Fortschr. Phys. **51**, No. 4–5, 449 – 457 (2003) / **DOI** 10.1002/prop.200310061

About the use of entanglement in the optical implementation of quantum information processing

M. G. A. Paris[1,*], **G. M. D'Ariano, P. Lo Presti,** and **P. Perinotti**

Quantum Optics & Information Group, INFM Udr Pavia, Italy

Received 13 May 2002, accepted 21 May 2002
Published online 30 April 2003

We review some applications of entanglement to improve quantum measurements and communication, with the main focus on the optical implementation of quantum information processing. The evolution of continuos variable entangled states in active optical fibers is also analyzed.

1 Introduction

Quantum information theory has developed dramatically over the past few years, driven by the prospects of quantum-enhanced communication, measurements and computation systems. Most of these concepts were initially developed for discrete quantum variables, in particular quantum bits, which have become the symbol of quantum information theory. Recently, however, much attention has been devoted to investigating the use of continuous variables (CV) in quantum information processing. Continuous-spectrum quantum variables may be easier to manipulate than quantum bits in order to perform various quantum information processes [1]. This is the case of Gaussian state of light, *e.g.* squeezed beams, by means of linear optical circuits [2]. Using CV one may carry out quantum teleportation [3] and quantum error correction. The concepts of quantum cloning and entanglement purification [4] have also been extended to CV, and secure quantum communication protocols have been proposed [5].

The key ingredients of quantum information is entanglement, which has become the essential resource for quantum computing, teleportation, and cryptographic protocols. Recently, entanglement has been proved as a valuable resource for improving optical resolution [6], spectroscopy [7], quantum interferometry [8], and has shown to be a crucial ingredient for making the tomography of a quantum device [9].

In this paper we review some applications of CV entangled states to improve quantum measurements [10] and communication in the optical implementation of quantum information processing. In Sect. 2 we analyze the estimation of a displacing amplitude, also in presence of noise, and the case of binary discrimination between two unitary operations. In Sect. 3 we study the role of entanglement in improving interferometric measurements, and show that an optimized two-mode interferometer requires an entangled input state, with ultimate scaling that may be achieved using twin-beam in a Mach-Zehnder interferometer. In Sect. 4, a secret key quantum criptographic scheme based on entangled twin beam and heterodyne detection is analyzed and shown to be effective both for binary quantum key distribution and as complex alphabet trasmission channel. Finally, in Sect. 5 we study the evolution of entangled twin-beam of light in a pair of active optical fibers, in order to evaluate the degradation rate of entanglement and determine a threshold value for the interaction time, above which the state become separable. Sect. 6 closes the paper summarizing results.

* Corresponding author E-mail: paris@unipv.it URL: www.qubit.it/~paris

2 Entanglement in quantum measurements

The measurement problem we are going to consider is the following: suppose one is given a quantum device, which perform an unknown unitary transformation chosen from a given set, and wants to discriminate which transformation (within the set) has been actually performed. The unitaries are labelled by a parameter, such that the discrimination is equivalent to the estimation of the value of the parameter. The inference strategy is that of preparing an input probe state and then measuring the outgoing signal, such to discriminate among the possible output states. In order to achieve the most accurate discrimination one has to optimize over the possible input signals and the possible output detection schemes. The question we want to answer is whether or not entanglement is convenient in such discrimination, i.e. if it is better to use single-mode probe, or to place the device such to act on a subsystem of a bipartite entangled systems, and then allowing for a measurement on both the modes. In the following we consider the estimation of a displacing amplitude, also in presence of noise, and the case of binary discrimination, i.e. when our device may perform a transformation chosen from a binary set $\{U_1, U_2\}$.

2.1 Estimation of amplitude

Let us consider the problem of estimating the amplitude of a displacement applied to a mode of the radiation field in the phase space, i. e. the parameter $\alpha \in C$ of the transformation $\rho \to \rho_\alpha = D(\alpha)\rho D^\dagger(\alpha)$, where $D(\alpha) = \exp(\alpha a^\dagger - \overline{\alpha} a)$. This transformation can be easily accomplished by a high trasmittivity beam splitter and an intense laser beam. For unentangled ρ, the estimation of α isotropic on the complex plane is equivalent to the optimal joint measurement of position and momentum, which, as well known, is affected by a unavoidable minimum noise of 3dB [11]. Here, the optimal state (for fixed minimum energy) is the vacuum, and the corresponding conditional probability of measuring z given α is $p(z|\alpha) = \pi^{-1} \exp\left[-|z-\alpha|^2\right]$.

Now, consider the case in which the estimation is made with $D(\alpha)$ acting on the entangled state $|x\rangle\rangle = \sqrt{1-x^2}\sum_p x^p |p\rangle|p\rangle$, i.e. the twin-beam state obtained by parametric downconversion of the vacuum, with $x \leq 1$ (without loss of generality we may assume x as real) and number of photons given by $N = 2x^2/(1-x^2)$. In this case, the optimal measurement is described by the POVM $|z\rangle\rangle\langle\langle z|$ of eigenvectors $|z\rangle\rangle = D_j(z)\sum_p |p\rangle|p\rangle$ (j may be either a or b) of $Z = a + b^\dagger$ with eigenvalue z (this is just a heterodyne measurement), now achieving $p(z|\alpha) = (\pi\Delta_x^2)^{-1} \exp\left[-\Delta_x^{-2}|z-\alpha|^2\right]$, with variance $\Delta_x^2 = \frac{1-x}{1+x}$ that, in principle, can be decreased at will with the state $|x\rangle\rangle$ approaching a state an eigenstate of Z (by increasing the gain of the downconverter).

