Continuous variable systems: Entanglement, decoherence and quantum cryptography

Arvind

Abstract | This article aims to review some aspects of quantum information processing (QIP) using continuous variable systems for one and two-modes. The objective of the article is to convey a flavor of the kind of developments which has taken place in this subfield of QIP in the past decade and not to write a comprehensive review of the field. We hence focus on Gaussian states, their entanglement and their utilization in various quantum cryptographic protocols that have been proposed and recently implemented.

1. Introduction

There has been a lot of interest in continuous variable systems as candidates for quantum information processing. Their connection with quantum optics makes them useful systems from the standpoint of experimental implementations based on the quadrature amplitudes of the electromagnetic field. Recently, quantum cryptographic protocols based on such quantum systems (as opposed to qubits) have been proposed and these developments have attracted a lot of attention.

Continuous variable states arise in many different fields in physics. Apart from material oscillators, bosonic fields such as phonons, plasmons and more importantly photons lend themselves to such a theoretical description. Optics has been an important test-bed for novel and counterintuitive aspects of quantum theory and currently, optical schemes are being actively considered for quantum information processing. Gaussian states with Gaussian-Wigner distribution functions play an important role in this context [1,2]. They are a family which can be easily generated and manipulated in the laboratory and have members from classical-like states to maximally entangled ones. Entanglement of Gaussian states is a fundamental resource in quantum information theory implemented using continuous variable systems [3,4]. Therefore, it is necessary to understand entanglement of these states qualitatively as well as quantitatively. A large body of work has been carried out in this direction; however there is still a long way to go before one achieves a complete understanding of the issues involved [5–8]. This particular family of states is playing a very important role in the newly emergent area of quantum information processing for continuous variables. They have been used to implement quantum teleportation [9], simulation of quantum processes on a classical computer [10] and quantum cryptography. Protection against decoherence is a major issue in quantum information processing, and it is hence important to study the evolution of this family of states under a dissipative environment[11, 12]. Various ways are being devised to protect these states against decoherence. Error correcting codes [13,14], understanding the physics of quantum channels [15] and distilling entanglement from the non-maximally entangled states have also been explored in this context [16–18].

Squeezing and entanglement are important signatures of nonclassicality in the states of the

Indian Institute of Science Education and Research Mohali, Transit Campus: MGSIPAP Complex, Sector 26, Chandigarh
arvind@iisermohali.ac.in

electromagnetic field. Squeezing is associated with noise in a certain quadrature of a quantum state falling below the coherent state value of $\hbar/2$. Entanglement on the other hand, arises when it is not possible to find any ensemble decomposition of the density matrix for the two-mode quantum system which is a convex sum of separable states. It turns out that although these two concepts are quite different there are some interesting interrelations between the two [19]. It is possible to use passive optics to interconvert mode squeezing and entanglement, particularly in the context of Gaussian states of two-mode fields [20–22]. Various experiments have been performed to obtain entangled Gaussian states and squeezed Gaussian states and to understand how they are affected by decoherence [23–25].

An important question in this context is the sensitivity of these features to noise or decoherence. Typically, one would imagine that entanglement is more fragile compared to single mode squeezing under a noisy environment because it is a two-mode non-classical feature as opposed to squeezing, which is a single mode non-classical feature. Fortunately, for this class of states one can quantify the amount of entanglement and it is therefore possible to answer this question precisely [26–28]. This interplay between entanglement and squeezing is a feature which does not have any analogue for qubit systems.

The first proposal to carry out cryptography based on continuous variable systems, where phase and amplitude modulation of light beams carry the key information and security is ensured by quantum entanglement, was proposed by Ralph [29,30]. Later a new scheme using coherent states was constructed by Grangier and collaborators where only coherent states were used [31]. This was a very interesting development because coherent states were considered to be as classical as possible within quantum theory, and it was not expected that they could be used to carry out a quantum information processing task such as cryptography. Several cryptographic protocols have been designed and implemented later using bosonic modes with Gaussian statistics. These schemes have indicated the possibility of reaching high secret key rates even in lossy quantum channels. However, their security can be affected by more general attacks where extra Gaussian noise is introduced by Eve. Recently, Pirandola et al have shown that the security thresholds of these cryptographic protocols can be increased by extending them to two-way quantum communication where one of the honest parties assists the secret encoding of the other [32]. For a detailed and comprehensive review of Gaussian states for quantum information processing see [33] and a few important studies in this context are described in [34–39].

2. Continuous variable quantum systems

The most straightforward route to quantize a bosonic field (for example the electromagnetic field) is through canonical quantization. To implement canonical quantization for this system we associate dimensionless Hermitian operators $\hat{q}_k$ and $\hat{p}_k$ with the quadrature components of the electric field q_k and p_k. The Poisson brackets become the canonical commutation relations

$$\begin{aligned} [\hat{q}_j,\hat{q}_k] &= [\hat{p}_j,\hat{p}_k]=0 \\ [\hat{q}_j,\hat{p}_k] &= i\delta_{jk} \\ j,k &= 1,2\cdots \end{aligned} \tag{1}$$

The corresponding annihilation and creation operators and their commutation relations are

$$\begin{aligned} \hat{a}_k &= \frac{1}{\sqrt{2}}(\hat{q}_k+i\hat{p}_k) \\ \hat{a}_k^\dagger &= \frac{1}{\sqrt{2}}(\hat{q}_k-i\hat{p}_k) \\ [\hat{a}_j,\hat{a}_k] &= [\hat{a}_j^\dagger,\hat{a}_k^\dagger]=0 \end{aligned} \tag{2}$$

$$[\hat{a}_j,\hat{a}_k^\dagger] = \delta_{jk} \tag{3}$$

The quantum mechanical Hamiltonian then becomes

$$\begin{aligned} \hat{H} &= \sum_k \hbar\omega_k\left(\hat{q}^2+\hat{p}^2\right) \\ &= \sum_k \hbar\omega_k\left(\hat{a}_k^\dagger a_k+\frac{1}{2}\right) \end{aligned} \tag{4}$$

The factor of half comes from the fact that $\hat{q}\hat{p}\neq\hat{p}\hat{q}$ and represents the zero point energy for each mode.

