Eur. Phys. J. D **18**, 219–228 (2002)
DOI: 10.1140/epjd/e20020026

THE EUROPEAN
PHYSICAL JOURNAL D
EDP Sciences

Statistical confidentiality tests for a quantum transmission using continuous variables

P. Navez[a]

INFM, Dipartimento di Scienze CC FF MM, Universita degli Studi dell'Insubria, Via Valleggio 11, 22100 COMO, Italy

Received 12 July 2001 and Received in final form 11 November 2001

Abstract. We describe a cryptographic protocol consisting of two entangled beams of squeezed light which makes use of statistical tests to deduce the secret key bit. The sender (Alice) encrypts a secret key by modulating the phase of the beam sent in public by the receiver (Bob) who keeps the other beam private. The knowledge of the degree of non classical correlation between the beam quadrature components measured in private and in public allows only Bob to decrypt the secret key. With a view towards absolute security, we formally prove that any external intervention from an eavesdropper (Eve) during the communication process introduces necessarily some modification susceptible to be detected. Statistical confidentiality tests are proposed to detect the presence of Eve.

PACS. 03.67.Dd Quantum cryptography – 03.67.Hk Quantum communication – 42.65.-k Nonlinear optics

1 Introduction

Quantum cryptography based on EPR correlation of continuous variables [1–7] provides a serious alternative to the more conventional methods using single photon pairs [8–10]. The use of intense photons beams presents many technological advantages and could cost less in comparison to the use of single photon pulses. First, the realisation of a beam pair EPR correlated in the quadratures presents less difficulties than that still encountered in the realisation of a beam which controls the production of a single pair of photons. Second, the dark counting phenomenon makes detectors much more efficient to detect many photons beams than one single photon. Even a protocol using continuous variables has been recently proven to be secure [6] as in the case for single photon systems [10–12].

In a previous paper [1], a quantum cryptography scheme using continuous variable was proposed allowing an invisible transmission of secret information. It consists of two EPR-correlated beams. One of the beams is used by the sender (Alice) to encrypt a secret information. The other beam is used by the receiver (Bob) to decrypt the secret information through the results of quadrature components measurement. It has been proven that, with this scheme, any intervention of an eavesdropper (Eve) is vulnerable to any subsequent detection of the secret information by Alice and Bob.

In this paper, we aim at developing more thoroughly the security considerations of this scheme by showing how the vulnerability could be effectively detected by Bob. A theorem imposes some conditions to Alice and Bob which allow to detect any modification introduced by Eve. These conditions involve random modifications on the parameters of the system which force Eve to modify the form of the probability distribution of the measured quadratures if she tries to obtain some secret information. A second theorem extends these considerations when the transmission channel of the quantum signal is lossy but only in the case of a single attack. The loss occuring in the channel is modelled by a quantum master equation [4].

Based on these theorems, we propose a protocol for sharing a key between Alice and Bob which makes use of statistical tests by Bob to deduce the key bit. Since some experimental constraints prevent to carry out a measurement on an exact quantum eigenstate, any secret shared bit is obtained by doing many measurements on a quantum state different from an eigenstate. Indeed, the experimental difficulties associated to the realisation of a high squeezing parameter [7] and the important losses generated during the transmission have the undesirable consequence to create a strongly imperfect eigenstate of the measured observables. In such circumstance, as long as some quantum and classical noises are generated, no perfect EPR anti/correlation is observed by carrying out only one quadrature components measurement as in the case of single photon pairs. Therefore, a scheme similar to the E91 protocol fails to work when the experimental system presents such strong imperfections [8]. For this reason, any shared key bit is obtained from an average over many measurements of the quadratures. Some statistical tests are performed on the collected set of measurements and allow to determine the key bit and if eavesdropping has occured.

[a] e-mail: navez@ptt.mi.infn.it
or e-mail: navez@ulam.fis.unico.it

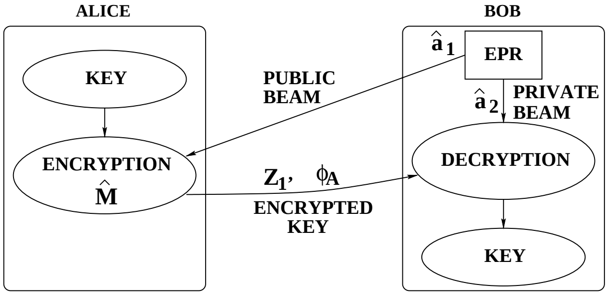

Fig. 1. Quantum cryptographic scheme with continuous variables.

Unlike the usual protocols in quantum cryptography, no data measured in a different basis by Alice and Bob are discarded in the proposed protocol but are used as a part of the information in order to deduce the key bits. Only some data are discarded in order to check the bit error rate. Such a new approach has the advantage to allow the use of a low value for the squeezing parameter.

The paper is divided as follows. The second section gives a description of the quantum cryptography scheme. The third and fourth section relate about the security of the scheme but, in the fourth section, the effect of a lossy quantum channel is taken into account. Section 5 concerns a possible practical protocol for key bit sharing.

2 The quantum cryptography scheme

Let us start with the description of the scheme illustrated in Figure 1 [1]. Suppose that Alice wishes to send a secret key to Bob. To this purpose, Bob produces an EPR state consisting of two entangled beams characterized by the photon annihilation operators $\hat{a}_1$ and $\hat{a}_2$ [13]. Written in occupation photon number representation, this state has the form:

$$|\Psi\rangle = \hat{S}|0\rangle_1|0\rangle_2 = \sum_{n=0}^{\infty} c_n|n\rangle_1|n\rangle_2 \qquad (1)$$

where $\hat{S} = \exp(r\hat{a}_1\hat{a}_2 - r\hat{a}_1^\dagger\hat{a}_2^\dagger)$ and $c_n = (\tanh r)^n/\cosh r$ and r is the squeezing real parameter. Bob then sends beam 1 to Alice and keeps private beam 2. All the information available to Alice can be extracted only from the diagonal density matrix resulting from the partial trace of the total wave function over the unknown beam 2:

$$\hat{\rho}_1 = \mathrm{Tr}_2(|\Psi\rangle\langle\Psi|) = \sum_{n=0}^{\infty} |c_n|^2|n\rangle_1\,{}_1\langle n|. \qquad (2)$$

With the beam received from Bob, Alice encrypts the secret information by making the unitary transformation $\hat{M} = \exp(\mathrm{i}\theta\hat{a}_1^\dagger\hat{a}_1)$ where θ carries the key bits. This transformation modifies the total wave function (1) but not the density matrix (2).

Then Alice and Bob carry out a measurement on the quadrature component observables on the beam 1 and 2 respectively:

$$\hat{Z}_{1'} = \mathrm{e}^{-\mathrm{i}\theta_A}\hat{a}_1 + \mathrm{e}^{\mathrm{i}\theta_A}\hat{a}_1^\dagger \qquad (3)$$

$$\hat{Z}_2 = \mathrm{e}^{-\mathrm{i}\theta_B}\hat{a}_2 + \mathrm{e}^{\mathrm{i}\theta_B}\hat{a}_2^\dagger \qquad (4)$$

where $\theta_A = \phi_A + \theta$. ϕ_A and θ_B are the phases introduced by Alice and Bob. θ_B must remain private to Bob whereas the result of the measurement of $\hat{Z}_{1'}$ and ϕ_A must be communicated in public to Bob at some stage of the protocol.

