetak, 2005). Since secret bits can be extracted from entanglement bits, we generally have $K(\mathcal{N}) \geq E(\mathcal{M})$. Using classical communication, Alice and Bob can improve all these capacities. However, they need feedback classical communication, since the capacities assisted by forward classical communication, i.e., $K_{\rightarrow}(\mathcal{M})$, $E_{\rightarrow}(\mathcal{M})$ and $Q_{\rightarrow}(\mathcal{M})$, coincide with the corresponding *unassisted* capacities, $K(\mathcal{M})$, $E(\mathcal{M})$ and $Q(\mathcal{M})$ (Barnum *et al.*, 2000; Devetak, 2005).

Unfortunately, the study of feedback-assisted capacities is a very difficult task. Alternatively, we can introduce simpler capacities, called reverse capacities, defined by the maximization over protocols which are assisted by a single feedback classical communication (known as reverse protocols). A reverse protocol can be explained considering the purified scenario of Fig. 3. Alice sends to Bob a large number of A modes while keeping the R modes. Then Bob applies a quantum operation over all the output B modes and communicates a classical variable to Alice (single final classical communication). Exploiting this information, Alice applies a conditional quantum operation on all the R modes. Thus we have the reverse ($\blacktriangleleft$) entanglement distribution capacity $E_{\blacktriangleleft}(\mathcal{M})$ and the reverse secret-key capacity $K_{\blacktriangleleft}(\mathcal{M})$, which clearly must satisfy $K_{\blacktriangleleft}(\mathcal{M}) \geq E_{\blacktriangleleft}(\mathcal{M})$. Interestingly, these capacities can be lower bounded by a quantity which is very easy to compute. In fact, as shown by García-Patrón *et al.* (2009), we can define the *reverse coherent information*

$$J_R(\mathcal{M}, \hat{\rho}_A) = S(\hat{\rho}_R) - S(\hat{\rho}_{RB}). \quad (134)$$

This quantity differs from the coherent information $J(\mathcal{M}, \hat{\rho}_A)$ by the replacement $S(\hat{\rho}_B) \to S(\hat{\rho}_R) = S(\hat{\rho}_A)$. For this reason, we can have $J_R(\mathcal{M}, \hat{\rho}_A) > J(\mathcal{M}, \hat{\rho}_A)$ for channels which decrease entropy, i.e., $S(\hat{\rho}_A) > S(\hat{\rho}_B)$. Optimizing the reverse coherent information over all the inputs, we can define the (one-shot) reverse coherent information capacity $E_R^{(1)}(\mathcal{M})$ and the corresponding regularization $E_R(\mathcal{M})$. Interestingly, this quantity turns out to be additive for all channels, so that we simply have $E_R(\mathcal{M}) = E_R^{(1)}(\mathcal{M})$. Now the capacity $E_R(\mathcal{M})$ provides a lower bound for the reverse capacities, i.e., $K_{\blacktriangleleft}(\mathcal{M}) \geq E_{\blacktriangleleft}(\mathcal{M}) \geq E_R(\mathcal{M})$. The expression of $E_R(\mathcal{M})$ can be very simple. As shown by Pirandola, García-Patrón, *et al.* (2009), an arbitrary one-mode Gaussian channel $\mathcal{G}$ with transmission $\tau \neq 1$ has

$$E_R(\mathcal{G}) = \max \left\{ 0, \log \left| \frac{1}{1 - \tau} \right| - g(\nu) \right\}, \quad (135)$$

where $\nu := 2\bar{n} + 1$ and $\bar{n}$ is the thermal number of the channel. Note that $E_R(\mathcal{G})$ can be positive for $\tau \leq 1/2$, where the channel is antidegradable and, therefore, $E(\mathcal{G}) = Q(\mathcal{G}) = 0$. Thus, despite the fact that the unassisted (forward-assisted) capacities are zero, the use of a single feedback classical communication is sufficient to distribute entanglement ($E_{\blacktriangleleft}(\mathcal{G}) > 0$) and secret keys ($K_{\blacktriangleleft}(\mathcal{G}) > 0$). In cryptographic terms, antidegradibility means that an eavesdropper is able to reconstruct the output state of Bob. Despite this, Alice and Bob are still able to extract a secret key from their shared correlations by using a reverse secret-key protocol. This is a remarkable feature of reverse reconciliation, further discussed in Chapter VI.

G. Gaussian channel discrimination and applications

The discrimination of quantum channels represents one of the basic problems in quantum information theory (Acín, 2001; Childs *et al.*, 2000; Chiribella *et al.*, 2008; Duan *et al.*, 2009; Harrow *et al.*, 2010; Hayashi, 2009; Invernizzi *et al.*, 2011; Sacchi, 2005; Wang and Ying, 2006). Here we discuss the problem of distinguishing between two Gaussian channels. Suppose that we have a black box which implements one of two possible (one-mode) Gaussian channels, $\mathcal{G}_0$ or $\mathcal{G}_1$, with the same probability, and we want to find out which one it is. In other words, the box contains an unknown Gaussian channel $\mathcal{G}_u$ encoding a logical bit $u = 0, 1$ and we want to retrieve the value of this bit. The basic approach involves probing the box with a one-mode quantum state $\hat{\rho}$ and detecting the corresponding output $\hat{\sigma}_u := \mathcal{G}_u(\hat{\rho})$ by means of a quantum measurement. However, this approach can be readily generalized. In fact, we can consider multiple access to the box by inputting M signal modes. Then, we can also consider additional L idler modes, which are not processed by the box but are directly sent to the output measurement, as shown in Fig. 4. Thus, for a given state $\hat{\rho}$ of the input $M + L$ modes, we have two possible output states, $\hat{\sigma}_0$ and $\hat{\sigma}_1$, described by the dichotomic state $\hat{\sigma}_u := (\mathcal{G}_u^{\otimes M} \otimes \mathcal{I}^{\otimes L})(\hat{\rho})$, where $\mathcal{G}_u^{\otimes M}$ is applied to the signals and the identity $\mathcal{I}^{\otimes L}$ to the idlers. This output is detected by a multimode quantum measurement whose outcome estimates the encoded bit. Now, since $\hat{\sigma}_0$ and $\hat{\sigma}_1$ are generally non-orthogonal, the bit is decoded up to an error probability p_{err}. Thus, the main goal of the problem is the minimization of p_{err}, which must be done on both input and output. For fixed input state $\hat{\rho}$, the optimal detection of the output is already known: this is the Helstrom's dichotomic POVM discussed in Sec. III.A. However, we do not know which state is optimal at the input. More precisely, we do not know the optimal input state when we constrain the signal energy irradiated over the box. Here there are two kinds of constraints that we can actually consider. The first one is a global energy constraint, where we restrict the mean total number of photons m_{tot} irradiated over the box. In this case the minimum value of p_{err} can be non-zero. The second one is a local energy constraint, where we restrict the mean number of photons $\bar{m}$ per signal mode. In this case, the value of p_{err} generally goes to zero for $M \to +\infty$ and the problem is to achieve the most rapid decaying behavior. In both cases finding the optimal input state for fixed energy is an open problem.

However, we can try to answer related questions: for fixed energy, does entanglement help? Or more generally: do we need non-classical states for minimizing p_{err}? By definition a state is called classical (non-classical) when it can (cannot) be written as a probabilistic mixture of coherent states, i.e., $\hat{\rho} = \int d\boldsymbol{\alpha} P(\boldsymbol{\alpha}) |\boldsymbol{\alpha}\rangle \langle\boldsymbol{\alpha}|$, where $|\boldsymbol{\alpha}\rangle = |\alpha_1\rangle \otimes \cdots \otimes |\alpha_{L+M}\rangle$ and $P(\boldsymbol{\alpha})$ is a probability density function. Classical states are always separable and represent the standard sources in today's optical applications. By contrast, non-classical states (such as number states, squeezed and entangled states) are only generated in quantum optics labs. Thus, we can formulate the following question: for fixed signal energy (m_{tot} or $\bar{m}$) and optimal output detection, can we find a non-classical state which outperforms any classical state in the discrimination of two Gaussian channels? This basic question has motivated several theoretical investigations (Pirandola, 2011; Tan *et al.*, 2008; Usha Devi and Rajagopal, 2009; Yuen and Nair, 2009). In particular, it has been answered in two interesting scenarios, with non-trivial implications in quantum technology.

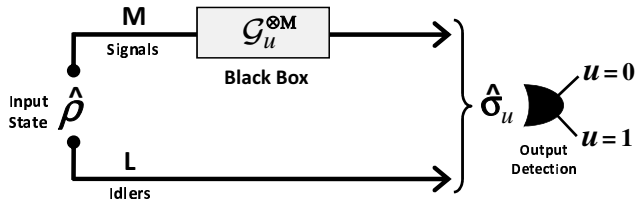


FIG. 4 Gaussian channel discrimination. The input state $\hat{\rho}$ describes M signal modes and L idler modes. Only the signals probe the black box which contains one of two possible (one-mode) Gaussian channels $\mathcal{G}_0$ or $\mathcal{G}_1$ (encoding a bit u). At the output, signals and idlers are described by a dichotomic quantum state $\hat{\sigma}_u$ whose detection gives an estimate of the bit.

The first scenario is known as *quantum illumination* (Lloyd, 2008) with Gaussian states (Tan *et al.*, 2008). Here the Gaussian channel discrimination $\mathcal{G}_0 \neq \mathcal{G}_1$ is related with the problem of sensing the presence of a low-reflectivity object in a bright thermal-noise environment. In this case, the black box of Fig. 4 represents a target region from where the signals are reflected back to the detector. If the object is absent (bit-value $u = 0$) we have a completely depolarizing channel $\mathcal{C}(0, 0, \bar{n})$ which replaces each signal mode with an environmental mode in a thermal state with $\bar{n} \gg 1$ photons. By contrast, if the object is present (bit-value $u = 1$), we have a lossy channel $\mathcal{L}(\kappa, \bar{n}')$ with high loss $\kappa \ll 1$ and high thermal number $\bar{n}' := \bar{n}/(1 - \kappa) \gg 1$. These channels are entanglement-breaking, i.e., no entanglement survives at the output. Now, assuming very few photons per signal mode $\bar{m} \ll 1$ (local constraint), we ask if a non-classical state is able to outperform any classical state. To this goal, we construct an EPR transmitter composed of M signals and M idlers in a tensor product of EPR states, i.e., $\Phi_M := \hat{\rho}_{11}(r) \otimes \cdots \otimes \hat{\rho}_{MM}(r)$, where $\hat{\rho}_{ij}(r)$ is an EPR state of squeezing r which entangles signal mode i and idler mode j. The corresponding error probability $p_{err} = p_{\text{EPR}}(M)$ can be computed using the Gaussian for-

mula of the quantum Chernoff bound (see Sec. III.A.2.a). For large M, we derive $p_{\rm EPR}(M) \simeq \exp(-M\kappa\bar{m}/\bar{n})/2$, which decays to zero more rapidly than the error probability of any classical state with M signals and arbitrary L idlers. In particular, if we restrict the classical states to coherent states, then we have an error probability $p_{coh}(M) \simeq \exp(-M\kappa\bar{m}/4\bar{n})/2$ which is 6 dB worse than $p_{\rm EPR}(M)$ (Tan *et al.*, 2008). Interestingly, the quantum illumination advantage accrues despite the fact that no entanglement survives at the output. In fact, even if the output signal-idler correlations are within the classical bounds, there is no classical input state that can produce a close approximation to this output state. Further studies on quantum illumination of targets have been pursued by Shapiro and Lloyd (2009) and Guha and Erkmen (2009).

The second scenario regards the use of non-classical transmitters to read data from classical digital memories, such as optical disks (CDs and DVDs). This is known as *quantum reading* (Pirandola, 2011). Here the discrimination of Gaussian channels is associated with the retrieval of information from a memory cell, modeled as a medium with two possible reflectivities. This cell is equivalent to the black box of Fig. 4 where the bit $u = 0, 1$ specifies two lossy channels, $\mathcal{L}(\kappa_0, \bar{n})$ and $\mathcal{L}(\kappa_1, \bar{n})$, with the same thermal number $\bar{n}$ but different losses $\kappa_0 \neq \kappa_1$. For optical disks, we can consider low noise ($\bar{n} \ll 1$) and κ_1 close to 1. In these conditions, and irradiating relatively few photons over the cell $m_{tot} \simeq 10$ (global constraint), we can find an EPR transmitter $\Phi_{M'}$, with small M', which is able to outperform any classical state with any M and L. As shown by Pirandola (2011), the difference in the readout of information can be surprising (up to one bit per cell), with non-trivial implications for the technology of data storage. Follow up studies on the quantum reading of memories have been pursued by various authors (Bisio *et al.*, 2011; Hirota, 2011; Nair, 2011; Pirandola *et al.*, 2011).

VI. QUANTUM CRYPTOGRAPHY USING CONTINUOUS VARIABLES

Cryptography is the theory and practice of hiding information (Menezes *et al.*, 1997). The development of the information age and telecommunications in the last century has made secure communication a must. In the 1970s, public-key cryptography was developed and deals with the tremendous demand for encrypted data in finance, commerce and government affairs. Public-key cryptography is based on the concept of one-way functions, i.e., functions which are easy to compute but extremely hard to invert. As an example, most of the current internet transactions are secured by the RSA protocol, which is based on the difficulty of factorizing large numbers (Rivest *et al.*, 1978). Unfortunately, its security is not unconditional, being based on the assumption that no efficient factorization algorithm is known for classical computers. Furthermore, if quantum computers were available today, RSA could be easily broken by Shor's algorithm (Shor, 1997).

Ideally, it would be desirable to have a completely secure way of communicating, i.e., unconditional security. Shannon (1949) proved that this is indeed possible using the one-time pad (Vernam, 1926). Here two parties, Alice and Bob, share a pre-established secret key unknown to a potential eavesdropper, Eve. In this technique, Alice encodes her message by applying a modular addition between the plaintext bits and an equal amount of random bits from the secret key. Then, Bob decodes the message by applying the same modular addition between the ciphertext received from Alice and the secret key. The main problem of the one-time pad is the secure generation and exchange of the secret key, which must be at least as long as the message and can only be used once. Distributing very long one-time pad keys is inconvenient and usually poses a significant security risk. For this reason, public-key cryptography is more widely used than the one-time pad.

Quantum cryptography, or quantum key distribution (QKD) as it is more accurately known[3], is a quantum technology allowing Alice and Bob to generate secret keys that can later be used to communicate with theoretically unconditional security. This is used in conjunction with the one-time pad or another symmetric cryptographic protocol such as pretty good privacy (Schneier, 1995). The unconditional security of QKD is guaranteed by the laws of quantum mechanics (Gisin *et al.*, 2002) and, more precisely, the no-cloning theorem (cf. Sec. V.E), which can be understood as a manifestation of the Heisenberg uncertainty principle. The first QKD protocol was the BB84 protocol (Bennett and Brassard, 1984). Since then QKD has become one of the leading fields in quantum information. Despite being a quantum technology, QKD is not hard to implement experimentally. In fact, the use of telecom components over normal optical fibers is sufficient to distribute secret keys with reasonable rates over metropolitan network areas, as recently demonstrated by the European Union's SECOQC project (SECOQC, 2007). Today QKD can be considered as a mature field (Scarani *et al.*, 2009) with several start-up companies formed around the world.

In this section, we review the continuous-variable version of QKD, whose key elements are the modulation (encoding) of Gaussian states and Gaussian measurements (decoding), e.g., homodyne and heterodyne detection. The first continuous-variable QKD protocols were based on a discrete modulation of Gaussian states (Hillery, 2000; Ralph, 1999a; Reid, 2000). The first protocol based on a continuous (Gaussian) modulation of Gaussian states was introduced by Cerf *et al.* (2001) and employed squeezed states for the secret encoding. This idea was readily extended by Grosshans and Grangier (2002) and Grosshans, van Assche, *et al.* (2003), with the design and implementation of the first continuous-variable QKD protocol based on the Gaussian modulation of coherent states and ho-

[3] Technically, quantum cryptography refers not only to quantum key distribution but also other secrecy tasks such as quantum money, quantum secret and state sharing (Lance *et al.*, 2004; Tyc and Sanders, 2002), quantum bit commitment (albeit with certain constraints (Magnin *et al.*, 2010; Mandilara and Cerf, 2011)), and quantum random number generators (Gabriel *et al.*, 2010). However, it is not uncommon for quantum cryptography and quantum key distribution to be used synonymously in the literature.

modyne detection. Shortly afterwards, another coherent-state protocol was proposed (Weedbrook *et al.*, 2004, 2006) and implemented (Lance *et al.*, 2005), known as the no-switching protocol, where homodyne detection is replaced by heterodyne detection. This enables the honest parties to exploit both quadratures in the distribution of the secret key. It is important to note that the coherent-state encoding introduced by Grosshans and Grangier (2002) is today at the core of the most promising continuous-variable QKD implementations, thanks to the possibility of using standard telecom components (Fossier *et al.*, 2009; Lodewyck *et al.*, 2007, 2005, 2007; Lodewyck and Grangier, 2007).

In order to reach significant transmission distances, i.e., corresponding to more than 3 dB of loss, two main techniques are commonly used: reverse reconciliation (Grosshans, van Assche, *et al.*, 2003) and postselection (Silberhorn *et al.*, 2002). Furthermore, the introduction of new protocols using two-way quantum communication (Pirandola, Mancini, *et al.*, 2008) and discrete modulation (Leverrier and Grangier, 2009, 2010b) have shown the possibility of further improvements in terms of transmission range. Recently, it was shown by Weedbrook *et al.* (2010) that a secure key could, in principle, be generated over short distances at wavelengths considerably longer than optical and down into the microwave regime, providing a potential platform for noise-tolerant short-range QKD.

The first security proof in continuous-variable QKD was given by Gottesman and Preskill (2001) using squeezed states. The proof used techniques from discrete-variable quantum error correction and worked for states with squeezing greater than 2.51 dB. Subsequent proofs for continuous-variable QKD followed, including a proof against individual attacks for coherent-state protocols (Grosshans and Cerf, 2004) and an unconditional security proof which reduced coherent attacks to collective attacks (Renner and Cirac, 2009). Using the latter result, a large family of QKD protocols can be analyzed against the simpler collective Gaussian attacks (García-Patrón and Cerf, 2006; Leverrier and Grangier, 2010a; Navascués *et al.*, 2006) which have been fully characterized by Pirandola, Braunstein, and Lloyd (2008). More recently, finite-size effects have begun to be studied (Leverrier *et al.*, 2010), with the aim of assessing unconditional security when only a finite number of quantum systems have been exchanged.

This section is structured as follows. In Sec. VI.A we present the various continuous-variable QKD protocols using Gaussian states. This is followed by an analysis of their security in Sec. VI.B and finally, in Sec. VI.C, we discuss the future directions of the field.

A. Continuous-variable QKD protocols

In this section we start by presenting a generic QKD protocol. Then we continue by illustrating the most important families of continuous-variable QKD protocols based on the use of Gaussian states. These protocols are presented as *prepare-and-measure* schemes, where Alice prepares an ensemble of signal states using a random number generator. In Sec. VI.A.5 we also discuss the entanglement-based representation, where Alice's preparation is realized by a suitable measurement over an entangled source.

1. A generic protocol

Any QKD protocol, be it based on discrete or continuous variables, can be divided into two steps: (1) quantum communication followed by (2) classical post-processing. During the quantum communication, Alice and Bob exchange a significant number of quantum states over a communication channel, which is modeled as a quantum channel. In each round, Alice encodes a classical random variable a onto a quantum system which is sent to Bob. This system is measured by Bob at the output of the channel, thus extracting a random variable b which is correlated to Alice's. Repeating this procedure many times, Alice and Bob generate two sets of correlated data, known as the raw keys.