Remarkably, measurement strategies employing entanglement are robust against decoherence induced by noise, i.e. they remain convenient also when the estimation is performed with the channel, before and after the unknown transformation, affected by noise. Let us reconsider the problem of estimating the displacement in the case of Gaussian noise, which maps states as follows $\rho \to \Gamma_{\overline{n}}(\rho) \doteq \int_C \frac{\mathrm{d}^2\gamma}{\pi\overline{n}} \exp\left[-|\gamma|^2/\overline{n}\right] D(\gamma)\rho D^\dagger(\gamma)$. The variance $\overline{n}$ of the noise is usually referred to as "mean thermal photon number". The case of Gaussian noise is simple, since one has the composition law $\Gamma_{\overline{n}} \circ \Gamma_{\overline{m}} = \Gamma_{\overline{n}+\overline{m}}$, and $\Gamma_{\overline{n}}\left[D(\alpha)\rho D^\dagger(\alpha)\right] = D(\alpha)\Gamma_{\overline{n}}(\rho)D^\dagger(\alpha)$. Therefore, if the measurement is made on the entangled state $|x\rangle\rangle$ one can easily derive a Gaussian probability distribution with variance $\sigma_2^2 = \Delta_x^2 + 2\overline{n}_T$, where $\overline{n}_T$ is the total Gaussian noise before and after the displacement $D(\alpha)$, and the noise is doubled since it acts indenpently on the two entangled beams. On the other hand, in the measurement scheme with unentangled input (remind that the optimal probe is the vacuum), one has $\sigma_1^2 = 1 + \overline{n}_T$. One concludes that the entangled input is no longer convenient if $\sigma_2^2 < \sigma_1^2$, i.e. above one thermal photon $\overline{n}_T = 1$ of noise. This is exactly the threshold of noise above which the entanglement is totally degraded to a separable state [12], and therefore the quantum capacity of the noisy channel vanishes. Since at optical frequencies $\bar{n}_T$ is a small quantity we conclude that entanglement is convenient also in presence of decoherence induced by noise.

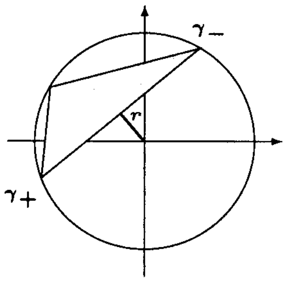

Fig. 1 r is the minimum distance between the origin and the polygon K.

2.2 Binary discrimination

Let us suppose that we have to distinguish among two unitaries U_1 and U_2. Given an input state $|\psi\rangle$, one optimizes over the possible measurements, and the minimum error probability in discriminating $U_1|\psi\rangle$ and $U_1|\psi\rangle$ [13] is given, in a Bayesian approach, by

$$P_E = \frac{1}{2}\left[1 - \sqrt{1 - |\langle\psi|U_2^\dagger U_1|\psi\rangle|^2}\right] , \tag{1}$$

so that one has to minimize the overlap $|\langle\psi|U_2^\dagger U_1|\psi\rangle|$ with a suitable choice of $|\psi\rangle$. Chosing as a basis the eigenvectors $\{|j\rangle\}$ of $U_2^\dagger U_1$, and writing $|\psi\rangle = \sum_j \psi_j|j\rangle$, we define $z_\psi \doteq \langle\psi|U_2^\dagger U_1|\psi\rangle = \sum_j |\psi_j|^2\,\mathrm{e}^{i\gamma_j}$, where $\mathrm{e}^{i\gamma_j}$ are the eigenvalues of $U_2^\dagger U_1$. The normalization condition for $|\psi\rangle$ is $\sum_j |\psi_j|^2 = 1$, so that the subset $K(U_2^\dagger U_1) \subset C$ described by z_ψ for varying $|\psi\rangle$ is the convex polygon having the points $\mathrm{e}^{i\gamma_j}$ as vertices. The minimum overlap $r(U_2^\dagger U_1) \doteq \min_{||\psi||=1} |\langle\psi|U_2^\dagger U_1|\psi\rangle|$ is the distance of $K(U_2^\dagger U_1)$ from $z = 0$. This geometrical picture indicates in a simple way what is the best one can do in discriminating U_1 and U_2: if K contains the origin then the two unitaries can be exactly discriminated, otherwise one has to find the point of K nearest to the origin, and the minimum probability of error is related to its distance from the origin [10]. Once the optimal point in K is found, the optimal states ψ are those corresponding to that point through the expression of P_E. If $\Delta(U_2^\dagger U_1)$ is the angular spread of the eigenvalues of $U_2^\dagger U_1$ (referring to Fig.1, it is $\Delta = \gamma_+ - \gamma_-$), from Eq. (1) for $\Delta < \pi$ one has $P_E = (1 - \sqrt{1 - \cos^4 \frac{\Delta}{2}})/2$ whereas for $\Delta \geq \pi$ one has $P_E = 0$ and the discrimination is exact. Given a pair U_1 and U_2 of non exactly discriminable unitaries, one is interested in understanding whether or not an entangled input state could be of some use. The answer is at first negative. In fact, using entanglement translates the problem into the one of distinguishing between $U_1 \otimes I$ and $U_2 \otimes I$, thus one has to analyze of the polygon $K(U_2^\dagger U_1 \otimes I)$. Since $U_2^\dagger U_1 \otimes I$ has the same eigenvalues as $U_2^\dagger U_1$, the polygons $K(U_2^\dagger U_1 \otimes I)$ and $K(U_2^\dagger U_1)$ are exactly the same, so that they lead to the same minimum probability of errror. The situation changes dramatically if N copies of the unitary transformation are used (multiple use of the channel). In this case one has to compare the "performance" of $K(U_2^\dagger U_1)$ to the one of $K((U_2^\dagger U_1)^{\otimes N})$. Since $\Delta((U_2^\dagger U_1)^{\otimes N}) = \min\{N \times \Delta(U_2^\dagger U_1), 2\pi\}$, it is clear that there will be an $\bar{N}$ such that $U_1^{\otimes N}$ and $U_2^{\otimes N}$ will be exactly discriminable, i.e. entanglement makes possible the exact discrimation of *any* pair of unitary transformation.