The Hilbert space on which the operators a_k and $a_k^\dagger$ act irreducibly, in the Fock representation has an orthogonal basis which has simultaneous eigenvectors of number operators corresponding to all the modes

$$\begin{aligned} &|n_1,n_2,\cdots n_k\cdots\rangle \\ &\quad=\frac{(a_1^\dagger)^{n_1}\,(a_2^\dagger)^{n_2}\cdots\,(a_k^\dagger)^{n_k}\cdots}{\sqrt{n_1!\,n_2!\cdots n_k!\cdots}}|0,0,\cdots\rangle\,, \\ &a_j|0,0,0,\cdots\rangle=0\,, \\ &a_j^\dagger\,a_j\,|n_1,n_2,\cdots n_k\cdots\rangle=n_j\,|n_1,n_2,\cdots n_k\cdots\rangle\,, \\ &\langle n_1',n_2',\cdots n_k'\cdots|n_1,n_2,\cdots n_k\cdots\rangle \\ &\quad=\delta_{n_1'\,n_1}\,\delta_{n_2'\,n_2}\cdots\delta_{n_k'\,n_k}\cdots. \end{aligned} \tag{5}$$

Arbitrary vectors in the Hilbert space can now be expanded in the above basis. There are several other useful basis systems which can be used to expand states of the electromagnetic field.

It is natural to look for transformations under which the canonical commutation relations (1) are invariant. For a situation where we limit ourselves to say n modes, the real linear transformations which preserve these commutation relations form the group $Sp(2n, \Re)$. It turns out that the unitary representation of this group, while acting on the Hilbert space of the n mode system is capable of implementing finite time evolution generated by arbitrary quadratic Hamiltonians. In other words, the generators of this group in this representation are all possible Hermitian quadratic expressions in $\hat{a}_k$'s and $\hat{a}_k^\dagger$'s. To start with, the free Hamiltonian is itself quadratic in the creation and annihilation operators and further one can have interactions which will generate more nontrivial quadratic terms in the Hamiltonian. The noncompact group $Sp(2n, \Re)$ naturally splits into two parts: the maximally compact $U(n)$ subgroup which comprises of "passive" transformations which preserve the total photon number and are generated by photon number conserving Hamiltonians; and the noncompact photon number nonconserving "active" part. This group plays a very important role; the compact part comes in handy in the analysis of various "nonclassical" properties as it does not alter the amount of nonclassicality in a state. The general strategy will be to perform such transformations on a given state to make the nonclassicality, if it is present and hidden, manifest. On the other hand, the noncompact part has the potential to take a classical state to a nonclassical state and vice versa. More precisely, it generates a squeezed state from a nonsqueezed one.

The symbol $\sim$ in the second column of the table above represents the local isomorphism between the groups i.e. isomorphism at the Lie algebra level. A useful account of $Sp(2n, \Re)$ is given in the review article [11].

3. Classical and nonclassical states within quantum theory

Coherent states

Coherent states were originally constructed by Schrödinger in the context of the harmonic oscillator as minimum uncertainty states and later applied to the electromagnetic field by Glauber and Sudarshan in 1963.

For the single mode electromagnetic field the coherent states are defined as

$$\begin{aligned} |z\rangle &= D(z)|0\rangle = e^{z\hat{a}^\dagger - z^*\hat{a}}|0\rangle \\ &= e^{-\frac{|z|^2}{2}} \sum_{n=0}^{\infty} \frac{z^n}{\sqrt{n!}}|n\rangle \\ \hat{a}|z\rangle &= z|z\rangle \end{aligned} \tag{6}$$

and they are eigen states of the annihilation operator $\hat{a}$. The generalization to multi-mode fields is straightforward, a multi-mode coherent state is just a product state with each mode being in a single mode coherent state. There are several interesting properties of coherent states which are worth mentioning at this stage.

- The commutation relations lead to the customary uncertainty relation among the variances of the quadrature components

  $$(\Delta q)^2 (\Delta p)^2 - \Delta(qp)^2 \geq \frac{1}{4} \tag{7}$$

  For coherent states we have

  $$\begin{aligned} (\Delta q)^2 &= (\Delta p)^2 = \frac{1}{2}, \\ \Delta(qp) &= 0. \end{aligned} \tag{8}$$

  Therefore they are minimum uncertainty states with the quantum noise being equally distributed among the quadratures. Further, this noise in each quadrature remains constant in time.

- Coherent states have a well defined classical limit. For the case of the harmonic oscillator, they represent an oscillating Gaussian wave packet of fixed width which is independent of its amplitude. Therefore, in the limit of large amplitudes, this width can be neglected and we recover the phase space trajectories of the classical harmonic oscillator. In the context of the em field, this limiting process gives us the appropriate solution of the Maxwell equations.

System	Group of linear canonical transformations	Max. compact subgroup
Single mode	$Sp(2, \Re) \sim SL(2, R) \sim SO(2, 1) \sim SU(1, 1)$	$U(1)$
Two mode	$Sp(4, \Re) \sim SO(3, 2)$	$U(2)$
n-mode	$Sp(2n, \Re)$	$U(n)$

- Arbitrary states can be expanded in terms of coherent states as they span the whole of Hilbert space. They are not just complete but are overcomplete with overlaps given by

$$\langle z|z'\rangle = \exp\left(-\frac{|z|^2}{2} - \frac{|z'|^2}{2} + z^\star z'\right) \quad (9)$$

- In the classical limit (in the limit of large amplitude), coherent states go over to the corresponding solution of the classical Maxwell equations; for cubic geometry they would be plane waves which have precisely defined phase. This for example, is in contrast to Fock states which have completely random phases even when one is dealing with a large number of photons.
- As is clear from the definition, the photon number distribution for coherent states is Poissonian. Moreover, in a typical photon counting experiment with coherent states one gets Poissonian statistics which can be mimicked by a classical plane wave being detected by a quantized detector.
- The quantum mechanical description of a monochromatic laser beam is through a coherent state.

In view of all the above properties, the coherent states are pure quantum states which come very close to a classical description and can be called "classical".

3.1. *Diagonal coherent state distribution function*

While working within the quantum theory, a given state is to be classified as classical or nonclassical based on some appropriate criterion or convention. Such a criterion has to be physically motivated and mathematically precise. The most prevalent prescription for such a classification is through the diagonal coherent state distribution function. Since every density matrix (pure or mixed) of the electromagnetic field can be expanded as an integral over projections onto the coherent states, the diagonal coherent state distribution function has complete information about any given state. Now if this function turns out to be nonnegative everywhere we can interpret the given state as a classical mixture of coherent states, and then using the normal ordering rule can calculate all correlation functions for such a state using the corresponding ensemble of solutions of the Maxwell equations. Such states can thus be defined to be classical. On the other hand, if the diagonal coherent state distribution function is negative somewhere or becomes more singular than a delta function then one cannot raise it to the status of a probability distribution and the corresponding state will be called nonclassical. These nonclassical states have one or the other nontrivial quantum features which cannot be captured by a classical treatment based on Maxwell equations. To cite a few examples the presence of squeezing, sub-Poissonian statistics, antibunching, violation of Bell's inequalities all imply that the underlying state is nonclassical in this precise sense.