Quantum communication is followed by classical post-processing where the two raw keys are mapped into a shared secret key (i.e., the final key used to encode the secret message). The classical post-processing is divided into several stages (Gisin *et al.*, 2002; Scarani *et al.*, 2009; van Assche, 2006). The first stage is the *sifting* of the keys where Alice and Bob communicate which basis or quadrature they used to encode/decode the information, thus discarding incompatible data. We then have *parameter estimation*, where the two parties compare a randomly chosen subset of their data. This step allows them to analyze the channel and upper-bound the information stolen by Eve. Next, we have *error correction*, where the two parties communicate the syndromes of the errors affecting their data. As a result, Alice's and Bob's raw keys are transformed into the same string of bits. Finally, we have *privacy amplification*. During this step, the two parties generate a smaller but secret key, reducing Eve's knowledge of the key to a negligible amount (van Assche, 2006). The amount of data to discard is given by the upper-bound on Eve's information which has been computed during the parameter estimation stage.

It is important to note that the classical post-processing stages of error correction and privacy amplification involves a public channel that Alice and Bob use by means of either one-way or two-way classical communication (the initial stages of sifting and parameter estimation always involve two-way communication). Two-way classical communication is allowed in the postselection protocol which we introduce later. When one-way classical communication is used and is forward, i.e., from Alice to Bob, we have direct reconciliation. In this case, Alice's data is the reference which must be estimated by Bob (and Eve). By contrast, if one-way classical communication is backward, i.e., from Bob to Alice, then we have reverse reconciliation, where Bob's data must be estimated by Alice (and Eve). As discussed by Pirandola, García-Patrón, *et al.* (2009), both direct and reverse reconciliation can be in principle realized by using a *single* classical communication. This observation enables a

simple definition of the most general protocols in direct and reverse reconciliation (direct and reverse protocols). By using these protocols we can define the direct and reverse secret-key capacities of an arbitrary quantum channel (see Sec. V.F). Another important observation is that the public channel used for the classical communication must be authenticated. This means that Alice and Bob have to identify themselves by using a pre-shared secret key (Renner and Wolf, 2005). As a result, QKD does not create secret keys out of nothing, but rather expands initial secret keys into longer ones.

2. Coherent-state protocol (homodyne detection)

A seminal result in QKD using continuous variables was the discovery that coherent states are sufficient to distribute secret keys (Grosshans and Grangier, 2002; Ralph, 2003). Because coherent states are much easier to generate in the lab than any other Gaussian state, this result opened the door to experimental demonstrations and field implementations. The first Gaussian modulated coherent state protocol utilized direct reconciliation (Grosshans and Grangier, 2002), followed shortly after by reverse reconciliation (Grosshans, van Assche, *et al.*, 2003). Since then nearly all proposals have used coherent states as its substrate. The security of coherent-state protocols is based on the fact that coherent states are non-orthogonal (cf. Eq. 30), which on its own is a sufficient condition for QKD (i.e., the no-cloning theorem applies). The quantum communication starts by Alice generating two real variables, a_q and a_p, each drawn from a Gaussian distribution of variance V_a and zero mean. These variables are encoded onto a coherent state resulting in a mean of (a_q, a_p). By imposing $V_a = V-1$, we obtain an average output state which is thermal of variance V. For each incoming state, Bob draws a random bit u' and measures either the $\hat{q}$ or $\hat{p}$ quadrature using homodyne detection based on the outcome of u'. After repeating these steps many times, Alice ends up with a long string of data encoding the values (a_q, a_p) which are correlated with Bob's homodyne outcomes b. The post-processing starts by Bob revealing his string of random bits u' and Alice keeping as the final string of data a the values (a_q or a_p) matching Bob's quadratures.

3. No-switching protocol (heterodyne detection)

In the previous protocols, Alice generates two real random variables but in the end only one is ultimately used for the key after the sifting stage. Thus, one can modify the protocol in order to use both values for the generation of the key, as shown by Weedbrook *et al.* (2004). The quantum communication part of the protocol is equivalent to the previous protocols except for Bob's measurement which is now replaced by heterodyne detection, and enables him to measure $\hat{q}$ and $\hat{p}$ simultaneously (albeit with a noise penalty demanded by the uncertainty principle). Since there is no longer the random switching between the two conjugated bases, the random number generator at Bob's side is no longer needed. After repeating these steps many times, Alice ends up with two strings of data (a_q, a_p) correlated with Bob's data (b_q, b_p). Heterodyne detection allows for a simpler experimental setup, producing higher secret-key rates and can be used in conjunction with all known continuous-variable QKD protocols.

4. Squeezed-state protocols

The ability to use coherent states was a milestone in continuous-variable QKD and is currently, by far, the most popular state to use both theoretically and experimentally. However, the first protocol based on the Gaussian modulation of Gaussian states with Gaussian measurements was given by Cerf *et al.* (2001) and involved using squeezed states. Here Alice generates a random bit u and a real variable a drawn from a Gaussian distribution of variance V_a and zero mean. Subsequently, she generates a squeezed vacuum state and displaces it by an amount a. Before sending the state through the quantum channel, Alice applies a random phase of $\theta = u\pi/2$. This is equivalent to randomly choosing to squeeze and displace either the $\hat{q}$ or $\hat{p}$ quadrature. Averaging the output states over the Gaussian distribution gives a thermal state whose variance V is the same for $u = 0$ and $u = 1$, which prevents Eve from extracting information on which quadrature was selected by Alice. This imposes the constraint $V_a + 1/V = V$ on Alice's modulation. Once the state has reached Bob, he generates a random bit u' informing him which quadrature he should measure. Alice and Bob then publicly reveal their strings of random bits keeping only the data which corresponds to the same measured quadrature.

Another squeezed state protocol was developed by García-Patrón and Cerf (2009) where Alice again randomly sends displaced squeezed states to Bob. However, this time Bob uses heterodyne detection rather than homodyne detection, but still disregards either one of his quadrature measurements, depending on Alice's quadrature choice. This reverse reconciliation protocol can be seen as a noisy version of the protocol with squeezed states and homodyne detection. Thanks to this addition of noise, the protocol has an enhanced robustness versus the noise of the channel which can be interpreted as the continuous-variable counterpart of the effect described by Renner *et al.* (2005) for qubit-based protocols. Note that such an effect can also be seen in the work of Navascués and Acín (2005), where the protocol with coherent states and homodyne detection has a better performance than the protocol with squeezed states and homodyne detection when using direct reconciliation. Further evidence that noise can improve the performance of QKD is provided in the work of Pirandola, García-Patrón, *et al.* (2009).

5. Fully-Gaussian protocols and entanglement-based representation

The previous protocols based on coherent states encoding and homodyne detection, together with the no-switching protocols and the squeezed states protocols are all based on the

Gaussian modulation of Gaussian states followed by Gaussian measurements. For this reason, we refer to these protocols as *fully-Gaussian protocols*. Because they can be implemented in direct or reverse reconciliation, they represent a family of eight protocols. As we will discuss afterwards, their unconditional security can be simply assessed against collective Gaussian attacks. By adopting an entanglement-based representation (Bennett *et al.*, 1992; Grosshans, Cerf, *et al.*, 2003), these protocols can be described by a unique scheme (García-Patrón, 2007) where Alice has an EPR state $|V\rangle_{A'A}$ with noise variance V and sends one mode A to Bob while keeping the other mode A' for herself (see Fig. 5). Then,

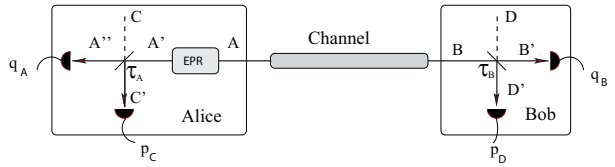


FIG. 5 Entanglement-based representation for the fully-Gaussian protocols. Alice has an EPR state $|V\rangle_{A'A}$ sending mode A to Bob while keeping mode A'. Alice (Bob) mixes her (his) mode A' (B) with a vacuum mode in a beam splitter of transmissivity τ_A (τ_B) and subsequently homodynes the output quadratures. Depending on the value of τ_A, Alice generates a source of squeezed states ($\tau_A = 1$) or coherent states ($\tau_A = 1/2$). Then, Bob applies homodyne ($\tau_B = 1$) or heterodyne ($\tau_B = 1/2$) detection.

Alice mixes her mode A' with a vacuum mode C into a beam splitter of transmissivity τ_A, followed by a measurement of the output quadratures $\hat{q}_A$ and $\hat{p}_C$. As a result, she projects the EPR mode A into a Gaussian state with mean $\mathbf{d} = (\gamma_q q_A, \gamma_p p_C)$ and covariance matrix $\mathbf{V} = \mathrm{diag}(x^{-1}, x)$, where $x = (\mu V + 1)/(V + \mu)$, $\mu = (1 - \tau_A)/\tau_A$ and

$$\gamma_q = \frac{\sqrt{\tau_A(V^2-1)}}{\tau_A V + (1-\tau_A)},\ \gamma_p = \frac{\sqrt{(1-\tau_A)(V^2-1)}}{(1-\tau_A)V + \tau_A}. \quad (136)$$

It is easy to check that Alice generates a source of squeezed (coherent) states for $\tau_A = 1$ ($\tau_A = 1/2$). Then, Bob applies homodyne ($\tau_B = 1$) or heterodyne ($\tau_B = 1/2$) detection depending on which protocol they want to implement. It is important to note that the entanglement-based representation is a powerful tool to study many other QKD protocols, including discrete modulation and two-way protocols. In general, any prepare-and-measure protocol admits an entanglement-based representation. This is because any ensemble of states on a system A can be realized by applying a partial measurement on a larger bipartite system $A + A'$ (Hughston *et al.*, 1993).

6. Postselection

Originally, it was believed that the range of continuous-variable QKD protocols could not exceed the 3 dB loss limit, as first encountered by direct reconciliation. Exceeding such a limit corresponds to having less than 50% transmission which intuitively means that Eve is getting more information on Alice's data than what Bob is. However, two proposals showed that such a limit can actually be surpassed, namely reverse reconciliation (as discussed previously) and postselection (Silberhorn *et al.*, 2002). The quantum communication part of the postselection protocol is equivalent to the previously mentioned coherent-state protocols. However, the main difference occurs in the classical post-processing stage. In the sifting stage, once Bob has revealed which quadrature he measured, Alice replies with the absolute value of her corresponding quadrature ($|a_q|$ or $|a_p|$). Subsequently, Bob, depending on Alice's revealed value and the absolute value of his measurement outcome $|b|$, decides, following a pre-established rule, whether they should discard or keep parts of their data. The main concept is that, every pair of values $(|a|, |b|)$ can be associated with a discrete channel and a binary protocol, based on the signs of a and b. A theoretical secret-key rate $K(|a|, |b|)$ can be calculated for each channel $(|a|, |b|)$ from the data obtained during the parameter estimation stage of the post-processing. The postselection protocol discards those channels for which $K(|a|, |b|) \leq 0$, keeping only those channels with a positive contribution. A variant of this protocol consists in Bob applying heterodyne instead of homodyne detection, i.e., a no-switching postselection protocol (Lance *et al.*, 2005; Lorenz *et al.*, 2004). In such a case, Alice and Bob can extract information from both quadratures thus increasing the secret-key rate. This version of the postselection protocol has also been experimentally demonstrated (Lance *et al.*, 2005; Lorenz *et al.*, 2006).

7. Discrete modulation of Gaussian states

The very first continuous-variable QKD protocols were based on a discrete (and hence, non-Gaussian) encoding of Gaussian states (Hillery, 2000; Ralph, 1999a; Reid, 2000). However, after the discovery of Gaussian modulated coherent states as a viable resource, the discrete encoding took a back seat with only a small number of papers continuing with the idea (Heid and Lütkenhaus, 2006; Namiki and Hirano, 2003, 2006). In recent times though, there has been renewed interest in the discrete encoding of coherent states (Leverrier and Grangier, 2009, 2010b,c; Sych and Leuchs, 2009; Zhao *et al.*, 2009) due to it being experimentally easier to implement as well as its higher error correction efficiencies which promotes continuous-variable QKD over longer distances. A generalized protocol using a discrete modulation (Sych and Leuchs, 2009) consists of an alphabet of N coherent states $|\alpha_k\rangle = \left|ae^{i2\pi k/N}\right\rangle$ with relative phase $2\pi k/N$, where k encodes the secret key. Bob uses either homodyne or heterodyne detection in order to estimate k. Such a multi-letter encoding scheme can achieve higher key rates under the assumption of a lossy channel. Of the proposals introduced thus far, the classical post-processing stage uses either postselection or reverse reconciliation. The current drawback with discrete modulation Gaussian protocols is the infancy of their security analysis, although promising advances have been made recently (Leverrier and Grangier, 2009, 2010b; Zhao *et al.*, 2009).

8. Two-way quantum communication

In standard QKD protocols the quantum communication is one-way, i.e., quantum systems are sent from Alice to Bob. In two-way protocols, this process is bidirectional, with the systems transformed by Bob and sent back to Alice (Boström and Felbinger, 2002, 2008). Recently, Pirandola, Mancini, *et al.* (2008) introduced this idea in continuous-variable QKD, showing how the use of two-way quantum communication can increase the robustness to noise of the key distribution. As a result, bosonic channels which are too noisy for one-way protocols may become secure for two-way protocols. This "security activation" can have non-trivial applications, especially in realistic communication lines where the noise is high. For simplicity, we discuss only the two-way coherent-state protocol depicted in Fig. 6, which is a two-way extension of the no-switching protocol. Let Alice prepare a random coherent state $|\alpha\rangle$, whose amplitude α is Gaussian modulated. This state is sent to Bob, who randomly chooses between two configurations, ON and OFF. In ON, Bob applies a random displacement $D(\beta)$ with β Gaussian modulated. In OFF, Bob heterodynes the incoming state with outcome α' and prepares another random coherent state $|\gamma'\rangle$. In both configurations, the state is finally sent back to Alice, who performs heterodyne detection with outcome γ. During sifting, Bob declares the configuration chosen in each round. In ON, Alice processes α and γ to estimate β. In OFF, Alice considers $\alpha \simeq \alpha'$ and $\gamma \simeq \gamma'$. During parameter estimation, Alice and Bob analyze the noise properties of the channel, checking for the presence of memory between the forward and backward paths. If memory is present, they select the OFF configuration only. In this way, they can destroy the effect of the memory in the post-processing, by choosing only one of the two paths and processing its data in direct or reverse reconciliation. In this case the protocol is at least as robust as the underlying one-way protocol. By contrast, if memory is absent, Alice and Bob can use both the ON and OFF configurations. In this case, the key distribution is more robust to the noise of the channel, with the enhancement provided by the use of the ON configuration (see Sec. VI.B.5.d for details.)

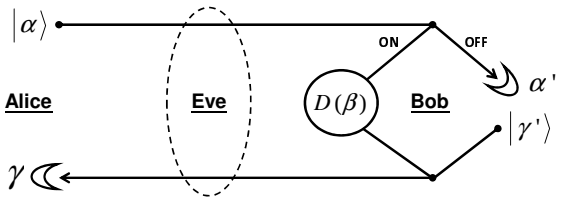


FIG. 6 Two-way coherent-state protocol. Alice sends a random coherent state to Bob, who selects between two configurations, ON or OFF. In ON, Bob applies a random displacement $D(\beta)$. In OFF, he heterodynes and prepares another random coherent state $|\gamma'\rangle$. In both configurations, the output state is sent back to Alice who performs heterodyne detection. The figure also displays a two-mode attack (discussed later).

9. Thermal state QKD

Generally, it is assumed in all the previous continuous-variable QKD protocols that Alice's initial states originate from encoding classical information onto pure vacuum states. However, in practice this is never possible with some level of impurity occurring due to experimental imperfections. Thermal state QKD therefore addresses this issue where the protocol is now analyzed with respect to Alice using noisy coherent states. This was first investigated by Filip (2008) and Usenko and Filip (2010) who showed that by using reverse reconciliation the distance over which QKD was secure, fell rapidly as the states became significantly impure. Extending upon this initial work, Weedbrook *et al.* (2010) showed that by using direct reconciliation, and provided that the channel transmission τ is greater than 50%, the security of quantum cryptography is not dependent on the amount of preparation noise on Alice's states. This is a counterintuitive result as we might naturally expect that as Alice's states become more and more thermalized, secure transmission over any finite distance would become impossible. Consequently, the best strategy to deal with preparation noise is to use a combination of direct ($\tau > 0.5$) and reverse reconciliation ($\tau \leq 0.5$). This motivated analysis into secure key generation at different wavelengths and was shown that secure regions exists from the optical and infrared all the way down into the microwave region (Weedbrook *et al.*, 2010).

B. Security analysis

The strongest definition of security in a quantum scenario was given by Renner (2005). A QKD protocol is said to be ϵ-secure if

$$D(\hat{\rho}_{abE}, \hat{\sigma}_{ab} \otimes \hat{\rho}_E) \leq \epsilon \tag{137}$$

where D is the trace distance as defined in Eq. (68). Here $\hat{\rho}_{abE}$ is the final joint state of Alice, Bob and Eve and $\hat{\sigma}_{ab} \otimes \hat{\rho}_E$ is the ideal secret-key state. Therefore, up to a probability ϵ Alice and Bob generate a shared secret key identical to an ideal key and with probability $1 - \epsilon$ they abort. In the following we present the necessary tools to calculate the secret-key rate K for various continuous-variable QKD protocols.

1. Main eavesdropping attacks

To prove the unconditional security of a QKD protocol, the following assumptions on Eve have to be satisfied: (1) full access to the quantum channel; (2) no computational (classical or quantum) limitation; (3) capable of monitoring the public channel, without modifying the messages (authenticated channel); (4) no access to Alice's and Bob's setups. Under these assumptions, the most powerful attack that Eve can implement is known as a *coherent attack*. This consists in Eve preparing a global ancillary system and making it interact with all the signals sent through the quantum channel, and then

storing the output ancillary system into a quantum memory[4]. Finally, after having listened to all the classical communication over the public channel, Eve applies an optimal joint measurement on the quantum memory. The security against coherent attacks is extremely complex to address. Interestingly, by using the quantum de Finetti theorem, proven by Renner (2007) for discrete variables and by Renner and Cirac (2009) for continuous variables, we can prove unconditional security in the asymptotic regime by analyzing the simpler class of collective attacks. For an arbitrary QKD protocol in the entanglement-based representation, if the multimode entangled state (shared between Alice and Bob after many uses of the channel) is permutationally invariant, then, for the quantum de Finetti theorem, this state can be approximated (asymptotically) by a mixture of independent and identically distributed two-mode states. This corresponds to considering the simpler case of a collective attack.

In a *collective attack* Eve has a set of independent and identically prepared systems (ancillas) each one interacting individually with a single signal sent by Alice. In the entanglement-based representation, this implies that the output state of Alice, Bob and Eve is in a tensor product of n identical states ($\hat{\rho}_{\mathbf{abE}}=\hat{\rho}_{abE}^{\otimes n}$). Eve's ancillas are stored in a quantum memory and then, after listening to Alice and Bob's classical communication, Eve applies an optimal measurement on the quantum memory. In the asymptotic regime ($n\rightarrow\infty$), the secret-key rate K can be computed via the formula (Renner *et al.*, 2005):

$$K=\varphi\left[I(a{:}b)-S(x{:}E)\right], \tag{138}$$

where $I(a{:}b)$ is the mutual information between the variables of Alice (a) and Bob (b) and $S(x{:}E)$ is the Holevo bound between Alice's (Bob's) variable $x=a$ ($x=b$) and Eve's quantum memory, when direct (reverse) reconciliation is used. For more on the mutual information and the Holevo bound see Sec. V.C. The coefficient $\varphi\in[0,1]$ models the effect of the sifting. For instance, we have $\varphi=1$ for the no-switching protocol, while $\varphi=1/2$ for the protocol with coherent states and homodyne detection.