3 Entanglement in quantum interferometry

In this section we want to emphasize the role of entanglement in improving interferometric measurements. In particular, we show that an optimized two-mode interferometer requires an entangled input state, and that the ultimate scaling may be achieved using feasible CV entangled states (i.e. twin-beam) in a Mach-Zehnder interferometer.

A general interferometric scheme consists of a source which prepares a state ϱ_0, an intermediate apparatus which may or may not act a perturbation, and a detector described by a generic POVM Π. In a Mach-Zehnder-like interferometer the perturbation is described by the unitary operator $U_\phi = \exp\{\mathrm{i}\phi J_x\}$, where we used the

Schwinger representation $J_+ = a^\dagger b$, $J_- = ab^\dagger$, $J_z = \frac{1}{2}(a^\dagger a - b^\dagger b)$, $[J_z, J_\pm] = \pm J_\pm$, $[J_+, J_-] = 2J_z$ in terms of two modes of the interferometer. The two possible interferometric outputs are thus given by ϱ_0, if no perturbation occurs, and $\varrho_\phi = U_\phi\, \varrho_0 U_\phi^\dagger$, in case of perturbation. Depending on the outcome of the measurement one decides for the most probable hypothesis on the state of the system. Interferometry is thus equivalent to a binary decision problem, and the corresponding POVM is binary, i.e. the possible outcomes are two [14]. Optimization of both the input signal and the detection scheme has two main goals: i) to maximize the probability of revealing a perturbation, when it occurs, and ii) to minimize the value of the smallest perturbation that can be effectively detected. If ϱ_0 and ϱ_ϕ are orthogonal the discrimination is trivial. In general, however, the states are not orthogonal and one has to apply an optimization scheme. Since interferometric schemes are frequently used for detecting low-rate events, we use, rather than Bayesian, the so-called Neyman-Pearson (NP) detection strategy [15], which consists in fixing the false-alarm probability Q_0—the probability of inferring that the state of the system is ϱ_ϕ while it is actually ϱ_0—and then maximizing the detection probability Q_ϕ, i.e. the probability of a correct inference of the state ϱ_ϕ. The problem is solved by diagonalizing the operator $\varrho_\phi - \mu\varrho_0$, μ (real) playing the role of a Lagrange multiplier accounting for the bound of fixed false alarm probability. The optimal POVM is the one in which Π_ϕ is the projection onto the eigenspaces of $\varrho_\phi - \mu\varrho_0$ relative to positive eigenvalues and $\Pi_0 = I - \Pi_\phi$. If $\varrho_0 = |\psi_0\rangle\langle\psi_0|$ and $\varrho_\phi = |\psi_\phi\rangle\langle\psi_\phi|$ are pure states we have $Q_\phi = \left[\sqrt{Q_0|\kappa|^2} + \sqrt{(1-Q_0)(1-|\kappa|^2)}\right]^2$ (if $0 \le Q_0 \le |\kappa|^2$, Q_ϕ=1, otherwise) where $|\kappa|^2 = |\langle\psi_0|\psi_\phi\rangle|^2 = |\langle\psi_0|U_\phi|\psi_0\rangle|^2$ is the overlap between the two states. The smaller is the overlap, the easier the discrimination. On the contrary, when the overlap approaches 1 one is forced to decrease the detection probability in order to keep the false alarm probability small.