Although the EPR state is not an eigenstate of these operators, the uncertainty in the quadrature difference $\hat{Z}_- = \hat{Z}_{1'} - \hat{Z}_2$ is close to zero as the squeezing parameter r becomes large and $\theta_A + \theta_B = 0$. We notice indeed from the expressions that for $r \gg 1$:

$$\begin{aligned}\sigma_-^2(\theta) &= \langle\Psi|\delta^2\hat{Z}_-|\Psi\rangle && (5)\\ &= 2\cosh(2r) - 2\cos(\theta_A+\theta_B)\sinh(2r) && (6)\\ &\cong 4\sinh(2r)\sin^2\frac{(\theta_A+\theta_B)}{2}\cdot && (7)\end{aligned}$$

The same happens for the quadrature sum $\hat{Z}_+ = \hat{Z}_{1'} + \hat{Z}_2$ but for different phases. The uncertainty is close to zero when r is large and $\theta_A + \theta_B = \pi$:

$$\begin{aligned}\sigma_+^2(\theta) &= \langle\Psi|\delta^2\hat{Z}_+|\Psi\rangle && (8)\\ &= 2\cosh(2r) + 2\cos(\theta_A+\theta_B)\sinh(2r) && (9)\\ &\cong 4\sinh(2r)\sin^2\frac{(\theta_A+\theta_B-\pi)}{2}\cdot && (10)\end{aligned}$$

On the other hand, supplementary/opposite phases generate, for strong squeezing, a quantum uncertainty which appears under the form of fluctuations during the measurement of the quadrature difference/sum.

In this manner, the secret key contained in θ is obtained by determining the intensity of the noise resulting from these fluctuations [13]. The joint statistics of many measured quadrature components allows only Bob to estimate $\sigma_+^2(\theta)$ and $\sigma_-^2(\theta)$ and therefore determine θ from (6) and (9) since θ_B, r and ϕ_A is known to Bob. In this statistical problem, two questions should be answered. First, we must find what is the best value or estimator $\overline{\theta}$ of θ that fits these data. Second, we should evaluate the statistical error in the estimation $\overline{\theta}$. More precisely, given a probability of confidence p, we should ensure that θ cannot be any other value permissible by the protocol. For any question of that kind, there is not an unique and rigorous answer but some recipes [14]. In this context, we should also determine what is the best one or what is the recipe which presents a maximum of practical advantages.

The security of the scheme is based on the fact that both r and θ_B are kept secret. Eves becomes vulnerable to any subsequent detection because any perturbation she is introducing without knowing r and θ_B is modifying the joint counting statistics [1].

3 A theorem on Eve's detection

Let us now discuss the matter of detection of Eve's attack by Alice and/or Bob. Let $\hat{Z}_{1'}$ and $\hat{Z}_2$ be the observables measured by Alice and Bob respectively.

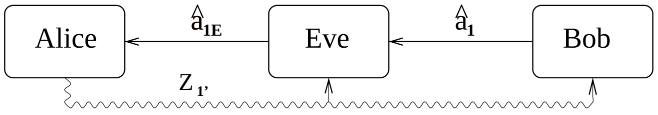

Fig. 2. Schematic set-up of Eve's attack.

Suppose that Eve tries to have access to the beam 1 as in the Figure 2 and thus modifies it by means of an unitary transformation:

$$\hat{a}_{1E} = \hat{U}^\dagger \hat{a}_1 \hat{U}. \tag{11}$$

The unitary operator $\hat{U}$ could depend on other external degrees of freedom (observables) introduced by Eve as an Ancilla. For example, Eve uses another photon beam or other modes of the same beam taken at a different time or even a detector in view of a measurement on the beam 1. We denote by $|\nu\rangle$ a basis of the Hilbert space characterizing these external degrees of freedom and assume that $|0\rangle$ is the initial state before the modification. Then the state after the unitary transformation is $\hat{U}|\Psi\rangle|0\rangle$. Let us define the joint probability distribution to find the system with the values z_1 and z_2 of the quadrature component observables $\hat{Z}_{1'}$ and $\hat{Z}_2$:

$$P(z_{1'}, z_2) = \langle\Psi|\delta\left(z_{1'} - \hat{Z}_{1'}\right)\delta\left(z_2 - \hat{Z}_2\right)|\Psi\rangle\,\cdot \tag{12}$$

This function can be calculated (see appendix). The result is:

$$P(z_{1'}, z_2) = \frac{\mathrm{e}^{-\dfrac{(z_1+z_2)^2}{2\sigma_+^2(\theta)} - \dfrac{(z_1-z_2)^2}{2\sigma_-^2(\theta)}}}{\pi\sigma_+(\theta)\sigma_-(\theta)}\,\cdot \tag{13}$$

After the encryption of Alice with the value of the angle $\theta_A = \theta_S$ and an eventual intervention of Eve, the probability distribution becomes

$$P_E(z_{1'}, z_2) = \langle 0|\langle\Psi|\hat{U}^\dagger\delta\left(z_{1'} - \hat{Z}_{1'}\right)\delta\left(z_2 - \hat{Z}_2\right)\hat{U}|\Psi\rangle|0\rangle|_{\theta_A=\theta_S}\,\cdot \tag{14}$$

Then Bob receives the secret information. He is expected to observe $\hat{Z}_{1'}$ and $\hat{Z}_2$ to follow a probability distribution parameterized by the value of the angle $\theta_A = \theta_R$ possibly different from θ_S:

$$P_B(z_{1'}, z_2) = \langle\Psi|\delta\left(z_{1'} - \hat{Z}_{1'}\right)\delta\left(z_2 - \hat{Z}_2\right)|\Psi\rangle|_{\theta_A=\theta_R}\,\cdot \tag{15}$$

In principle, the secret information received could depend on the other parameters sent by Alice $\theta_R = \theta_R(\theta_S, \theta_B, r)$.

To avoid being detected, both probability distributions must be equal for the particular values of r, θ_S and θ_B chosen by Alice and Bob. Since these values are unknown to Eve, she cannot exclude any possibility and is forced to ensure equality for all of these values. But this strategy does not work as it is shown by the following theorem.

Theorem 1

If we require that the probability distributions (14) and (15) remain unchanged by Eve and this, for all values of θ_B, for at least two different values of r and for at least two different and not opposite values of $\theta_A = \phi_A + \theta = \theta_S$, then $\hat{U}$ must be a phase transformation on the beam 1 which does not introduce an interaction effect between $|\Psi\rangle$ and $|0\rangle$, i.e.

$$\langle\nu|\,{}_1\langle n'|\hat{U}|n\rangle_1|0\rangle = \delta_{n',n}\mathrm{e}^{-\mathrm{i}\delta}u_\nu \tag{16}$$

where u_ν are coefficients of the projection onto the state ν which do not depend on n.

From this theorem, we conclude that Eve could only modify θ_S into $\theta_R = \theta_S + \delta$ and make it unreadable to Bob. Otherwise she is susceptible to be detected since the probability distribution is not the one predicted by the theory and therefore she cannot safely extract information. The only additional requirement is that r and θ_B must be a random number.

Proof. Let us examine the consequence of

$$P_E(z_{1'}, z_2) = P_B(z_{1'}, z_2). \tag{17}$$

Taking the Fourier transform on z_1 and z_2, the equation (17) becomes (we insert the explicit dependence θ_A in $\hat{Z}_{1'}$):

$$\langle 0|\langle\Psi|\hat{U}^\dagger\mathrm{e}^{\mathrm{i}\hat{Z}_{1'}(\theta_S)s_1+\mathrm{i}\hat{Z}_2 s_2}\hat{U}|\Psi\rangle|0\rangle = \langle\Psi|\mathrm{e}^{\mathrm{i}\hat{Z}_{1'}(\theta_R)s_1+\mathrm{i}\hat{Z}_2 s_2}|\Psi\rangle\,\cdot \tag{18}$$

This equality should be satisfied for any value of the parameters r, s_1, s_2, and θ_B and at least two different and non opposite values of θ_S. Let us first determine the dependence of $\theta_R(\theta_S, \theta_B, r)$. It is legitime to make a Taylor expansion in s_1 and s_2 since each term of the serie is finite in the r.h.s. of (18). For each order of the expansion, the coefficients of the expansion must be equal. In particular, for the coefficients linear in the quadrature,

$$\langle 0|\langle\Psi|\hat{U}^\dagger\hat{Z}_{1'}(\theta_S)\hat{Z}_2\hat{U}|\Psi\rangle|0\rangle = \langle\Psi|\hat{Z}_{1'}(\theta_R)\hat{Z}_2|\Psi\rangle. \tag{19}$$