2. Finite-size analysis

Until now we have considered the asymptotic scenario where Alice and Bob exchange infinitely many signals. This ideal situation is useful when we are interested in comparing the optimal performances of different protocols. However, in practice the number of signals is always finite. The formalism to address this problem was recently developed for discrete-variable QKD (Cai and Scarani, 2009; Scarani and Renner, 2008). In what follows we explain the most important features of finite-size analysis in the continuous-variable scenario (Leverrier *et al.*, 2010). In such a situation, the secret-key rate reads

$$K=\frac{\varphi n}{N}\left[\beta I(a{:}b)-S_{\epsilon_{PE}}(a(b){:}E)-\Delta(n)-D(n)\right], \tag{139}$$

where N is the total number of signals exchanged; n is the numbers of signals used for the establishment of the key ($N-n$ is used for parameter estimation); β is the *reconciliation efficiency* (ranging from 0 when no information is extracted to 1 for perfect reconciliation); $S_{\epsilon_{PE}}(a(b){:}E)$ is the maximal value of Eve's information compatible with the parameter estimation data; $\Delta(n)$ is related to the security of the privacy amplification and the speed of convergence of the smooth min-entropy towards the von Neumann entropy; $D(n)$ is the penalty due to considering collective attacks instead of coherent attacks (Christandl *et al.*, 2009; Renner, 2007; Renner and Cirac, 2009). The principal finite-size negative effect in discrete-variable QKD is due to the parameter estimation (Cai and Scarani, 2009) which is expected to be also the case for continuous-variable QKD (Leverrier *et al.*, 2010).

Despite the fact that Renner and Cirac (2009) have shown that collective attacks are as powerful as coherent attacks in the asymptotic regime, the correction $D(n)$ provided for the finite regime leads to a result that could be improved. An alternative approach using the natural symmetries of bosonic channels, was suggested by Leverrier *et al.* (2009), with only partial results obtained so far (Leverrier and Cerf, 2009). An ideal solution would be finding a generalization of the Leverrier and Grangier (2010a) result by showing that collective Gaussian attacks are optimal in the finite regime, i.e., $D(n)=0$ (which is the case for the asymptotic scenario as discussed in the next section). The study of finite-size effects in continuous-variable QKD is very recent and further investigations are needed.

3. Optimality of collective Gaussian attacks

The fully-Gaussian protocols, have the most developed security proofs due to their high symmetry. As we have discussed, Renner and Cirac (2009) have shown that, assuming the permutation symmetry of the classical post-processing, collective attacks are as efficient as coherent attacks. Therefore, in order to guarantee the security against collective attacks we need to know what type of collective attack is the most dangerous. A crucial step in that direction was the discovery that the optimal attack Eve can implement is one based on Gaussian operations (García-Patrón and Cerf, 2006; Leverrier and Grangier, 2010a; Navascués *et al.*, 2006). This consequently makes the security analysis much easier. García-Patrón and Cerf (2006) showed that, for an entanglement-based QKD protocol characterized by a tripartite state $\hat{\rho}_{abE}$, i.e., resulting from Alice's and Bob's measurements on the pure state $|\psi\rangle_{ABE}$, of covariance matrix $\mathbf{V}_{ABE}$, the secret-key is minimized by the Gaussian state $\hat{\rho}_{abE}^{G}$ of the

[4] Quantum memory is a device that allows the storage and retrieval of quantum information. It plays a role in many continuous-variable quantum information protocols. For more theoretical details and the status of experimental demonstrations, see e.g., Hammerer *et al.* (2010) and Lvovsky *et al.* (2009).

same covariance matrix, i.e.,

$$K(\hat{\rho}_{abE}) \geq K(\hat{\rho}^{G}_{abE}). \tag{140}$$

As a result, collective Gaussian attacks represent the fundamental benchmark to test the asymptotic security of continuous-variable QKD protocols based on the Gaussian modulation of Gaussian states.

4. Full characterization of collective Gaussian attacks

The most general description of a collective Gaussian attack is achieved by dilating the most general one-mode Gaussian channel into an environment which is controlled by Eve. As discussed in Sec. V.B, an arbitrary one-mode Gaussian channel $\mathcal{G}$ is associated with three symplectic invariants: transmissivity τ, rank r, and thermal number $\bar{n}$. These quantities identify a simpler channel, the canonical form $\mathcal{C}(\tau, r, \bar{n})$, which is equivalent to $\mathcal{G}$ up to a pair of Gaussian unitaries U and W (see Fig. 7). The canonical form can be dilated into a symplectic transformation $\mathbf{L}(\tau, r)$ which mixes the incoming state $\hat{\sigma}$ with an EPR state $|\nu\rangle$ of variance $\nu = 2\bar{n} + 1$ (see Fig. 7). Now if we treat the environment as a large but finite box, the dilation is unique up to a unitary $\tilde{U}$ which transforms the output EPR modes $\mathbf{E}$ together with a countable set of vacuum modes $\mathbf{F}$ (see Fig. 7). Thus, for each use of the channel, Eve's modes $\{\mathbf{E}, \mathbf{F}\}$ are transformed by some $\tilde{U}$ and then stored in a quantum memory. This memory is detected at the end of the protocol by means of an optimal coherent measurement $\mathcal{M}$ which estimates Alice's data (in direct reconciliation) or Bob's data (in reverse reconciliation). This is the most general description of a collective Gaussian attack (Pirandola, Braunstein, and Lloyd, 2008).

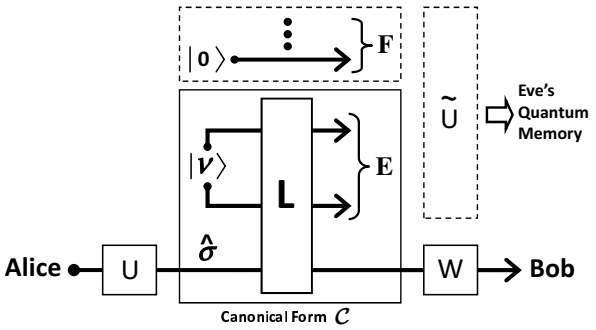


FIG. 7 Construction of a collective Gaussian attack in four steps. (1) Any one-mode Gaussian channel $\mathcal{G}$ can be reduced to a canonical form $\mathcal{C}$ via two Gaussian unitaries U and W. (2) Form $\mathcal{C}$ can be dilated into a symplectic transformation $\mathbf{L}$ mixing the input state $\hat{\sigma}$ with an EPR state $|\nu\rangle$. (3) In a finite box, the dilation is unique up to a unitary $\tilde{U}$ combining the output EPR modes $\mathbf{E}$ with a countable set of vacuum modes $\mathbf{F}$. (4) After $\tilde{U}$ all of the output is stored in a quantum memory that Eve measures at the end of the protocol.

This scenario can be greatly simplified if we use the Holevo bound for Eve's accessible information. For instance, this happens when we consider the asymptotic regime, so that Eq. (138) holds. In this case, we can ignore the details of $\mathcal{M}$, the extra unitary $\tilde{U}$ and the extra ancillas $\mathbf{F}$. As a result, the attack is simply described by the canonical dilation $\{\mathbf{L}(\tau, r), |\nu\rangle\}$ and the one-mode Gaussian unitaries $\{U, W\}$ (see solid boxes in Fig. 7). As discussed in Ch. II, the Gaussian unitaries $\{U, W\}$ can be further decomposed in displacements, rotations and squeezings. By definition, we call 'canonical' the attacks with $U = W = I$. These attacks are fully described by the canonical dilation $\{\mathbf{L}(\tau, r), |\nu\rangle\}$ (Pirandola, Braunstein, and Lloyd, 2008). The most important canonical attack is the (collective) entangling-cloner attack (Grosshans, van Assche, *et al.*, 2003). In this attack, the symplectic transformation $\mathbf{L}$ represents a beam splitter of transmissivity $0 < \tau < 1$ mixing the incoming signal mode with one mode only of the EPR state $|\nu\rangle$. Thus, from the point of view of Alice and Bob, we have a lossy channel with transmissivity τ and thermal number $\bar{n} = (\nu - 1)/2$. This channel is the most common, representing the standard description for communication lines such as optical fibers.

5. Secret-key rates

In this section, we discuss the secret-key rates of the continuous-variable QKD protocols given in Sec. VI.A. These rates are derived in the presence of a collective entangling cloner attack which is the most important collective Gaussian attack in the experimental sense. This attack can be identified by the parameters of the corresponding lossy channel, i.e., transmission τ and thermal number $\bar{n}$. Equivalently, we can consider τ and the excess noise $\chi := 2\bar{n}(1 - \tau)\tau^{-1}$, i.e., the noise on Bob's side referred to the input (Alice). These parameters are inferred by Alice and Bob during the parameter estimation stage. Given a specific protocol, the corresponding secret-key rate can be expressed in terms of the two channel parameters as $K = K(\tau, \chi)$. Furthermore, the equation $K = 0$ defines the security threshold of the protocol, expressed in terms of tolerable excess noise $\bar{\chi}$ versus the transmissivity of the channel, i.e., $\bar{\chi} = \bar{\chi}(\tau)$.

Note that we can derive more general expressions for the secret-key rates by considering the most general form of a collective Gaussian attack (cf. Sec. VI.B.4). This generalization can be found in Pirandola, Braunstein, and Lloyd (2008) for the no-switching protocol of Weedbrook *et al.* (2004). The secret-key rates of the other protocols could be generalized as well. This generalization involves not only the study of other canonical attacks but also the analysis of phase-effects (mixing of the quadratures) which derive from the Gaussian unitaries U and W. These effects can be taken into account by introducing suitable corrections in the expressions of the rates. Another possibility is reducing an attack to a canonical attack ($U = W = 1$) by means of random transformations in the post-processing stage, which sacrifices part of the secret data. This symmetrization has been recently used by Leverrier *et al.* (2009) to delete phase-effects from lossy channels.

a. Fully-Gaussian protocols

Here we discuss the secret-key rates for the family of fully-

Gaussian protocols. In the entanglement-based description, one mode of an EPR state of variance V is sent through the lossy channel with transmissivity τ and excess noise χ. At the output of the channel, Alice and Bob's bipartite state is Gaussian with covariance matrix

$$\mathbf{V}_{AB} = \begin{pmatrix} x\mathbf{I} & z\mathbf{Z} \\ z\mathbf{Z} & y\mathbf{I} \end{pmatrix}, \tag{141}$$

$x = V$, $y = \tau(V + \chi)$ and $z = \sqrt{\tau(V^2 - 1)}$. Now the various protocols differ for the measurements of both Alice and Bob and the kind of reconciliation used. In order to estimate Eq. (138) we first calculate Alice and Bob's mutual information (García-Patrón, 2007)

$$I(a{:}b) = \frac{w}{2} \log \left[(V + \chi)/(\chi + \lambda V^{-1}) \right], \tag{142}$$

where $w = 1$, except for the no-switching protocol where $w = 2$; then $\lambda = V$ ($\lambda = 1$) for protocols with coherent (squeezed) states. The calculation of Eve's information is more involved. As an example, we consider the calculation of $S(b{:}E) = S(E) - S(E|b)$ for reverse reconciliation using coherent states and homodyne detection. First we use the fact that Eve's system E purifies AB, i.e., $S(E) = S(AB)$, where $S(AB)$ can be calculated from the symplectic eigenvalues of the matrix $\mathbf{V}_{AB}$ using Eq. (54), which are then substituted into Eq. (46). Next, to calculate the term $S(E|b)$ we find the symplectic eigenvalues of the covariance matrix $V_{E|b}$, computed using Eq. (64), and then proceed as before.

b. Postselection

Determining the secret-key rates for postselection is more challenging than either direct or reverse reconciliation. Despite the fact that the postselection protocol involves Gaussian elements in the quantum communication part, its description becomes non-Gaussian after the filtering of data. Consequently, using Eq. (140) to upper-bound Eve's information no longer applies. Therefore, a subtler analysis has to be carried out to obtain tighter bounds. Here we present the basic security analysis for the postselection protocol against collective entangling cloner attacks (Heid and Lütkenhaus, 2007; Symul *et al.*, 2007). When Bob performs homodyne detection, the mutual information between Alice and Bob for a given pair of variables $(|a_{q(p)}|, |b|)$ is given by Shannon's formula for a binary channel (Shannon, 1948)

$$I(a:b) = 1 + p_e \log p_e + (1 - p_e) \log(1 - p_e). \tag{143}$$

Here p_e is Bob's error in determining the value of Alice's sign and is given by

$$p_e = \left\{ 1 + \exp \left[8\sqrt{\tau} |a_{q(p)} b| / (1 + \chi) \right] \right\}^{-1}. \tag{144}$$

Now if Bob performs heterodyne detection, we have to consider the Shannon formula for two parallel binary channels, one per quadrature, and is given by (Lance *et al.*, 2005)

$$p_e = \left\{ 1 + \exp \left[4\sqrt{2\tau} |a_{q(p)} b| / (1 + \chi) \right] \right\}^{-1}. \tag{145}$$

Eve's information is calculated using the Holevo bound between Eve's system and the information bits used as reference for the key (a in direct reconciliation and b in reverse reconciliation). The key rate for a given pair of values (a, b) reads

$$\Delta K = \varphi \max\{\beta I(a:b) - S^{a,b}(E:x), 0\}, \tag{146}$$

where again φ accounts for the sifting and β for the reconciliation efficiency. The postselection is then modeled by the *maximum* function, imposing a zero contribution of the effective binary channel when $\beta I(a:b) - S^{a,b}(E:x) < 0$, as expected. Finally, the evaluation of the overall secret-key rate needs to be calculated numerically and is given by

$$K = \int p(a,b)\, \Delta K(a,b)\, da\, db, \tag{147}$$

where $p(a, b)$ is a joint probability distribution. A detailed experimental analysis was carried out by Symul *et al.* (2007) using postselection with the no-switching protocol.

c. Discrete modulation of Gaussian states

One of the technical advantages of continuous-variable QKD is that it relies solely on standard high-speed optical telecom components. However to date, field implementations have been restricted to short distances (27 km by Fossier *et al.* (2009)). The main reason is the low efficiency of the reconciliation stage for protocols using Gaussian modulation (Lodewyck *et al.*, 2007). This is especially true at low signal-to-noise ratios (Leverrier *et al.*, 2008), which is the working regime when distributing secret keys over long distances. On the other hand, extremely good reconciliation protocols exist for discrete modulations, as the error correction procedure is greatly simplified. In this case, the problem can be mapped onto a binary channel with additive noise, for which there exists very good codes, such as low-density-parity check codes (Richardson *et al.*, 2001). Unfortunately, protocols based on discrete modulation, even if using Gaussian states, have non-Gaussian entanglement-based representations. As a result, the calculation of Eve's information can no longer rely on the previous optimality proofs (García-Patrón and Cerf, 2006; Leverrier and Grangier, 2010a; Navascués *et al.*, 2006).

However, the proof by García-Patrón and Cerf (2006) can still be used to provide a (non-tight) Gaussian upper bound on Eve's information. This idea was used by Leverrier and Grangier (2009), where a protocol with four coherent states was shown to outperform Gaussian-modulated protocols in the regime of low signal-to-noise ratio. The crucial point was the observation that the four-state modulation well approximates the Gaussian modulation for low modulation variances. As a result, the Gaussian upper bound can still be used, being nearly tight in the studied regime. The following year Leverrier and Grangier (2010b) proposed another non-Gaussian (but continuous) modulation protocol able to exploit the Gaussian upper bound. In this protocol, Alice generates points centered on an eight-dimensional sphere to decide which ensemble of four successive coherent states

are to be sent. Then, Bob uses the no-switching protocol (heterodyne detection) to guess the point selected by Alice. The secret-key rate reached by this new protocol is higher, by nearly an order of magnitude, for realistic parameters, which enables the distribution of a secret keys over distances of the order of 50 km, even after taking all finite-size effects into account.

d. Two-way quantum communication

In general, the security analysis of two-way protocols is quite involved. For simplicity, here we consider the two-way coherent-state protocol of Fig. 6. Using symmetrization arguments (Renner, 2005; Renner and Cirac, 2009), one can reduce an arbitrary coherent attack to a two-mode attack, affecting each round-trip independently. This attack can have a residual memory between the two uses of the quantum channel. If this memory is present, Alice and Bob use the OFF configuration, thus collapsing the protocol to one-way quantum communication. Correspondingly, the attack is reduced to one-mode, i.e., collective, which can be bounded by assuming a Gaussian interaction (collective Gaussian attack). Thus, in OFF, the security threshold is given by the underlying one-way protocol (the no switching protocol in this case). The advantage occurs when no memory is present, which is the most practical situation. In particular, this happens when the original attack is already collective. In this case, Alice and Bob can use both the ON and OFF configurations to process their data. While the OFF configuration is equivalent to two instances of one-way protocol (forward and backward), the ON configuration is based on a coherent two-way quantum communication. Let us consider the case of a collective entangling cloner attack, which results in a one-mode lossy channel with transmissivity τ and excess noise χ. For every $\tau \in (0,1)$, the key distribution is possible whenever the excess noise χ is below a certain value $\bar{\chi}$ specified by the security threshold $\bar{\chi} = \bar{\chi}(\tau)$. As shown by Pirandola, Mancini, *et al.* (2008), the security threshold in ON configuration is higher than the one in OFF configuration. For instance, if we consider reverse reconciliation, we have $\bar{\chi}_{\text{ON}}(\tau) > \bar{\chi}_{\text{OFF}}(\tau)$ for every $\tau \in (0,1)$. As a result, there are lossy channels whose excess noise χ is intolerable in OFF but still tolerable in ON. Thanks to this security activation, the two-way coherent-state protocol is able to distribute secret keys in communication lines which are too noisy for the corresponding one-way protocol. This result, which has been proven for large modulation and many rounds (asymptotic regime), is also valid for other Gaussian modulation protocols, extended to two-way quantum communication via the hybrid ON/OFF formulation.

C. Future directions

Continuous-variable QKD offers a promising alternative to the traditional discrete-variable QKD systems (for a state-of-the-art comparison between the various QKD platforms see Scarani *et al.* (2009)). An important next step for continuous-variable QKD is to prove unconditional security in a fully realistic scenario, for example, by improving the reconciliation procedures and taking finite-size effects into account. This could potentially provide extremely high secret-key rates over distances which are comparable to the ones of discrete-variable protocols (about 100 km). Thus, additional research efforts are focused to extend the range of continuous-variable QKD protocols. As opposed to the single-photon detectors of discrete-variable QKD, the use of homodyne detection in continuous-variable QKD provides an outcome even for the vacuum input. Filtering out this vacuum noise is the main weakness in the reconciliation procedures. From this point of view, postselection is the best choice. Therefore, proving the unconditional security of the postselection protocol would be of great interest[5]. Another possibility is the design of new protocols which are more robust to excess noise, i.e., with higher security thresholds. This would enable the reconciliation procedures to work much more efficiently. Such a possibility has been already shown by the use of two-way protocols. Thus further directions include the full security analysis of protocols based on multiple quantum communication.

The further development of continuous-variable quantum repeaters is also an important research direction. Quantum repeaters would allow one to distribute entanglement between two end-points of a long communication line, which can later be used to extract a secret key. This technique combines entanglement distillation, entanglement swapping, and the use of quantum memories. Unfortunately, Gaussian operations cannot distill Gaussian entanglement which poses a serious limitation to this approach. However, there has been ongoing research effort in the direction of Gaussian preserving optical entanglement distillation employing non-Gaussian elements (Browne *et al.*, 2003; Eisert *et al.*, 2004; Fiurášek *et al.*, 2003; Menzies and Korolkova, 2007; Ralph and Lund, 2009).

VII. CONTINUOUS-VARIABLE QUANTUM COMPUTATION USING GAUSSIAN CLUSTER STATES

Quantum computation using continuous variables was first considered by Lloyd and Braunstein (1999) in the circuit model of quantum computing (Nielsen and Chuang, 2000). They showed that arbitrary quantum logic gates (i.e., simple unitaries) could be created using Hamiltonians that are polynomial in the quadrature operators $\hat{q}$ and $\hat{p}$ of the harmonic oscillator. Years later, a different but computationally equivalent model of continuous-variable quantum computation, known as cluster state quantum computation, was developed by Zhang and Braunstein (2006) and Menicucci *et al.* (2006). This measurement-based protocol of quantum computation was originally developed by Raussendorf and Briegel (2001) for discrete variables and forgoes actively implementing quantum gates. Instead, the computation is achieved via local mea-

[5] At the time of writing a paper by Walk *et al.* (2011) has appeared which addresses this issue.

surements on a highly entangled multimode state, known as a cluster state. In the ideal case, the continuous-variable cluster state is created using infinitely squeezed states, but in practice, is approximated by a finitely squeezed Gaussian entangled state.