For a single-mode field the expansion in terms of diagonal coherent states is given by

$$\hat{\rho} = \frac{1}{\pi}\int \varphi(z)\, |z\rangle\langle z|\, d^2z \quad (10)$$

Here $\varphi(z)$ is the diagonal coherent state distribution function and we have the classification.

Classical states	$\varphi(z) \geq 0$
Nonclassical states	$\varphi(z) \ngeq 0$

The above arguments are completely general and are valid for any number of modes.

When a state undergoes a unitary Hilbert space transformation corresponding to a passive canonical transformation, its diagonal coherent state distribution function transforms by a point transformation through the defining representation of $U(n)$. Hence this function is covariant under the action of $U(n)$ implying that the new function at an arbitrary given point is just the old function at some other point. Obviously the "positive everywhere" character or the "singular" character of the function is retained under such transformations.

Thus an initial classical(nonclassical) state will remain classical(nonclassical) while it undergoes a Hilbert space unitary transformation corresponding to the passive canonical transformations $U(n)$ which is the same as finite time evolution under quadratic photon number conserving Hamiltonians. However as we will see on various occasions the nature of nonclassicality may qualitatively change when a state undergoes a $U(n)$ transformation. For example, a nonentangled state can get transformed to an entangled one, hidden squeezing can become manifest, etc.

Nonclassicality of a state manifests itself through one or the other of its measurable signatures. Most of these signatures are physically important as they qualitatively explore some particular quantum feature of the field. We discuss here some important signatures of nonclassicality. We however emphasize that though the presence of any of these signatures does imply that the underlying state is nonclassical, the absence of one or a few of them does not confirm its classical nature.

3.2. *Squeezing*

Squeezing is essentially a process of manipulating the quantum noise in the quadrature components of the electromagnetic field. Beginning with a coherent state, without losing its minimum uncertainty character, the noise in the quadrature components can be redistributed such that at a given time, some quadrature component has noise less than the "shot noise" limit. If one focuses attention on a particular quadrature component then the noise present in it is time dependent and oscillates around the coherent state value.

For a single-mode situation we define the quadrature noise matrix to be

$$V = \begin{pmatrix} (\Delta q)^2 & \Delta(qp) \\ \Delta(qp) & (\Delta p)^2 \end{pmatrix} \quad (11)$$

The uncertainty relation then becomes $\mathrm{Det} V \geq \frac{1}{4}$ and the minimum uncertainty states are the ones for which $\mathrm{Det} V = \frac{1}{4}$. A single-mode minimum uncertainty state is squeezed if one of the eigenvalues of V is less than $\frac{1}{2}$ with the product remaining $\frac{1}{4}$. This definition of squeezing is invariant under the passive canonical transformations $U(1)$ and paves the way for analyzing multimode squeezing in a $U(n)$ invariant manner. The remaining canonical transformations are actually squeezing transformations and, when they act on an originally unsqueezed state, can convert it into a squeezed one.

The original interest in squeezing was motivated by the possibility of using squeezed light to enhance the phase sensitivity of an interferometer. However, now it is clear that squeezed states are very important for quantum information processing.

For the two-mode situation there is a possibility of intrinsically quantum mechanical correlations between the modes; when such correlations are present the state cannot be of the product form with one factor belonging to each mode and thus the state is "entangled". Two-mode squeezed states can exhibit such properties. For two-mode case the situation is a little more subtle [2]. The passive canonical transformations with respect to which squeezing is invariant here form the group $U(2)$. Therefore, it becomes imperative to be able to experimentally implement arbitrary $U(2)$ transformations on a state before actual detection.

Wigner representation

The first quasi-probability distribution to characterize the state $|\psi\rangle$ in phase space was introduced by Wigner in 1932. The Wigner function may be defined as the Fourier transform of the symmetrically ordered characteristic function $\chi(\eta)$

$$W(\alpha) = \frac{1}{\pi^2}\int \exp(\eta^*\alpha - \eta\alpha^*)\chi(\eta)d^2\eta \quad (12)$$

where the characteristic function $\chi(\eta)$ is given by the following:

$$\chi_N(\eta) = \mathrm{Tr}(\rho e^{\eta a^\dagger} e^{-\eta^* a}) \quad (13)$$

where subscript N stands for Normal order and η is a complex number. We can obtain the symmetrically ordered characteristic function from the normal ordered characteristic function using Baker Hausdorff relation.

$$\chi_S(\eta) = \mathrm{Tr}(\rho e^{\eta a^\dagger - \eta^* a}) \quad (14)$$

Note that the Wigner distribution always exists but is not necessarily positive and so it cannot be interpreted as a probability distribution as was the case for the diagonal coherent state representation. The relationship between the Wigner distribution and the $\phi(\alpha)$ distribution may be obtained via the characteristic functions. The two distributions are related to each other as follows:

$$\begin{aligned} W(\alpha) &= \frac{1}{\pi^2}\int \exp(\eta^*\alpha - \eta\alpha^*)\chi_N \\ &\quad \times(\eta)e^{-1/2|\eta|^2}d^2\eta \\ &= \frac{1}{\pi^2}\int \mathrm{Tr}\{\rho e^{\eta(a^\dagger - \alpha^*)}e^{\eta^*(a-\alpha)}\} \\ &\quad \times e^{-1/2|\eta|^2}d^2 \\ &= \frac{1}{\pi^2}\int \phi(\beta)\exp[\eta(\beta^* - \alpha^*) \\ &\quad -\eta^*(\beta-\alpha) - \frac{1}{2}|\eta|^2]d^2\eta d^2\beta \quad (15) \end{aligned}$$

The final relation between the two functions is given by

$$W(\alpha) = \frac{2}{\pi}\int \phi(\beta)\exp(-2|\beta-\alpha|^2)d^2\beta \quad (16)$$

Thus, the Wigner function is a Gaussian convolution of the diagonal coherent state representation function.

When the Wigner distribution corresponding to a quantum state is Gaussian, we call it a Gaussian state. Gaussian states are determined completely by first and second order noise moments. As we will see, the first order moments can be trivially manipulated and therefore the Gaussian states are characterizable via their second order moments which can be arranged in the form of a variance matrix. Gaussian states are an extremely important and interesting family of states and they include coherent states, squeezed states, and thermal states. Fock states are not Gaussian states. Gaussian states can be defined for any number of modes. In our analysis, we will confine ourselves to two-mode Gaussian states.