Using the explicit expression for the wave function (1) and the Bogoliubov relations (81, 82), we notice that since photons are produced in pairs $\langle\Psi|\hat{a}_1^\dagger\hat{a}_2|\Psi\rangle = 0$ and that the only non zero in the r.h.s. is $A = \langle\Psi|\hat{a}_1^\dagger\hat{a}_2^\dagger|\Psi\rangle = \sinh r\cosh r$. Thus, using the explicit expression for the quadratures (3), (4), the equality (19) becomes:

$$\cos(\theta_R + \theta_B) = \alpha_1\cos(\theta_S + \theta_B + \delta) + \alpha_2\cos(\theta_S - \theta_B + \delta') \tag{20}$$

where $\alpha_1 = A_1/A$, $\alpha_2 = A_2/A$, $A_1\mathrm{e}^{\mathrm{i}\delta} = \langle 0|\langle\Psi|\hat{U}^\dagger a_1^\dagger\hat{a}_2^\dagger\hat{U}|\Psi\rangle|0\rangle$ and $A_2\mathrm{e}^{\mathrm{i}\delta'} = \langle 0|\langle\Psi|\hat{U}^\dagger\hat{a}_1^\dagger\hat{a}_2\hat{U}|\Psi\rangle|0\rangle$. Combining this result together with the explicit expression (85) (see appendix)

$$\langle\Psi|\mathrm{e}^{\mathrm{i}\hat{Z}_{1'}(\theta_R)s_1+\mathrm{i}\hat{Z}_2 s_2}|\Psi\rangle = \mathrm{e}^{-\frac{1}{2}\left[\cosh(2r)(s_1^2+s_2^2)+\sinh(2r)\cos(\theta_R+\theta_B)2s_1 s_2\right]} \tag{21}$$

and defining the complex variables

$$\alpha = \alpha_1 \mathrm{e}^{\mathrm{i}(\delta+\theta_S)} + \alpha_2 \mathrm{e}^{-\mathrm{i}(\delta'+\theta_S)} = |\alpha| \mathrm{e}^{\mathrm{i}\phi} \tag{22}$$

we notice also that:

$$\langle \Psi | \mathrm{e}^{\mathrm{i}\hat{Z}_{1'}(\phi)|\alpha| s_1 + \mathrm{i}\hat{Z}_2 s_2} | \Psi \rangle = \\ \mathrm{e}^{-\frac{1}{2}\left[\cosh(2r)(|\alpha|^2 s_1^2 + s_2^2) + \sinh(2r)(\alpha \mathrm{e}^{\mathrm{i}\theta_B} + \alpha^* \mathrm{e}^{-\mathrm{i}\theta_B})2 s_1 s_2\right]}. \tag{23}$$

Proceeding to the identification between (21) and (23), we rewrite the r.h.s. of (18) in a form in which the explicit dependence in θ_B appears only in $\hat{Z}_2$:

$$\langle \Psi | \mathrm{e}^{\mathrm{i}\hat{Z}_{1'}(\theta_R) s_1 + \mathrm{i}\hat{Z}_2 s_2} | \Psi \rangle = \\ \mathrm{e}^{-\frac{1}{2}(1-|\alpha|^2)\cosh(2r) s_1^2} \langle \Psi | \mathrm{e}^{\mathrm{i}\hat{Z}_{1'}(\phi)|\alpha| s_1 + \mathrm{i}\hat{Z}_2 s_2} | \Psi \rangle. \tag{24}$$

Having obtained an explicit dependence in θ_B in $\hat{Z}_2$, we redefine the complex parameter $\xi = \xi_X + \mathrm{i}\xi_Y = \mathrm{e}^{\mathrm{i}\theta_B} s_2$. in such a way that $\hat{Z}_2 s_2 = \xi \hat{a}_2^\dagger + \xi^\star \hat{a}_2$. Let us introduce:

$$T_{n,n'}(\xi, \xi^*) = {}_2\langle n' | \mathrm{e}^{-\mathrm{i}\left(\xi \hat{a}_2^\dagger + \xi^\star \hat{a}_2\right)} | n \rangle_2. \tag{25}$$

A calculation [1] shows that for all occupation number n and n' of the beam 2:

$$\int \frac{\mathrm{d}^2\xi}{\pi} T_{n,n'}(\xi, \xi^*) \mathrm{e}^{\mathrm{i}\left(\xi \hat{a}_2^\dagger + \xi^\star \hat{a}_2\right)} = |n\rangle_2 \, {}_2\langle n'|. \tag{26}$$

Since the equality (18) is valid for all values of the complex parameter ξ, we can apply the transformation (26) using (24) and the exponential term containing $\hat{Z}_2 s_2$ is transformed into $|n\rangle_2 \, {}_2\langle n'|$. Using the property of entanglement in (1), we eliminate the states describing the second beam since $\hat{U}$ does not affect beam 2. We obtain for all occupation numbers n and n' for beam 1:

$$\langle 0 | \, {}_1\langle n' | \hat{U}^\dagger \mathrm{e}^{\mathrm{i}\hat{Z}_{1'}(\theta_S) s_1} \hat{U} | n \rangle_1 | 0 \rangle = \\ \mathrm{e}^{-\frac{1}{2}(1-|\alpha|^2)\cosh(2r) s_1^2} \, {}_1\langle n' | \mathrm{e}^{\mathrm{i}\hat{Z}_{1'}(\phi)|\alpha| s_1} | n \rangle_1 \tag{27}$$

or in operatorial form

$$\langle 0 | \hat{U}^\dagger \mathrm{e}^{\mathrm{i}\hat{Z}_{1'}(\theta_S) s_1} \hat{U} | 0 \rangle = \\ \mathrm{e}^{-\frac{1}{2}(1-|\alpha|^2)\cosh(2r) s_1^2} \mathrm{e}^{\mathrm{i} s_1 \hat{Z}_{1'}(\phi)|\alpha|}. \tag{28}$$

Since r is kept private to Bob, the unitary transformation $\hat{U}$ introduced by Eve should not depend on that parameter. This implies that the r.h.s. of (28) does not depend on r. In order to satisfy that requirement for all s_1 and at least two distinct values of r, α must necessarily not depend on r as well. Thus, the only possibility to satisfy (28) is that $|\alpha|^2 = 1$ or, more explicitly, using (22):

$$\alpha_1^2 + \alpha_2^2 + 2\alpha_1\alpha_2 \cos(\delta + \delta' + 2\theta_S) = 1. \tag{29}$$

Since (29) holds for any value of θ_S, the last term of the l.h.s. is canceled and we are left with the two possible cases $\alpha_1 = 1$ and $\alpha_2 = 0$ or $\alpha_1 = 0$ and $\alpha_2 = 1$. Let us analyse the two cases separately and show that only the first case is of relevance since the second case leads to an absurdity.

Case 1: $\alpha = \mathrm{e}^{\mathrm{i}(\delta+\theta_\mathrm{S})}$

We define $\hat{V} = \mathrm{e}^{\mathrm{i}\delta \hat{a}_1^\dagger \hat{a}_1}$ which is a phase transformation of an angle δ such that $\hat{V}\hat{a}_1\hat{V}^\dagger = \mathrm{e}^{-\mathrm{i}\delta}\hat{a}_1$ so that the equality (28) becomes:

$$\langle 0 | \hat{U}^\dagger \mathrm{e}^{\mathrm{i}\hat{Z}_{1'}(\theta_S) s_1} \hat{U} | 0 \rangle = \hat{V} \mathrm{e}^{\mathrm{i}\hat{Z}_{1'}(\theta_S) s_1} \hat{V}^\dagger. \tag{30}$$