These two models of continuous-variable computation must be associated with a fault tolerant and error correctable system, where at some point the continuous variables are discretized. With this in mind, there is a third type of continuous-variable quantum computer, known as the Gottesman-Kitaev-Preskill quantum computer (Gottesman *et al.*, 2001). This proposal shows how to encode finite-dimensional qubits into the infinite-dimensional harmonic oscillator, thus facilitating fault tolerance and quantum error correction. In this section, we focus primarily on cluster state quantum computation while still using important elements of the Gottesman-Kitaev-Preskill computer and the Lloyd-Braunstein model.

This section is structured as follows. We begin by introducing important continuous-variable gates as well as defining what constitutes a universal set of gates. In Sec. VII.B we introduce the notion of one-way quantum computation using continuous variables and how one can gain an understanding of it by considering a teleportation circuit. The important tools of graph states and nullifiers follows in Sec. VII.C, while the realistic case of Gaussian computational errors due to finite squeezing is discussed in Sec. VII.D. The various proposals for optically implementing Gaussian cluster states are revealed in Sec. VII.E. In Secs. VII.F and VII.G, achieving universal quantum computation and quantum error correction for continuous variables, are discussed respectively. Two examples of algorithms for a continuous-variable quantum computer are given in Sec. VII.H, before ending with future directions of the field in Sec. VII.I.

A. Continuous-variable quantum gates

Before introducing the quantum gates used in continuous-variable quantum computation we remind the reader that the displacement gate $D(\alpha)$, the beam splitter gate B, and the one and two-mode squeezing gates, S and S_2, are important Gaussian gates which have already been introduced in Sec. II.B. To begin with, in Gaussian quantum information processing there are the Heisenberg-Weyl operators which comprise of the position and momentum phase-space displacement operators, given respectively as

$$X(s) = \exp(-is\hat{p}/2), \qquad Z(t) = \exp(it\hat{q}/2), \tag{148}$$

where $X(s)$ gives a shift by an amount s in the q direction and $Z(t)$ a momentum shift by an amount t, i.e., in terms of the displacement operator $D(\alpha)$ they can be rewritten as $X = D(s/2)$ and $Z = D(it/2)$. They are related via $X(s)Z(t) = e^{-ist/2}Z(t)X(s)$ and act on the position computational basis states $|q\rangle$ as

$$X(s)\,|q\rangle = |q+s\rangle\,, \qquad Z(t)\,|q\rangle = e^{itq/2}\,|q\rangle\,. \tag{149}$$

and on the momentum basis states $|p\rangle$ as

$$X(s)\,|p\rangle = e^{-isp/2}\,|p\rangle\,, \qquad Z(t)\,|p\rangle = |p+t\rangle\,. \tag{150}$$

The position and momentum basis states are related via a Fourier transform as defined in Eq. (9). The Fourier gate F is the Gaussian version of the qubit Hadamard gate and can be defined in terms of the annihilation and creation operators as well as the quadrature operators

$$F = \exp\Big(\frac{i\pi}{4}\Big)\exp\Big[\frac{i\pi}{2}\hat{a}^\dagger\hat{a}\Big] = \exp\Big[\frac{i\pi}{8}\Big(\hat{q}^2+\hat{p}^2\Big)\Big]. \tag{151}$$

In the phase-space picture, the Fourier gate is a $\pi/2$ rotation, e.g., from one quadrature to the other

$$F^\dagger\hat{q}F = -\hat{p}, \qquad F^\dagger\hat{p}F = \hat{q}. \tag{152}$$

The Fourier gate acts on the displacement gates as follows

$$F^\dagger Z(t)F = X(t), \qquad FX(s)F^\dagger = Z(s). \tag{153}$$

Finally, the Fourier gate acting on the quadrature eigenstates gives

$$F\,|x\rangle_q = |x\rangle_p\,, \qquad F^\dagger\,|x\rangle_q = |-x\rangle_p\,, \tag{154}$$

$$F\,|x\rangle_p = |-x\rangle_q\,, \qquad F^\dagger\,|x\rangle_p = |x\rangle_q\,, \tag{155}$$

where the subscript is used to remind us whether we are in the computational q basis or the conjugate p basis. The phase gate $P(\eta)$ can be thought of as a type of shearing operation, i.e., a combination of rotations and squeezers. It is defined as

$$P(\eta) = \exp\Big[\Big(\frac{i\eta}{4}\Big)\hat{q}^2\Big]. \tag{156}$$

where $\eta \in \mathbb{R}$. The phase gate acts on the $X(s)$ displacement gate as

$$P^\dagger X(s)P = e^{i\eta s^2/4}X(s)Z(\eta s), \tag{157}$$

while leaving Z unaltered. The phase gate affects the quadratures as

$$P^\dagger\hat{q}P = \hat{q}, \qquad P^\dagger\hat{p}P = \hat{p} + \eta\hat{q}. \tag{158}$$

The controlled-phase gate, or *CPHASE* for short, is a two-mode Gaussian gate defined as

$$C_Z = \exp\Big[\Big(\frac{i}{2}\Big)\hat{q}_1 \otimes \hat{q}_2\Big]. \tag{159}$$

The effect of this two-mode gate on the computational basis states is given by

$$C_Z\,|q_1\rangle\,|q_2\rangle = e^{iq_1q_2/2}\,|q_1\rangle\,|q_2\rangle\,, \tag{160}$$

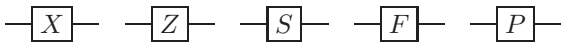
In the Heisenberg picture, the CPHASE gate transforms the momentum quadratures according to

$$\hat{p}_1 \to \hat{p}_1 + \hat{q}_2, \qquad \hat{p}_2 \to \hat{p}_2 + \hat{q}_1, \tag{161}$$

while doing nothing to the position quadratures $\hat{q}_1 \to \hat{q}_1$ and $\hat{q}_2 \to \hat{q}_2$. The CPHASE gate and the phase gate both get their names from the analogous discrete-variable gates and their

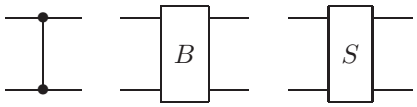
similar actions on the Pauli matrices (Nielsen and Chuang, 2000).

Finally, we note the graphical representation of the quantum gates in the circuit model of computation. The single-mode Gaussian gates: Heisenberg-Weyl displacement gates, single-mode squeeze gate, Fourier gate and the phase gate are given respectively as



(162)

While the two-mode Gaussian gates: the *CPHASE* gate, the beam splitter gate and the two-mode squeeze gate, are denoted respectively by



(163)

1. Universal set of quantum gates

A continuous-variable quantum computer is said to be universal if it can implement an arbitrary Hamiltonian with arbitrarily small error. So what are the necessary and sufficient conditions for a continuous-variable quantum computer to be universal? This is given by the Lloyd-Braunstein criterion (Lloyd and Braunstein, 1999) which tells us which gates are needed to generate any unitary transformation to arbitrary accuracy. This consists of the two families of gates:

1. $Z(t)$, $P(\eta)$, F and U_G (which is any multimode Gaussian gate, e.g., C_Z or B), $\forall\, t, \eta \in \mathbb{R}$. This first family generates all possible Gaussian operations.

2. $\exp[it\hat{q}^{n\geq 3}]$ (for some value of t) which is a non-linear transformation of polynomial degree 3 or higher and corresponds to a family of non-Gaussian gates.

Note that if we were restricted to using only Gaussian gates we would not be able to synthesize an arbitrary Hamiltonian. In fact, the continuous-variable version (Bartlett *et al.*, 2002) of the Gottesman-Knill theorem (Gottesman, 1998) tells us that starting from an initial Gaussian state, Gaussian processing (which includes Gaussian measurements and Gaussian operations) can be efficiently simulated on a classical computer.

B. One-way quantum computation using continuous variables

One-way quantum computation (Raussendorf and Briegel, 2001) using continuous variables (Gu *et al.*, 2009; Menicucci *et al.*, 2006; Zhang and Braunstein, 2006) allows one to perform any computational algorithm by implementing a sequence of single-mode measurements on a specially entangled state known as a cluster state (note that we often begin our analysis using a perfectly entangled state but move to the more realistic case of a Gaussian cluster state as we progress). Here quantum gates are not required, as arbitrary Hamiltonians are simulated via measurements alone. After each measurement is performed the resulting measurement outcome is used to select the basis of the next measurement. In general, the order in which measurements are made does matter, a property known as *adaptiveness*. However, when implementing only Gaussian gates, this condition is relaxed and the order no longer matters, a property known as *parallelism*. The two basic steps of continuous-variable cluster state quantum computation can be summarized as follows:

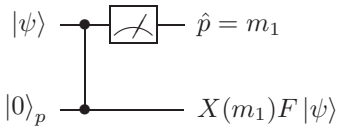
1. Cluster state preparation: All qumodes are initialized as highly squeezed vacuum states, approximating momentum eigenstates $|0\rangle_p$. The C_Z gate is applied to the relevant qumodes in order to create the entangled cluster state.

2. Measurements: single-mode measurements are made on the relevant qumodes where each result is used to select the subsequent measurement basis.

Here a quantum mode, or *qumode* for short, is the continuous-variable analogue of the discrete-variable qubit and is simply a continuous-variable quantum state or mode. Note that, up until this point in the review, we have simply referred to such states as modes. However in line with the terminology used in the current research of continuous-variable cluster states, we will refer to such quantum states as qumodes.

1. Understanding one-way computation via teleportation

To get a feel of how measurements allow us to generate arbitrary evolutions in cluster state computation, it is helpful to look at quantum teleportation from the perspective of the quantum circuit model. The quantum circuit for the gate teleportation of a single-mode continuous-variable quantum state $|\psi\rangle$ is given by (Menicucci *et al.*, 2006)



(164)

The above circuit can be understood in the following way. The input states consist of the arbitrary state $|\psi\rangle$ that we wish to teleport and a momentum eigenstate $|0\rangle_p$ (note that we will begin by considering the unphysical case of perfectly squeezed vacuum states with the realistic case of Gaussian squeezed states discussed later). They are entangled using a C_Z gate. A $\hat{p}$ quadrature measurement is performed resulting in the outcome m_1. The state $|\psi\rangle$ is thus teleported from the top quantum wire to the bottom wire and can be fully restored by applying the corrections $F^\dagger X^\dagger(m_1)$ to the output state. We will now go through the above circuit in more detail. First, the two initial input states can be written as $|\psi\rangle\,|0\rangle_p$. Expanding them into the position basis gives $|\psi\rangle\,|0\rangle_p = (2\sqrt{\pi})^{-1}\int dq_1 dq_2 \psi(q_1)\,|q_1\rangle\,|q_2\rangle$ where $|\psi\rangle = \int dq_1 \psi(q_1)\,|q_1\rangle$ and $|0\rangle_p = (2\sqrt{\pi})^{-1}\int dq_2\,|q_2\rangle$. Applying

the CPHASE gate leads to

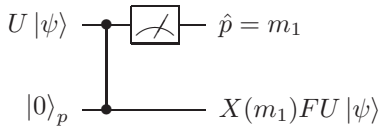
$$C_Z \left|\psi\right\rangle \left|0\right\rangle_p = \frac{1}{2\sqrt{\pi}} \int dq_1 dq_2 \psi(q_1) e^{iq_1 q_2/2} \left|q_1\right\rangle \left|q_2\right\rangle . \tag{165}$$

After measuring $\hat{p}$ of the first mode, using the projector $\left|m_1\right\rangle \left\langle m_1\right|_p$, and obtaining the result m_1 we get

$$\frac{1}{4\pi} \int dq_1 dq_2 \psi(q_1) e^{iq_1(q_2 - m_1)/2} \left|q_2\right\rangle ,$$

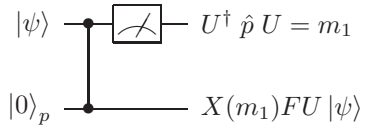
where we used $\left\langle m_1 \right| \left. q_1 \right\rangle = (2\sqrt{\pi})^{-1} \exp(-iq_1 m_1/2)$. The above state can be rewritten as: $\left|\psi'\right\rangle = X(m_1) F \left|\psi\right\rangle$. As mentioned before applying the corrections gives back the initial state: $F^\dagger X^\dagger(m_1) \left|\psi'\right\rangle = \left|\psi\right\rangle$.

Having considered the teleportation of an arbitrary state, we are now in a position to consider the teleportation of a quantum gate (Bartlett and Munro, 2003), which is at the heart of the measurement-based model of computation. This requires only a slight alteration to the previous circuit as we will be considering teleporting gates that are diagonal in the computational basis and thus commute through the CPHASE gate. For example, the circuit below teleports the state $\left|\psi'\right\rangle = U \left|\psi\right\rangle$ where $U = \exp[if(\hat{q})]$ is a gate diagonal in the computational basis



(166)

The above circuit is equivalent to the circuit below, where U can be absorbed into the measurement process



(167)

The above circuit forms the basis for our understanding of measurement-based quantum computation. Let us stop for a moment to consider why this is. Circuit (166) is the typical quantum circuit where an algorithm (in this case gate teleportation) is achieved by first implementing a quantum gate U onto a quantum state $\left|\psi\right\rangle$. However, circuit (167) shows us that we no longer need to explicitly implement the quantum gate but we can simulate the effect of the gate using only measurements in a new basis. This effect is the building block of cluster state computation where we can concatenate a number of these circuits to form a larger cluster state.

2. Implementing gates using measurements

We have just shown that by performing a measurement in the basis $U^\dagger \hat{p} U$ we can simulate the effect of the U gate on an arbitrary state. Using this result with the previously mentioned Lloyd-Braunstein criterion, we are able to implement the set of universal Hamiltonians $\hat{q}, \hat{q}^2, \hat{q}^3$ using only measurements. We can forget about the two-mode Gaussian gate U_G from the set as we have already used it in creating the cluster via the C_Z gate. We also use the Hamiltonian $\hat{q}^3$, rather than any other higher order polynomial, because we know how to optically implement it (more on this in Sec. VII.F). This corresponds to the following three transformations

$$U_j^\dagger \hat{p}\, U_j = \hat{p} + t\hat{q}^{j-1} \tag{168}$$

for $j = 1, 2, 3$ and where the gates diagonal in the computational basis are conveniently written as $U_j = \exp[(it/2j)\hat{q}^j]$. Notice that U_1 corresponds to the Heisenberg-Weyl displacement operator $Z(t)$, U_2 is the phase gate $P(t)$ and U_3 is known as the cubic phase gate, denoted as $V(t)$. So how are the above transformations optically implemented? Well, the first one is achieved by simply measuring $\hat{p}$ and adding t to the measurement result. The second one is a homodyne measurement in a rotated quadrature basis: $(\hat{p}\cos\theta - \hat{q}\sin\theta)/\cos\theta$. However, the cubic Hamiltonian is a little more difficult to implement than the previous two and will be discussed in more detail in Sec. VII.F.

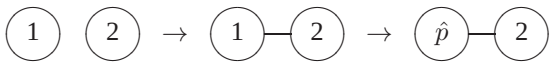
C. Graph states and nullifiers

1. Graph states

A common and convenient way of depicting cluster states is by using graphs. The continuous-variable version of graph states was defined by Zhang and Braunstein (2006) where every continuous-variable cluster state can be represented by a graph (Gu *et al.*, 2009) known as a graph state[6]. Specifically, a graph $G = (V, E)$ consists of a set of vertices (or nodes) V and a set of edges E. The following recipe allows us to construct a corresponding graph state

1. Each squeezed momentum eigenstate becomes a vertex in the graph.
2. Each C_Z operation applied between two qumodes is an edge in the graph.

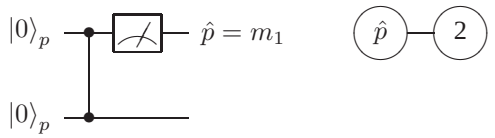
To illustrate, we give a simple example of a two-mode cluster state. Below we have the first step of initializing the two squeezed momentum eigenstates (represented by vertices and labeled 1 and 2). In the second step the C_Z gate is applied, indicated by the edge joining vertices 1 and 2. The final step illustrates how measurements are indicated on a graph. Here a $\hat{p}$ quadrature measurement on the first node is implemented



(169)

[6] From now on we will use the terms "cluster states" and "graph states" interchangeably. Note that some authors technically refer to a cluster state as one which has a graph that is universal for measurement-based computation (e.g., a square lattice); while a graph state could be any arbitrary graph. However, in the continuous-variable literature (Flammia *et al.*, 2009; Menicucci, 2011; Menicucci *et al.*, 2008, 2011, 2010, 2006) it is common to use them synonymously with context providing clarity.

Previously we introduced the quantum circuit formalism to understand measurement-based computation. Therefore we give below an equivalence between the teleportation circuit (on the left) and the graph state formalism (on the right)



(170)

The concept of continuous-variable graph states has been developed in a number of papers by Zhang (Zhang, 2008a,b, 2010) and independently by others (Aolita *et al.*, 2011; Flammia *et al.*, 2009; Flammia and Severini, 2009; Menicucci *et al.*, 2008, 2007; Pfister, 2007; Zaidi *et al.*, 2008; Zhang *et al.*, 2009). Recently, a more general approach was introduced by Menicucci *et al.* (2011) allowing the graphical calculus formalism to be applied to the practical case where continuous-variable cluster states are created using finitely squeezed Gaussian states rather than ideal perfectly squeezed eigenstates.

2. Stabilizers and nullifiers

The stabilizer formalism (Gottesman, 1997) for continuous variables (Barnes, 2004; Gottesman *et al.*, 2001; van Loock *et al.*, 2007) is a useful way of both defining and analyzing cluster states (or graph states). An operator $\hat{O}$ is a stabilizer of a state $|\psi\rangle$ if $\hat{O}|\psi\rangle = |\psi\rangle$, i.e., it has an eigenvalue of $+1$. For example, a zero momentum eigenstate $|0\rangle_p$ is stabilized by the displacement operator $X(s)$, i.e., $X(s)|0\rangle_p = |0\rangle_p$ for all values of s. For an arbitrary continuous-variable graph state $|\phi\rangle$ with graph $G = (V, E)$ on n qumodes, the stabilizers are defined as

$$K_i(s) = X_i(s) \prod_{j \in N(i)} Z_j(s), \tag{171}$$

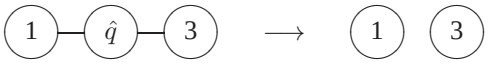
for $i = 1, ..., n$ and for all $s \in \mathbb{R}$. Here $N(i)$ means the set of vertices in the neighborhood of v_i, i.e., $N(i) = \{j | (v_j, v_i) \in E\}$. A variation of these stabilizers K_i involves using what is known as *nullifiers* H_i. Here every stabilizer is the exponential of a nullifier, i.e., $K_i(s) = e^{-isH_i}$ for all $s \in \mathbb{R}$. This results in $H_i|\phi\rangle = 0$ where the set of nullifiers are given by

$$H_i = \hat{p}_i - \sum_{j \in N(i)} \hat{q}_j. \tag{172}$$

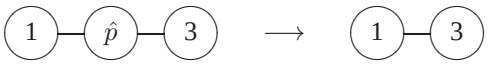
Therefore the graph state $|\phi\rangle$ is a zero eigenstate of the above nullifiers where any linear superposition satisfies $H_i|\psi\rangle = 0$ and $[H_i, H_j] = 0$. An example might be helpful here. Suppose we have a simple three-node linear cluster where the nodes are labeled $1, 2$ and 3. Then, according to Eq. (172), the nullifiers are given by: $\hat{p}_1 - \hat{q}_2, \hat{p}_2 - \hat{q}_1 - \hat{q}_3, \hat{p}_3 - \hat{q}_2$. Furthermore, according to Eq. (171), the set of stabilizers can be written as: $X_1(s)Z_2(s), Z_1(s)X_2(s)Z_3(s), Z_2(s)X_3(s)$, for all s. Therefore, by simply looking at a given graph we can write down the nullifiers and stabilizers of that particular graph. We note another useful way of analyzing graph states, other than the nullifier formalism, is by using the Wigner representation (Gu *et al.*, 2009).