After having determined the optimal POVM, i.e. the optimal detection scheme, the whole setup can be furtherly optimized looking for the best input state, that is a state for which $|\kappa|$ assumes its minimum value $|\kappa|_{\text{min}}$. As we saw in Sect. 2.2, the value $|\kappa|_{\text{min}}$ depends on the eigenvalues of the unitary operator U_ϕ. Since the spectrum of J_x is the set of relative integers, the spectrum of U_ϕ is the discrete subset $\{e^{im\phi}\ ,\ m \in Z\}$ of the unit circle in the complex plane. Apart from the null measure set $\Phi = \{(q/p)\pi\ ,\ q \in 2Z+1\ ,\ p \in Z\}$ of values of ϕ, the spectrum of U_ϕ is dense in the unit circle and its convex hull contains the origin of the complex plane, although there is no couple of diametrically opposed eigenvalues. If $\phi \in \Phi$ then the optimal state is given by a superposition of two eigenstates of V_ϕ with eigenvalues differing by a factor $e^{i\pi}$ [16]. In the general case, the optimal state is any superposition of three or more eigenstates of U_ϕ, such that the polygon with vertices on their eigenvalues encloses the origin of the complex plane. Since $J_x = W^\dagger J_z W$ with $W = \exp\left\{i\frac{\pi}{2} J_y\right\}$, the eigenvectors of U_ϕ are entangled. In fact they are obtained from the eigenstates of $a^\dagger a - b^\dagger b$ (nonclassical states) by the beam-splitter-like transformation $W^\dagger = \exp\{-\frac{\pi}{4}(a^\dagger b - ab^\dagger)\}$ [19]. Actually, these optimal states are far from being practically realizable. However, we have proved that they are entangled, and this suggests to explore the possibility of performing a reliable discrimination by physically realizable entangled states, e.g. twin-beams $|x\rangle\rangle$ [8]. The overlap for the probe prepared in a twin-beam state is given by $\kappa = \langle\langle x|U_\phi|x\rangle\rangle$. After minor algebra we get

$$|\kappa|^2 = \left(1 + \frac{4x^2 \sin^2\phi}{(1-x^2)^2}\right)^{-1} = \left[1 + N(N+2)\sin^2\phi\right]^{-1} .$$

This value is not zero but it can be arbitrarily small depending on the mean photon number of the input state. The sensitivity of the interferometer corresponds to the minimum detectable value ϕ_{min}, which is the minimum value of ϕ such that $Q_\phi/Q_0 = \gamma^* \gg 1/p$, where p is the *a priori* probability of the perturbation. The value of γ^* is fixed by the experimenter and is called *acceptance ratio*. In order to understand its meaning we notice that, if the setup detects a perturbation, the probability that this inference is true is $P(p,\phi) = pQ_\phi/\left[pQ_\phi + (1-p)Q_0\right] = p\gamma^*/\left[p\gamma^* + (1-p)\right]$. Therefore, the greater is γ^*, the nearer is this probability to one. In terms of $|\kappa|$ the condition $Q_\phi/Q_0 = \gamma^* \gg 1/p$ reads as $|\kappa|^2 = 1 - g(Q_0, \gamma^\star)$ with $g(Q_0,\gamma^\star) = Q_0\left[1 + \gamma^\star(1-2Q_0) - 2\sqrt{\gamma^\star(1-Q_0)(1-\gamma^\star Q_0)}\right]$ where $|\kappa|^2$ parametrically depends on

ϕ. Accordingly, the minimum detectable ϕ is given by

$$\phi_{\text{min}} = \arcsin\left(\sqrt{\frac{\Lambda(Q_0,\gamma^\star)}{1-\Lambda(Q_0,\gamma^*)}}\frac{1}{\sqrt{N(N+2)}}\right) \simeq \sqrt{\frac{\Lambda(Q_0,\gamma^\star)}{1-\Lambda(Q_0,\gamma^*)}}\frac{1}{N}\,. \tag{2}$$

Now, we consider twin-beam as input signal of the usual Mach-Zehnder interferometer, where the detection stage consists of a difference photocurrent measurement. The scheme should be feasible, at least in principle, and, as we will see, would approach the ultimate sensitivity bound that has been obtained for the ideal detection. After preparation, the twin-beam enters the interferometer, where is possibly subjected to the action of the unitary U_ϕ. At the output the two beams are detected and the difference photocurrent $D = a^\dagger a - b^\dagger b$ is measured. If no perturbation occurs, then the output state is still a twin-beam, and since $|x\rangle\rangle$ is an eigenstate of D with zero eigenvalue we have a constant zero outcome for the difference photocurrent. On the other hand, when a perturbation occurs the output state is no longer an eigenstate of D, and we detect fluctuations which reveals the perturbation. The false-alarm and the detection probabilities are given by $Q_0 = P(d \neq 0|\text{not } U_\phi) \equiv 0$ and $Q_\phi = P(d \neq 0|U_\phi) = 1 - P(d \equiv 0|U_\phi)$, where the probability of observing zero counts at the output, after the action of U_ϕ, is given by $P(d \equiv 0|U_\phi) = \sum_n \left|\langle\langle n,n|U_\phi|x\rangle\rangle\right|^2$ since the eigenvalue $d = 0$ is degenerate. In this case the false-alarm probability is zero and therefore it is not necessary to introduce an acceptance ratio. The scaling of the minimum detectable perturbation can be obtained directly in term of the detection probability

$$P(d=0|\phi\neq 0) = 1 - \tfrac{1}{2}\phi^2 N^2 + O(\phi^2) \quad\longrightarrow\quad \phi_{\text{min}} \simeq \frac{\sqrt{2Q_\phi}}{N}\,. \tag{3}$$

One can see that a Mach-Zehnder interferometer fed by twin-beam shows a sensitivity that scales with the energy as the ideal scheme. Such scaling does not depend on any parameter but the energy of the input state. This should be compared with the sensitivity of the customary squeezed states interferometry [17], where the same scaling is achieved only for a very precise tuning of the phase of the squeezing. This means that the entanglement-assisted interferometry provides a more stable and reliable scheme.