4. Two-mode continuous variable systems

A two-mode system is the simplest composite system for continuous variables where we can have entangled states. It turns out that although the Hilbert space is infinite-dimensional, there are entangled states which have a simple description. The most interesting and useful of these states of such systems are Gaussian states. We now take up the discussion of such states and their entanglement properties.

We consider two orthogonal modes of the radiation field, with annihilation operators a_1 and a_2. To handle the analysis of the two-mode fields compactly, we introduce the column vectors

$$\xi^{(c)} \equiv \left(\xi^{(c)}_a\right) = \begin{pmatrix} a_1 \\ a_2 \\ a_1^\dagger \\ a_2^\dagger \end{pmatrix}, \qquad \xi \equiv (\xi_a) = \begin{pmatrix} q_1 \\ q_2 \\ p_1 \\ p_2 \end{pmatrix}. \tag{17}$$

$\xi^{(c)}$ being the vector of creation and annihilation operators and ξ the vector of the quadrature operators, with their components having the usual relation, $q_j = \frac{1}{\sqrt{2}}(a_j + a_j^\dagger)$ and $p_j = -\frac{i}{\sqrt{2}}(a_j - a_j^\dagger)$. The canonical commutation relations can be written compactly in terms of these column vectors as

$$\begin{aligned} \left[\xi^{(c)}_a, \xi^{(c)}_b\right] &= \beta_{ab} \\ &\quad \text{with} \quad (\beta_{ab}) = \begin{pmatrix} 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \\ -1 & 0 & 0 & 0 \\ 0 & -1 & 0 & 0 \end{pmatrix} \\ \left[\xi_a, \xi_b\right] &= i\beta_{ab} \end{aligned} \tag{18}$$

The linear canonical transformations of the quadrature operators q_j and p_j are those real linear transformations that preserve the commutation relations given in Equation (18). They constitute the four-dimensional symplectic group $Sp(4,R)$:

$$\begin{aligned} &\xi \longrightarrow \xi' = S\,\xi, \qquad S \in Sp(4,R) \\ &Sp(4,R) = \left\{ S = 4 \times 4 \text{ real matrix } \mid S\beta S^T = \beta \right\} \end{aligned} \tag{19}$$

In the Hilbert space this group acts via its infinite dimensional unitary representation called the Metaplectic representation. This group describes the action of all possible quadratic Hamiltonians on the quantum states of the two-mode field. In particular this includes squeezing transformations and optically passive transformations. The maximally compact subgroup $K = U(2)$ of $Sp(4,R)$, can be identified as

$$\begin{aligned} &K = \left\{ S(X,Y) \in Sp(4,R) \mid U = X - iY \in U(2) \right\} \\ &S(X,Y) = \begin{bmatrix} X & Y \\ -Y & X \end{bmatrix} \end{aligned} \tag{20}$$

The action of this subgroup on the creation and annihilation operators is through its defining representation

$$\begin{bmatrix} a'_1 \\ a'_2 \end{bmatrix} = U \begin{bmatrix} a_1 \\ a_2 \end{bmatrix}, \qquad U \in U(2) \tag{21}$$

The standard way of distinguishing classical from non-classical states is through the diagonal coherent state description. A given two-mode density operator ρ can always be expanded in terms of coherent states

$$\rho = \int \frac{d^2 z_1 d^2 z_2}{\pi^2} \phi(z_1, z_2) |z_1, z_2\rangle\langle z_1, z_2| \tag{22}$$

where $|z_1, z_2\rangle$ are the two-mode coherent states. The unique normalized weight function $\phi(z_1, z_2)$ provides a complete description of the two-mode state ρ and can in general be a distribution which is quite singular. For the case when $\phi(z_1, z_2)$ can be interpreted as a probability distribution (i.e. it is non-negative and nowhere more singular than a delta function), Equation (22) implies that the state ρ is a classical mixture of coherent states which have a natural classical limit. Such quantum states are referred to as "classical"; in contrast those states for which $\phi(z_1, z_2)$ either becomes negative or more singular than a delta function, are defined as "non-classical". Classical states are clearly unentangled.

When the two-mode state described by density operator ρ, transforms under a unitary operator corresponding to the compact $U(2)$ subgroup of $Sp(4,\Re)$, the distribution $\phi(z_1,z_2)$ undergoes a point transformation given in terms of the $U(2)$ element

$$\rho' = \mathcal{U}(S(X,Y))\ \rho\ \mathcal{U}(S(X,Y))^{-1} \Longleftrightarrow$$
$$\phi'(z_1,z_2) = \phi(z_1',z_2'),$$
$$\begin{bmatrix} z_1' \\ z_2' \end{bmatrix} = U \begin{bmatrix} z_1 \\ z_2 \end{bmatrix}, \quad U = X - iY \in U(2) \quad (23)$$

Thus under $U(2)$ (the group of passive transformations), classical states map onto classical ones and non-classical states onto non-classical ones; these transformations are incapable of generating a non-classical state from a classical one or vice versa. However, these states can generate entanglement provided that the original state is nonclassical.

We recapitulate some interesting and important properties of the maximally compact subgroup $K = U(2)$ of $Sp(4,R)$ here:

(a) The action of the elements of $U(2)$ on a quantum state does not change the distribution of the total photon number.

(b) The diagonal coherent state distribution function is covariant under $U(2)$ transformations.

(c) One requires only passive optical elements (mirrors, beam splitters, phase shifters etc.) to experimentally implement any $U(2)$ transformation on a state of the two-mode field.

We will see that passive $U(2)$ transformations are a useful tool to analyze the nonclassicality of a two-mode state and we can convert nonclassicality into entanglement by employing these transformations.

Upto this point we have been considering general two mode states. From this point onwards we will confine our discussion to those states for which the Wigner distribution is Gaussian. Such states are called Gaussian states.

The Wigner distribution is related to the density operator in the following manner and is a complete description of the quantum state of the system.

$$W(\xi) = \pi^{-2}\int d^2q' \langle q-q'|\,\hat{\rho}\,|q+q'\rangle \times \exp(2i\,q'\cdot p). \quad (24)$$

where $q = (q_1,q_2)$, $p = (p_1,p_2)$.