3. Shaping clusters: removing nodes and shortening wires

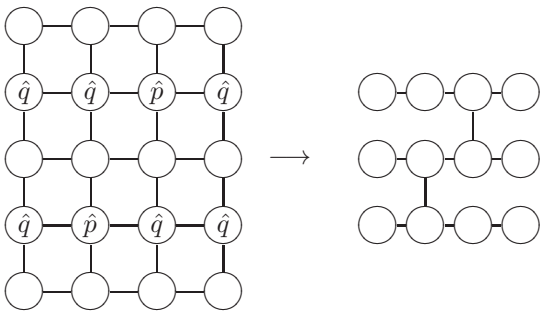
The nullifier formalism provides a useful way of understanding how graph states are transformed by quadrature measurements. It can be shown (Gu *et al.*, 2009) that $\hat{q}$ (computational) measurements remove a given node (modulo some known displacement), while $\hat{p}$ quadrature measurements also remove the node but preserve the correlations between neighboring nodes (modulo a displacement and Fourier transform). For example, in the graph state picture, a position quadrature measurement on the second node has the following effect



and a momentum measurement on the second node we have



Using the above techniques we can shape a Gaussian cluster in order to put it into the required topology to perform a specific algorithm. For example, below we can create the graph state on the right by first performing a sequence of quadrature measurements on an initial 4×5 cluster given on the left



(173)

Recently, an experimental demonstration of continuous-variable cluster state shaping was performed using a four-mode linear cluster using homodyne detection and feedforward (Miwa, *et al.*, 2010).

D. Gaussian errors from finite squeezing

In the next section, we will look at ways in which Gaussian cluster states can be implemented optically. As soon as we start discussing practical implementations we have to consider using finitely squeezed Gaussian states in our analysis which inevitably introduces errors into our computations. To illustrate the effect of finite squeezing we show what happens to the propagation of quantum information in a simple teleportation protocol. We now go back to the teleportation circuits from Sec. VII.B.1 where we showed the effect of teleporting,

first a qumode and then a gate diagonal in the computational basis, from one quantum wire to another. In that particular scenario, the nodes of the cluster were momentum eigenstates. In the calculations that follow they will be replaced by Gaussian squeezed states, i.e., $|0\rangle_p \longrightarrow |0, V_S\rangle_p$ where $V_S < 1$ is the variance of the input squeezing. Suppose we initially start off with the two input states $|\psi\rangle$ and $|0, V_S\rangle_p$ where both can again be expanded in terms of arbitrary position bases, i.e., $|\psi\rangle = \int dq_1 \psi(q_1) |q_1\rangle$ and

$$|0, V_S\rangle_p = (\pi V_S)^{-1/4} \int dq_2 \; e^{-q_2^2/2V_S} |q_2\rangle \,, \tag{174}$$

Applying the CPHASE gate to these two states gives

$$(\pi V_S)^{-1/4} \int dq_1 dq_2 \psi(q_1) e^{-q_2^2/2V_S} e^{iq_1 q_2/2} |q_1\rangle |q_2\rangle \,. \tag{175}$$

After performing a measurement on the first mode in the momentum basis we end up with: $|\psi'\rangle = \mathcal{M}X(m_1)F|\psi\rangle$, where $\mathcal{M}$ is a Gaussian distortion (Menicucci *et al.*, 2006)

$$\mathcal{M}|\psi\rangle \propto \int dq \; e^{q^2 V_S/2} |q\rangle \langle q|\psi\rangle. \tag{176}$$

So effectively what we have is a Gaussian distortion, with zero mean and variance $1/V_S$, applied to the original input state as a result of propagating through a cluster created using finite squeezing (equivalently, this can be thought of as a convolution in momentum space by a Gaussian of variance V_S). The same reasoning holds when we consider the gate teleportation situation where the output is given by $\mathcal{M}X(m_1)FU|\psi\rangle$. We note that the above distortions due to finite squeezing errors of both state propagation and universal gate teleportation have also been analyzed by Gu *et al.* (2009) from the point of view of the Wigner representation.

E. Optical implementations of Gaussian cluster states

Here we look at the various methods to optically implement continuous-variable cluster states using Gaussian elements. The advantage of the continuous-variable optical approach, compared to the discrete-variable approach, is that the generation of continuous-variable cluster states is completely deterministic. Furthermore, once the cluster is setup only homodyne detection is needed to implement any multimode Gaussian transformation (Ukai, Yoshikawa, *et al.*, 2010). However, the errors introduced into the computations, due to the finitely squeezed resources, are a downside to this unconditionality. The five methods for cluster state production are outlined below.

1. Canonical method

The canonical method was first introduced in 2006 (Menicucci *et al.*, 2006; Zhang and Braunstein, 2006) and proposed a literal interpretation of how to implement an optical Gaussian cluster state. By that we mean each mode is first prepared as a momentum squeezed vacuum state and then an appropriate number of C_Z gates are applied to create the required cluster. The C_Z gate is optically implemented using two beam splitters and two online[7] squeezers (Walls and Milburn, 2008; Yurke, 1985). One of the advantages of this method is that the C_Z gates commute with one another (i.e., the order in which they are applied does not matter) and thus facilitates theoretical analysis. On the other hand, the implementation of the C_Z gate is experimentally challenging (Ukai *et al.*, 2011) due to the difficulty of online squeezing (La Porta *et al.*, 1989; Yoshikawa *et al.*, 2007; Yurke, 1985) and therefore is not very efficient as C_Z gates are needed for every link in the cluster. Note that the demonstration of another type of quantum non-demolition (QND) gate (the SUM gate) has also been achieved (Yoshikawa *et al.*, 2008).

2. Linear-optics method

The linear-optics method was conceived by van Loock (van Loock *et al.*, 2007) and provided a way of greatly simplifying the optical implementation of the canonical method. Put simply, the linear-optics method allows the creation of a cluster state using only offline squeezed states and a beam splitter network. Experimentally this represented an important advancement in the building of continuous-variable cluster states as the difficult part of online squeezing was now moved offline (Gu *et al.*, 2009). In this work (van Loock *et al.*, 2007) two algorithms were developed using squeezed vacuum states and linear optics to create two varieties of cluster states: (1) canonical Gaussian cluster states and (2) generalized cluster-type states. The first algorithm, known as the decompositional algorithm, used the Bloch-Messiah reduction (cf. Sec. II.C.2) to show that the canonical method can be decomposed into offline squeezed states and beam splitters to create the original canonical cluster. The second algorithm (this time independent of the Bloch-Messiah reduction) showed how to create a more general class of Gaussian cluster states, known as cluster-type states (from which the canonical cluster states are a special case). This was shown by requiring that the final cluster state (again created from squeeze vacuum states and carefully configured passive linear optics) satisfies the nullifier relation of Eq. (172) in the limit of infinite squeezing. However, when the finite squeezing case is also considered a larger family of non-canonical cluster states are created.

One of the benefits of the second algorithm is that the antisqueezing components are suppressed thus making it experimentally more appealing (Yukawa *et al.*, 2008). Also smaller levels of input squeezing are required to create cluster-

[7] An online squeezer (also known as inline squeezer) is the squeezing of an arbitrary, possibly unknown, state. An offline squeezer is the squeezing of a known state, typically the vacuum.

type states compared to using the canonical method to create canonical states with the same kind of correlations. A number of experiments using the linear-optics method have been demonstrated from setting up an initial four-mode Gaussian cluster (Su *et al.*, 2007; Yukawa *et al.*, 2008) (including linear, T-shape and square clusters (Yukawa *et al.*, 2008)) to simple continuous-variable one-way quantum computations on a four-mode linear cluster (Miwa, *et al.*, 2010; Ukai, Iwata, *et al.*, 2011).

3. Single-OPO method

The single-OPO-method (Flammia *et al.*, 2009; Menicucci *et al.*, 2008, 2007) was developed around the same time as the linear-optics method and shows how to create an ultra-compact and scalable, universal N-mode cluster state using only a single optical parametric oscillator[8](OPO). Effectively this means that the cluster state can be created in just a single step using a top-down approach and requires the same amount of resources as the linear-optics method (i.e., $\mathcal{O}(N^2)$). However, unlike the linear-optics method it does not require an interferometer which can be cumbersome for large N thus removing the beam splitter network altogether. It therefore holds great promise of scalability for universal continuous-variable cluster states.

The initial proposal (Menicucci *et al.*, 2007) showed that, by using an appropriately constructed multi-frequency pump beam, the single OPO could generate any continuous-variable cluster state with a bipartite graph. Mathematically this result relied on showing a connection between continuous-variable cluster states and Hamiltonian graphs or $\mathcal{H}$-graphs for short (Flammia *et al.*, 2009; Flammia and Severini, 2009; Menicucci *et al.*, 2008, 2007; Zaidi *et al.*, 2008). These $\mathcal{H}$-graphs correspond to those states produced by an OPO. With this result we have effectively gone from requiring N single-mode squeezers (OPOs) to a single multimode OPO which is pumped by an $\mathcal{O}(N^2)$-mode beam. Further progress showed (Flammia *et al.*, 2009; Menicucci *et al.*, 2008) that this method can in fact produce a whole family of universal continuous-variable cluster states where the encoding scheme of the single-OPO involves using the optical frequency comb. Here each independent qumode corresponds to a different frequency in the optical frequency comb (which derives its name from the equal spacings between each qumode). The main advantage of this method is that the number of pump frequencies is not $\mathcal{O}(N^2)$ but in fact constant. Recently, the first experimental demonstration of cluster state generation in the optical frequency was performed (Pysher, 2011). Here 15 quadripartite cluster states were created over 60 cavity qumodes, exhibiting its potential for scalable quantum computation.

[8] A simple OPO consists of an optical cavity (e.g., two facing mirrors) with a crystal inside. Typically this crystal is nonlinear (e.g., second-order $\chi^{(2)}$) and is pumped by a laser beam which can lead to the down-conversion or the up-conversion of the initial frequencies.

4. Single-QND-gate method

In the four years since the canonical method, and its reliance on C_Z gates, all of the previous methods have purposely shied away from using this non-demolition gate due to its difficulty in being experimentally implemented (Ukai *et al.*, 2011). However, in a novel approach (Menicucci *et al.*, 2010), the C_Z gate once again makes an appearance in a compact scheme devised to generate arbitrarily large cluster states. In the canonical method, $O(N^2)$ low-noise C_Z gates are needed to set up the initial N-mode cluster. However, in this new approach, all that is required is a single C_Z gate. In fact, for universal quantum computation, only a single copy of the following key optical ingredients are needed: a single-mode vacuum squeezer, a C_Z gate, a homodyne detector and a photon counter. The basic premise of the single-QND-gate method involves building the cluster on the go where the cluster is extended and measured as needed, according to the particular algorithm to be executed.

The specific design of this method can be understood from considering a simple linear cluster. In this case momentum squeezed vacuum states are generated at regular intervals and repeatedly fed into a single C_Z gate. One output of the gate is directed towards a detector while the other is fed back into the C_Z gate. Because in general all qumodes travel the same optical path, but importantly at different times, the encoding scheme of the qumodes is temporal. This process of creating and measuring is repeated over and over during the duration of the algorithm and can be extended in much the same way to create universal cluster states. One advantage that the single-QND-gate method offers over the previous approaches is that maintaining the coherence of a large cluster becomes less of an issue. This is because we are only concerned with the coherence of a small instance of the cluster at any one time.

5. Temporal-mode-linear-optics method

The latest approach was developed by Menicucci (2011) and combines the essential features and benefits of the previous three methods into one. This method, known as the temporal-mode-linear optics method, offers an improvement over the single-QND-gate approach in that it uses the techniques from the linear-optics scheme to move the experimentally challenging online squeezing, offline. This new temporal-mode encoding, where again the input squeezed vacuum states are repeatedly sent through the same optical hardware but at different times, still maintains the finite coherence and scalability features of the previous model. This implementation is achieved by recognizing that the output states of the single-OPO method are in fact Gaussian projected entangled pair states (Ohliger *et al.*, 2010). Gaussian projected entangled pair states are pairs of Gaussian two-mode squeezed states that are locally projected down to a lower-dimensional subspace. For example, in the cluster state formalism, this corresponds to having two two-node graph states where a measurement projects the ends of both nodes down

to a single node and in doing so creates a linear three-node graph (Ohliger *et al.*, 2010). The graphical formalism developed by Menicucci *et al.* (2011) is used to describe and formulate this Gaussian projected entangled pair states construction and can be optically implemented using single-mode offline squeezers and linear optics.

F. Universal quantum computation

As previously noted, the Lloyd-Braunstein criterion tells us that in order to achieve universal quantum computation, i.e., the ability to generate an arbitrary Hamiltonian, we need the addition of a non-Gaussian element, such as a non-Gaussian operation or a non-Gaussian state, to our tool box. In continuous-variable cluster state quantum computation the cubic phase gate and the cubic phase state, respectively, are examples of such elements. The cubic phase gate is defined as

$$V = \exp(i\gamma\hat{q}^3), \tag{177}$$

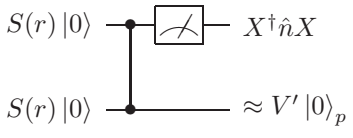
where $\gamma \in \mathbb{R}$. The action of the cubic phase gate on a zero momentum eigenstate $|0\rangle_p$ creates what is known as the cubic phase state $|\gamma\rangle$ which is an unnormalizable non-Gaussian state

$$|\gamma\rangle = V\,|0\rangle_p = \frac{1}{2\sqrt{\pi}} \int dq\; e^{i\gamma q^3}\,|q\rangle\,. \tag{178}$$

Ultimately the cubic phase state will be used as a resource to implement the cubic phase gate onto an arbitrary state in the cluster. We begin by first showing how to create such a state and then explore two methods of implementing the cubic phase gate.

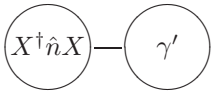
1. Creating the cubic phase state

It was shown by Gottesman *et al.* (2001) that the cubic phase state could be created by implementing the following quantum circuit (Gu *et al.*, 2009)



(179)

where $V' = \exp(i\gamma'(n)\hat{q}^3)$ and the strength of the gate depends on the probabilistic measurement result: $\gamma'(n) = (6\sqrt{2n+1})^{-1}$. Therefore the above circuit corresponds to a simple two-mode graph state with a displaced photon counting measurement on the first node



(180)

Notice that the output state above is not quite in the form we would like, i.e., it is γ' and not γ. To correct this note that V' can be decomposed into two squeeze gates and the cubic phase gate (Gottesman *et al.*, 2001), i.e.,

$$V' = S(f)VS^\dagger(f), \tag{181}$$

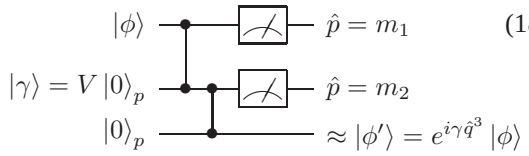
where $f := f(n) = [\gamma/\gamma'(n)]^{1/3}$. Once these squeezing corrections are implemented the cubic phase state can be synthesized.

2. Implementing the cubic phase gate

Now that we have a way of creating the cubic phase state we look at two possible approaches to inducing the action of the cubic phase gate onto an arbitrary state using the cubic phase state as a resource. The first approach deviates from the typical measurement-based scheme by performing Gaussian measurements on a non-Gaussian cluster state. The second approach revisits the typical setup of a Gaussian cluster but requires that the measurement tool box now consists of both Gaussian and non-Gaussian measurements.

a. Non-Gaussian cluster and Gaussian measurements

In the standard cluster-state model of computation all nodes are initialized as zero momentum eigenstates before becoming entangled via the CPHASE gate. However, one way to implement the cubic phase gate is to first embed the cubic phase state into the original cluster. In the regime of finite squeezing the initial Gaussian cluster state now becomes non-Gaussian. A computation is performed as before using only Gaussian (homodyne) measurements. Once the cubic phase state $|\gamma\rangle$ is part of the initial cluster a variation of gate teleportation can be used to teleport V onto an arbitrary state $|\phi\rangle$ of the cluster (where for instance $|\phi\rangle$ is the state of a node in the cluster at a particular point in time). The following circuit achieves this (Gu *et al.*, 2009)



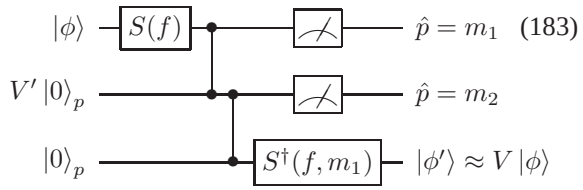
(182)

modulo known Gaussian corrections (Weedbrook, 2009) (hence the $\approx$). In the graph state formalism the above circuit is depicted as

Note that the above graph corresponds to a subgraph of a much larger cluster. One way to think about what is happening is that we have the cubic phase gate V acting on a zero momentum eigenstate on the second node and by performing momentum quadrature measurements on the first and second nodes we are effectively teleporting V onto $|\phi\rangle$ (modulo corrections) with the resulting state appearing at the third node. The beauty of using a non-Gaussian cluster from the beginning is that once it is created only quadrature measurements are needed to perform any algorithm. However, creating such an improved resource is experimentally challenging.

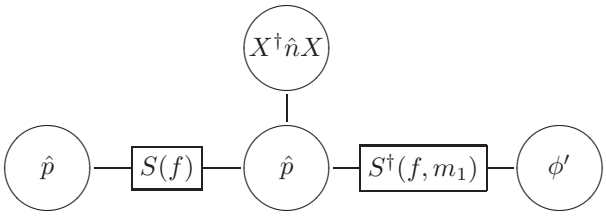
b. Gaussian cluster and non-Gaussian measurements

Now the previous approach is tailored to creating the cubic phase state offline, i.e., as one of the initial resource states prior to the entangling gate. However, if we wanted to emulate the original cluster state formalism by beginning with a universal Gaussian cluster, our set of measurements would need to be both Gaussian and non-Gaussian (e.g., photon counting). One consequence of this is the need to perform the squeezing corrections of Eq. (181) online. With this in mind circuit (182) now becomes



(183)

where the second squeezing correction is dependent on the first measurement result m_1 because it is itself dependent on the photon counting result n (Weedbrook, 2009). Translating the above circuit into the graph state formalism and using graph (180) gives the following



where the input state $|\phi\rangle$ is the first node from the left. Here the square boxes represent subgraphs through which the squeezing corrections, $S(f)$ and $S^\dagger(f, m_1)$, are implemented via homodyne measurements (van Loock, 2007). Another consequence of the non-Gaussian measurement is that the concept of parallelism is not longer valid as the center top node needs to be measured first due to the probabilistic nature of the measurement outcome. After which the amount of squeezing required on the first node is dependent on the result n. Hence the time ordering of measurements now matters and adaptiveness plays a role (depending on the specific algorithm performed, the value of γ might also depend on previous measurement results as well). From the above graph one can notice that ideally the top center node is only attached to the node below it. This is where the shaping tools from Sec. VII.C.3 play a part. For example, if there is a point in the computation on the Gaussian cluster where the cubic phase state needs to be created then removing or deleting nodes from the cluster would allow one to have it in the required form.

G. Quantum error correction

To argue that a particular physical system is capable of universal quantum computation it is not sufficient to show that the system in question can implement arbitrary unitary evolutions. In any physical implementation there will be imperfections in the system that will inevitably lead to random errors being introduced. Even if these errors are small, when large scale quantum processing is considered, we have to worry about their propagation during gate operations. If uncorrected, such errors will grow uncontrollably and make the computation useless. The answer to this problem is fault tolerant error correction (Shor, 1995; Steane, 1996). Thus to make a necessary and sufficient argument that a particular physical system is capable of continuous-variable quantum computation, strictly one must also show that fault tolerant error correction is possible.