4 Entanglement in secure communication

In this section, a secret key quantum criptographic scheme based on entangled twin beam and heterodyne detection is analyzed. The scheme can be effectively employed both for binary quantum key distribution and as complex alphabet trasmission channel, and the use of entangled signals results in a decrease of the error probability. A quantum encoding of the secret-key in a cryptographic communication is motivated by the possibility of achieving extensive key-expansion, due to the physical limitations in a quantum-measurement based eavsdropping. Such an idea for a quantum secret-key cryptographic communication was first suggested by Yuen [18]. The secret key is imposed as a random displacement transformation, such that the scheme is secure in principle, i.e. the best strategy for an eavesdropper is just pure guess. Effects of practical imperfections will be taken into account.

4.1 Binary communication

The two values of the bit are encoded in two *quasi*-eigenstates of the heterodyne photocurrent $Z = a + b^\dagger$, i.e. as "0" $\rightarrow |z_0\rangle\rangle_x = D(z_0)|x\rangle\rangle$ and "1" $\rightarrow |z_1\rangle\rangle_x = D(z_1)|x\rangle\rangle$ where $|x\rangle\rangle$ is the twin-beam. The $|x\rangle\rangle$'s (and thus the $|z\rangle\rangle_x$'s) become orthogonal states for $x \rightarrow 1$. We will use the notation $\sigma_0 = |z_0\rangle\rangle_{xx}\langle\langle z_0|$, $\sigma_1 = |z_1\rangle\rangle_{xx}\langle\langle z_1|$.

The criptographic protocol consists in applying a random displacement transformation $D(\alpha)$ to the bit *before* the transmission. The value of α represents the key that should be secretely shared before the transmission. The receiver (Bob) knows the key, and therefore can apply the inverse transformation $D^\dagger(\alpha)$

at the end of the line and then measure the bit. For this task he has to measure a two-value POVM $\{\Pi_0, \Pi_1 \equiv 1 - \Pi_0\}$. The two states are not orthogonal, and therefore such a POVM should be optimized to achieve the minimum error probability $P_E = \frac{1}{2}\mathrm{Tr}\,[\Pi_0\sigma_1 + \Pi_1\sigma_0] = \frac{1}{2}\left[1 - \sum_i U(\lambda_i)\lambda_i\right]$, where λ_i are the eigenvalues of the matrix $\Lambda = \sigma_1 - \sigma_0$, and $U(x)$ denotes the Heaviside step function. Since the two initial states σ_j are pure the solution is well known: the POVM is projective [13] (this is true also for mixed σ's) and the error probability is given by $P_E = \frac{1}{2}\left[1 - \sqrt{1 - |{}_x\langle\langle z_1|z_0\rangle\rangle_x|^2}\right]$, where $|{}_x\langle\langle z_1|z_0\rangle\rangle_x|^2 = \exp\{-|z_0 - z_1|^2(1+N)\}$. For large N or $|z_1 - z_0|$ we have $P_E \simeq 1/4\exp\{-|z_0 - z_1|^2(1+N)\}$. This result should be compared with the analogue scheme based on displaced unentangled states i.e., "0" $\rightarrow |\alpha_0\rangle = D(\alpha_0)|0\rangle$, "1" $\rightarrow |\alpha_1\rangle = D(\alpha_1)|0\rangle$ where $|\alpha_j\rangle$ are single-mode coherent state and $|0\rangle$ denotes the vacuum state. In this case we have $P_E = \frac{1}{2}\left[1 - \sqrt{1 - |\langle\alpha_1|\alpha_0\rangle|^2}\right]$ with $|\langle\alpha_1|\alpha_0\rangle|^2 = \exp\{-|\alpha_0 - \alpha_1|^2\}$ and $P_E \simeq 1/4\exp\{-|\alpha_0 - \alpha_1|^2\}$ for large $|\alpha_0 - \alpha_1|$. As a matter of fact, entanglement is always convenient to improve precision of the transmission channel.

Let's go back to the entangled scheme: an eavesdropper, say Eve, does not know the key, and therefore, to measure the bit, she has (in principle) to discriminate between the two mixed states $\varrho_0 = 1/\pi \int d^2\alpha D(\alpha)\sigma_0 D^\dagger(\alpha)$ and $\varrho_1 = 1/\pi \int d^2\alpha\, D(\alpha)\, \sigma_1\, D^\dagger(\alpha)$. Since the set of displacement operators is a UIR of a group we have, according to Schur lemma, $\Lambda = 1/\pi \int d^2\alpha\, D(\alpha)\ (\sigma_1 - \sigma_0)\ D^\dagger(\alpha) = \mathrm{tr}\,[\sigma_1 - \sigma_0]\,1 = 0$, and therefore $P_E = 1/2$ i.e. the best strategy for Eve is just pure guess.