We reverse all the unitary operators in r.h.s. to the l.h.s. of (30) and express the matrix elements over the states ${}_1\langle n'|$ and $|n\rangle_1$ to get:

$$\langle 0 | \, {}_1\langle n' | \hat{W}^\dagger \mathrm{e}^{\mathrm{i}\hat{Z}_{1'}(\theta_S) s_1} \hat{W} \mathrm{e}^{-\mathrm{i}\hat{Z}_{1'}(\theta_S) s_1} | n \rangle_1 | 0 \rangle = \delta_{n',n} \tag{31}$$

where $\hat{W} = \hat{U}\hat{V}$. We write the explicit dependence of $\hat{W}$ on the observables associated to the first beam as $\hat{U}(\hat{Z}_{1'}(\theta_S), \hat{Z}_{1'}^\perp(\theta_S))$, where $\hat{Z}_{1'}^\perp(\theta_S) = \hat{Z}_{1'}(\theta_S + \pi/2) = (\hat{a}_1 \mathrm{e}^{-\mathrm{i}\theta_S} - \hat{a}_1^\dagger \mathrm{e}^{\mathrm{i}\theta_S})/\mathrm{i}$ is the observable canonically conjugated to $\hat{Z}_{1'}(\theta_S)$. The exponential operator is the generator of translations:

$$\mathrm{e}^{\mathrm{i}\hat{Z}_{1'}(\theta_S) s_1} \hat{Z}_{1'}^\perp(\theta_S) \mathrm{e}^{-\mathrm{i}\hat{Z}_{1'}(\theta_S) s_1} = \hat{Z}_{1'}^\perp(\theta_S) - 2s_1. \tag{32}$$

Equation (31) becomes (omitting the dependence on θ_S):

$$\langle 0 | \, {}_1\langle n' | \hat{W}^\dagger \left(\hat{Z}_{1'}, \hat{Z}_{1'}^\perp\right) \hat{W} \left(\hat{Z}_{1'}, \hat{Z}_{1'}^\perp - 2s_1\right) | n \rangle_1 | 0 \rangle = \delta_{n',n}. \tag{33}$$

Because two normalized states with unity scalar product are necessarily equal, we infer that for all s_1 and n and the particular angle θ_S used by Alice:

$$\hat{W}\left(\hat{Z}_{1'}, \hat{Z}_{1'}^\perp\right) | n \rangle_1 | 0 \rangle = \hat{W}\left(\hat{Z}_{1'}, \hat{Z}_{1'}^\perp - 2s_1\right) | n \rangle_1 | 0 \rangle. \tag{34}$$

To satisfy (34), the expression $\langle \nu | \hat{W}\left(\hat{Z}_{1'}(\theta_S)\right) | 0 \rangle$ should only depend on $\hat{Z}_{1'}(\theta_S)$. If Alice chooses to measure between at least two distinct and non opposite quadratures then $\langle \nu | \hat{W} | 0 \rangle$ should depend on two distinct quadratures. Since the quadratures are independent, the only possibility is that $\langle \nu | \hat{W} | 0 \rangle = u_\nu$ is a constant independent of any observable relative to the beam 1. Using the definition of $\hat{W} = \hat{U}\hat{V}$ and multiplying by the inverse transformation $\hat{V}^{-1}$, we obtain finally: $\langle \nu | \hat{U} | 0 \rangle = \mathrm{e}^{-\mathrm{i}\delta \hat{a}_1^\dagger \hat{a}_1} u_\nu$ which is equivalent to equation (16).

Case 2: $\alpha = \mathrm{e}^{-\mathrm{i}(\delta'+\theta_\mathrm{S})}$

In a similar way to the case 1, we define $\hat{V}' = \mathrm{e}^{-\mathrm{i}\delta' \hat{a}_1^\dagger \hat{a}_1}$ and, from equation (28), we establish the relation:

$$\langle 0 | \, {}_1\langle n' | \hat{W}'^\dagger \mathrm{e}^{\mathrm{i}\hat{Z}_{1'}(\theta_S) s_1} \hat{W}' \mathrm{e}^{-\mathrm{i}\hat{Z}_{1'}(-\theta_S) s_1} | n \rangle_1 | 0 \rangle = \delta_{n',n} \tag{35}$$

where $\hat{W}' = \hat{U}\hat{V}'$. Again observing that two normalised states whose scalar product is unity should be equal, we must obey for all s_1 and n:

$$\hat{W}' | n \rangle_1 | 0 \rangle = \mathrm{e}^{\mathrm{i}\hat{Z}_{1'}(\theta_S) s_1} \hat{W}' \mathrm{e}^{-\mathrm{i}\hat{Z}_{1'}(-\theta_S) s_1} | n \rangle_1 | 0 \rangle \, \cdot \tag{36}$$

Let us define the position and momentum operators $\hat{Q} = \hat{Z}_{1'}(\theta_S = 0)/\sqrt{2} = \left(\hat{a}_1 + \hat{a}_1^\dagger\right)/\sqrt{2}$ and $\hat{P} = \hat{Z}_{1'}(\theta_S = \pi/2)/\sqrt{2} = \left(\hat{a}_1 - \hat{a}_1^\dagger\right)/\sqrt{2}\mathrm{i}$ verifying $\left[\hat{Q}, \hat{P}\right] = \mathrm{i}$. Let us define the associated eigenstates $|Q\rangle$ and $|P\rangle$ such that $\hat{Q}|Q\rangle = Q|Q\rangle$ and $\hat{P}|P\rangle = P|P\rangle$. Finally, let us define the operator $\hat{W}_\nu = \langle\nu|\hat{U}\hat{V}'|0\rangle$ possibly depending on $\hat{Q}$ and $\hat{P}$. Replacing $|n\rangle_1$ by $|Q\rangle$ in (36) and taking the bra $\langle\nu|\langle Q'|$, we deduce:

$$\langle Q'|\hat{W}_\nu|Q\rangle = \langle Q'|\mathrm{e}^{\mathrm{i}\hat{Z}_{1'}(\theta_S)s_1}\hat{W}_\nu \mathrm{e}^{-\mathrm{i}\hat{Z}_{1'}(-\theta_S)s_1}|Q\rangle \cdot \tag{37}$$

Taking the first order term expansion in s_1 we get:

$$\langle Q'|\left(\hat{Z}_{1'}(\theta_S)\hat{W}_\nu - \hat{W}_\nu\hat{Z}_{1'}(-\theta_S)\right)|Q\rangle = 0 \tag{38}$$

or more explicitly noticing the relation $\hat{Z}_{1'}(\theta_S) = \sqrt{2}\left(\cos\theta_S\hat{Q} + \sin\theta_S\hat{P}\right)$

$$\begin{aligned}(Q' - Q)\langle Q'|\hat{W}_\nu|Q\rangle\cos\theta_S \\ + \langle Q'|\left(\hat{P}\hat{W}_\nu + \hat{W}_\nu\hat{P}\right)|Q\rangle\sin\theta_S = 0.\end{aligned} \tag{39}$$

If the last expression must be valid for at least two different and non opposite value of θ_S then obviously the two coefficients of the trigonometric functions must be equal to zero *i.e.*:

$$(Q' - Q)\langle Q'|\hat{W}_\nu|Q\rangle = 0 \tag{40}$$

$$\langle Q'|\left(\hat{P}\hat{W}_\nu + \hat{W}_\nu\hat{P}\right)|Q\rangle = 0. \tag{41}$$

The first equation (40) means that for $Q \neq Q'$ $\hat{W}_\nu$ is diagonal and a function only of the position operator $\hat{W}_\nu(\hat{Q})$. Using this property into the second equation (41), we get:

$$\left(\hat{W}_\nu(Q') + \hat{W}_\nu(Q)\right)\langle Q'|\hat{P}|Q\rangle = 0. \tag{42}$$

Since the matrix element is different from zero for $Q = Q'$, we should necessarily conclude that $\hat{W}_\nu(Q) = 0$ or that the second case is impossible.

The facts that the probability distributions must be equal for any value of θ_B and r and that the second beam has been kept private have permitted to achieve the demonstration. If the value of θ_B remains fixed, the linear transformation cannot be carried out since the integration in (26) must be done over all ξ. If on the other hand r is fixed then (29) is not necessarily valid. Finally, if Eve has access to the second beam, then the unitary operator depends on $\hat{a}_2$ and $\hat{a}_2^\dagger$ and the passage from (18) to (27) is not necessarily valid.