The most general centered Gaussian Wigner Distribution function is given as follows

$$W(\xi) = \frac{1}{4\pi^2\sqrt{\det V}} \exp\left(-\frac{1}{2}\,\xi^T\, V^{-1}\xi\right) \quad (25)$$

where the variance matrix V is given by

$$V = \begin{pmatrix} \langle q_1^2\rangle & \langle q_1q_2\rangle & \frac{1}{2}\langle\{q_1,p_1\}\rangle & \langle q_1p_2\rangle \\ \langle q_1q_2\rangle & \langle q_2^2\rangle & \langle q_2p_1\rangle & \frac{1}{2}\langle\{q_2,p_2\}\rangle \\ \frac{1}{2}\langle\{q_1,p_1\}\rangle & \langle q_2p_1\rangle & \langle p_1^2\rangle & \langle p_1p_2\rangle \\ \langle q_1p_2\rangle & \frac{1}{2}\langle\{q_2,p_2\}\rangle & \langle p_1p_2\rangle & \langle p_2^2\rangle \end{pmatrix} \quad (26)$$

The non zero displacement can always be added by considering the phase space displacement of this centered Gaussian via transformations of the type

$$\xi \to \xi + \xi_0 \quad (27)$$

Where ξ_0 is a constant phase space displacement (not an operator like ξ). Coherent states, squeezed states and thermal states are all Gaussian in nature. This family of states is very rich and contains states ranging in nature from classical to maximally entangled.

5. Evolution of entanglement under dissipation

The decoherence of quantum systems is one of the major issues in quantum information processing. Understanding and controlling decoherence is a key step in building quantum information processors. We take up here the decoherence in two-mode quantum systems modeled via the Master Equation approach.

The time evolution for a general two-mode state in a dissipative thermal bath is given by the Master Equation [43]

$$\begin{aligned}\frac{d\rho}{dt} &= \frac{\gamma}{2}(N+1)(2a_1\rho a_1^\dagger - a_1^\dagger a_1\rho - \rho a_1^\dagger a_1) \\ &\quad + \frac{\gamma}{2}N(2a_1^\dagger\rho a_1 - a_1a_1^\dagger\rho - \rho a_1a_1^\dagger) \\ &\quad + \frac{\gamma}{2}(N+1)(2a_2\rho a_2^\dagger - a_2^\dagger a_2\rho - \rho a_2^\dagger a_2) \\ &\quad + \frac{\gamma}{2}N(2a_2^\dagger\rho a_2 - a_2a_2^\dagger\rho - \rho a_2a_2^\dagger) \quad (28)\end{aligned}$$

where we have assumed that the two modes of the system are interacting with two different (independent) baths. The two baths have the same temperature given by the average thermal photon number N. The decay constants for the modes is given by γ and has been assumed to be the same.

The Master Equation given in Eq. (28) gives us the evolution of any general two mode state. We are interested in the time evolution of a specific set of states, namely Gaussian states. As we have seen in the previous section, a Gaussian state can be described completely by its variance matrix (and averages). We obtain the equations of motion for the variance matrix from the above Master Equation

$$V(t) = X(t)(V(0) - N' I_d)X(t) + N' I_d \tag{29}$$

where $V(0)$ is the variance matrix of the system state at time $t = 0$, I_d is a 4×4 identity matrix, N' is a constant dependent upon the bath temperature and X is

$$X(t) = \begin{pmatrix} e^{-\gamma t} & 0 & 0 & \\ 0 & e^{-\gamma t} & 0 & 0 \\ 0 & 0 & e^{-\gamma t} & 0 \\ 0 & 0 & 0 & e^{-\gamma t} \end{pmatrix} \tag{30}$$

We now turn to the entanglement properties of two-mode Gaussian states. It has been shown by Simon [44] that the positivity of the partially transposed density matrix is a necessary and sufficient condition for the separability of any two-mode Gaussian state. Given a variance matrix V corresponding to some Gaussian state, let $\tilde{V}$ be the ‘variance matrix’ after the partial transposition. Then the necessary and sufficient condition for the state to be separable is

$$\tilde{V} + \frac{i}{2}\beta \geq 0 \tag{31}$$

where β is defined in Equation (18). Based on this result, a quantitative measure of entanglement can be constructed. A simple measure is the amount by which $\tilde{V} + \frac{i}{2}\beta$ turns negative. Further, if the smallest symplectic eigen value of $\tilde{V}$ is n_- we can define the logarithmic negativity measuring entanglement quantitatively as

$$E = \max\{0, -\ln(2n_-)\} \tag{32}$$

Let us now consider the vacuum state of the two-mode field given by the variance matrix

$$V_0 = \frac{1}{2}\begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix} \tag{33}$$

The squeezing transformations (which are noncompact, canonical transformations), that we consider for each mode are

$$S_1 = \begin{pmatrix} e^{-\frac{\lambda 1}{2}} & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & e^{\frac{\lambda 1}{2}} & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix},$$

$$S_2 = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & e^{-\frac{\lambda 2}{2}} & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & e^{\frac{\lambda 1}{2}} \end{pmatrix}. \tag{34}$$

Where λ_1 and λ_2 correspond to squeezing parameters for the first and second mode respectively. We will typically squeeze both the modes via a transformation $S(\lambda_1, \lambda_2) = S_1 S_2$ acting on the variance matrix as $V \rightarrow SVS^T$.

A one parameter family of passive symplectic transformation (belonging to the maximally compact subgroup $U(2)$ of $Sp(4,R)$) that we will use in our calculations is given by

$$R(\theta) = \begin{pmatrix} \cos\theta & 0 & 0 & -\sin\theta \\ 0 & \cos\theta & -\sin\theta & 0 \\ 0 & \sin\theta & \cos\theta & 0 \\ \sin\theta & 0 & 0 & \cos\theta \end{pmatrix} \tag{35}$$

Beginning with the vacuum state, we can squeeze it by the application of the squeezing transformation S and entangle it via the passive transformation $R(\theta)$. It turns out that maximum entanglement is obtained when we use $R(\pi/4)$. Furthermore, we consider the case with $\lambda_1 = \lambda_2$ i.e equal amount of squeezing in both the modes. This gives us the final variance matrix :

$$V_{SR} = \frac{1}{2}\begin{pmatrix} \cosh\lambda & 0 & 0 & -\sinh\lambda \\ 0 & \cosh\lambda & -\sinh\lambda & 0 \\ 0 & -\sinh\lambda & \cosh\lambda & 0 \\ -\sinh\lambda & 0 & 0 & \cosh\lambda \end{pmatrix} \tag{36}$$

where λ is the squeezing parameter.

To see the amount of entanglement in this variance matrix we compute the eigen values of $\tilde{V} + \frac{i}{2}\beta$. The smallest eigen value turns out to be $\frac{1}{2}(e^{-\lambda} - 1)$, which is always negative for positive values of λ. Further this negativity increases with increasing values of λ. Thus for these states the entanglement is directly proportional to the amount of squeezing and the squeezing parameter of the original state gives a measure of the entanglement of the final state after the implementation of the passive transformation $R(\pi/4)$. It is worth emphasizing here that this passive transformation has converted nonclassicality, which was present in the form of squeezing, into entanglement.