In practice, however, it is not possible to impose displacements with uniform probability in the complex plane. What we can reliably implement is the following criptographic protocol (random state transformation) $\varrho_j = \int d^2\alpha\, g_\kappa(|\alpha|^2)\, D(\alpha)\, \sigma_j\, D^\dagger(\alpha)$ where $g_\kappa(|\alpha|^2) = \exp(-|\alpha|^2/\kappa)/\kappa\pi$ is a Gaussian distribution, and to find the error probability for Eve, we have to diagonalize $\Lambda = \int d^2\alpha\, g_\kappa(|\alpha|^2)\, D(\alpha)\ (\sigma_1 - \sigma_0)\ D^\dagger(\alpha)$. In order to prove that the present protocol is secure we have to compare the best stratey employable by Eve with a feasible strategy that Bob can use. Therefore, we suppose that Eve is trying to eavsdrop a maximally entangled channel ($x \rightarrow 1$) which is not perfectly protected (κ finite). In this case we have $\varrho_j = D(z_j)\nu D^\dagger(z_j)$ with $\nu = \int d^2\alpha\, g_\kappa(|\alpha|^2)\, |\alpha\rangle\rangle_{11}\langle\langle\alpha|$, such that the matrix to be diagonalized is given by

$$\Lambda = \int d^2\alpha\, g_\kappa(|\alpha|^2)\ [|\alpha + z_1\rangle\rangle_{11}\langle\langle\alpha + z_1| - |\alpha + z_0\rangle\rangle_{11}\langle\langle\alpha + z_0|] = \int d^2\beta\, f(\beta)\, |\beta\rangle\rangle_{11}\langle\langle\beta|\,,$$

with $f(\beta) = g_\kappa(|\beta - z_1|^2) - g_\kappa(|\beta - z_0|^2)$. The sum S_+ of positive eigenvalues of Λ correspond to integral of $f(\beta)$ over its positivity region i.e. $|\beta - z_1|^2 < |\beta - z_0|^2$. Suppose that $z_1 = a$ and $z_0 = -a$, with a real, then

$$S_+ = \int_0^\infty \frac{dx}{\sqrt{\pi\kappa}}\left[\exp\{-(x-a)^2/\kappa\} - \exp\{-(x+a)^2/\kappa\}\right] = \mathrm{Erf}\left(\frac{a}{\sqrt{\kappa}}\right)\,. \tag{4}$$

The error probability for Eve is thus given by

$$P_E = \frac{1}{2}\left[1 - \mathrm{Erf}\left(\frac{a}{\sqrt{\kappa}}\right)\right] \overset{a\gg 1}{\simeq} \frac{\sqrt{\kappa}}{2a\sqrt{\pi}}\ \exp\left\{-\frac{a^2}{\kappa}\right\}\,. \tag{5}$$

Bob uses a scheme based on heterodyne detection and a threshold strategy as follows: suppose again that z_0 and z_1 are real amplitude given by $z_0 = -a$ and $z_1 = a$. After having revealed the outcome z from the heterodyne detector we employ the following inference rule: if Re[z] < 0 then infer bit "0", "1" otherwise. The corresponding error probability is given by

$$P_E^h = \tfrac{1}{2}\Big[p(\mathrm{Re}[z] > 0|-a) + p(\mathrm{Re}[z] < 0|a)\Big] = \int_{\mathrm{Re}[z]<0} d^2z\, |{}_1\langle\langle z|a\rangle\rangle_x|^2 = \tfrac{1}{2}\left[1 - \mathrm{Erf}\left(\frac{a}{\sqrt{2\sigma_x^2}}\right)\right]\,, \tag{6}$$

where $\sigma_x^2 = 1/2(1-x)(1+x)$. For large a we have $P_E^h \simeq \sqrt{2\sigma_x^2/a^2\pi}\exp\{-a^2/2\sigma_x^2\}$. The error probability of this Bob' feasible strategy is smaller than optimal Eve's one as far as $2\sigma_x^2 < \kappa$. The corresponding error probability for Bob' ideal scheme is given by $P_E = 1/4\exp\{-4a^2(1+N)\}$, whereas the analogue "not entangled" channel would achieve only $P_E = 1/2[1-\text{Erf}(a)]$.