4 Generalisation in presence of losses

The losses are due to the absorption of photons in the public beam channel. We study this effect by modelling the loss on a damping channel by means of the master equation [4,6]:

$$\dot{\hat{\rho}}(t) = \mathcal{L}\hat{\rho}(t) = \mathit{\Gamma}\left(\hat{a}_1\hat{\rho}(t)\hat{a}_1^\dagger - \frac{1}{2}\hat{a}_1^\dagger\hat{a}_1\hat{\rho}(t) - \frac{1}{2}\hat{\rho}(t)\hat{a}_1^\dagger\hat{a}_1\right) \tag{43}$$

where $\hat{\rho}(t)$ is the density matrix associated to the two beams 1 and 2 and such that $\hat{\rho}(t = 0) = |\mathit{\Psi}\rangle\langle\mathit{\Psi}|$. $\mathit{\Gamma} = \kappa c$ is the decay rate and is equal to the attenuation length κ^{-1} (typically of the order of 10 km) multiplied by the velocity of propagation c. The solution of this equation has the formal expression:

$$\hat{\rho}(t) = \mathrm{e}^{\mathcal{L}t}[\hat{\rho}(0)]. \tag{44}$$

In [6], some useful properties have been shown. We deduce indeed that:

$$\frac{\mathrm{d}}{\mathrm{d}t}\left\langle \hat{a}_1^{\dagger\,k}\hat{a}_1^l\right\rangle_t = -\frac{1}{2}(k+l)\mathit{\Gamma}\left\langle \hat{a}_1^{\dagger\,k}\hat{a}_1^l\right\rangle_t \tag{45}$$

where:

$$\left\langle\hat{O}\right\rangle_t = \mathrm{tr}_{12}(\hat{O}\hat{\rho}(t)) \tag{46}$$

denotes the expectation value of the operator $\hat{O}$ at time t and tr_{12} means that the trace has been done over the beam 1 and 2. Integrating from the time $t = 0$ where Bob has produced the EPR beams until the time t_{AB} where Alice has received it, we find:

$$\left\langle \hat{a}_1^{\dagger\,k}\hat{a}_1^l\right\rangle_{t_{AB}} = \mathrm{e}^{-\frac{1}{2}(k+l)\mathit{\Gamma}t_{AB}}\left\langle \hat{a}_1^{\dagger\,k}\hat{a}_1^l\right\rangle_0 \cdot \tag{47}$$

By expanding in power series, we deduce

$$\left\langle :\, f\left(\hat{a}_1^\dagger, \hat{a}_1\right)\, :\right\rangle_{t_{AB}} = \left\langle :\, f\left(\zeta\hat{a}_1^\dagger, \zeta\hat{a}_1\right)\, :\right\rangle_0 \tag{48}$$

where $\zeta = \mathrm{e}^{-\mathit{\Gamma}t_{AB}/2}$ and f is an analytic function. The notation $:\ f\ :$ means normal ordering where all the $\hat{a}_1^\dagger$ are placed to the left and all the $\hat{a}_1$ are placed to the right. In particular using the property:

$$\mathrm{e}^{\mathrm{i}\hat{Z}_{1'}(\theta_A)s_1} = \mathrm{e}^{\mathrm{i}s_1\mathrm{e}^{\mathrm{i}\theta_A}\hat{a}_1^\dagger}\mathrm{e}^{\mathrm{i}s_1\mathrm{e}^{-\mathrm{i}\theta_A}\hat{a}_1}\mathrm{e}^{-s_1^2/2} \tag{49}$$

we deduce

$$\begin{aligned}\left\langle\mathrm{e}^{\mathrm{i}\hat{Z}_{1'}(\theta_A)s_1+\mathrm{i}\hat{Z}_2s_2}\right\rangle_{t_{AB}} &= \mathrm{e}^{-(1-\zeta^2)s_1^2/2}\left\langle\mathrm{e}^{\mathrm{i}\hat{Z}_{1'}(\theta_A)\zeta s_1+\mathrm{i}\hat{Z}_2s_2}\right\rangle_0 \\ &= \mathrm{e}^{-[(1-\zeta^2)s_1^2+\cosh(2r)(\zeta^2s_1^2+s_2^2)+2\sinh(2r)\cos(\theta_A+\theta_B)\zeta s_1s_2]/2}.\end{aligned} \tag{50}$$

The inverse Fourier transform defined in the appendix gives the probability distribution:

$$P(z_{1'}, z_2) = \frac{\mathrm{e}^{-\dfrac{(\gamma z_1 + \gamma^{-1}z_2)^2}{2\sigma_+^2(\theta)} - \dfrac{(\gamma z_1 - \gamma^{-1}z_2)^2}{2\sigma_-^2(\theta)}}}{\pi\sigma_+(\theta)\sigma_-(\theta)} \tag{51}$$

where

$$\gamma = \left[\zeta^2 + \frac{1-\zeta^2}{\cosh(2r)}\right]^{1/4} \tag{52}$$

and the variances get modified by the expression:

$$\sigma_\pm^2(\theta) = \left\langle \delta^2\left(\gamma \hat{Z}_1 \pm \gamma^{-1}\hat{Z}_2\right)\right\rangle_{t_{AB}} = 2\gamma^2\cosh(2r) \pm 2\cos(\theta_A+\theta_B)\zeta\sinh(2r). \tag{53}$$

Let us reexamine the possibility of an intervention of Eve who is trying to intercept the public beam. We can apply a reasoning similar to the case without losses. Since the time for the signal to travel between Bob and Alice is t_{AB}, let us suppose that Eve makes a single attack *i.e.* she intercepts only at one position in the communication channel such that the time needed for the signal to travel from Bob is t_{EB} and to reach Alice is $t_{AE} = t_{AB} - t_{EB}$. This particular case excludes other possibilities of multiple attacks in which Eve intercepts at many positions. In that situation, after the encryption of Alice of the message $\theta_A = \theta_S$ and an eventual intervention of Eve, the probability distribution becomes:

$$P_E(z_{1'}, z_2) = \mathrm{tr}_{12}(\delta(z_{1'} - \hat{Z}_{1'})\delta(z_2 - \hat{Z}_2)\hat{\rho}_E(t_{AB}))|_{\theta_A=\theta_S} \tag{54}$$

where

$$\hat{\rho}_E(t_{AB}) = \mathrm{tr}_\nu\left(\mathrm{e}^{\mathcal{L}t_{AE}}\left[\hat{U}|0\rangle\mathrm{e}^{\mathcal{L}t_{EB}}[|\Psi\rangle\langle\Psi|]\langle 0|\hat{U}^\dagger\right]\right) \tag{55}$$

and where tr_ν denotes the trace over the other degrees of freedom introduced by Eve as an Ancilla. Then Bob is expected to measure $\hat{Z}_{1'}$ and $\hat{Z}_2$ which follows the probability distribution:

$$P_B(z_{1'}, z_2) = \mathrm{tr}_{12}(\delta(z_{1'} - \hat{Z}_{1'})\delta(z_2 - \hat{Z}_2)\hat{\rho}(t_{AB}))|_{\theta_A=\theta_R}. \tag{56}$$

Theorem 2

The theorem 1 is verified in the presence of losses i.e. when the probability distributions are replaced by (54) and (56).