Next we ask the question as to what happens to this entanglement if a thermal bath is introduced? We choose to do this in two different ways:

Case 1: In this case, we consider a two-mode entangled state as discussed above and subject it to dissipation via a thermal bath. We then ask the question how entanglement decays in time. We compute the final variance matrix at time T using Equation (29) to obtain

$$\begin{aligned} V_{SRT} &= X(T)(RSV(0)S^T R^T \\ &\quad -N' I_d)X(T) + N' I_d \end{aligned} \tag{37}$$

Case 2: In this case after squeezing we switch on the bath and allow the state to evolve for a time T and then entangle via R. We call the final variance matrix in this case as V_{STR} given by

$$\begin{aligned} V_{STR} &= R(X(T)(SV(0)S^T - N' I_d)X(T) \\ &\quad + N' I_d)R^T \end{aligned} \tag{38}$$

It turns out that these two variance matrices have the same amount of entanglement at all times. Actually, it turns out that $V_{SRT} + \frac{i}{2}\beta$ and $V_{STR} + \frac{i}{2}\beta$ possess an identical spectrum. Thus we conclude that it does not matter if we entangle first and switch on the dissipative bath later or if we reverse the process. In case 1, dissipation acts on an entangled state while in the case 2 dissipation acts on a state which is mode-squeezed but separable. Under a dissipative evolution, one would have expected that the inter-mode quantum correlations present in the entangled case are more fragile than intra-mode correlations present in the mode-squeezed state. However, we find that they both decay in the same way. This means that single mode squeezing is as sensitive to dissipation as is entanglement. We have shown this for a special case with certain values of the parameters. In general the outcome will depend upon the details, the amounts of squeezing in each mode and so on.

6. Continuous variable quantum cryptography

Quantum cryptography using quantum systems with infinite dimensional Hilbert spaces is becoming increasingly important [32,45–49]. Such systems are in general referred to as continuous variable (CV) systems and can be described using bosonic modes of the radiation field. In quantum optics, bosonic modes are generated in states with Gaussian statistics. Quantum cryptographic schemes use intrinsic properties of quantum systems to ensure the protection of random number keys. The security of such schemes against attack by an eavesdropper (Eve) relies on the fact that quantum measurement inevitably disturbs the system and also on the fact that for single quanta such as a photon, simultaneous measurements of noncommuting variables is forbidden. If the information is randomly encoded between noncommuting variables of a stream of single photons, Eve will be forced to guess which observable to measure for each photon. On average, Eve will guess wrong half the time and reveal herself through the back action of the measurement to the sender (Alice) and the receiver (Bob).

Quantum key distribution (QKD) refers to the distribution of secret information between a sender (Alice) and a receiver (Bob) via an optical channel. The key that Alice and Bob share has to be kept secret from an eavesdropper (Eve) and this can be achieved without leaking any secret key information. This unconditional security cannot be achieved by classical cryptographic schemes and therein lies the power of quantum cryptography. Further, it has been shown that the presence of entanglement in the quantum state distributed between Alice and Bob is a necessary precondition for any secure QKD protocol [50]. QKD can be implemented with current photonic technology, hence its popularity as compared to other quantum information protocols. A standard test of secure QKD is to check for optimal entanglement witnesses (these are observables that detect entanglement), given a set of local operations and a corresponding joint classical probability distribution. An example of such an entanglement witness is the violation of Bell's inequalities [51]. Standard QKD protocols (such as the BB84 protocol proposed by Bennett and Brassard [52] and their variants) use single photons or photon pairs for secure communication between Alice and Bob. These protocols have been proved to be unconditionally secure if implemented using a perfect single photon source. The quantum information in these communication schemes is encoded as pairs of canonical variables such as the polarization or relative phases of single-photon superposition states. Hence the maximum achievable information transfer rate of such schemes is limited to one bit per photon. Higher key distribution rates (higher than one bit per photon) are in principle possible in continuous variable multiphoton systems where the information is encoded in the amplitude and phase quadratures of coherent states or squeezed states. It has been suggested that single-photon CV-QKD using position and momentum observables can increase information transfer rate by encoding more than one bit per photon. The advantages of single-photon CV-QKD over quadrature-based CV-QKD is the elimination of local oscillators required in homodyne detection and the decoupling of channel loss from quantum correlations. The feasibility of such schemes has been experimentally demonstrated using spatial coordinates of single photons and pairs of entangled photons generated by parametric down-conversion.

Another major difference between CV-QKD protocols and standard QKD protocols is the use of homodyne measurements (where the quadrature amplitude of the signal is measured, which is a continuous variable) instead of photon-counting measurements. CV-QKD protocols do not require single photon technology as they only require standard off-the-shelf telecom components such as diode lasers, electro-optics modulators and PIN photodiodes. However, CV-QKD protocols require elaborate classical error correction algorithms to efficiently extract secret bits from correlated continuous variables.

Current schemes to use CV for quantum key distribution (QKD) use nonclassical light (light with Gaussian statistics) such as squeezed light or pairs of light beams that are correlated for two different quadrature components (the so-called "EPR" beams). These amplitude and phase quadratures are analogous to the position and momentum for a light mode and are hence continuous conjugate variables. Simultaneous measurements of these noncommuting observables can be made in different ways, for example, by using a beam splitter and then making homodyne measurements on each beam. The information that is finally obtained is limited by the generalized uncertainty principle for simultaneous measurements. If an ideal measurement of one quadrature component produces a result with a signal to noise ratio

$$(S/N)^{\pm} = \frac{V_s^{\pm}}{V_n^{\pm}} \tag{39}$$

where $V_s^{\pm}$ and $V_n^{\pm}$ are respectively the signal and noise power of the amplitude (+) or phase (-) quadrature at a particular rf frequency with respect to the optical carrier. A simultaneous measurement of both quadratures cannot exceed a signal to noise ratio of

$$(S/N)_{sim}^{\pm} = \left(\frac{\eta^{\pm} V_s^{\pm}}{\eta^{\pm} V_n^{\pm} + \eta^{\mp} V_m^{\pm}} S/N^{\pm} \right) \tag{40}$$