The idea of error correction is self-explanatory, though the description of its application to quantum systems requires some care. Classically we might consider using a redundancy code such that, for example, $0 \to 000$ and $1 \to 111$. If a bit flip occurs on one of the bits we might end up with 010 or 101 but we can recover the original bit value by taking a majority vote. An example of a quantum redundant encoding for qubits is $\alpha|0\rangle + \beta|1\rangle \to \alpha|000\rangle + \beta|111\rangle$ where we have created an entangled state rather than copies. It is then possible to identify an error without collapsing the superposition, by reading out the parity of pairs of qubits. For example a bit-flip error might result in the state $\alpha|001\rangle + \beta|110\rangle$. The parity of the first two qubits will be zero whilst the parity of the second two qubits will be one, thus unambiguously identifying that an error has occurred on the last qubit. Because we are measuring the parity, not the qubit value, the superposition is not collapsed. Such codes can be expanded to cope with the possibility of more than one error occurring between correction attempts and to cope with multiple types of errors. Of course the gates being used to detect and correct the errors may themselves be faulty. An error correction code is said to be fault tolerant if error propagation can be prevented even if the components used to do the error correction introduce errors themselves. Typically this is only possible if the error rate per operation is below some level known as the fault tolerant threshold.

The first error correction protocol for continuous variables (Braunstein, 1998a; Lloyd and Slotine, 1998) was developed as a direct generalization of the qubit redundancy codes (Shor, 1995). In Braunstein's simplified version (Braunstein, 1998b), eight ancilla squeezed states are mixed on beam splitters with the signal state to create a nine-mode encoded state. Decoding is similarly achieved with beam splitters, with homodyne detection on eight of the modes providing information about errors on the remaining signal mode. This protocol has recently been demonstrated experimentally (Aoki *et al.*, 2009). On any particular run the code can correct any error that occurs on any single mode of the encoded state (Walker and Braunstein, 2010). This was shown to extend to multiple errors provided they occur in a stochastic way (van Loock, 2008). Unfortunately, error models of this kind are non-Gaussian error models and do not correspond to the Gaussian errors that typically occur in experiments due to loss and thermal noise. Other protocols for correcting more specific types of non-Gaussian noise imposed on Gaussian states have been proposed and experimentally demonstrated (Lassen *et al.*, 2010; Niset *et al.*, 2008). It has been proven that error correction of Gaussian noise, imposed

on Gaussian states, using only Gaussian operations is impossible (Niset *et al.*, 2009).

This no-go theorem does not apply if the initial states are non-Gaussian. An example of such a protocol is that developed by Gottesman *et al.* (2001). Here, the information is discretized by encoding qubit states as non-Gaussian continuous-variable states. Such states could be generated in optical modes by means of cross-Kerr interactions (Pirandola *et al.*, 2004). Error correction against Gaussian errors can then be achieved using Gaussian operations. This protocol is known to be fault tolerant, although the threshold requirements are quite extreme (Glancy and Knill, 2006). A simpler encoding of qubits into continuous-variable states is the coherent state encoding (Ralph *et al.*, 2003). Fault tolerant error correction against Gaussian errors can also be achieved with this system, with a better threshold behavior (Lund *et al.*, 2008). The price paid for this improvement though, is that non-Gaussian operations are also required.

A third possibility that is not explicitly forbidden by the no-go theorem is to error correct Gaussian states against Gaussian noise using non-Gaussian operations, that none-the-less result in a Gaussian output state. Such protocols have been proposed (Browne *et al.*, 2003) and demonstrated (Xiang *et al.*, 2010) for continuous-variable entanglement distillation. Entanglement distillation (Bennett, Brassard, *et al.*, 1996) is a non-deterministic error detection protocol, useful for extending the reach of quantum communication systems. Continuous-variable protocols have also been developed to distill entanglement against non-Gaussian noise (Dong *et al.*, 2008; Hage *et al.*, 2008) and for non-Gaussian states against Gaussian noise (Ourjoumtsev *et al.*, 2009). In principle, continuous-variable teleportation and continuous-variable distillation protocols based on noiseless amplification can be combined to error correct Gaussian states against Gaussian noise (Ralph, 2011). However, it is not currently known if such protocols can be made fault tolerant.

Error correction cannot be directly introduced into the continuous-variable cluster state model by simply simulating a circuit model error correction protocol with the cluster (Cable and Browne, 2010; Ohliger *et al.*, 2010). This is a generalization of the result of Nielsen and Dawson (2005) that similarly restricts error correction for discrete-variable cluster states. These authors showed that error correction could only be incorporated into the cluster state computation model provided the construction and measurement of the cluster occurred concurrently, and the off-line, non-deterministic production of special states was allowed. In continuous-variable cluster state computation, without fully-fletched continuous-variable fault tolerance, continuous-variable cluster states based on any finite squeezing are strictly speaking not resources for continuous-variable cluster state quantum computing (Ohliger *et al.*, 2010). However, it has been argued that in principle, combining the techniques of Nielsen and Dawson (2005) with the oscillator encoding scheme of Gottesman *et al.* (2001) would allow fault tolerant continuous-variable cluster state computation to be carried out (Gu *et al.*, 2009), though this has not been shown explicitly.

H. Continuous-variable algorithms

Finally, before discussing future directions, we briefly mention two algorithms that have been developed for a continuous-variable quantum computer: Grover's search algorithm (Grover, 1997) and the Deutsch-Jozsa algorithm (Deutsch and Jozsa, 1992). These algorithms were originally developed for discrete-variable systems (Nielsen and Chuang, 2000) and later analogs were found for continuous-variable systems in terms of the quantum circuit model formalism. Grover's search algorithm using continuous variables was presented by Pati *et al.* (2000) and showed that a square-root speed-up in searching an unsorted database could be achieved in analogy with the qubit case. A continuous-variable version of one of the earliest quantum algorithms, the Deutsch-Jozsa algorithm, was first developed by Pati and Braunstein (2003). Here the goal of determining whether a function is constant or balanced was constructed in the ideal case of perfectly squeezed qumodes. Later, this algorithm was analyzed in more detail by Adcock *et al.* (2009) and reformulated using Gaussian states by Zwierz *et al.* (2010).

I. Future directions

Research interest in the field of continuous-variable quantum computation has increased significantly in the last few years. This is particularly true in the case of cluster state quantum computation. Therefore it is worth making a brief comparison between the continuous-variable cluster states discussed here and the discrete-variable approach based on single-photon qubits and linear optics techniques (Knill *et al.*, 2001; Nielsen, 2004). The key trade-off is between construction of the cluster and its measurements. In the continuous-variable approach construction is deterministic, whilst in the single-photon approach it is non-deterministic and requires a very large overhead in terms of photon sources and memory in order to make it near deterministic. On the other hand, all required measurements are trivial in the single-photon approach, whilst non-Gaussian measurements pose a major challenge in the continuous-variable approach. At this point it is difficult to say which of these problems represents the biggest impediment to building a large scale system.

There are a number of important avenues for future research in continuous-variable quantum computation. Perhaps the most important at this stage is the development of continuous-variable fault tolerance for cluster state quantum computation. Another avenue would be to incorporate continuous-variable quantum algorithms, such as Grover's algorithm and the Deutsch-Jozsa algorithm, into the cluster state model. Additionally, the development of further algorithms for a continuous-variable quantum computer, e.g., an optical version of Shor's factoring algorithm (Shor, 1997), would also be interesting, especially for future experimental demonstrations.

VIII. CONCLUSION AND PERSPECTIVES

This review examined the power of continuous-variable quantum information from a Gaussian perspective. The processing of Gaussian quantum information involves the use of any combination of Gaussian states, Gaussian operations, and Gaussian measurements. The ability to characterize Gaussian states and operations via their first and second-order statistical moments offers a major simplification in the mathematical analysis of quantum information protocols. Over the last decade, optical and atomic Gaussian states and operations have being recognized as key resources for quantum information processing. For example, continuous-variable quantum teleportation only requires Gaussian entanglement and Gaussian operations, while it can be used to teleport arbitrary, even highly non-Gaussian, quantum states. Similarly, continuous-variable quantum key distribution works with coherent states, while it achieves the unconditional security once believed to reside only with highly non-classical resources. Yet another unexpected property is that a Gaussian cluster state is provably a universal resource for quantum computation. All of these findings have put forward the idea that Gaussian protocols deserve a front row position in quantum information science.

Beyond a comprehensive description of Gaussian quantum information protocols, this review also examined bounds on the distinguishability of Gaussian states, and features of Gaussian bosonic quantum communication channels such as their capacity and statistical discrimination. Future directions in quantum information sciences include the exploration of more complex scenarios of quantum communication, involving different protocols such as quantum cloning or teleportation networks. In this context, the Gaussian approach is particularly promising, allowing us to explore these future directions with powerful mathematical tools and standard optical components.

From a purely Gaussian perspective, i.e., when one is restricted to using states, operations and measurements that are all Gaussian, certain protocols are not possible. For example, universal quantum computation, entanglement distillation, and error correction all require that the protocol be supplemented with either a non-Gaussian state, operation, or measurement. For some tasks, hybrid systems, which combine elements from continuous and discrete-variable quantum information processing, are then favored as they may outperform purely discrete-variable systems. Interestingly, the powerful mathematical tools of Gaussian analysis can sometimes be used even when non-Gaussian processing or non-Gaussian states are involved. For example, in certain quantum key distribution protocols, even if Alice and Bob use non-Gaussian distributions or Eve makes a non-Gaussian attack, the security can be ensured by considering the worst case of a Gaussian attack against a Gaussian protocol. Such an analysis would still hold if quantum repeaters based on non-Gaussian processing were used by Alice and Bob. Similarly, universal quantum computation achieved by a Gaussian cluster state and non-Gaussian detection is an example of the power brought by the application of Gaussian analysis tools to hybrid quantum systems.

In conclusion, we anticipate that Gaussian quantum information will play a key role in future developments of quantum information sciences, both theoretical and experimental. This is due to the simplicity and versatility of the involved protocols as well as the availability of the required technologies. We hope that this review will help encourage these developments.

Acknowledgments

We would like to thank Sam Braunstein, Jens Eisert, Chris Fuchs, Saikat Guha, Alexander Holevo, Anthony Leverrier, Stefano Mancini, Christoph Marquardt, Nick Menicucci, Matteo Paris, Eugene Polzik, Joachim Schäfer, Denis Sych, Graeme Smith, David Vitali, Nathan Walk, Mark Wilde, Howard Wiseman, and Jing Zhang for providing valuable feedback on the manuscript. C. W. would also like to thank Hoi-Kwong Lo and Shakti Sivakumar. C. W. acknowledges support from the Ontario postdoctoral fellowship program, CQIQC postdoctoral fellowship program, CIFAR, Canada Research Chair program, NSERC, QuantumWorks and the W. M. Keck Foundation. S. P. acknowledges support from the W. M. Keck Foundation and the European Community (Marie Curie Action). R. G. P acknowledges support from the W. M. Keck Foundation and the Alexander von Humboldt foundation. N. J. C acknowledges support of the Future and Emerging Technologies programme of the European Commission under the FP7 FET-Open grant no. 212008 (COMPAS) and by the Interuniversity Attraction Poles program of the Belgian Science Policy Office under grant IAP P6-10 (photonics@be). T. C. R acknowledges support from the Australian Research Council. J. H. S acknowledges support from the W. M. Keck Foundation, the ONR, and DARPA. S. L. acknowledges the support of NSF, DARPA, NEC, Lockheed Martin, and ENI via the MIT energy initiative.

References

Acín, A., 2001, Phys. Rev. Lett. **87**, 177901.
Adcock, M. R. A, P. Høyer, and B. C. Sanders, 2009, New J. Phys. **11**, 103035.
Adesso, G., and A. Datta, 2010, Phys. Rev. Lett. **105**, 030501.
Adesso, G., and F. Illuminati, 2005, Phys. Rev. Lett. **95**, 150503.
Adesso, G., and F. Illuminati, 2007, J. Phys. A: Math. Theor. **40**, 7821.
Adesso, G., A. Serafini, and F. Illuminati, 2004, Phys. Rev. A **70**, 022318.
Aoki, T., G. Takahashi, T. Kajiya, J. Yoshikawa, S. L. Braunstein, P. van Loock, and A. Furusawa, 2009, Nature Physics **5**, 541.
Aolita, L., A. J. Roncaglia, A. Ferraro, and A.Acín, 2011, Phys. Rev. Lett. **106**, 090501.
Andersen, U. L., V. Josse, and G. Leuchs, 2005, Phys. Rev. Lett. **94**, 240503.
Andersen, U. L., G. Leuchs, C. Silberhorn, 2010, Laser & Photonics Reviews **4**, 337.
Arthurs, E., and J. L. Kelly, Jr., 1965, Bell Syst. Tech. J. **44**, 725.

Arvind, B. Dutta, N. Mukunda, and R. Simon, 1995, Pramana J. Phys. **45**, 471.

Audenaert, K. M. R., J. Calsamiglia, L. Masanes, R. Munoz-Tapia, A. Acín, E. Bagan, and F. Verstraete, 2007, Phys. Rev. Lett. **98**, 160501.

Audenaert, K. M. R., M. Nussbaum, A. Szkola, and F. Verstraete, 2008, Commun. Math. Phys. **279**, 251.

Bachor, H. -A., and T. C. Ralph, 2004, *A Guide to Experiments in Quantum Optics* (Wiley-VCH, Weinheim).

Ban, M., 1999, J. Opt. B: Quantum Semiclass. Opt. **1**, L9.

Barnes, R. L., 2004, "Stabilizer Codes for Continuous-variable Quantum Error Correction", arXiv:quant-ph/0405064.

Barnum, H., E. Knill, and M. A. Nielsen, 2000, IEEE Trans. Info. Theor. **46**, 1317.

Bartlett, S. D., and W. J. Munro, 2003, Phys. Rev. Lett. **90**, 117901.

Bartlett, S. D., B. C. Sanders, S. L. Braunstein, and K. Nemoto, 2002, Phys. Rev. Lett. **88**, 097904.

Bennett, C. H., H. J. Bernstein, S. Popescu, and B. Schumacher, 1996, Phys. Rev. A **53**, 2046.

Bennett, C. H., and G. Brassard, 1984, in *Proceedings of the IEEE International Conference on Computers, Systems and Signal Processing*, (Bangalore, India, (IEEE, New York)), 175.

Bennett, C. H., G. Brassard, C. Crepeau, R. Jozsa, A. Peres, and W. K. Wootters, 1993, Phys. Rev. Lett. **70**, 1895.

Bennett, C. H., G. Brassard, and N. D. Mermin, 1992, Phys. Rev. Lett. **68**, 557.

Bennett, C. H., G. Brassard, S. Popescu, B. Schumacher, J. A. Smolin, and W. K. Wootters, 1996, Phys. Rev. Lett. **76**, 722.

Bennett C. H., D. P. DiVincenzo, J. A. Smolin, and W. K. Wootters, 1996, Phys. Rev. A **54**, 3824.

Bennett, C. H., P. W. Shor, J. A. Smolin, and A. V. Thapliyal, 2002, IEEE Trans. Inf. Theor. **48**, 2637.

Bennett, C. H., and S. J. Wiesner, 1992, Phys. Rev. Lett. **69**, 2881.

Bergou, J., U. Herzog, and M. Hillery, 2004, in *Lecture Notes in Physics*, edited by M. Paris and J. Rehacek, (Springer, Berlin), **649**, 417.

Bisio A., M. Dall'Arno, and G. M. D'Ariano, 2011, Phys. Rev. A **84**, 012310.

Bondurant, R. S., 1993, Opt. Lett. **18**, 1896.

Boström, K., and T. Felbinger, 2002, Phys. Rev. Lett. **89**, 187902.

Boström, K., and T. Felbinger, 2008, Phys. Lett. A **372**, 3953.

Botero, A., and B. Reznik, 2003, Phys. Rev. A **67**, 052311.

Bowen, W. P., N. Treps, B. C. Buchler, R. Schnabel, T. C. Ralph, H. -A. Bachor, T. Symul, and P. K. Lam, 2003, Phys. Rev. A **67**, 032302.

Braunstein, S. L., 1990, Phys. Rev. A **42**, 474.

Braunstein, S. L., 1998a, Phys. Rev. Lett. **80**, 4084.

Braunstein, S. L., 1998b, Nature **394**, 47.

Braunstein, S. L., 2005, Phys. Rev. A **71**, 055801.

Braunstein, S. L., N. J. Cerf, S. Iblisdir, P. van Loock, and S. Massar, 2001, Phys. Rev. Lett. **86**, 4938.

Braunstein, S. L., and D. D. Crouch, 1991, Phys. Rev. A **43**, 330.

Braunstein, S. L, C. A. Fuchs, and H. J. Kimble, 2000, J. Mod. Opt. **47**, 267.

Braunstein, S. L, C. A. Fuchs, H. J. Kimble, and P. van Loock, 2001, Phys. Rev. A **64**, 022321.

Braunstein, S. L., and H. J. Kimble, 1998, Phys. Rev. Lett. **80**, 869.

Braunstein, S. L., and H. J. Kimble, 1999, Phys. Rev. A **61**, 042302.

Braunstein, S. L., and A. K. Pati, 2003, *Quantum information with continuous variables* (Kluwer Academic, Dordrecht).

Braunstein, S. L., and P. van Loock, 2005, Rev. Mod. Phys. **77**, 513.

Bravyi, S., 2005, Quantum Inf. and Comp. **5**, 216.

Browne, D. E., J. Eisert, S. Scheel, and M. B. Plenio, 2003, Phys. Rev. A **67**, 062320.

Buono, D., G. Nocerino, V. D'Auria, A. Porzio, S. Olivares, and M. G. A. Paris, 2010, J. Opt. Soc. Am. B **27**, A110.

Bužek, V., and M. Hillery, 1996, Phys. Rev. A **54**, 1844.

Cable, H., and D. E. Browne, 2010, New J. Phys. **12**, 113046.

Cai, R. Y. Q., and V. Scarani, 2009, New J. Phys. **11**, 045024.

Calsamiglia, J., R. Munoz-Tapia, L. Masanes, A. Acín, and E. Bagan, 2008, Phys. Rev. A **77**, 032311.

Caruso, F., V. Giovannetti, and A. S. Holevo, 2006, New Journal of Physics **8**, 310.

Caruso, F., and V. Giovannetti, 2006, Phys. Rev. A **74**, 062307.

Caruso, F., J. Eisert, V. Giovannetti, and A. S. Holevo, 2008, New J. Phys. **10**, 083030.

Caruso, F., J. Eisert, V. Giovannetti, and A. S. Holevo, 2011, Phys. Rev. A **84**, 022306.

Caves, C. M., and P. D. Drummond, 1994, Rev. Mod. Phys. **66**, 481.

Cerf, N. J., 2003, in *Quantum Information with Continuous Variables*, edited by S. L. Braunstein and A. K. Pati, (Kluwer Academic, Dordrecht), 277-293.

Cerf, N. J., and J. Fiurà̌šek, 2006, in *Progress in Optics*, edited by E. Wolf, (Elsevier, Amsterdam), 455-545.

Cerf, N. J., and P. Grangier, 2007, J. Opt. Soc. Am. B **24**, 324.

Cerf, N. J., and S. Iblisdir, 2000, Phys. Rev. A **62**, 040301(R).

Cerf, N. J., and S. Iblisdir, 2001a, Phys. Rev. Lett. **87**, 247903.

Cerf, N. J., and S. Iblisdir, 2001b, Phys. Rev. A **64**, 032307.

Cerf, N. J., S. Iblisdir and G. van. Assche, 2002, Eur. Phys. J. D **18**, 211.

Cerf, N. J., A. Ipe, and X. Rottenberg, 2000, Phys. Rev. Lett. **85**, 1754.

Cerf, N. J., O. Krüger, P. Navez, R. F. Werner, and M. M. Wolf, 2005, Phys. Rev. Lett. **95**, 070501.

Cerf, N. J., M. Levy, and G. van Assche, 2001, Phys. Rev. A **63**, 052311.

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

Chefles, A., 2000, Contemp. Phys. **41**, 401.

Chefles, A., and S. M. Barnett, 1998a, J. Mod. Opt. **45**, 1295.

Chefles, A., and S. M. Barnett, 1998b, Phys. Lett. A **250**, 223.