Proof. The demonstration proceeds in the same way as the case without losses. After taking the Fourier transform, we collect the first order term of expansion in s_1 and s_2. We deduce the relation (20) with an appropriate redefinition of the parameters. We arrive at a relation similar to (24):

$$\left\langle \mathrm{e}^{\mathrm{i}\hat{Z}_{1'}(\theta_R)s_1 + \mathrm{i}\hat{Z}_2 s_2}\right\rangle_{t_{AB}} = \mathrm{e}^{-\frac{1}{2}(1-|\alpha|^2)\cosh(2r)\zeta^2 s_1^2}\left\langle \mathrm{e}^{\mathrm{i}\hat{Z}_{1'}(\phi)|\alpha|s_1 + \mathrm{i}\hat{Z}_2 s_2}\right\rangle_{t_{AB}}. \tag{57}$$

Applying the transformation (26) and using (1, 44, 55), we eliminate the state describing the second beam. to find a relation generalizing (27):

$$\mathrm{tr}_{1\nu}\left(\mathrm{e}^{\mathrm{i}\hat{Z}_{1'}(\theta_S)s_1}\mathrm{e}^{\mathcal{L}t_{AE}}\left[\hat{U}|0\rangle\mathrm{e}^{\mathcal{L}t_{EB}}[|n\rangle_1\,{}_1\langle n'|]\langle 0|\hat{U}^\dagger\right]\right) = \mathrm{e}^{-\frac{1}{2}(1-|\alpha|^2)\cosh(2r)\zeta^2 s_1^2}\mathrm{tr}_1\left(\mathrm{e}^{\mathrm{i}\hat{Z}_{1'}(\phi)|\alpha|s_1}\mathrm{e}^{\mathcal{L}t_{AB}}[|n\rangle_1\,{}_1\langle n'|]\right). \tag{58}$$

Since r is kept private to Bob, by a reasoning similar to the cases without losses, we conclude that $|\alpha|^2 = 1$ and the only possible form for (58) is:

$$\mathrm{tr}_{1\nu}\left(\mathrm{e}^{\mathrm{i}\hat{Z}_{1'}(\theta_S)s_1}\mathrm{e}^{\mathcal{L}t_{AE}}\left[\hat{U}|0\rangle\mathrm{e}^{\mathcal{L}t_{EB}}[|n\rangle_1\,{}_1\langle n'|]\langle 0|\hat{U}^\dagger\right]\right) = \mathrm{tr}_1\left(\mathrm{e}^{\mathrm{i}\hat{Z}_{1'}(\pm\theta_S+\delta)s_1}\mathrm{e}^{\mathcal{L}t_{AB}}[|n\rangle_1\,{}_1\langle n'|]\right). \tag{59}$$

Using the relation (50) but applied to the interval of time t_{AE}, we can reexpress (59) in the form:

$$\mathrm{tr}_{1\nu}\left(\mathrm{e}^{\mathrm{i}\hat{Z}_{1'}(\theta_S)\zeta_{AE}s_1}\left[\hat{U}|0\rangle\mathrm{e}^{\mathcal{L}t_{EB}}[|n\rangle_1\,{}_1\langle n'|]\langle 0|\hat{U}^\dagger\right]\right) = \mathrm{tr}_1\left(\mathrm{e}^{\mathrm{i}\hat{Z}_{1'}(\pm\theta_S+\delta)\zeta_{AE}s_1}\mathrm{e}^{\mathcal{L}t_{EB}}[|n\rangle_1\,{}_1\langle n'|]\right) \tag{60}$$

where $\zeta_{AE} = \mathrm{e}^{-\Gamma t_{AE}/2}$. Equation (60) is valid for any n and any n'. Thus, the expression $|n\rangle_1\,{}_1\langle n'|$ can be replaced by any density matrix $\hat{\rho}_1$. In particular, we can choose:

$$\hat{\rho}_1 = \mathrm{e}^{-\mathcal{L}t_{EB}}|n\rangle_1\,{}_1\langle n'|. \tag{61}$$

Inserting that expression into (60), we arrive finally to a relation identical to (27) except that s_1 has been replaced by $\zeta_{AE}s_1$. Following similar steps to the case 1 and 2 of the previous theorem, the theorem including the presence of losses is demonstrated.

5 Example of a bit transmission

Let us illustrate how the previous theorems can be effectively applied to realise a protocol which transmits secret bits of information. Let us consider that the EPR beams are made of entangled pulses and that the results of N independent (uncorrelated) measurements obtained by a homodyne detection are given by $Z_1'^{(i)}$ $(1 \leq i \leq N)$ for Alice measuring with an angle $\theta_A^{(i)} = \phi_A^{(i)} + \theta$ and $Z_2{}^{(i)}$ for Bob measuring $\theta_B^{(i)}$ [7]. Suppose that during each measurement, the squeezing parameter $r^{(i)}$ and the phase $\theta_B^{(i)}$ chosen by Bob are kept private to him and susceptible to be different for each measurement. These two requirements are suggested in order to guarantee security during the transmission by the strict application of the assumptions of the theorem.

Assume the transmission is made of bits with value 0 when $\theta = 0$ and 1 when $\theta = \pi/2$. Then we need to check that one of the value $\theta = 0$ or $\theta = \pi/2$ is compatible with the data using statistical tests.

5.1 Variance tests

We start by noticing that the observables:

$$\hat{Y}_1^{(i)}(\theta) = \frac{\gamma^{(i)}\hat{Z}_{1'}^{(i)} + \gamma^{(i)\,-1}\hat{Z}_2^{(i)}}{\sigma_+^{(i)}(\theta)} \tag{62}$$

$$\hat{Y}_2^{(i)}(\theta) = \frac{\gamma^{(i)}\hat{Z}_{1'}^{(i)} - \gamma^{(i)\,-1}\hat{Z}_2^{(i)}}{\sigma_-^{(i)}(\theta)} \tag{63}$$

Table 1. Possible results for variance tests.

	$\theta = 0$ accepted	$\theta = 0$ rejected
$\theta = \pi/2$ accepted	The data does not allow to distinguish between the two. More data is needed to make the distinction.	If eavesdropping has not occurred, $\theta = \pi/2$ is the value that Alice has encoded.
$\theta = \pi/2$ rejected	If eavesdropping has not occured, $\theta = 0$ is the value that Alice has encoded.	If Alice has really between $\theta = 0$ or $\theta = \pi/2$ then eavesdropping has occured.

where

$$\gamma^{(i)} = \left[\zeta^2 + \frac{1-\zeta^2}{\cosh(2r^{(i)})}\right]^{1/4} \tag{64}$$

and

$$\sigma_\pm^{(i)}(\theta) = \sqrt{2\gamma^{(i)2}\cosh\left(2r^{(i)}\right) \pm 2\zeta\cos\left(\theta_A^{(i)}+\theta_B^{(i)}\right)\sinh\left(2r^{(i)}\right)} \tag{65}$$

follow a normal reduced distribution (with variance equal to unity). As a consequence, the observable:

$$\hat{\chi}^2(\theta) = \sum_{i=1}^{N} \hat{Y}_1^{(i)2}(\theta) + \hat{Y}_2^{(i)2}(\theta) \tag{66}$$

follows a Chi square distribution with $2N$ degrees of freedom. For large N,

$$\frac{\hat{\chi}^2(\theta) - 2N}{\sqrt{4N}} \tag{67}$$

follows a normal reduced distribution. The statistical test consists in checking the plausibility of the value $\theta = 0$ by verifying if the observed value $\chi^2_{\text{obs}}(\theta = 0)$ of $\hat{\chi}^2(\theta = 0)$ is within an interval of confidence with probability p. We define l_p such that:

$$\text{Prob}\left(\frac{|\hat{\chi}^2(\theta = 0) - 2N|}{\sqrt{4N}} < l_p\right) = p \tag{68}$$

or

$$\text{erf}(l_p/\sqrt{2}) = \frac{1}{\sqrt{2\pi}}\int_{-l_p}^{l_p} \mathrm{d}\xi \mathrm{e}^{-\xi^2/2} = p \tag{69}$$

with $|\chi^2_{\text{obs}}(\theta = 0) - 2N|/\sqrt{4N} < l_p$. If the observed value is not within this interval then within the probability p of confidence, we can reject the value $\theta = 0$.

In order to decide if the value of θ is wrong or if eavesdropping has occured, another identical test is realised for $\theta = \pi/2$. These two tests leads to four possibilities with four possible conclusions with a probability p of confidence: see Table 1.