4.2 Complex alphabet quantum communication

In this case Alice send through the transmission line the symbol z_0, chosen from a complex alphabet, encoded into the state $|z_0\rangle\rangle_x$ and protected by applying a random displacement $D(\alpha)$ whose amplitude is known to Bob. Bob should estimate z_0 on the state $|z\rangle\rangle_x$ whereas Eve, for the same task, has at disposal the state $D(z)\nu D^\dagger(z)$ with $\nu = \int d^2\alpha\, g_\kappa(|\alpha|^2)\, |\alpha\rangle\rangle_{11}\langle\langle\alpha|$. If both use heterodyne detection i.e. the POVM $\Pi(z) = |z\rangle\rangle_{11}\langle\langle z|$ we have

$$p_B(z) = |_1\langle\langle z|z_0\rangle\rangle_x|^2 = \frac{1}{\pi\Delta_x^2}\exp\left\{-\frac{|z-z_0|^2}{\Delta_x^2}\right\}$$

$$p_E(z) = {}_1\langle\langle z|\zeta|z\rangle\rangle_1 = \int\frac{d^2\alpha}{\kappa\pi}\; \mathrm{e}^{-|\alpha|^2/\kappa}\; |_1\langle\langle z|D(\alpha)|z_0\rangle\rangle_x|^2 = \frac{1}{\pi(\Delta_x^2+\kappa)}\exp\left\{-\frac{|z-z_0|^2}{\Delta_x^2+\kappa}\right\}, \qquad (7)$$

and again the security of the protocol is assured by the random distribution of the displacing amplitudes.

5 Degradation of entanglement in active fibers

In applications such teleportation or cryptography one needs to transfer entanglement among distant partners, and therefore to transmit entangled states along some kind of channel. For optical implementation this is usually accomplished by means of (active) optical fibers. As a matter of fact, the propagation of twin-beam in optical fibers unavoidably lead to degradation of entanglement due to decoherence induced by losses and noise. In this section, we study the evolution of twin-beam in active optical media, such the pair of optical fibers that may be used to transmit twin-beam, and analyze the separability of the evolved state as a function of the fiber parameters. A threshold value for the interaction time, above which the entanglement is destroyed, will be analytically derived.
If the twin-beam are produced from the vacuum by a parametric optical amplifier with evolution operator $U = \exp\left[r_0\left(a^\dagger b^\dagger - ab\right)\right]$, then we have $x = \tanh r_0$, whereas the number of photons of the twin-beam is $N = 2\sinh^2 r_0 = 2x^2/(1-x^2)$. The propagation inside the fibers can be modeled as the coupling of each part of the twin-beam with a non zero temperature reservoir. The fibers dynamics can be described in terms of the two-mode Master equation $\dot\varrho_t \equiv \mathcal{L}\varrho_t = \Gamma_a(1+M_a)L[a]\varrho_t + \Gamma_b(1+M_b)L[b]\varrho_t + \Gamma_a M_a L[a^\dagger]\varrho_t + \Gamma_b M_b L[b^\dagger]\varrho_t$ where $\varrho_t \equiv \varrho(t)$, $\Gamma_a = \Gamma_b = \Gamma$ denotes the (equal) damping rate, $M_a = M_b = M$ the number of background thermal photons, and $L[O]$ is the Lindblad superoperator $L[O]\varrho_t = O\varrho_t O^\dagger - \frac{1}{2}O^\dagger O\varrho_t - \frac{1}{2}\varrho_t O^\dagger O$. The terms proportional to $L[a]$ and $L[b]$ describe the losses, whereas the terms proportional to $L[a^\dagger]$ and $L[b^\dagger]$ describe the linear phase-insensitive amplification process taking place into the fibers. Of course, the dynamics inside the two fibers are independent on each other. The master equation can be transformed into a Fokker-Planck equation for the two-mode Wigner function $W(x_1, y_1; x_2, y_2)$. Using the differential representation of the superoperators the corresponding Fokker-Planck equation reads as follows $\partial_\tau W_\tau(x_1, y_1; x_2, y_2) \;=\; \left[\frac{1}{8}\left(\sum_{j=1}^2 \partial^2_{x_j x_j} + \partial^2_{y_j y_j}\right) + \frac{\gamma}{2}\left(\sum_{j=1}^2 \partial_{x_j} x_j + \partial_{y_j} y_j\right)\right] W_\tau(x_1, y_1; x_2, y_2)$, where τ denotes the rescaled time $\tau = \Gamma/\gamma\; t$, and the drift term γ is given by $\gamma = (2M+1)^{-1}$. The Wigner function of a twin-beam is given by

$$W_0(x_1, y_1; x_2, y_2) = \left(2\pi\sigma_+^2\, 2\pi\sigma_-^2\right)^{-1}\exp\left[-\frac{(x_1+x_2)^2}{4\sigma_+^2} - \frac{(y_1+y_2)^2}{4\sigma_-^2} - \frac{(x_1-x_2)^2}{4\sigma_-^2} - \frac{(y_1-y_2)^2}{4\sigma_+^2}\right],$$

where $\sigma_+^2 = 1/4\exp\{2r_0\}, \sigma_-^2 = 1/4\exp\{-2r_0\}$. The Gaussian form of the Wigner function is mantained during the evolution whereas the variances are increased to

$$\Sigma_+^2 = \left(\mathrm{e}^{-\gamma\tau}\,\sigma_+^2 + D^2\right) \qquad \Sigma_-^2 = \left(\mathrm{e}^{-\gamma\tau}\,\sigma_-^2 + D^2\right),$$