where the quantum noise that is always added when dividing the mode is $V_m^{\pm}$, the splitting ratio is $\eta^{\pm}$ and $\eta^{+} = 1 - \eta^{-}$. For a coherent beam $V_n^{\pm} = 1$. For a classical light beam ($V_n^{\pm} >> 1$) the penalty is negligible but for a coherent beam the signal to noise ratio for both quadratures is halved when the splitting ratio is half. The Hartley-Shannon law applies to Gaussian channels wherein, if information of a fixed bandwidth is sent down a channel at a rate corresponding to the channel capacity and the signal to noise ratio is reduced, errors will inevitably appear at the receiver. Thus any attempt by an eavesdropper to make simultaneous measurements will introduce errors in the transmission of the information. While usage of squeezed states are fundamentally interesting, coherent-state protocols are in practice easier to achieve. CV-QKD using coherent states over a 1-km optical fiber path has been experimentally demonstrated at a 1.55 μm communication wavelength. It has also been shown that there is no need for squeezed light and that an equivalent level of security for CV-QKD can be obtained by generating and transmitting random distributions of coherent states. The performance of QKD is limited by the presence of transmission loss: in the beam-splitting attack scenario, Eve replaces the lossy transmission path with a lossless one and a beam splitter. She then gets signals corresponding to the loss without disturbing the signal. At first, above an existing 50% loss (3 dB loss), it seems impossible to distill the secret key in this coherent-state scheme since Eve can get a stronger signal than Bob. However, since signal information depends on the measurement, the coherent-state protocol can provide a secure key by postselection (i.e conditional use of measurement results) even in the presence of higher loss. In addition to the loss, excess Gaussian noise is always imposed on the quadrature distribution. Since any excess noise tapers off when the state falls into vacuum at high loss, the excess noise added by Eve near Alice's side will disappear at Bob's side for a long transmission distance and eavesdropping will not be detected. Hence CV-QKD protocols using coherent states cannot work for arbitrarily long transmission distance in the presence of excess noise. There have been several experimental demonstrations of key distribution at high repetition rates based on Gaussian modulation of coherent or squeezed states of light implemented with homodyne detection.

In a quantum communication channel, interaction with the environment leads to noisy transformations of the quantum state. In general Gaussian statistics are preserved under such noisy transformations. Hence in a single-mode Gaussian channel, the coupling with the external environment is a completely positive trace-preserving map that transforms Gaussian states into Gaussian states and does not lead to the creation of correlations among the bosonic modes. In the framework of CV-QKD, Gaussian attacks have been identified as the most powerful collective attacks and single-mode Gaussian channels between users can be modeled as the effect of such collective Gaussian attacks. There have been several studies examining the quantum cryptographic security of CV schemes based on coherent light and squeezed light, and it has been shown that while the coherent light scheme is inferior to single quanta schemes, the squeezed light scheme provides in principle equivalent security. However, it is essential that the coherence between the two squeezed modes is destroyed.

Coherent state CV-QKD

In a coherent state CV-QKD protocol, random values are encoded in the complex amplitude of the coherent state signal. Encoding schemes are based on either the Gaussian modulation or the discrete modulation format. In the Gaussian modulation format, information is continuously encoded in the two-dimensional phase space of the coherent state $|\alpha\rangle$ with complex amplitude α. For a homodyne measurement, a single bit value is encoded, whereas a two-bit value is encoded for a heterodyne measurement (called the doubly encoding scheme). In the discrete modulation setup, the signal is phase modulated by a fixed amount depending on the randomly chosen basis and bit value. Coherent states are efficiently transferred via an optical fiber or via free-space propagation. The coherent state decoding scheme depends on whether the encoding has been performed using Gaussian modulation or discrete modulation. For the discrete modulated case, Bob tries to read out the discrete variable encoded by Alice. In the case of Gaussian modulation, Bob uses a prefixed decoding scheme. As an illustration, Bob measures the x component of the complex amplitude (a continuous variable). Bob then interprets the measurement outcome x as the bit value 0 or 1 if n is even or odd, where $(2n-1)c < x \leq (2n+1)c$ and $n = \ldots -3, -2, -1, 0, 1, 2, 3, \ldots$ and c is a positive constant. Decoding for the doubly encoding scheme is done in the same way but with respect to both x and p.

In the homodyne measurement setup, either the x or p component of the complex amplitude is randomly read out. In the heterodyne measurement setup, the incoming light is split up and both the x and p components of the complex amplitude are randomly read out. The splitting enlarges the variance of the statistic of the measurement outcomes.

Security of coherent state CV-QKD protocols

There has been a lot of work on the security of single Gaussian beam protocols against any individual attack. Such protocols are those that do not transmit simultaneously several quantum-correlated modes of the electromagnetic field. In a single Gaussian beam QKD protocol, Alice randomly modulates a Gaussian beam and sends it to Bob through a Gaussian noisy channel. Both phase and amplitude are modulated with Gaussian random numbers which allows for an optimal information transfer rate. Bob then measures either the phase or amplitude of the received beam and informs Alice about the measurement performed. Alice and Bob now have two correlated sets of Gaussian variables, from which they can extract a common secret string of bits. Since such a protocol does not require squeezed light, it can be implemented by sending light pulses in a low-loss optical fiber. It has been shown that in such a scheme, half of the information sent by Alice will be lost and that the protocol is secure for losses smaller than 3 dB. Unconditional security of coherent state protocols remains an open question.

Squeezed state CV-QKD protocols

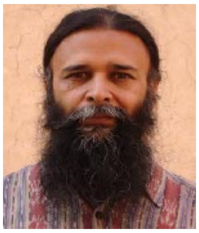
Hillery [53] was one of the first to investigate the utility of squeezed states for QKD and the security of this protocol under two kinds of eavesdropper attacks: intercept-resend attacks and quantum-tap attacks. Other entanglement based quantum cryptographic schemes have been proposed that are based on correlations of the quadratures of two-mode squeezed states. [29,54,55]. Further, it has been shown that when different types of attacks are considered, there is a tradeoff between the extractable classical information and the disturbance of signals passed on to the receiver. Enhanced security requires high level of squeezing and low levels of loss in the channel [31,56,57]. Apart from these single-Gaussian non-collective attacks, a continuous variable analog of the original BB84 protocol has been considered and a detailed proof of absolute theoretical security worked out [58]. Much work needs to be done to work out the real experimental implementations of such theoretical squeezed state cryptographic protocols. Quantum cryptography using continuous variables has been described in detail in recent reviews [33,59,60].

Received 03 June 2009.

References

1. R. Simon, N. Mukunda, and B. Dutta, Phys. Rev. A **49**, 1567 (1994).
2. Arvind, B. Dutta, N. Mukunda, and R. Simon, Phys. Rev. A **52**, 1609 (1995).