The number N of measurements, necessary to choose between one or the other value of θ with a probability p of confidence, can be estimated in the following way. Suppose that we test the value $\theta = 0$ knowing that the observables follow a normal distribution but with a value $\theta = \pi/2$. The variance of the observed values corresponds on average to the mean variance but with $\theta = \pi/2$ and we estimate $\hat{Z}_{1'}^{(i)} + \hat{Z}_2^{(i)} \sim \sigma_+^{(i)}(\theta = \pi/2)$ and $\hat{Z}_{1'}^{(i)} - \hat{Z}_2^{(i)} \sim \sigma_-^{(i)}(\theta = \pi/2)$. In these conditions, an order of magnitude for the observed Chi square can be evaluated:

$$\chi_{\text{obs}}(\theta = 0) \simeq \sum_{i=1}^{N} \frac{\sigma_+^{(i)2}(\theta = \pi/2)}{\sigma_+^{(i)2}(\theta = 0)} + \frac{\sigma_-^{(i)2}(\theta = \pi/2)}{\sigma_-^{(i)2}(\theta = 0)} \cdot \tag{70}$$

Let us assume that the sets $r^{(i)}$ and $\phi_A^{(i)} + \theta_B^{(i)}$ are distributed according to the probability distribution $g(r, \phi_A + \theta_B)$ with

$$\int_0^\infty \mathrm{d}r \int_0^{2\pi} \mathrm{d}(\phi_A + \theta_B) g(r, \phi_A, \theta_B) = 1. \tag{71}$$

If the set of values of $\phi_A^{(i)} + \theta_B^{(i)}$ are uniformly distributed over the interval $[0, 2\pi[$, $g(r, \phi_A + \theta_B) = g(r)/(2\pi)$ depends only on the squeezing parameter r. For N large, we can replace in good approximation the sum by an integral over the distribution function $g(r, \phi_A + \theta_B) = g(r)/(2\pi)$ depending only on the squeezing parameter r

$$\chi_{\text{obs}}(\theta = 0) \simeq N \int_0^\infty \mathrm{d}r \int_0^{2\pi} \frac{\mathrm{d}(\phi_A + \theta_B)}{2\pi} g(r) \times \left[\frac{\sigma_+^{(i)2}(\theta = \pi/2)}{\sigma_+^{(i)2}(\theta = 0)} + \frac{\sigma_-^{(i)2}(\theta = \pi/2)}{\sigma_-^{(i)2}(\theta = 0)}\right] \cdot \tag{72}$$

The integral over θ_B can be carried out and we get more simply:

$$\chi_{\text{obs}}(\theta = 0) \simeq 2N \int_0^\infty \mathrm{d}r\, g(r) \times \sqrt{\frac{(1-\zeta^2)\cosh(2r) + \zeta^2\cosh^2(2r)}{(1-\zeta^2)\cosh(2r) + \zeta^2}} \cdot \tag{73}$$

Thus, on average, the observed Chi square function is much greater than $2N$ since the square root term in (73) is always greater than unity. If we allow only two possible values for the squeezing parameter r_1 and r_2 with equal probability $1/2$ of occurrence then

$$g(r) = \frac{1}{2}\delta(r - r_1) + \frac{1}{2}\delta(r - r_2). \tag{74}$$

Table 2. Possible results for normality tests.

	$\theta = 0$ accepted	$\theta = 0$ rejected
$\theta = \pi/2$ accepted	The data does not allow to distinguish between the two. More data is needed to make the distinction.	$\theta = \pi/2$ is the value that Alice has encoded.
$\theta = \pi/2$ rejected	$\theta = 0$ is the value that Alice has encoded.	If Alice has really between $\theta = 0$ or $\theta = \pi/2$ then eavesdropping has occured.

Given a probability p of confidence, the application of relations (68, 69) allows to express the number of measurements which must be carried out in order to reject the assumption $\theta = 0$ and admit that $\theta = \pi/2$ is the correct value:

$$\mathrm{erf}\left(\sum_{k=1,2}\sqrt{\frac{N(\zeta^{-2}-1)\cosh(2r_k)+\cosh^2(2r_k)}{8(\zeta^{-2}-1)\cosh(2r_k)+8}} - \sqrt{\frac{N}{2}}\right) = p. \quad (75)$$

For example, let us choose the two values of squeezing such that $\cosh(2r_1) = 2$ and $\cosh(2r_2) = 3$ and the distance between Alice and Bob of 14 km ($\zeta = 0.5$ for $\kappa^{-1} = 10$ km). If we require a probability of confidence such that the error rate is $1 - p = 10^{-12}$, then we estimate that $N \sim 20$ without the presence of losses and $N \sim 700$ with the presence of losses.

Once θ is determined, we test if the shape of the observed probability distribution is compatible with the one predicted by the theory. Let us assume that the observables $\hat{Y}_1^{(i)}(\theta)$ and $\hat{Y}_2^{(i)}(\theta)$ are known up to an error ϵ. This error is limited by the finite photon number in the detector during the homodyne detection. Then, we build an histogram of the probability distribution. We divide the probability distribution function into m intervals as follows in the real axis of the possible value for $\hat{Y}_1^{(i)}(\theta)$ and $\hat{Y}_2^{(i)}(\theta)$. $m-2$ intervals are equidistant with a size given by the precision ϵ and the two others represent the tails. More precisely, they are defined as $A_1 = \left]-\infty, -\frac{(m-2)}{2}\epsilon\right]$, $A_2 = \left]-\frac{(m-2)}{2}\epsilon, -\frac{(m-4)}{2}\epsilon\right]$, $\ldots$, $A_{m-1} = \left]\frac{(m-4)}{2}\epsilon, \frac{(m-2)}{2}\epsilon\right]$, $A_m = \left]\frac{(m-2)}{2}\epsilon, +\infty\right[$. Since for value $\frac{m-2}{2}\epsilon \geq 3$ the probability that the observation falls in the tails are very small (10^{-3}), we can fix the number of interval to be $m \sim 6/\epsilon$ to have significant intervals. The $2N$ data are distributed statistically among the m intervals. If these data are compatible with a normal distribution, the number of data $O_k(\theta)$ falling in a specific interval k should be close to the expected number E_k defined as:

$$E_k = 2N\int_{y\in A_k} \mathrm{d}y \frac{1}{\sqrt{2\pi}} \mathrm{e}^{-y^2/2}. \quad (76)$$

The normalisation condition imposes $\sum_{k=1}^m E_k = 2N$. According to standard statistic analysis [14], one shows that for large sample sizes $2N$, the quantity:

$$\chi_E^2 = \sum_{k=1}^m \frac{(E_k - O_k(\theta))^2}{E_k} \quad (77)$$

follows a Chi square distribution with $m-1$ degrees of freedom. We define p_E the probability of confidence for which we can accept the assumption of the Gaussian distribution for the observables $\hat{Y}_1^{(i)}(\theta)$ and $\hat{Y}_2^{(i)}(\theta)$ given the particular value of θ chosen. For large m, this interval is delimited by $\chi_E^2 < \chi_{Ep}^2$ such that:

$$\frac{1}{2} + \frac{1}{2}\mathrm{erf}\left(\frac{\chi_{Ep}^2 - (m-1)}{\sqrt{2(m-1)}}\right) = p_E. \quad (78)$$

If on the other hand, the observed values are within the complementary interval, we can reject the assumption of a normal distribution and thus conclude that within a probability p_E of confidence eavesdropping has occured.

5.2 Normality tests

Rather than carrying out both type of tests, it is sufficient to carry out only two normality tests. To determine what is the correct value for θ, we test if the probability distribution or histogram obtained with the two possible values of θ is compatible with what is predicted by the theory. We test the normality of the observable for both the observed distribution sets $O_k(\theta = 0)$ and $O_k(\theta = \pi/2)$ given a probability p of confidence. Again there are four possibilities: see Table 2.

The number of measurement N necessary to estimate θ within probability p of confidence is difficult to express. But we can use the formula (75) since any data which presents larger variance than expected has a different histogram.

From these considerations, we are ready to define a protocol.

5.3 Protocol

1. In order to receive l bits of information, Bob creates Nl pairs of entangled squeezed modes with squeezing parameter $r^{(i,j)}$ ($1 \leq i \leq N$, $1 \leq j \leq l$). One mode of the pair is kept private and measured by Bob, the other is sent to Alice.