with $D^2 = \frac{1}{4\gamma}(1-\mathrm{e}^{-\gamma\tau})$. A necessary condition for disentanglement, or separability, is the positivity of the density matrix ϱ^T, obtained by partial transposition of the original density matrix (PPT condition) [21]. In general, PPT has been proved to be only a necessary condition for separability. However, for some specific sets of states PPT is also a sufficient condition. These includes Gaussian states (states with a Gaussian Wigner function) of a bipartite continuos variable system [12, 22]. Our analysis is based on this results. In fact, the Wigner function of a twin-beam is Gaussian, and the evolution in an active medium preserves such Gaussian character. Therefore, we are able to characterize the entanglement at any time and to give conditions on the parameters to preserve entanglement after a given interaction lenght. The PPT condition on the density matrix can be rephrased as a condition on the covariance matrix of the Wigner function of the two modes. In the case of an evolved twin-beam we have that the state is separable iff *both* the variances satisfies the condition $\Sigma_+^2 \geq \frac{1}{4}$, $\Sigma_-^2 \geq \frac{1}{4}$. Given the parameters M, Γ and λ the threshold value τ_s above which the state become separable is given by

$$\tau_s = \frac{1}{\gamma}\,\log\left(1+\gamma\frac{1-\mathrm{e}^{-2\lambda}}{1-\gamma}\right) = (2M+1)\,\log\left(1-\frac{N-\sqrt{N(N+2)}}{2M}\right),$$

(remind that N is the mean photon number of the twin-beam). In terms of the unrescaled time t the threshold for separability reads as

$$t_s = 3D\frac{1}{\Gamma}\,\log\left(1-\frac{N-\sqrt{N(N+2)}}{2M}\right), \tag{8}$$

apart from the case $M = 0$ in which the threshold diverges. Eq. (8) says if the state was initially sufficiently entangled the interaction with the environment is not destroying its character. In this case we have approximately $t_s \simeq \frac{1}{\Gamma}\log\left(1+\frac{1}{2M}\right)$.

6 Summary

The technology of entanglement can be of great help in improving precision, stability and performances of quantum optical schemes meant to process quantum information. In this paper we reviewed some applications of continuous variables entangled states, aimed to improve quantum measurements, interferometry and communication. Since the optical implementation of quantum information processing will involve optical fibers to establish an entangled channel between two distant users, we also study the evolution of entangled twin-beam of light in an active optical medium, such to evaluate the degradation rate of entanglement, and establish a threshold on the interaction time, above which the entangled is no longer present and the channel become useless.

Acknowledgements This work has been sponsored by the INFM through the project PRA-CLON, and by EEC through the projects IST-2000-29681 (ATESIT), IST-1999-11053 (EQUIP).

References

[1] B. Julsgaard, A. Kozhekin, E. S. Polzik, LANL ArXive quant-ph/0106057.
[2] See for example S. L. Braunstein and A. K. Pati (eds.), Quantum Information Theory with Continuous Variables (Kluwer, 2002).
[3] A. Furusawa et al., Science **282**, 706 (1998).
[4] L. Duan, G. Giedke, J. I. Cirac, and P. Zoller, Phys. Rev. Lett. **84**, 4002 (2000).
[5] F. Grosshans and P. Grangier, Phys. Rev. Lett. **88**, 057902 (2002).
[6] M. I. Kolobov and C. Fabre, Phys. Rev. Lett. **85**.
[7] B. E. A. Saleh, B. M. Jost, H.-B. Fei, and M. C. Teich, Phys. Rev. Lett. **80** 3483 (1998).
[8] G. M. D'Ariano, M. G. A. Paris, and P. Perinotti, Phys. Rev A **65** 062106 (2002).
[9] G. M. D'Ariano and P. Lo Presti, Phys. Rev. Lett. **86** 4195 (2001).
[10] G. M. D'Ariano, P. Lo Presti and M. G. A. Paris, Phys. Rev. Lett. **87**, 270404 (2001).
[11] E. Arthurs, M. S. Goodman, Phys. Rev. Lett. **60**, 2447 (1988).
[12] R. Simon, Phys. Rev. Lett. **84** 2726 (2000).
[13] C. W. Helstrom, Quantum Detection and Estimation Theory (Academic Press, New York, 1976).
[14] M. G. A. Paris, Phys. Lett. A **225**, 23 (1997).
[15] J. Neyman, E. Pearson, Proc. Camb. Phil. Soc. **29**, 492 (1933); Phil. Trans. Roy. Soc. London A **231**, 289 (1933).
[16] K. R. Parthasarathy, Inf. Dim. Anal. Quant. Prob. **2**, 557 (1999).
[17] C. M. Caves, Phys. Rev. D **23**, 1693 (1981); R. S. Bondurant and J. H. Shapiro, Phys. Rev. A **30**, 2548 (1984).
[18] H. Yuen, in: Quantum Communication, Measurement, and Computing, edited by P. Tombesi and O. Hirota (Kluwer Academic/Plenum Publishers, 2001).
[19] Wang Xiang-bin, LANL arXive quant-ph/0204039.
[20] G. M. D'Ariano, M. G. A. Paris, M. F. Sacchi, F. De Martini, Phys. Rev. A **61**, 063813 (2000).
[21] A. Peres, Phys. Rev. Lett. **77**, 1413-1415 (1996).
[22] Lu-Ming Duan, G. Giedke, J. I. Cirac, and P. Zoller, Phys. Rev. Lett. **84** 2722 (2000).