3. G. Adesso, A. Serafini, and F. Illuminati, Phys. Rev. Lett. **92**, 087901 (2004).
4. A. Botero and B. Reznik, Phys. Rev. A **67**, 052311 (2002).
5. T. Opatrný, N. Korolkova, and G. Leuchs, Phys. Rev. A **66**, 053813 (2002).
6. A. Serafini, F. Illuminati, M. G. A. Paris, and S. D. Siena, Phys. Rev. A **69**, 022318 (2004).
7. G. Giedke, M. M. Wolf, O. Krˋuger, R. F. Werner, , and J. I. Cirac, Phys. Rev. Lett. **91**, 107901 (2003).
8. R. Filip and L. M. Jr., Phys. Rev. A **66**, 044309 (2002).
9. J. Fiurášek, Phys. Rev. A **66**, 012304 (2002).
10. S. D. Bartlett, B. C. Sanders, S. L. Braunstein, and K. Nemoto, Phys. Rev. Lett. **88**, 097904 (2002).
11. Arvind, B. Dutta, N. Mukunda, and R. Simon, Pramana Jr. of Physics **45**, 471 (1995).
12. S. L. Braunstein and H. J. Kimble, Phys. Rev. Lett. **80**, 869 (1998).
13. D. Gottesman, A. Kitaev, and J. Preskil, Phys. Rev. A **64**, 012310 (2001).
14. F. Grosshans, G. V. Assche, J. Wenger, R. Brouri, N. J. Cerf, and P. Grangier, Nature **421**, 238 (2002).
15. J. Harrington and J. Preskill, Phys. Rev. A **64**, 062301 (2001).
16. G. Giedke and J. I. Cirac, Phys. Rev. A **66**, 032316 (2002).
17. J. Eisert, S. Scheel, and M. B. Plenio, Phys. Rev. Lett. **89**, 137903 (2002).
18. J. Fiurášek, L. M. Jr., and R. Filip, Phys. Rev. A **67**, 022304 (2003).
19. V. Josse, A. Dantan, A. Bramati, and E. Giacobino, Journal of Optics B **6**, 532 (2004).
20. R. Schnabel, W. P. Bowen, N. Treps, B. Buchler, T. C. Ralph, P. K. Lam, , and H. A. Bachor, Optics and Spectroscopy **94**, 651 (2003).
21. W. Xiang-bin, Phys. Rev. A **66**, 064304 (2002).
22. M. G. A. Paris, Phys. Rev. A **64**, 014304 (2002).
23. W. P. Bowen, R. Schnabel, P. K. Lam, and T. C. Ralph, Phys. Rev. Lett. **90** (2003).
24. W. P. Bowen, N. Treps, R. Schnabel, and P. K. Lam, Phys. Rev. Lett. **89**, 253601 (2002).
25. B. Kraus, K. Hammerer, G. Giedke, and J. I. Cirac, Phys. Rev. A **67**, 042314 (2003).
26. M. M. Wolf, J. Eisert, and M. B. Plenio, Phys. Rev. Lett. **90**, 047904 (2003).
27. S. Scheel and D.-G. Welsch, Phys. Rev. A **64**, 063811 (2001).
28. B.-G. Englert and K. Wíodkiewicz, Phys. Rev. A **65**, 054303 (2002).
29. T. C. Ralph, pra **61**, 103031 (2000).
30. T. C. Ralph, pra **62**, 062306 (2000).
31. F. Grosshans and P. Grangier, prl **88**, 057902 (2002).
32. S. Pirandola, S. Mancini, S. Lloyd, and S. L. Braunstein, naturephy **4**, 726 (2008).
33. X. Wang, T. Hiroshima, A. Tomito, and M. Hayashi, phyrep **448**, 1 (2007).
34. F. Grosshans and N. J. Cerf, prl **92**, 047905 (2004).
35. R. Namiki and T. Hirano, pra **72**, 024301 (2005).
36. J. Lodewyck, M. Bloch, R. Garcia-Patron, S. Fossier, E. Karpov, E. Diamanti, T. Debuisschert, N. J. Cerf, R. Tualle-Brouri, S. W. McLaughlin, et al., pra **76**, 042305 (2007).
37. M. Heid and N. Lutkenhaus, pra **76**, 022313 (2007).
38. L. Zhang, C. Silberhorn, and I. A. Walmsley, prl **100**, 110504 (2008).
39. S. Pirandola, S. L. Braunstein, and S. Lloyd, prl **101**, 200504 (2008).
40. D. F. Walls and G. J. Milburn, *Quantum Optics* (Springer-Verlag, 1994).
41. P.Meystre and M. S. III, *Elements of Quantum Optics* (Springer-Verlag, 2002).
42. S. M. Barnett and P. M. Radmore, *Methods in Theoretical Quantum Optics* (Clarendon Press, 1997).
43. G. S. Agarwal, Phys. Rev. A **4**, 739 (1971).
44. R. Simon, Phys. Rev. Lett. **84**, 2726 (2000).
45. F. C. et al, njp **8**, 310 (2006).
46. R. Garcia-Patron and N. J. Cerf, prl **97**, 190503 (2006).
47. J. Eisert and M. B. Plenio, Int. J. Quantum Inf. **1**, 479 (2003).
48. N. J. Cerf, M. Levy, and G. V. Assche, pra **63**, 523111 (2001).
49. F. Grosshans, G. V. Asschet, J. Wenger, R. Brouri, N. J. Cerf, and P. Grangier, Nature **421**, 238 (2003).
50. M. Curty, M. Lewenstein, and N. Lutkenhaus, prl **92**, 217903 (2004).
51. A. K. Ekert, Phys. Rev. Lett. **67**, 661 (1991).
52. C. H. Bennett and G. Brassard, Proc. IEEE Int. Conference on Computers, Systems and Signal Processing, IEEE, Bangalore, India pp. 175–179 (1984).
53. M. Hillery, pra **61**, 223091 (2000).
54. O. Cohen, Helv. Phys. Acta **70**, 710 (1997).
55. S. F. Pereira, Z. Y. Ou, and H. J. Kimble, pra **62**, 042311 (2000).
56. M. D. Reid, pra **62**, 062308 (2000).
57. C. Silberhorn, T. C. Ralph, N. Lutkenhaus, and G. Leuchs, prl **89**, 167901 (2002).
58. D. Gottesman and J. Preskill, pra **63**, 1 (2001).
59. S. L. Braunstein and A. K. Pati, *Quantum information theory with continuous variables* (Kluwer Academic, Dordrecht, 2003).
60. S. L. Braunstein and P. van Loock, Rev. Mod. Phys. **77**, 513 (2005).



Dr Arvind is a theoretical physicist whose research interests encompass quantum optics, foundations of quantum mechanics, quantum information theory and physics education. He did his PhD from IISc Bangalore and a postdoctoral stint at Carnegie Mellon university USA. He has been on the faculty of Guru Nanak Dev University, Amritsar and IIT-Madras. He is currently an Associate Professor (Physics) at the Indian Institute of Science Education & Research (IISER) Mohali.