2. Bob chooses to measure the quadrature $\hat{Z}_2^{(i,j)}$ under the angle $\theta_B^{(i,j)}$.
3. Alice encodes the secret bit $\theta^{(j)}$ and chooses to measure the quadrature $\hat{Z}_1^{(i,j)}$ under the angle $\theta_A^{(i,j)} = \phi_A^{(i,j)} + \theta^{(j)}$.
4. Alice communicates to Bob her results $\hat{Z}_1^{(i,j)}$ and the angle $\phi_A^{(i,j)}$ through a public channel.
5. For each bit taken separately, Bob carries out two Chi square statistical tests on variance to determine the value of the bit $\theta = 0$ or $\pi/2$ or if eavesdropping has occured or even if we should discard the bit information. Once θ is determined, Bob carries out the test on normality to determine effectively if eavesdropping has occured.
   or
   For each bit taken separately, Bob carries out two statistical tests on normality to determine the value of the bit $\theta = 0$ or $\pi/2$ or if eavesdropping has occured or even if we should discard the bit information.
6. We discard at random a subset of bit data which are used publicly to test the bit error rate caused by an eventual shift transformation of an angle δ.
7. The remaining bits are used to create a key distribution known only to Alice and Bob.

6 Conclusion

In summary, we developed a quantum cryptography protocol using EPR correlated continuous variables. This scheme is based on the principle that any decryption of the message requires both measurements of a private signal and an encrypted signal by Alice. On the contrary to the single photon system, the determination of any shared key bit requires many quadrature measurements and no data are discarded when Alice and Bob use a different basis (quadratures components) for their measurements. As a consequence, statistical tests are provided to determine the key bit and if eavedropping has occured.

The protocol works also for a lossy quantum communication channel but more data are needed in order to determine the key bit with a high probability of confidence.

Although security considerations have been established, a complete proof of the unconditional security for our protocol remains still an open issue. Nevertheless, we showed that in the case of a perfect transmission any modification introduced by Eve induces necessarily some modification in the probability distribution. In the presence of losses in the transmission, Eve is restricted to make a single attack.

To prove unconditional security, we still need to show that the statistical tests determine efficiently any modification of the distribution. The protocol described in this paper is not the only possibility and could fail, for example, to be sensitive to an attack of small intensity or some coherent attack. No analysis has been done on whether better statistical tests are more efficient or on whether there exists a more confidential way to encode the key. The elegant concept of mutual information introduced by Shannon could help us to progress in this analysis [5].

Other directions for a future research work include the extension to continuous waves and the study of the imperfection in the photon counting of the detector which also degrades the correlations.

The author thanks L.A. Lugiato for useful remarks and suggestions on the manuscript and A. Gatti, N. Lutkenhaus, N.J. Cerf, S.M. Barnett and N. Korolkova for helpful discussions. This work was supported by the network QSTRUCT of the TMR program of the EU.

7 Appendix

We start from the Fourier transform of (12):

$$\int_{-\infty}^{\infty} \mathrm{d}s_1 \int_{-\infty}^{\infty} \mathrm{d}s_2 \, \mathrm{e}^{\mathrm{i}(s_1 z_{1'} + s_2 z_2)} P(z_{1'}, z_2) = \langle \Psi | \mathrm{e}^{\mathrm{i}\hat{Z}_{1'}(\theta_A)s_1 + \mathrm{i}\hat{Z}_2 s_2} | \Psi \rangle \cdot \quad (79)$$

Using (1), equation (79) becomes:

$$\begin{aligned} \langle \Psi | \mathrm{e}^{\mathrm{i}\hat{Z}_{1'}(\theta_A)s_1 + \mathrm{i}\hat{Z}_2 s_2} | \Psi \rangle & \\ &= {}_1\langle 0|_2\langle 0| \hat{S}^\dagger \mathrm{e}^{\mathrm{i}\hat{Z}_{1'}(\theta_A)s_1 + \mathrm{i}\hat{Z}_2 s_2} \hat{S} |0\rangle_1 |0\rangle_2 \\ &= {}_1\langle 0|_2\langle 0| \mathrm{e}^{\mathrm{i}\hat{S}^\dagger(\hat{Z}_{1'}(\theta_A)s_1 + \hat{Z}_2 s_2)\hat{S}} |0\rangle_1 |0\rangle_2 \cdot \quad (80) \end{aligned}$$

Taking the explicit expression for the quadrature operators (3, 4), we can apply the Bogoliubov transformation to each individual operator:

$$\hat{S}^\dagger \hat{a}_1 \hat{S} = \cosh r \hat{a}_1 + \sinh r \hat{a}_2^\dagger \quad (81)$$

$$\hat{S}^\dagger \hat{a}_2 \hat{S} = \cosh r \hat{a}_2 + \sinh r \hat{a}_1^\dagger . \quad (82)$$

We obtain:

$$\langle \Psi | \mathrm{e}^{\mathrm{i}\hat{Z}_{1'}(\theta_A)s_1 + \mathrm{i}\hat{Z}_2 s_2} | \Psi \rangle = {}_1\langle 0|_2\langle 0| \mathrm{e}^{\mathrm{i}(u_1 \hat{a}_1^\dagger + u_2 \hat{a}_2^\dagger + c.c.)} |0\rangle_1 |0\rangle_2 \quad (83)$$

where $u_1 = s_1 \mathrm{e}^{\mathrm{i}\theta_A} \cosh r + s_2 \mathrm{e}^{-\mathrm{i}\theta_B} \sinh r$ and $u_2 = s_1 \mathrm{e}^{-\mathrm{i}\theta_A} \sinh r + s_2 \mathrm{e}^{\mathrm{i}\theta_B} \cosh r$. The exponential operator is a displacement operator which acts on the vacuum state to give a coherent state. Using the property that for any u:

$$\langle 0| \mathrm{e}^{\mathrm{i}(u\hat{a}^\dagger + u^* \hat{a})} |0\rangle = \langle 0| \mathrm{e}^{-|u|^2/2} \sum_{n=0}^{\infty} \frac{(\mathrm{i}u)^n}{\sqrt{n!}} |n\rangle = \mathrm{e}^{-|u|^2/2} . \quad (84)$$

Equation (83) becomes:

$$\langle \Psi | \mathrm{e}^{\mathrm{i}\hat{Z}_{1'}(\theta_A)s_1 + \mathrm{i}\hat{Z}_2 s_2} | \Psi \rangle = \mathrm{e}^{-\frac{1}{2}\left[\cosh(2r)(s_1^2 + s_2^2) + \sinh(2r)\cos(\theta_A + \theta_B) 2 s_1 s_2\right]} . \quad (85)$$

Making the inverse Fourier transform of (85), we arrive at (13).

References

1. P. Navez, A. Gatti, L.A. Lugiato, `quant-ph/0101113` accepted in Phys. Rev. A.
2. M.D. Reid, Phys. Rev. A **62**, 062308 (2000).
3. T.C. Ralph, Phys. Rev. A **61**, 010303(R) (2000).
4. M. Hillery, Phys. Rev. A **61**, 022309 (2000).
5. N.J. Cerf, M. Levy, G. van Assche, Phys. Rev. A. **63**, 052311 (2001).
6. D. Gottesman, J. Preskill, Phys. Rev. A **63**, 022309 (2001).
7. Ch. Silberhorn, P.K. Lam, O. Weiss, F. König, N. Korolkova, G. Leuchs, Phys. Rev. Lett. **86**, 4267 (2001).
8. A.K. Eckert, Phys. Rev. Lett. **67**, 661 (1991).
9. C.H. Bennett, G. Brassard, in *Proceedings of IEEE International Conference on Computer, Systems and Signal* (Processing Bangalore, India, 1984), p. 175; C.H. Bennett, G. Brassard, A.K. Ekert, Sci. Am. **267**, 50 (1992).
10. C.H. Bennett, P.W. Shor, Science **284**, 747 (1999).
11. H.-K. Lo, H.F. Chau, Science **283**, 2050 (1999) and reference therein.
12. G. Brassard, N. Lütkenhaus, T. Mor, B.C. Sanders, Phys. Rev. Lett. **85**, 1330 (2000).
13. M.D. Reid, P.D. Drummond, Phys. Rev. Lett. **60**, 2731 (1988); Z.Y. Ou, S.F. Pereira, H.J. Kimble, Appl. Phys. B **55**, 265 (1992).
14. W.H. Press, B.P. Flannery, S.A. Teukolsky, W.T. Vetterling, *Numerical Recipes* (Cambridge University Press, New York, 1986).