Chen, H., and J. Zhang, 2007, Phys. Rev. A **75**, 022306.

Childs, A., J. Preskill, and J. Renes, 2000, J. Mod. Opt. **47**, 155.

Chiribella, G., G. D'Ariano, and P. Perinotti, 2008, Phys. Rev. Lett. **101**, 180501.

Chizhov, A. V., L. Knöll, and D. G. Welsch, 2002, Phys. Rev. A **65**, 022310.

Christandl, M., R. König, and R. Renner, 2009, Phys. Rev. Lett. **102**, 020504.

Cochrane, P. T., T. C. Ralph, and A. Dolinska, 2004, Phys. Rev. A **69**, 042313.

Cook, R. L., P. J. Martin, and J. M. Geremia, 2007, Nature **446**, 774.

Cover, T. M., J. A. Thomas, 2006, *Elements of Information Theory* (Wiley, Hoboken).

D'Auria, V., S. Fornaro, A. Porzio, S. Solimeno, S. Olivares, and M. G. A. Paris, 2009, Phys. Rev. Lett. **102**, 020502.

Demoen, B., P. Vanheuverzwijn, and A. Verbeure, 1977, Lett. Math. Phys. **2**, 161.

Deutsch, D., and R. Jozsa, 1992, Proc. R. Soc. London A **439**, 553.

Devetak, I., 2005, IEEE Trans. Inf. Theory **51**, 44.

Devetak, I., and P. W. Shor, 2005, Commun. Math. Phys. **256**, 287.

Devetak, I., and A. Winter, 2004, Phys. Rev. Lett. **93**, 080501.

Dieks, D., 1982, Phys. Lett. **92A**, 271.

Di Vincenzo, D. P., P. W. Shor, and J. A. Smolin, 1998, Phys. Rev. A **57**, 830.

Di Vincenzo, D. P., and B. M. Terhal, 2005, Found. Phys. **35**, 1967.

Dolinar, S., 1973, Research Laboratory of Electronics, MIT, Quar-

terly Progress Report **111**, 115.
Dong, R., M. Lassen, J. Heersink, C. Marquardt, R. Filip, G. Leuchs, and U. L. Andersen, 2008, Nature Physics **4**, 919.
Duan, L. -M., G. Giedke, J. I. Cirac, and P. Zoller, 2000, Phys. Rev. Lett. **84**, 2722.
Duan, R., Y. Feng, and M. Ying, 2009, Phys. Rev. Lett. **103**, 210501.
Eisert, J., 2001, Ph.D. thesis (Potsdam).
Eisert, J., D. E. Browne, S. Scheel, and M. B. Plenio, 2004, Annals of Physics **311**, 431.
Eisert, J., M. Cramer, and M. B. Plenio, 2010, Rev. Mod. Phys. **82**, 277.
Eisert, J., and M. B. Plenio, 2003, Int. J. Quant. Inf. **1**, 479.
Eisert, J., S. Scheel, and M. B. Plenio, 2002, Phys. Rev. Lett. **89**, 137903.
Eisert, J., and M. M. Wolf, 2007, in *Quantum Information with Continuous Variables of Atoms and Light*, edited by E. Polzik, N. Cerf, and G. Leuchs, (Imperial College Press, London).
Enk, S. V., 2002, Phys. Rev. A **66**, 042313.
Fernholz, T., H. Krauter, K. Jensen, J. F. Sherson, A. S. Sorensen, and E. S. Polzik, 2008, Phys. Rev. Lett. **101**, 073601.
Ferraro, A., S. Olivares, and M. G. A. Paris, 2005, *Gaussian states in quantum information* (Biliopolis, Napoli).
Filip, R., 2008, Phys. Rev. A **77**, 022310.
Fiurà̌sek, J., 2001, Phys. Rev. Lett. **86**, 4942.
Fiurà̌sek, J., 2002a, Phys. Rev. Lett. **89**, 137904.
Fiurà̌sek, J., 2002b, Phys. Rev. A **66**, 012304.
Fiurà̌sek, J., 2003, Phys. Rev. A **67**, 012321.
Fiurà̌sek, J., and N. J. Cerf, 2007, Phys. Rev. A **75**, 052335.
Fiurà̌sek, J., N. J. Cerf, and E. S. Polzik, 2004, Phys. Rev. Lett. **93**, 180501.
Fiurà̌sek, J., L. Mišta, Jr., and R. Filip, 2003, Phys. Rev. A **67**, 022304.
Flammia, S. T., N. C. Menicucci, and O. Pfister, 2009, J. Phys. B **42**, 114009.
Flammia, S. T, and S. Severini, 2009, J. Phys. A **42**, 065302.
Fossier, S., E. Diamanti, T. Debuisschert, A. Villing, R. Tualle-Brouri, and P. Grangier, 2009, New J. Phys. **11**, 045023.
Fuchs, C. A., 2000, in *Quantum Communication, Computing, and Measurement*, edited by P. Kumar, G. M. D'Ariano, and O. Hirota, (Kluwer, Dordrecht), **649**, 11.
Fuchs, C. A., and J. V. de Graaf, 1999, IEEE Trans. Inf. Theory **45**, 1216.
Furusawa, A., J. L. Sørensen, S. L. Braunstein, C. A. Fuchs, H. J. Kimble, and E. S. Polzik, 1998, Science **282**, 706.
Furusawa, A., and P. van Loock, 2011, *Quantum Teleportation and Entanglement: A Hybrid Approach to Optical Quantum Information Processing* (Wiley-VCH, Weinheim).
Gabriel, C., C. Wittmann, D. Sych, R. Dong, W. Mauerer, U. L. Andersen, C. Marquardt, and G. Leuchs, 2010, Nature Photonics **4**, 711.
García-Patrón, R., 2007, Ph.D. thesis (Université Libre de Bruxelles).
García-Patrón, R., and N. J. Cerf, 2006, Phys. Rev. Lett. **97**, 190503.
García-Patrón, R., and N. J. Cerf, 2009, Phys. Rev. Lett. **102**, 130501.
García-Patrón, R., S. Pirandola, S. Lloyd, J. H. Shapiro, 2009, Phys. Rev. Lett. **102**, 210501.
Geremia, J. M., 2004, Phys. Rev. A **70**, 062303.
Gerry, C. C., and P. L. Knight, 2000, *Introductory Quantum Optics* (Cambridge University Press, Cambridge).
Giedke, G., and J. I. Cirac, 2002, Phys. Rev. A **66**, 032316.
Giedke, G., L. -M. Duan, J. I. Cirac, and P. Zoller, 2001, Int. J. Quant. Inf. **3**, 79.
Giedke, G., B. Kraus, M. Lewenstein, and J. I. Cirac, 2001, Phys. Rev. Lett. **87**, 167904.
Giedke, G., M. M. Wolf, O. Kruger, R. F. Werner, and J. I. Cirac, 2003, Phys. Rev. Lett. **91**, 107901.
Giorda, P., and M. G. A. Paris, 2010, Phys. Rev. Lett. **105**, 020503.
Giovannetti, V., S. Guha, S. Lloyd, L. Maccone, J. H. Shapiro, and H. P. Yuen, 2004a, Phys. Rev. Lett. **16**, 027902.
Giovannetti, V., S. Guha, S. Lloyd, L. Maccone, and J. H. Shapiro, 2004b, Phys. Rev. A **70**, 032315.
Giovannetti, V., and S. Lloyd, 2004, Phys. Rev. A **70**, 062307.
Giovannetti, V., S. Lloyd, L. Maccone, J. H. Shapiro, and B. J. Yen, 2004, Phys. Rev. A **70**, 022328.
Giovannetti, V., S. Lloyd, L. Maccone, and P. W. Shor, 2003, Phys. Rev. A **68**, 062323.
Gisin, N., S. Fasel, B. Kraus, H. Zbinden, and G. Ribordy, 2006, Phys. Rev. A **73**, 022320.
Gisin, N., G. Ribordy, W. Tittel, and H. Zbinden, 2002, Rev. Mod. Phys. **74**, 145.
Glancy, S., and E. Knill, 2006, Phys. Rev. A **73**, 012325.
Gottesman, D., 1997, Ph.D. thesis (California Institute of Technology).
Gottesman, D., 1998, "The Heisenberg Representation of Quantum Computers", arXiv:quant-ph/9807006v1.
Gottesman, D., A. Kitaev, and J. Preskill, 2001, Phys. Rev. A **64**, 012310.
Gottesman, D., and J. Preskill, 2001, Phys. Rev. A **63**, 022309.
Grosshans, F., and N. J. Cerf, 2004, Phys. Rev. Lett. **92**, 047905.
Grosshans, F., N. J. Cerf, J. Wenger, R. Tualle-Brouri, and P. Grangier, 2003, Quantum Inf. Comput. **3**, 535.
Grosshans, F., and P. Grangier, 2001, Phys. Rev. A **64**, 010301 (R).
Grosshans, F., and P. Grangier, 2002, Phys. Rev. Lett. **88**, 057902.
Grosshans, F., G. van Assche, J. Wenger, R. Tualle-Brouri, N. J. Cerf, and P. Grangier, 2003, Nature **421**, 238.
Grover, L. K., 1997, Phys. Rev. Lett. **79**, 325.
Gu, M., C. Weedbrook, N. C. Menicucci, T. C. Ralph, and P. van Loock, 2009, Phys. Rev. A **79**, 062318.
Guha, S., 2008, Ph.D. thesis (Massachusetts Institute of Technology, Cambridge).
Guha, S., and B. Erkmen, 2009, Phys. Rev. A **80**, 052310.
Hage, B., A. Samblowski, J. DiGuglielmo, A. Franzen, J. Fiurà̌sek, and R. Schnabel, 2008, Nature Physics **4**, 915.
Hall, M. J. W., 1994, Phys. Rev. A **50**, 3295.
Hammerer, K., M. M. Wolf, E. S. Polzik, and J. I. Cirac, 2005, Phys. Rev. Lett. **94**, 150503.
Hammerer, K., A. S. Sorensen, and E. S. Polzik, 2010, Rev. Mod. Phys. **82**, 1041.
Harrington, J., and J. Preskill, 2001, Phys. Rev. A **64**, 062301.
Harrow, A. W, A. Hassidim, D. W. Leung, and J. Watrous, 2010, Phys. Rev. A **81**, 032339.
Hastings, M. B., 2009, Nature Physics **5**, 255.
Hayashi, M., 2009, IEEE Trans. Inf. Theory **55**, 3807.
Heid, M., and N. Lütkenhaus, 2006, Phys. Rev. A **73**, 052316.
Heid, M., and N. Lütkenhaus, 2007, Phys. Rev. A **76**, 022313.
Helstrom, C. W., 1976, *Quantum Detection and Estimation Theory*, Mathematics in Science and Engineering, **123**, (Academic Press, New York).
Hillery, M., 2000, Phys. Rev. A **61**, 022309.
Hiroshima, T., 2006, Phys. Rev. A **73**, 012330.
Hirota, O., 2011, "Error free quantum reading by quasi bell state of entangled coherent states", arXiv:1108.4163.
Holevo, A. S., 1972, Probl. Inform. Transm. **8**, 63.
Holevo, A. S., 1973, Probl. Inform. Transm. **9**, 177.
Holevo, A. S., 1975, IEEE Trans. Inform. Theory **21**, 533.
Holevo, A. S., 1998, IEEE Trans. Inf. Theory **44**, 269.
Holevo, A. S., 2005, Theory of Probability and its Applications **50**, 86.

Holevo, A. S., 2007, Prob. of Inf. Transm. **43**, 1.

Holevo, A. S., 2011, *Probabilistic and Statistical Aspects of Quantum Theory* (Edizioni della Normale, Pisa).

Holevo, A. S., M. Sohma, and O. Hirota, 1999, Phys. Rev. A **59**, 1820.

Holevo, A. S., and R. F. Werner, 2001, Phys. Rev. A **63**, 032312.

Horn, R. A., and C. R. Johnson, 1985, *Matrix Analysis* (Cambridge University Press, Cambridge).

Horodecki, M., P. Horodecki, and R. Horodecki, 1996, Phys. Lett. A **223**, 1.

Horodecki, M., P. Horodecki, and R. Horodecki, 1998, Phys. Rev. Lett. **80**, 5239.

Horodecki, M., P. Horodecki, and R. Horodecki, 2000, Phys. Rev. Lett. **84**, 2014.

Horodecki, M., P. Horodecki, and R. Horodecki, 2009, Rev. Mod. Phys. **81**, 865.

Hudson, R. L., 1974, Rep. Math. Phys. **6**, 249.

Hughston, L. P., R. Jozsa, and W. K. Wootters, 1993, Phys. Lett. A **183**, 14.

Hyllus, P., and J. Eisert, 2006, New J. Phys. **8**, 51.

Ide, T., H. F. Hofmann, T. Kobayashi, and A. Furusawa, 2001, Phys. Rev. A **65**, 012313.

Invernizzi, C., M. G. A. Paris, and S. Pirandola, 2011, Phys. Rev. A **84**, 022334.

Jeong, H., and T. C. Ralph, 2007, in *Quantum Information with Continuous Variables of Atoms and Light*, edited by E. Polzik, N. Cerf, and G. Leuchs, (Imperial College Press, London).

Jia, X., X. Su, Q. Pan, J. Gao, C. Xie, and K. Peng, 2004, Phys. Rev. Lett. **93**, 250503.

Josse, V., M. Sabuncu, N. J. Cerf, G. Leuchs, and U. L. Andersen, 2006, Phys. Rev. Lett. **96**, 163602.

Jozsa, R., 1994, J. Mod. Opt. **41**, 2315.

Julsgaard, B., A. Kozhekin, and E. S. Polzik, 2001, Nature **413**, 400.

Kennedy, R. S., 1973, Research Laboratory of Electronics, MIT, Quarterly Progress Report **108**, 219.

Knill, E., R. Laflamme, and G. J. Milburn, 2001, Nature **409**, 46.

Kok, P., and B. Lovett, 2010, *Introduction to optical quantum information processing* (Cambridge University Press, Cambridge).

Lam, P. K., T. C. Ralph, E. H. Huntington, and H. -A. Bachor, 1997, Phys. Rev. Lett. **79**, 1471.

Lance, A. M., T. Symul, W. P. Bowen, B. C. Sanders, and P. K. Lam, 2004, Phys. Rev. Lett. **92**, 177903.

Lance, A. M., T. Symul, V. Sharma, C. Weedbrook, T. C. Ralph, and P. K. Lam, 2005, Phys. Rev. Lett. **95**, 180503.

La Porta, A., R. E. Slusher, and B. Yurke, 1989, Phys. Rev. Lett. **62**, 28.

Lassen, M., M. Sabuncu, A. Huck, J. Niset, G. Leuchs, N. J. Cerf, and U. L. Andersen, 2010, Nature Physics **4**, 700.

Leonhardt, U., 2010, *Essential Quantum Optics* (Cambridge University Press, Cambridge).

Leverrier, A., R. Alláume, J. Boutros, G. Zémor, and P. Grangier, 2008, Phys. Rev. A **77**, 042325.

Leverrier, A., and N. J. Cerf, 2009, Phys. Rev. A **80**, 010102.

Leverrier, A., and P. Grangier, 2009, Phys. Rev. Lett. **102**, 180504.

Leverrier, A., and P. Grangier, 2010a, Phys. Rev. A **81**, 062314.

Leverrier, A., and P. Grangier, 2010b, "Long distance quantum key distribution with continuous variables", arXiv:1005.0328.

Leverrier, A., and P. Grangier, 2010c, "Continuous-variable quantum key distribution protocols with a discrete modulation", arXiv:1002.4083.

Leverrier, A., F. Grosshans, and P. Grangier, 2010, Phys. Rev. A **81**, 062343.

Leverrier, A., E. Karpov, P. Grangier, and N. J. Cerf, 2009, New J. Phys. **11**, 115009.

Li, X., Q. Pan, J. Jing, J. Zhang, C. Xie, and K. Peng, 2002, Phys. Rev. Lett. **88**, 047904.

Lindblad G., 2000, J. Phys. A **33**, 5059.

Lita, A. E., A. J. Miller, and S. W. Nam, 2008, Optics Express **16**, 3032.

Lloyd, S., 1997, Phys. Rev. A **55**, 1613.

Lloyd, S., 2008, Science **321**, 1463.

Lloyd, S., and S. L. Braunstein, 1999, Phys. Rev. Lett. **82**, 1784.

Lloyd, S., V. Giovannetti, L. Maccone, N. J. Cerf, S. Guha, R. Garcia-Patron, S. Mitter, S. Pirandola, M. B. Ruskai, J. H. Shapiro, and H. Yuan, 2009, "The bosonic minimum output entropy conjecture and Lagrangian minimization", arXiv:0906.2758.

Lloyd, S., and J.-J. E. Slotine, 1998, Phys. Rev. Lett. **80**, 4088.

Lodewyck, J., M. Bloch, R. García-Patrón, S. Fossier, E. Karpov, E. Diamanti, T. Debuisschert, N. J. Cerf, R. Tualle-Brouri, S. W. McLaughlin, and P. Grangier, 2007, Phys. Rev. A **76**, 042305.

Lodewyck, J., T. Debuisschert, R. Tualle-Brouri, and P. Grangier, 2005, Phys. Rev. A **72**, 050303.

Lodewyck, J., T. Debuisschert, R. García-Patrón, R. Tualle- Brouri, N. J. Cerf, and P. Grangier, 2007, Phys. Rev. Lett. **98**, 030503.

Lodewyck, J., and P. Grangier, 2007, Phys. Rev. A **76**, 022332.

Lorenz, S., N. Korolkova, and G. Leuchs, 2004, Appl. Phys. B: Lasers Opt. **79**, 273.

Lorenz, S., J. Rigas, M. Heid, U. L. Andersen, N. Lütkenhaus, and G. Leuchs, 2006, Phys. Rev. A **74**, 042326.

Lund, A. P., T. C. Ralph, and H. L. Haselgrove, 2008, Phys. Rev. Lett. **100**, 030503.

Lupo, C., V. Giovannetti, S. Pirandola, S. Mancini, and S. Lloyd, 2011, Phys. Rev. A **84**, 010303 (R).

Lupo, C., S. Pirandola, P. Aniello, and S. Mancini, 2011, Phys. Scr. **T143**, 014016.

Lvovsky, A. I., and M. G. Raymer, 2009, Rev. Mod. Phys. **81**, 299.

Lvovsky, A. I., B. C. Sanders, and W. Tittel, 2009, Nature Photonics **3**, 706.

Magnin, L., F. Magniez, A. Leverrier, and N. J. Cerf, 2010, Phys. Rev. A **81**, 010302 (R).

Mancini, S., D. Vitali, and P. Tombesi, 2003, Phys. Rev. Lett. **90**, 137901.

Mandilara, A., and N. J. Cerf, 2011, "Quantum bit commitment under Gaussian constraints", arXiv:1105.2140v1.

Mandilara, A., E. Karpov, and N. J. Cerf, 2009, Phys. Rev. A **79**, 062302.

Mari, A., and D. Vitali, 2008, Phys. Rev. A **78**, 062340.

Mattle, K., H. Weinfurter, P. G. Kwiat, and A. Zeilinger, 1996, Phys. Rev. Lett. **76**, 4656.

Menezes, A., P. van Oorschot, S. Vanstone, 1997, *Handbook of Applied Cryptography* (CRC Press, Boca Raton).

Menicucci, N. C., 2011, Phys. Rev. A **83**, 062314.

Menicucci, N. C., S. T. Flammia, and O. Pfister, 2008, Phys. Rev. Lett. **101**, 130501.

Menicucci, N. C., S. T. Flammia, and P. van Loock, 2011, Phys. Rev. A **83**, 042335.

Menicucci, N. C., S. T. Flammia, H. Zaidi, and O. Pfister, 2007, Phys. Rev. A **76**, 010302(R).

Menicucci, N. C., X. Ma, and T. C. Ralph, 2010, Phys. Rev. Lett. **104**, 250503.

Menicucci, N. C., P. van Loock, M. Gu, C. Weedbrook, T. C. Ralph, and M. A. Nielsen, 2006, Phys. Rev. Lett. **97**, 110501.

Menzies, D., and N. Korolkova, 2007, Phys. Rev. A **76**, 062310.

Milburn, G. J., and S. L. Braunstein, 1999, Phys. Rev. A **60**, 937.

Miwa, Y., R. Ukai, J. Yoshikawa, R. Filip, P. van Loock, and A. Furusawa, 2010, Phys. Rev. A **82**, 032305.

Mizuno, J., K. Wakui, A. Furusawa, M. Sasaki, 2005, Phys. Rev. A **71**, 012304.

Nair, R., 2011, Phys. Rev. A **84**, 032312.

Namiki R., and T. Hirano, 2003, Phys. Rev. A **67**, 022308.

Namiki R., and T. Hirano, 2006, Phys. Rev. A **74**, 032302.

Navascués, M., and A. Acín, 2005, Phys. Rev. Lett. **94**, 020505.

Navascués, M., F. Grosshans, and A. Acín, 2006, Phys. Rev. Lett. **97**, 190502.

Nha, H., and H. J. Carmichael, 2005, Phys. Rev. A **71**, 032336.

Nielsen, M. A., 2004, Phys. Rev. Lett. **93**, 040503.

Nielsen, M. A., and I. L. Chuang, 2000, *Quantum Computation and Quantum Information* (Cambridge University Press, Cambridge).

Nielsen, M. A., and C. M. Dawson, 2005, Phys. Rev. A **71**, 042323.

Niset, J., A. Acín, U. L. Andersen, N. J. Cerf, R. García-Patrón, M. Navascues, and M. Sabuncu, 2007, Phys. Rev. Lett. **98**, 260404.

Niset, J., U.L. Andersen, and N.J. Cerf, 2008, Phys. Rev. Lett. **101**, 130503.

Niset, J., J. Fiurà̌šek, and N J. Cerf, 2009, Phys. Rev. Lett. **102**, 120501.

Nussbaum, M., and A. Szkola, 2009, Ann. Stat. **37**, 1040.

Ohliger, M., K. Kieling, and J. Eisert, 2010, Phys. Rev. A **82**, 042336.

Olivares, S., and M. G. A. Paris, 2004, J.Opt.B: Quantum Semiclass. Opt. **6**, 69.

Olivares, S., M. G. A. Paris, and U. L. Andersen, 2006, Phys. Rev. A **73**, 062330.

Osaki M., M. Ban, and O. Hirota, 1996, Phys. Rev. A **54**, 1691.

Ourjoumtsev, A., F. Ferreyrol, R. Tualle-Brouri, and Ph. Grangier, 2009, Nature Physics **5**, 189.

Ourjoumtsev, A., H. Jeong, R. Tualle-Brouri, and P. Grangier, 2007, Nature **448**, 784.

Parker, S., S. Bose, and M. B. Plenio, 2000, Phys. Rev. A **61**, 032305.

Pati, A. K., and S. L. Braunstein, 2003, in *Quantum information with continuous variables*, edited by S. L. Braunstein, and A. K. Pati, (Kluwer Academic, Dordrecht), 31-36.

Pati, A. K., S. L. Braunstein, and S. Lloyd, 2000, "Quantum searching with continuous variables", arXiv:quant-ph/0002082v2.

Paulsen, V., 2002, *Completely bounded maps and operator algebras* (Cambridge University Press, Cambridge).

Pereira, S. F, Z. Y. Ou, and H. J. Kimble, 2000, Phys. Rev. A **62**, 042311.

Peres, A., 1996, Phys. Rev. Lett. **77**, 1413.

Pfister, O., 2007, "Graph states and carrier-envelope phase squeezing", arXiv:quant-ph/0701104.

Pirandola, S., 2005, Int. J. Quant. Inf. **3**, 239.

Pirandola, S., 2011, Phys. Rev. Lett. **106**, 090504.

Pirandola, S., S. L. Braunstein, and S. Lloyd, 2008, Phys. Rev. Lett. **101**, 200504.

Pirandola, S., R. García-Patrón, S. L. Braunstein, and S. Lloyd, 2009, Phys. Rev. Lett. **102**, 050503.

Pirandola, S., and S. Lloyd, 2008, Phys. Rev. A **78**, 012331.

Pirandola, S., C. Lupo, V. Giovannetti, S. Mancini, and S. L. Braunstein, 2011, "Quantum reading capacity", arXiv:1107.3500.

Pirandola, S., and S. Mancini, 2006, Laser Physics **16**, 1418.

Pirandola, S., S. Mancini, S. Lloyd, and S. L. Braunstein, 2008, Nature Physics **4**, 726.

Pirandola, S., S. Mancini, and D. Vitali, 2005, Phys. Rev. A **71**, 042326.

Pirandola, S., S. Mancini, D. Vitali, and P. Tombesi, 2003, Phys. Rev. A **68**, 062317.

Pirandola, S., S. Mancini, D. Vitali, and P. Tombesi, 2004, Europhys. Lett. **68**, 323.

Pirandola, S., A. Serafini, and S. Lloyd, 2009, Phys. Rev. A **79**, 052327.

Pirandola, S., D. Vitali, P. Tombesi, and S. Lloyd, 2006, Phys. Rev. Lett. **97**, 150403.

Plenio, M. B., 2005, Phys. Rev. Lett. **95**, 090503.

Polkinghorne, R. E. S, and T. C. Ralph, 1999, Phys. Rev. Lett. **83**, 2095.

Pysher, M., Y. Miwa, R. Shahrokhshahi, R. Bloomer, and O. Pfister, 2011, Phys. Rev. Lett. **107**, 030505.

Ralph, T. C., 1999a, Phys. Rev. A **61**, 010303.

Ralph, T. C, 1999b, Optics Letters **24**, 348.

Ralph, T. C., 2001, Phys. Rev. A **65**, 012319.

Ralph, T. C., 2003, in *Quantum Information with Continuous Variables*, edited by S. L. Braunstein and A. K. Pati, (Kluwer Academic Publishers, The Netherlands).

Ralph, T. C, 2011, Phys. Rev. A **84**, 022339.

Ralph, T. C., A. Gilchrist, G. J. Milburn, W. J. Munro, and S.Glancy, 2003, Phys. Rev. A **68**, 042319.

Ralph, T. C., and E. H. Huntington, 2002, Phys. Rev. A **66**, 042321.

Ralph, T. C., and P. K. Lam, 1998, Phys. Rev. Lett. **81**, 5668.

Ralph, T. C., and Lund, A. P., 2009, in *Proceedings of 9th International Conference on Quantum Communication Measurement and Computing*, edited by A. Lvovsky, (AIP), 155160.

Raussendorf, R., and H. J. Briegel, 2001, Phys. Rev. Lett. **86**, 5188.

Reid, M. D., 2000, Phys. Rev. A **62**, 062308.

Renner, R., 2005, Ph.D. thesis (ETH, Zurich).

Renner, R., 2007, Nature Physics **9**, 645.

Renner, R., and J. I. Cirac, 2009, Phys. Rev. Lett. **102**, 110504.

Renner, R., N. Gisin, and B. Kraus, 2005, Phys. Rev. A **72**, 012332.

Renner, R., and S. Wolf, 2005, *Advances in Cryptology: CRYPTO 2003*, Lecture Notes in Computer Science **2729**, 78.

Richardson, T. J., M. A. Shokrollahi, and R. L. Urbanke, 2001, IEEE Trans. Inf. Theory **47**, 619.

Rivest, R., A. Shamir, and L. Adleman, 1978, Commun. ACM **21**, 120.

Sacchi, M., 2005, Phys. Rev. A **72**, 014305.

Sasaki, M., and O. Hirota, 1996, Phys. Rev. A **54**, 2728.

Sasaki, M., and O. Hirota, 1997, Phys. Lett. A **224**, 213.

Scarani, V., H. Bechmann-Pasquinucci, N. J. Cerf, M. Dušek, N. Lütkenhaus, and M. Peev, 2009, Rev. Mod. Phys. **81**, 1301.

Scarani, V., S. Iblisdir, N. Gisin, and A. Acín, 2005, Rev. Mod. Phys. **77**, 1225.

Scarani, V., and R. Renner, 2008, Phys. Rev. Lett. **100**, 200501.

Schneier, B., 2000, *Applied Cryptography* (Wiley, New York).

Schumacher B., and M. A. Nielsen, 1996, Phys. Rev. A **54**, 2629.

Schumacher, B., and M. D. Westmoreland, 1997, Phys. Rev. A **56**, 131.

Scutaru, H., 1998, J. Phys. A **31**, 3659.

SECOQC, 2007, http://www.secoqc.net/

Serafini, A., 2006, Phys. Rev. Lett. **96**, 110402.

Serafini, A., and G. Adesso, 2007, J. Phys. A: Math. Theor. **40**, 8041.

Serafini A., G. Adesso, and F. Illuminati, 2005, Phys. Rev. A **71**, 032349.

Serafini, A., J. Eisert, and M. M. Wolf, 2005, Phys. Rev. A **71**, 012320.

Serafini, A., F. Illuminati, and S. De Siena, 2004, J. Phys. B: At. Mol. Opt. Phys. **37**, L21.

Shannon, C. E., 1948, Bell Syst. Tech. J. **27**, 379.

Shannon, C. E., 1949, Bell Syst. Tech. J. **28**, 656.

Shapiro, J. H., 1984, IEEE J. Quantum Electron. **20**, 803.

Shapiro, J. H., S. Guha, B. I. Erkmen, 2005, Journal of Optical Networking: Special Issue **4**, 501.

Shapiro, J. H., and Seth Lloyd, 2009, New J. Phys. **11**, 063045.

Sherson, J., H. Krauter, R. K. Olsson, B. Julsgaard, K. Hammerer, I. Cirac, and E. S. Polzik, 2006, Nature **443**, 557.

Shor, P., 1995, Phys. Rev. A **52**, 2493.

Shor, P., 1997, SIAM J. Comput. **26**, 1484.

Shor, P., 2002, *The quantum channel capacity and coherent information*, Lecture Notes, MSRI Workshop on Quantum Computation.

Shor, P., 2004, Comm. Math. Phys. **246**, 453.

Silberhorn, Ch., T. C. Ralph, N. Lütkenhaus, and G. Leuchs, 2002, Phys. Rev. Lett. **89**, 167901.

Simon, R., 2000, Phys. Rev. Lett. **84**, 2726.

Simon, R., S. Chaturvedi, and V. Srinivasan, 1999, J. Math. Phys. **40**, 3632.

Simon, R., N. Mukunda, and B. Dutta, 1994, Phys. Rev. A **49**, 1567.

Smith, G., and J. A. Smolin, 2007, Phys. Rev. Lett. **98**, 030501.

Smith, G., J. A. Smolin, and J. Yard, 2011, Nature Photonics **5**, 624.

Smith, G., and J. Yard, 2008, Science **321**, 1812.

Soto, F., and P. Claverie, 1983, J. Math. Phys. **24**, 97.

Steane, A. M., 1996, Phys. Rev. Lett. **77**, 793.

Stinespring, W. F., 1955, Proc. Am. Math. Soc. **6**, 211.

Su, X., A. Tan, X. Jia, J. Zhang, C. Xie, and K. Peng, 2007, Phys. Rev. Lett. **98**, 070502.

Sabuncu, M., U. L. Andersen, and G. Leuchs, 2007, Phys. Rev. Lett. **98**, 170503.

Sych, D., and G. Leuchs, 2009, New J. Phys. **12**, 053019.

Symul, T, D. J. Alton, S. M. Assad, A. M. Lance, C. Weedbrook, T. C. Ralph, and P. K. Lam, 2007, Phys. Rev. A **76**, 030303 (R).

Takahashi, H., J. S. Neergaard-Nielsen, M. Takeuchi, M. Takeoka, K. Hayasaka, A. Furusawa, and M. Sasaki, 2010, Nature Photonics **4**, 178.

Takei, N., H. Yonezawa, T. Aoki, and A. Furusawa, 2005, Phys. Rev. Lett. **94**, 220502.

Takeoka, M., M. Sasaki, P. van Loock, and N. Lütkenhaus, 2005, Phys. Rev. A **71**, 022318.

Takeoka, M., and M. Sasaki, 2008, Phys. Rev. A **78**, 022320.

Tan, S.-H., B. I. Erkmen, V. Giovannetti, S. Guha, S. Lloyd, L. Maccone, S. Pirandola, and J. H. Shapiro, 2008, Phys. Rev. Lett. **101**, 253601.

Tsujino, K., D. Fukuda, G. Fujii, S. Inoue, M. Fujiwara, M. Takeoka, and M. Sasaki, 2011, Phys. Rev. Lett. **106**, 250503.

Tyc, T., and B. C. Sanders, 2002, Phys. Rev. A **65**, 042310.

Ukai, R., S. Yokoyama, J. Yoshikawa, P. van Loock, and A. Furusawa, 2011, "Demonstration of a controlled-phase gate for continuous-variable one-way quantum computation", arXiv:1107.0514.

Ukai, R., J. Yoshikawa, N. Iwata, P. van Loock, and A. Furusawa, 2010, Phys. Rev. A **81**, 032315.

Ukai, R., N. Iwata, Y. Shimokawa, S, C. Armstrong, A. Politi, J. Yoshikawa, P. van Loock, and A. Furusawa, 2011, Phys. Rev. Lett. **106**, 240504.

Uhlmann, A., 1976, Rep. Math. Phys. **9**, 273.

Usenko, V. C., and R. Filip, 2010, Phys. Rev. A **81**, 022318.

Usha Devi, A. R., and A. K. Rajagopal, 2009, Phys. Rev. A **79**, 062320.

Vahlbruch, H., M. Mehmet, S. Chelkowski, B. Hage, A. Franzen, N. Lastzka, S. Goszler, K. Danzmann, and R. Schnabel, 2008, Phys. Rev. Lett. **100**, 033602.

Vaidman, L., 1994, Phys. Rev. A **49**, 1473.

van Assche, G., 2006, *Quantum Cryptography and Secret-Key Distillation* (Cambridge University Press, Cambridge).

van Loock, P., 2007, J. Opt. Soc. Am. B **24**, 2.

van Loock, P., 2008, "A note on quantum error correction with continuous variables", arXiv:0811.3616.

van Loock, P., and S. L. Braunstein, 1999, Phys. Rev. A **61**, 010302(R).

van Loock, and S. L. Braunstein, 2000, Phys. Rev. Lett. **84**, 3482.

van Loock, and S. L. Braunstein, 2001, Phys. Rev. Lett. **87**, 247901.

van Loock, P., C. Weedbrook, and M. Gu, 2007, Phys. Rev. A **76**, 032321.

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

Vidal, G., 2000, J. Mod. Opt. **47**, 355.

Vernam, G. S., 1926, J. Am. Inst. Electr. Eng. **45**, 109.

Vidal, G., and R. F. Werner, 2002, Phys. Rev. A **65**, 032314.

Walk, N., T. Symul, T. C. Ralph, P. K. Lam, 2011, "Security of post-selection based continuous-variable quantum key distribution against arbitrary attacks", arXiv:1106.0825.

Walker, T. A., and S. L. Braunstein, 2010, Phys. Rev. A **81**, 062305.

Walls, D. F., and G. Milburn, 2008, *Quantum Optics* (Springer, Berlin).

Wang, X. -B., T. Hiroshima, A.Tomita, and M. Hayashi, 2007, Physics Reports **448**, 1-111.

Wang, G., and M. Ying, 2006, Phys. Rev. A **73**, 042301.

Weedbrook, C., 2009, Ph.D. thesis (University of Queensland, Brisbane).

Weedbrook, C., N. B. Grosse, T. Symul, P. K. Lam, and T. C. Ralph, 2008, Phys. Rev. A **77**, 052313.

Weedbrook, C., A. M. Lance, W. P. Bowen, T. Symul, T. C. Ralph, and P. K. Lam, 2004, Phys. Rev. Lett. **93**, 170504.

Weedbrook, C., A. M. Lance, W. P. Bowen, T. Symul, T. C. Ralph, and P. K. Lam, 2006, Phys. Rev. A **73**, 022316.

Weedbrook,C., S. Pirandola, S. Lloyd, and T. C. Ralph, 2010, Phys. Rev. Lett. **105**, 110501.

Werner, R. F., and M. M. Wolf, 2001, Phys. Rev. Lett. **86**, 3658.

Williamson, J., 1936, Am. J. Math. **58**, 141.

Wittmann, C., U. L. Andersen, M. Takeoka, D. Sych, and G. Leuchs, 2010a, Phys. Rev. Lett. **104**, 100505.

Wittmann, C., U. L. Andersen, M. Takeoka, D. Sych, and G. Leuchs, 2010b, Phys. Rev. A **81**, 062338.

Wittmann, C., M. Takeoka, K. N. Cassemiro, M. Sasaki, G. Leuchs, and U. L. Andersen, 2008, Phys. Rev. Lett. **101**, 210501.

Wolf, M. M., J. Eisert, and M. B. Plenio, 2003, Phys. Rev. Lett. **90**, 047904.

Wolf, M. M., G. Giedke, and J. I. Cirac, 2006, Phys. Rev. Lett. **96**, 080502.

Wolf, M. M., G. Giedke, O. Krüger, R. F. Werner, and J. I. Cirac, 2004, Phys. Rev. A **69**, 052320.

Wolf, M. M., D. Pérez-García, and G. Giedke, 2007, Phys. Rev. Lett. **98**, 130501.

Wootters, W. K., and W. .H. Zurek, 1982, Nature **299**, 802.

Xiang, G. Y., T. C. Ralph, A. P. Lund, N. Walk, and G. J. Pryde, 2010, Nature Photonics **4**, 316.

Yamamoto, Y., and H. A. Haus, 1986, Rev. Mod. Phys. **58**, 1001.

Yeoman, G., and S. M. Barnett, 1993, J. Mod. Opt **40**, 1497.

Yonezawa, H., T. Aoki, and A. Furusawa, 2004, Nature **431**, 430.

Yoshikawa, J., T. Hayashi, T. Akiyama, N. Takei, A. Huck, U. L. Andersen, and A. Furusawa, 2007, Phys. Rev. A **76**, 060301.

Yoshikawa, J., Y. Miwa, A. Huck, U. L. Andersen, P. van Loock, and A. Furusawa, 2008, Phys. Rev. Lett. **101**, 250501.

Yuen, H. P., 1976, Phys. Rev. A **13**, 2226.

Yuen, H. P., and R. Nair, 2009, Phys. Rev. A **80**, 023816.

Yuen, H. P., and M. Ozawa, 1993, Phys. Rev. Lett. **70**, 363.

Yuen, H. P., and J. H. Shapiro, 1978, IEEE Trans. Inf. Theory **24**, 657.

Yuen, H. P., and J. H. Shapiro, 1980, IEEE Trans. Inf. Theory **26**, 78.

Yukawa, M., R. Ukai, P. van Loock, and A. Furusawa, 2008, Phys. Rev. A **78**, 012301.

Yurke, B., 1985, J. Opt. Soc. Am. B **2**, 732.

Zaidi, H., N. C. Menicucci, S. T. Flammia, R. Bloomer, M. Pysher, and O. Pfister, 2008, Laser Phys. **18**, 659.

Zhang, J., 2008a, Phys. Rev. A **78**, 034301.

Zhang, J., 2008b, Phys. Rev. A **78**, 052307.

Zhang, J., 2010, Phys. Rev. A **82**, 034303.
Zhang, J., G. Adesso, C. Xie, and K. Peng, 2009, Phys. Rev. Lett. **103**, 0708501.
Zhang, J., and S. L. Braunstein, 2006, Phys. Rev. A **73**, 032318.
Zhang, T. C., K. W. Goh, C. W. Chou, P. Lodahl, and H. J. Kimble, 2003, Phys. Rev. A **67**, 033802.
Zhao Y. -B., M. Heid, J. Rigas, and N. Lütkenhaus, 2009, Phys. Rev. A **79**, 012307.
Zwierz, M., C. A. Pérez-Delgado, and P. Kok, 2010, Phys. Rev. A **82**, 042320.